臺灣數位犯罪及數位鑑識發展現況與未來趨勢--以「創新司法警察 IEK Model 智慧模型」為例

林宜隆*

目　次

摘　要

隨著網際網路技術（ICT）的提升，手機不再是傳統的通話功能，透過智慧型手機，可以使用通訊軟體互相聯絡（如 LINE、Messenger、Wechat、Juiker）、上網瀏覽網頁與交易、儲存個人相關資訊數位記錄（如照片、記事等），如同行動電腦。手機帶來的便利性，成為有心人士的網路（數位）犯罪工具（如 2016 年 5 月中華郵政商城網路個資外洩案、2016 年 7 月第一銀行 ATM 盜領案、2017 年 2 月臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件、2017 年 5 月新型勒索病毒 WannaCry 重創臺灣、2017 年 6 月全球多個國家遭受新一輪 Petya 勒索病毒攻擊、2017 年 10 月遠東銀行 SWIFT 系統遭駭客入侵 18 億案、2016 年網路詐欺事件、2017 年智慧型手機詐欺等事件），智慧型手機如同行動電腦存在大量的電磁記錄（即數位證據），這些記錄是具備鑑識價值的數位證據。有鑑於此，傳統的鑑識設備與方法，將不足以蒐集手機裡的數位證據。對於數位證據的認知與理解、鑑識工具的選擇與使用，將是數位鑑識人員必需具備的主要專業知識與基本認知。

* 林宜隆，元培醫事科技大學資訊管理系暨數位創新管理碩士班教授，台灣數位鑑識發展協會（ACFD）創會理事長，前中央警察大學教授，法務部調查局資通安全諮詢委員，消基會資通訊委員會委員兼副召集人，Email: cyberpaul747@gmail.com。

國內司法警察對於數位鑑識工作剛起步，對於數位證據採集方法、保全技術、工具軟體與所需技術亦有所欠缺，實有必要對此議題進行深入的研討；因此本文將針對我國『資通安全及數位證據鑑識能量』發展現況與未來趨勢加以研究，達到掌握我國資通安全與數位證據鑑識技術研發及建置重點，且有效整合現有資通安全與數位證據鑑識技術研發計畫與整體資源運用，提供政府與民間企業技術研發主管單位編列預算參考。

對於資通安全及數位證據鑑識能量規劃之研究取向應以數位鑑識實驗室（含工具軟體）、數位證據鑑識標準作業程序及資安專業人才三個領域為重點，本文將先介紹我國數位證據鑑識能量之發展現況，接著再由數位鑑識實驗室設立、建構數位證據鑑識標準作業程序（DEFSOP）、及資安專業人才培育三個方向進行資料蒐集和深入研究與未來趨勢，最後即針對我國資通安全及數位證據鑑識能量提出結果及建議事項，並將以建立創新司法警察 IEK Model 智慧模型架構與芻議的參考依據。透過此三個方向的探討，對我國資通安全及數位證據鑑識能量提出改善建議及提昇整合「科技建警」與「偵防並重」之警政新策略（如數位鑑識科技能量、科技建警與偵防並重之警政新策略），並將確保數位證據之證據能力與證明力，且提昇其證據有效性與公信力。

關鍵字：數位犯罪、數位鑑識、IEK Model、科技建警與偵防並重

A Study on Current Situation and Future Trend of Cybercrime and Digital Forensics in Taiwan -Take the "Innovative Judicial Police IEK Intelligence Model" as an Example

I-Long Lin*

Abstract

With the upgrading of Internet technology, mobile phones are no longer traditional call features, through the smart phone, you can use communication software to contact each other (such as LINE, Messenger, Wechat, Juiker), Internet browsing and electronic trading, storage Personal information (such as SMS, photos, notes, etc.). The convenience of smartphones has become an Internet of people (digital) criminal tools, smart phones like mobile computers there are a lot of electromagnetic records (ie, digital evidence), these records are valuable evidence of the forensics science. In view of this, the traditional forensic equipment and methods, will not be enough to collect digital evidence in the mobile phones. For the recognition and understanding of digital evidence, the selection and use of forensic tools will be the main professional knowledge and basic knowledge that digital forensics must have.

The domestic judicial police for the digital forensic work has just started, for the digital evidence collection methods, preservation technology, software tools and the required technology is also lacking, it is necessary to conduct in-depth discussion of this issue; Therefore, this article will be the cyber security and digital evidence forensics capability development status and future trends to be

* I-Long Lin, Professor, Department of Information Management/Master's Program in Digital Technology Innovation and Management of Yuanpei University of Medical Technology, E-mail: cyberpaul747@gmail.com

studied to achieve our grasp of security and digital evidence forensics technology research and development and focus on the integration of effective resources to provide government and private enterprise technology research and development units in charge of budget reference.

For the study of capability, the cyber security and digital evidence forensics capability planning should be digital forensics laboratory (including software tools), digital evidence forensics standard operating procedures (DEFSOP) and security professionals in three areas as the focus, this paper will first introduce our digital evidence forensics capability (DEFSOP), and for cyber security and safety of resources and the development of a number of indicators, digital evidence to forensics the results of capability and recommendations, and will establish the innovative judicial police IEK intelligence model structure and the reference basis. Finally, through these three directions, we will make suggestions on improving the safety of our country's security and intelligence, and enhance the new strategy of integrating the "science and technology police" and "investigation and prevention", and will ensure the evidence ability of digital evidence and prove the effectiveness and enhance the effectiveness and credibility.

Key Words:**Cybercrime, Digital Forensics, IEK Model, Science and Technology to Build Police**

壹、前言

網際網路（Internet）的發展肇始於 1960 年代，於 1990 年代中成熟，今天則逐漸大眾化，成為未來資訊時代網路社會主要的生活方式。就網際網路發展的演進而言，從網路族群的形成以及其網際網路特有文化的出現，更能印證網路資訊社會（Cybersociety）的存在性及其價值。網際網路由過去學術菁英社群專屬時代，專用於學術與研究的使用型態，過渡到商業化且普及於社會大眾各階層，從學術菁英階層演進到社會普羅階層，大量網路使用者湧入網路世界（如 2017 年 6 月止全球人口約 74 億人，而全球網際網路用戶已突破 38 億人大關，其所占全球人口之比例已超 50%），從網路蠻荒開拓了一片新世界，在此世界中網路使用者用網路語言及即時通訊軟體（如 LINE、Messenger、Juiker、Wechat、WhatsApp 等）進行交談，暢所欲言，是對真實世界的反應，在真實社會中有各種階級的區隔，在網路社會裡，此種區隔就顯的毫無意義，每個網路使用者，均有相同的網路使用空間，不因個人身份、地位、職業、背景等，而有所不同。

網際網路由原有之學術菁英所建立的網路文化，在網際網路商業化後所造成的網路文化變遷，無論是否造成網路資訊社會規範的巨幅轉變，甚有人擔心網路（數位）犯罪問題（Cybercrimes or Digital Crimes），而遲遲不願面對網路資訊社會存在的事實及價值，其實應用平常心來看待網際網路的發展，自從有人類文明開始，犯罪就無法避免，誠如社會學家涂爾幹（Durkheim）所言犯罪是一種正常而非病態的社會現象。如果一種社會現象是普遍（Universal）和必需（Necessary）的，則這種社會現象是一種正常的現象，網路（數位）犯罪如同真實社會中有犯罪，是人類生活的一部份。有時犯罪對社會是有用的，且是社會健康化（如資訊健康化與健康資訊化）所必需的，網路（數位）犯罪的存在說明了網路資訊社會變遷的可能，假使犯罪不存在，則每個人的行為態樣將會相同，也無法分辨是非善惡，這種普遍性的一致將會凍結了網路資訊社會原有的創造性和獨立思考。網際網路發展至今，已自成一格，擁有自己的文化、價值、規範與影響力等，我們實無法再用其他的理由來否定他的存在及其價值，網路資訊社會未來是人類社會變遷重要的一環，是潮流趨勢無法抵擋，我們不能再死背著傳統規範包袱不放，用網路人的新觀念來經營網路資訊社會，打破傳統既存的社會藩籬，用宏觀的智慧和創新來勾勒出未來網路資訊社會遠景與達成**健康智慧生活**目標（如 DIGI^{+}**2025 數位國家及創新經濟方案**、**Google**、**Amazon**、**Microsoft**、**Alibaba Group** 等）。

隨著國際間網際網路快速地普及與發展，2017 年 6 月止全球人口約 74 億人，而全球網際網路用戶已突破 38 億人大關，其所占全球人口之比例已超 50%，伴隨網際網路而來的網路（數位）犯罪問題亦快速地入侵我國。隨著案件不斷地發生，網路（數位）犯罪的問題亦因而受到國人的重視。目前發生在我國的網路（數位）犯罪形態種類繁多，包括利用網路犯色情犯罪、恐嚇、誹謗、詐欺、賭博、販賣非法有害物品、竊取或破壞工商機密及經濟金融犯罪（如洗錢、走私、販毒）等，而且仍在不斷增加新的數位犯罪類型當中，如最近（2017 年 2 月 4 日）國內傳出多家證券商遭駭客攻擊，恐嚇交付比特幣，刑事局統計共有 14 家證券商受害，且已有數家證券商遭零星「DDOS」手法攻擊。另外中華郵政經過調查發現商城後台被有心人士蓄意侵入並植入木馬程式，從 2015 年 10 月至 2016 年 05 月 24 日，約有 8 個月的消費者訂單資料都遭竊，約有 1 萬 7,000 多筆，這也是中華郵政商城首度發生遭駭事件。如 2016 年 7 月 10、11 日周末凌晨，第一銀行爆發了臺灣有史以來第一次的大規模 ATM 遭駭盜領案，東歐駭客集團暗中駭入臺灣第一銀行的 41 臺 ATM，從倫敦一臺電話錄音伺服器，橫跨 1 萬公里，遠端遙控北中兩地 22 家一銀分行的 41 臺 ATM，還派出十多名車手兵分多路，神不知鬼不覺地盜領 8,327 萬多元。但是，為何向來是資安優等生的第一銀行，事前一點跡象都沒有察覺？再如今（2017）年 2 月 9 日外交部領務局遭受不明來源 IP 成功駭入數十個外館領務信箱，可能使 1 萬 5,000 筆人次個資遭竊取，而為了近 3 個月以來出國登錄系統個資遭竊而公開向國人（消費者）道歉。

目前國內各機構對於資通安全及數位鑑識技術（Cyber Forensics Technology）普遍缺乏瞭解及正確認知，仍以為電腦鑑識（Computer Forensics）或稱數位鑑識（Digital Forensics）、資安鑑識（Cyber Forensics）是專屬於警政單位的工作，而留待警政單位系統發展。事實上，我們若無法確保系統完美安全（Secure System），就必須在安全出現問題時能及時找出問題所在、追蹤出攻擊來源，這就是數位鑑識必須擔負的任務。數位證據鑑識的搜集，必須在案件發生之事前（預防及警訊）、事中（偵測及處理）及事後（鑑識及復原）三個階段，都必須加以保留與保護，建立一詳細清單「證據保管鍊(Chain of Custody)」，保管其證據且確保證據記載之資訊的完整性及有效性，最後呈現法院，以利犯罪事件始末的重建及追蹤。因此，針對資通安全及數位鑑識相關核心技術與其能量之建置，我國實在需要有一個完整之規劃策略，以利統籌研發資源，進而提昇我國在資通安全與數位鑑識技術之能力與能量。

作者於 1999 年仍在中央警察大學資訊管理系任教時前往美國芝加哥馬歇爾法學院進修訪問結束後，有感於美國對於資通訊科技與安全議題的成熟

度，以及擴大至數位鑑識科技（Digital Forensics Technology）與數位犯罪偵防（Cybercrime Investigation）之運用及發展，返國後以所見、所聞、所學、所得之資訊法律及科技偵查方法（**如數位鑑識科技能量、科技建警與偵防並重之警政新策略**），運用、融會貫通於優質網路資訊社會及科技犯罪偵查之範疇，隨即於 2000 年在國內開始籌畫舉辦國內第一屆「2000 Cyberspace 網際空間：資安、法律與社會」學術研討會至今（2017），提供研究學者與實務專家一個交流與分享研究心得、實務經驗的園地，期望對國內正從事於摸索**翻轉資安科技，創新服務、風險管理與物聯網（IoT）技術應用**、DIGI+**2025 數位國家及創新經濟、數位鑑識應用與發展**、**i**de@Taiwan 及安全管理、雲端計算與應用服務、雲端服務與安全管理、國家安全及國土安全、入出國人流管理服務及安檢、海洋海岸安全、ICT 治理與鑑識會計、資安治理與安全工程、資通安全治理及資通安全管理、網路犯罪理論及實務、**數位證據 SOP 及鑑識工程**、資訊法律與優質資訊社會、**智慧醫療、精準醫療、智慧醫院、智慧健康照護與智慧健康生活等**相關問題研究的學術機構與政府單位有更深入的助益。

自 2005 年以來迄今 ISO 國際標準的資訊安全管理系統驗證(ISO27001）已取代了 BS 英國標準，發展至今更擴大到各特定領域的延伸指引與驗證，如雲安全 ISO27017:2016、電信事業 ISO27011:2016（最新版）、金融事業 ISO27015:2012、醫療領域 ISO27799:2016（最新版）等。在隱私暨個資（Personally Identifiable Information, PII）保護領域，自 2011 年開始 ISO 發佈了隱私框架標準 ISO29100，於 2014 年發佈了公用雲個資保護標準 ISO27018，此兩標準也成為 CNS 國家標準，基於個資為資訊（Information）之一特殊類別的基礎上，ISO 自 2017 年將發佈隱私衝擊評鑑 ISO29134:2017 及個資保護 ISO29151:2017 標準，做為個資安全管理系統（PIIMS，基於 ISO27001）延伸指引與驗證（經由 ISO27009）的標準，自此個資保護的標準與驗證也將跨入了新的紀元，各組織可以經由現有的 ISMS:ISO27001 驗證而延伸至 PIIMS（ISO29151）驗證，做為展現良善資安與個資管理的最佳途徑，並符合個人資料保護法施行細則第十二條第二項所列十一款事項，得以與所欲達成之個人資料保護目的間，具有適當比例為原則。

近日來，台中檢調於 2017 年 2 月 4 日破獲史上最大宗個資外洩案！梁兆德個資蟑螂集團，涉從不詳管道取得全台 1.7 億筆全民個資，製成「客戶開發搜尋系統」販售給房仲，房仲可透過系統內建的駭客程式連線到地政機關，破解並海量比對，查出單一地主、屋主個資，包括總統蔡英文、首富郭台銘與天后蔡依林的個資，檢調搜索帶回主嫌梁兆德、蘇慶典與房仲買家等六十二人，依違反《個人資料保護法》將蘇男、梁男聲押獲准，並續查資料外洩

來源。另外美國資安研究人員證實，於 2017 年 6 月 12 日一家為共和黨全國委員會和其他共和黨人士服務的資料分析公司「深根（Deep Root）」，疑似在一次更新時不小心解除檔案的加密保護,2017 年 6 月 1 日起把 1.1TB 檔案，包括約占 62％美國人口的 1.98 億選民姓名、生日、住家地址、電話號碼等個資，暴露在公開的網路世界十二天，期間任何人都能輕易下載這些資料。該起事件據信為史上最大宗的美國選民資料外洩案。因此，國內外沸騰一時的資安與個資洩漏事件層出不窮，如勒索病毒（Ransomware）、智慧支付平台的洩密風險等，再度突顯了資安與個資管理的重要性！為展現良善資安與個資管理的最佳途徑，透過全球最新公告的國際個資標準（如 ISO29134/ISO29151）解析，讓大家對於如何強化資訊安全及提升個資保護能力有更多瞭解。

國內對於數位偵查鑑識工作剛起步,對於數位證據採集方法、保全技術、工具軟體與所需技術亦有所欠缺，實有必要對此議題進行深入的研討；因此本文進一步將針對我國『資通安全及數位鑑識能量』發展現況與未來趨勢加以研究，達到掌握我國資通安全與數位鑑識技術研發及建置重點，且有效整合現有資通安全及數位鑑識技術研發計畫與整體資源運用，提供政府與民間企業技術研發主管單位編列預算參考。

對於資通安全及數位鑑識能量規劃之研究取向應以數位證據鑑識標準作業程序、數位鑑識實驗室及資安專業人才三個領域為重點，本文將先介紹**我國數位鑑識能量**之發展現況，接著再由數位鑑識實驗室設立、建構數位證據鑑識標準作業程序（DEFSOP）、及資安專業人才培育三個方向進行資料蒐集和深入研究與未來趨勢，最後即針對我國資通安全及數位鑑識能量提出結果及建議事項。透過此三個方向的探討，對我國資通安全及數位鑑識能量提出改善建議及提昇整合「科技建警」與「偵防並重」之警政新策略（**如數位鑑識科技能量、科技建警與偵防並重之警政新策略**），並將確保數位證據之證據能力與證明力，且提昇其證據有效性與公信力。

貳、數位犯罪與數位鑑識論述

作者於 1999 年仍在中央警察大學資訊管理系任教時前往美國芝加哥馬歇爾法學院進修訪問結束後，有感於美國對於資通訊科技與安全議題的成熟度,以及擴大至數位鑑識科技與數位犯罪偵防之運用及發展,返國後以所見、所聞、所學、所得之資訊法律及科技偵查方法（**如數位鑑識科技能量、科技建警與偵防並重之警政新策略**），運用、融會貫通於優質網路資訊社會及科技犯罪偵查之範疇。隨即於 2000 年在國內開始籌畫舉辦國內第一屆「2000

Cyberspace 網際空間：資安、法律與社會」學術研討會至今（2017）年。

回顧這 18 年（2000-2017）來的研討會舉辦過程，慶幸此一主題也深受政府與民間企業重視，尤其是行政院院會修正通過建立「我國通資訊基礎建設安全機制」的長期計畫（2001~2016 年），由基礎建置與教育訓練著手，陸續規劃了「DIGI^{+} **2025 數位國家及創新經濟**」方案、「**數位匯流及數位經濟**」計畫、「**資訊素養與倫理法律**」推廣計畫案等，並參考美國國務院國家資通安全白皮書（2003 National Strategy to Secure Cyberspace）、美國國務院國家安全策略（2010/2015 National Security Strategy）、美國國土安全部（DHS）推動國土安全政策（2002/3 National Strategy to Secure Homeland）、美國白宮最近推動一系列之網際空間審議政策（2009 Cyberspace Review Policy）、確保 IoT 安全策略原則（**2016 Strategic Principles for Securing the Internet of Things**）、雲端安全聯盟之雲端運算關鍵領域安全指南（Cloud Security Alliance, CSA）及 **ISO27017 雲端安全國際標準**、**ISO27018 雲個資保護國際標準**、ISO27014 資安治理國際標準與 ISO27037、ISO27041、ISO27042 及 ISO27043 數位證據 SOP、資安事件偵查及數位鑑識 SOP 國際標準等。其中**數位國家、創新經濟發展方案（DIGI+2025）（2017~2025 年）**計畫內容，並配合政府創新產業（5+2），包含鞏固國家數位基礎，營造友善法制環境，研發先進數位科技，培育跨域數位人才，開拓安康富裕數位國土等**打造優質數位國家創新經濟生態環境**，另行政院資通安全處積極推動「資通安全管理法（草案）」，於今（2017）年 4 月 27 日行政院會通過行政院資通安全處擬具的「資通安全管理法」草案，已送請立法院審議。政府進一步推動「數位健康生活與智慧環境：數位科技、數位內容、數位產業、數位服務與數位安全」等智慧型相關服務與應用，其影響至為重要。

自 2010 年起雲端（Cloud）、大數據分析（Big Data Analysis, BDA）及物聯網（IoT）議題的持續發酵，以及各大雲端及物聯網廠商新服務與解決方案的陸續推出，雲端運算（CC）、大數據分析（BDA）、物聯網（IoT）及人工智慧（AI）等已被視為全球資通訊科技的未來發展重點及方向，同時，為配合行政院資通安全辦公室（2016 年 8 月 1 日改制為行政院資通安全處）推動「我國通資訊基礎建設安全機制」（2013~2017 年）：建構安全資通訊環境邁向優質資訊社會，特由**台灣數位鑑識發展協會（Association of Cyber Forensics Development in Taiwan, ACFD）**及大同大學（TTU）等單位共同主辦 2016 Cyberspace 網際空間、數位生活與物聯網聯合研討會暨第十八屆「網際空間：資安、犯罪與法律社會」學術與實務研討會和第七屆「數位健康生活與智慧環境：數位科技、數位內容、數位產業、數位服務與數位安全」產學研討會及第一屆「物聯網：物聯網技術、產業與創新應用」產學研討會；

並促成我國強化資通安全體系、打造資通安全環境、建構數位證據機制及鑑識工程能量、具數位科技化的犯罪偵防機制、推動 ICT 治理與風險管理的深耕，最終建構安全臺灣（Secure-Taiwan）。再者由**台灣數位鑑識發展協會（ACFD）、中央研究院資訊科技創新研究中心（CITI of SINICA）及元培醫事科技大學**等單位共同主辦 2017 Cyberspace 網際空間國際聯合研討會，大會主題為「**網際空間治理、資安鑑識與創新經濟（Cyberspace Governance，cyber Forensics and Digital Economics）**」，並促成建立我國網際空間（數位國土）治理機制與資安鑑識及創新經濟商業新模式。

尤其近一年來，國內外沸騰一時的資安與個資洩漏事件層出不窮，如勒索病毒、智慧支付平台的洩密風險等，再度突顯了資安與個資管理的重要性！為展現良善資安與個資管理的最佳途徑，並符合個人資料保護法施行細則第十二條第二項所列十一款事項，得以與所欲達成之個人資料保護目的間，具有適當比例為原則。透過全**球最新公告的國際個資管理標準（ISO29134/ISO29151）解**析，讓大家對於如何強化資通安全管理及提升個資保護能力有更多瞭解及落實。另最近我國發生**食安問題（包括食材健康化、健康資訊化、資訊透明化、透明稽查化、稽查專業化及專業驗證化等六大食安控管目標）**不僅是讓社會大眾產生恐慌，對於其後續利用食品雲、發票雲、健康雲、警政雲、經濟雲、交通雲、生活雲、安全雲等解決方案，也正好是運用大數據分析（BDA）理論的最佳範例，更可以印證在雲端環境中，其**創新應用、安全管理與數位鑑識議題是相輔相成**，缺一不可。

一、網路犯罪學相關理論

傳統「日常活動理論」、「理性選擇理論」對預防網路犯罪或駭客的犯罪行為（如惡意程式、勒索病毒及 DOS/DDoS, APT 等），在解釋上具有相當意義，尤其在維護資通安全所建置的防火牆（firewall）、網路病毒入侵偵測系統（IDS/IPS）或防毒軟體（Anti-Virus）等設備，雖無法完全杜絕網路犯罪的發生，但在避免形成有利犯罪情境，本文認為該論述具有防制效益與效能。

（一）網路（數位）犯罪理論

所謂「**網路（數位）犯罪（Cybercrime）**」固係屬電腦犯罪之延伸，為電腦系統與通訊網路相結合之犯罪，但相較於電腦犯罪而言，更偏重於「網際網路」的應用，而係指具有網際網路特性的犯罪，亦即行為人所違犯之故意或過失的犯罪行為具有網際網路特性者；就實際應用而言，亦即犯罪者在犯罪過程中需借助網際網路方能遂行其犯罪意圖之犯罪，當然並非所有犯罪

都可經由電腦或網路予以實施，刑法上所謂的「親手犯」，其性質強調行為之親手性，指行為人必須親自實施該行為始能成立犯罪，如重婚罪、通姦罪，即不可能成立網路（數位）犯罪。

網路（數位）犯罪不僅是電腦犯罪的延伸，且包含網路與網路間犯罪、網路與人的犯罪、網路與社會的犯罪、網路與文化的犯罪、網路與經濟的犯罪、網路與法律的犯罪、網路與政治（數位國土）的犯罪等等，而目前專家學者，對網路犯罪並沒有嚴格定義及統一意見，且它是最近一新興的電腦網路犯罪型態，故從網路犯罪之特性與網路犯罪行為人之特質之描述，及電腦犯罪之特性與電腦犯罪行為人之特質為說明對象，以其對網路犯罪有更深的瞭解。從狹義來說，網路是電腦系統與通訊網路之結合體，而網路犯罪應該是電腦系統犯罪與通訊網路犯罪之組合體，因此，電腦犯罪之特性與行為人之特質均適用於網路犯罪。而網路犯罪者意圖為自己或第三人不法之所有，直接或間接以操作電腦或進入網際網路之方式，阻害或非法使用電腦、網際網路（互聯網）或其內部資料的犯罪模式成為關於電腦網路領域犯罪問題的一項新的課題─電腦網路犯罪（或稱網際網路犯罪（Internet Crime），簡稱網路（數位）犯罪（Cybercrime））。

（二）網路（數位）犯罪學理論

所謂「**網路（數位）犯罪學（Cyber Criminology）**」主要是以科學的方法研究網路（數位）犯罪現象和網路社會對其的反應措施的一門科學，來探討多變與複雜的網路（數位）犯罪現象，以科學的方法，解釋網路（數位）犯罪的發生與形成，網路（數位）犯罪學深受因科技的影響，當網際網路越發達時，網路社會對網路（數位）犯罪的研究則越迫切需要，對網路（數位）犯罪問題更須超科技來整合，運用各個不同的研究領域，如醫學、生物學、心理學、社會學、網路學、經濟學、法律學、資訊學、公司治理、科技治理及哲學治理等，將之整合而成為新的一門學科--**網路（數位）犯罪學**。

網路（數位）犯罪學本質上已是一種超科技的學科，從一個網路資訊社會（Cyber Society）中探討網路犯罪問題，擁有一個明顯的領域而能自主的知識體系，網路犯罪學目前從事研究的議題，似乎比傳統犯罪學少，但以資通訊科技（ICT）的快速進步來看，網路（數位）犯罪學應是一門顯學，將不同的領域之概念和訊息，在網路資訊社會中融合而成，使其有依完整的理論概念與知識生態體系，而其探討的網路（數位）犯罪與網路資訊社會中秩序的建立，是未來網路資訊社會進步的原動力。

（三）網路犯罪類型

網路（數位）犯罪的類型可區分為，妨害電腦網路機能及非法使用電腦

網路等二類犯罪類型。依前述有關網路犯罪的定義，本研究將網路犯罪細分為三項：(1) 以網路空間作為犯罪場所；(2) 以網路作為犯罪工具；(3) 以網路作為犯罪客體（如表 1）。

表 1　網路犯罪之分類及其常見型態

分類標準	特點	常見型態	知悉程度	偵查難度	鑑識難度	犯罪者技術程度	鑑識工具準備複雜度
以網路為犯罪工具（特定目標）	針對特定目標予以侵害性質，藉由網路作為犯罪工具	1.網路恐嚇 2.網路誹謗 3.網路詐財 4.網路釣魚 5.網路遊戲寶物變更 6.勒索病毒	中	中	中	中	中
以網際空間為犯罪場所（被動）	被動性質，引誘吸引一般人進入	1.網路色情 2.網路援交 3.販賣盜拷 4.網路賭博 5.網路遊戲 6.販賣槍械 7.教授製仿炸彈 8.散佈夾藏木馬程式的色情圖片	高	低	低	低	低
以網路為犯罪客體（為攻擊目標）	對網路或電腦系統的攻擊或破壞性	1.網路入侵（駭客） 2.散播電腦病毒 3.網路竄改 4.SQL Injection 5.網站漏洞入侵 6.網頁替換 7.密碼掃描 8.DoS/DDoS	低	高	高	高	高

二、數位證據與數位鑑識

（一）數位證據

凡是以電腦或相關電子裝置所處理、儲存、傳輸的電子記錄，包含文字、聲音、影像、照片、符號或其他資料等，透過適當的設備將之讀取出來，用以支持或反證犯罪的證據者都可稱為數位證據（Digital Evidence）。數位證據就是以電腦為基礎或是和電腦及行動裝置有關的證據，儲存於電腦及行動裝置媒體或藉由各類型電腦及行動裝置媒體傳送之資料。任何可以證明犯罪構成要件、犯罪意圖或不在場證明等有關聯的數位資料，為物理證據之一種。目前世界各國及我國法律都尚未對數位證據有正式的定義，只有對電子紀錄、電磁紀錄及電子文件加以定義，使得數位證據的定義非常模糊，根據我國法律及學者的定義，將其定義為藉由電腦或網路設備儲存或傳送可供證據使用，稱之為數位證據，即包括電子文件、電子紀錄、數位紀錄及電磁紀錄。因此，唯有專業的數位偵查及鑑識人員，嚴謹的鑑識流程，以及專業的鑑識工具，才能確保蒐集到的數位證據具有法律效力及避免同樣的證據產生不同的解讀。

2013 年轟動一時，讓郭台銘公開表示「非常痛心」的鴻海內部舞弊案，調查局更扮演破案關鍵角色。檢警搜索弊案相關人士在臺住所扣押的幾個隨身碟（USB），便是送到調查局將刪除資料還原，關鍵帳目才因此曝光，幾個協助嫌犯洗錢的「白手套」因此招供，案情才急轉直下，在 2014 年破案。該案於 2012 年爆發，主導鴻海採購大權的 SMT 委員會前資深副總廖 O 城、前經理鄧 O 賢等人，涉嫌長期向供應商收回扣。鴻海接獲檢舉，隨即向中國當地公安報案，但最後卻以不起訴結案。郭台銘不死心，回國向刑事警察局報案。但後來承辦檢察官找上調查局協助，10 個月後破案，於 2014 年 5 月起依「證券交易法」的特別背信罪及「刑法」的普通背信等罪嫌起訴廖 O 城等 6 人，總共收取賄款 1.6 億臺幣。

另於 2016 年發生在聯發科、台塑化、長春等大企業，屢屢傳出內賊竊取商業機密，或收取巨額回扣的今日，硬碟、隨身碟跟電子郵件，甚至通訊軟體 Line 裡頭的「**數位證據**」，已成為多起商業大案的破案關鍵--「**數位鑑識**」。再如 2016 年 7 月發生第一銀行 ATM 盜領案、2016 年 5 月發生中華郵政商城網路個資外洩案、2017 年 2 月發生臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件、2017 年 5 月新型勒索病毒 WannaCry 重創臺灣、2017 年 6 月全球多個國家遭受新一輪 Petya 勒索病毒攻擊、2017 年 10 月遠東銀行 SWIFT 系統遭駭客入侵 18 億案，其破案關鍵技術--「**數位鑑識**」。(SWIFT, Society for Worldwide Interbank Financial Telecommunications---環球同業銀行金融電訊協會)。

（二）數位鑑識與行動鑑識

數位鑑識（Digital Forensics）又稱電腦鑑識（Computer Forensics）或資安鑑識（Cyber Forensics），屬於鑑識科學（Forensics Science）的分支，用以取得數位資料中存在的數位化法律證據。數位鑑識可以定義為：利用科學驗證的方式調查數位證據，經由數位證據的擷取、分析、還原等過程，還原事件原貌，以利事件調查，並提供法庭訴訟之完整依據。行動鑑識屬於數位鑑識的其中一部份，指所有對行動裝置上的數位資料進行保存、識別、萃取、分析及鑑定的行為。手機中儲存的資料，以電磁紀錄存在，此即所謂的數位證據，手機上的證據，屬於數位證據在行動鑑識的延伸。

「數位鑑識」又稱數位鑑識科學（Cyber Forensics Science），是鑑識科學的分支，主要針對數位裝置中的內容進行調查與復原，這常常是與電腦犯罪有所相關；數位鑑識原與電腦鑑識為同義詞，但現已擴展到調查所有能夠儲存數位資料的裝置（如智慧型手機、行動電腦、行動設備、雲端儲存設備等）。

「資安鑑識」為台灣數位鑑識發展協會（Association of Cyber Forensics Development in Taiwan，ACFD）創會理事長林宜隆教授所提出最新名詞，資安鑑識廣義領域包括「資安預防（Prevention）、資安防護（Protection）、證據保全（Preservation）及專業鑑識（Presentation）」等四大階段，由國內學者林宜隆教授與澳大利亞教授 Jill Slay 共同提出之 4P’s Model Forensics Computing 理論，基於資安鑑識領域中要如何建立需具備強大資安鑑識能量，其應包括 CyberLab.實驗室（如符合 ISO17025）、標準作業程序 SOP（如符合 ISO27037）與國際專業鑑識人才（如符合 ISO17024）。

對於資通安全及數位鑑識能量規劃之研究取向應包括國家級數位鑑識實驗室設立、數位證據鑑識標準作業程序建構、資安專業人才培育等三個領域（如圖 1），本文將先介紹**我國數位鑑識能量**之發展現況，接著再由數位鑑識實驗室設立、建構數位證據鑑識標準作業程序（DEFSOP）、及資安專業人才培育三個方向進行資料蒐集和深入研究，最後即針對我國資通安全及數位鑑識能量提出結果及建議事項。透過此三方向的探討，對我國資通安全及數位鑑識能量做出改善及提昇整合**科技建警與偵防並重之警政新策略（如數位鑑識科技能量）**，並將確保數位證據之證據能力與證明力，並提昇其證據有效性與公信力。

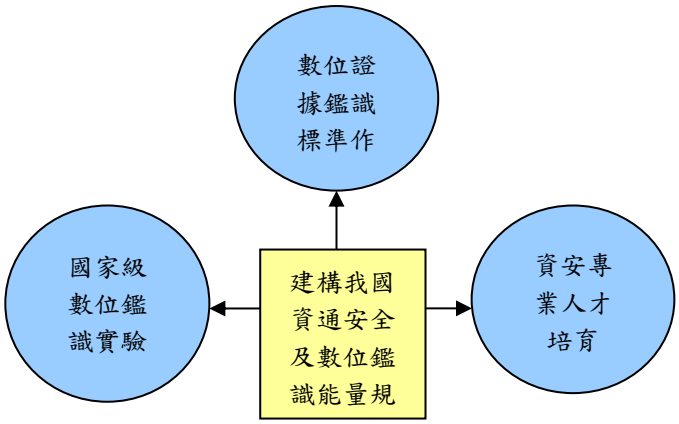

圖 1 我國資通安全及數位鑑識能量規劃

參、建立 M-O-P 網路犯罪三要素動態模式

一、日常活動理論

「日常活動理論」(Routine Activity Theory, RAT) 由美國學者柯恩及費爾遜 (Cohen & Felson) 於 1979 年首先提出。該理論強調犯罪活動的發生在時空因素上，必須與日常生活各項活動相互配合，亦即日常生活活動型態將會直接影響犯罪發生的「機會」，進而導致「直接接觸掠奪性犯罪」(Direct-contact Predatory violation) 的發生。認為一個犯罪活動的發生，必須在以下三個情境要素同時聚合 (1) 有動機、能力的犯罪者 (Motivated Offender)；(2) 合適的標的 (Suitable Target)；(3) 監控或抑制犯罪者不在場 (Absence of Capable Guardian Against Crime)。日常活動理論 (RAT) 認為，直接接觸掠奪性違法行為的發生，均需具備下列三要素：

(一) 有機動之犯罪者 (Motivated Offender) 在場：

依據前述的看法，日常活動理論跳脫出傳統討論犯罪原因的模式，而是以「機會」(Opportunity) 來說明犯罪的發生。該理論認為，社會中原本即有相當數量的潛在犯罪人，若將犯罪傾向者控制在一定的數量，則犯罪率應可維持不變，但由於社會變遷結果，導致人類活動型態產生變化，直接造成犯罪機會的增加，而提高犯罪率。

(二) 合適的標的物 (Suitable Targets) 存在：

合適的標的物乃根據標的物之價值、標的物之可見性及對犯罪者之防禦

性等三項指標而定。

1.標的物之價值（Value）：係依據犯罪者對人或物的標的，其需求如何而定。例如：駭客入侵網路銀行破解密碼取得金錢的需求；網路援交，以肉體尋求金錢援助需求等皆是。

2.標的物的可見性（Visibility）及可接近性（Access）：菲爾森對可見性及可接近性舉出三個原則來說明：

（1）最省力原則（Principle of Least Effort）：亦即是犯罪人以最短的路、最少的時間及最簡單的方法完成犯罪。

（2）最大可見度原則（Principle of the Most Obvious）：本原則依據第一項原則衍生而出，也就是人們依賴現成的資訊去做選擇，例如：駭客依其知名的大企業，去選擇最適宜組織目標攻擊，然而也許在其可見範圍之外，存有更合適的目標，但因為無法接觸或獲取資訊，就不可能在遠處實施犯罪。

（3）暴露自己於危險最短時間及最小空間：這是由第二原則發展而來，網路犯罪者假借縮短犯罪時間與空間，以減少被捕或發現的機會，例如：入侵之後將進出記錄刪除。

3.對犯罪者之防禦性（Defense）：以物品而言，包含大小、重量以及是否上鎖，也就是端視其自我的防禦力而言，物品愈大、愈重，搬運困難而較不容易被竊。被害者對加害者的防禦力越高，相對的其被侵害的可能性就降低。

（三）有能力遏止犯罪發生之抑制者不在場（Absence of Capable Guardian Against Crime）：

所謂足以遏止犯罪發生之抑制者不在場，並不單指警察人員而言，乃泛指一般足以遏止犯罪發生之抑制力缺乏，例如：個人離開家庭，家中空無一人，營業處所夜間無警衛看守等。日常活動理論的基本命題認為，非法活動依附於日常合法活動所建構的社會體系中，此乃說明了如果人們減少留在家的時間，則居家財產就較無保障的機會，而人們在夜晚獨自外出或逗留，就有較多遭受侵害的機會。修格・巴羅（Hugh Barlow）。在此一方面中就舉出一種論述：「發生商店竊盜（shoplifting）的原因，大多是因為商店有寬廣、開放式的場地，而且又缺乏有效的監控所致。」

二、理性選擇理論

美國經濟學者 Becker 於 1968 年提出「犯罪懲罰：經濟觀點」之研究，主張認為犯罪理論是延伸來自於經濟學中，有關理性投資報酬率的觀點。

Clarke & Cornish（1987）繼之延續該理念提出「理性選擇理論」（Rational Choice Theory, RCT），支持強調犯罪行為與經濟行為間，當事人的決策模式相類似，有關選擇與決定的思維過程是一致的；即人們會透過當時所蒐集的情報或資訊，運用有限的理性進行分析，並做出對自己最有利的決定。本文支持該理論的主張，認為必需關注的是網路（數位）犯罪行為人與網路（數位）犯罪行為的當下犯罪情境，即對網路犯罪或駭客所造成的風險高低問題。

三、建立 M-O-P 網路犯罪三角理論

國內學者林宜隆教授從預防網路（數位）犯罪的觀點，主張以「M-O-P 網路（**數位**）犯罪三角理論」（MOP Cybercrime Triangle）將構成網路（數位）犯罪的要件細分為：「動機（Motivation）」、「標的物（Object）」及「抑制機制（Protection）」等三角關係，而與這三者分別對應則為「日常活動理論」中所謂一個犯罪活動的發生，必須在三個情境要素同時聚合：有動機、能力的犯罪者（Motivated Offender）、合適的標的（Suitable Target）、監控或抑制犯罪者不在場（Absence of Capable Guardian Against Crime）。

如圖 2 日常活動犯罪理論犯罪三要素動態模式（E1，E2，E3 分別表示家庭環境、學校環境及社會環境），此理論中的三個要素對於解釋為何會發生犯罪行為具有可操作性，有時也稱為犯罪基本三角（The Basic Crime Triangle）。由上述日常活動理論得知下列一個推論：「當網際網路使用越普及，則網路犯罪發生的可能性就越大」。為防止網路犯罪的發生，必須相對的提高網路安全科技（如防火牆（Firewall）、入侵偵測系統（IDS）設置及密碼技術）（即代表 P），及儘速制訂網路使用管理辦法（如訂定網路使用倫理及行為準則、數位匯流法草案）（即代表 M），資訊使用相關法令（如過濾軟體及分級制度、資通安全管理法草案）（即代表 O）等以確保網路系統之安全。在網路空間中亦存在與真實世界相同價值的要素，且因網路的商業化與普及化，使人人都有機會與能力遨遊於網路世界，相對的因資訊具有的利益價值，使網路資訊安全如未能有效防範，網路使用者就如同夜間經過無人看管的金庫一樣，網路犯罪就會因時空的聚合而發生。

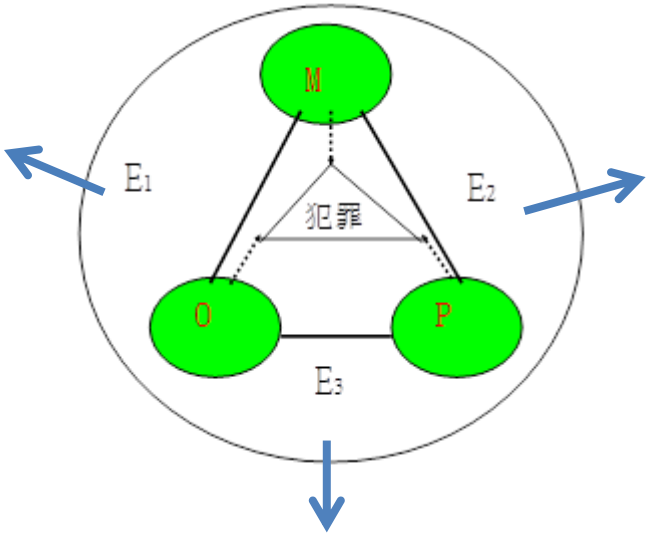

圖 2　「M-O-P 網路犯罪三角理論」（by Paul Lin）

註：E1：家庭環境、E2：學校環境、E3：社會環境

四、整合日常活動犯罪理論之 M-O-P 與社會控制理論預防模式

網路（數位）犯罪根據實證學派犯罪學之社會控制理論及日常活動犯罪理論即可說明其發生及預防措施，亦是本文研究整合及利用其控制因子，並強調犯罪的動機和犯罪人可說是一常數，亦即社會上有固定比例的人總會因特殊的理由（需要、貪婪及好奇等）而犯罪，赫胥（Hirschi）的社會控制理論（所謂的四個「鍵」(social bond)，包括「依附」(attachment)、「參與」(involvement)、「奉獻」(commitment)、「信仰」(belief)。再者，美國犯罪學者 L. Cohen and M. Felson 在 1979 年所提日常活動犯罪理論，加上前一節所推論出的 MOP 理論觀點，均認為犯罪是人們日常生活型態的一種結果，且犯罪事件要發生必須有三種要素在時空的聚合：(1) 有動機及能力的犯罪者（Motivation，以字母 M 為代表）、(2) 合適的犯罪標的物（Object，以字母 O 為代表）及 (3) 抑制犯罪發生者的不在場（Protection，以字母 P 為代表），在此以 (M-O-P) 代號來予代表，再加上環境 (environment) 的因素 (E1、E2 及 E3 分為代表家庭、學校及社會的環境)，故給合上述兩的理論，針對有動機及能力的犯罪者，若能利用社會控制理論的四個社會鍵來控制，得知整合日常活動犯罪理論之 M-O-P 與社會控制理論預防模式，如圖 3 所示。

故本文研究認同學者林宜隆教授經由「M-O-P 網路（**數位**）犯罪三角理

論」的實證研究，結合「日常活動理論」及「社會控制理論」（Society Control Theory），針對有動機、能力的網路犯罪者，利用「社會鍵理論」的四個社會鍵 來控制其犯罪意圖，進而形成偵防網路（數位）犯罪新策略（New Prevention Strategy of Cybercrimes Investigation）（如圖 3）。

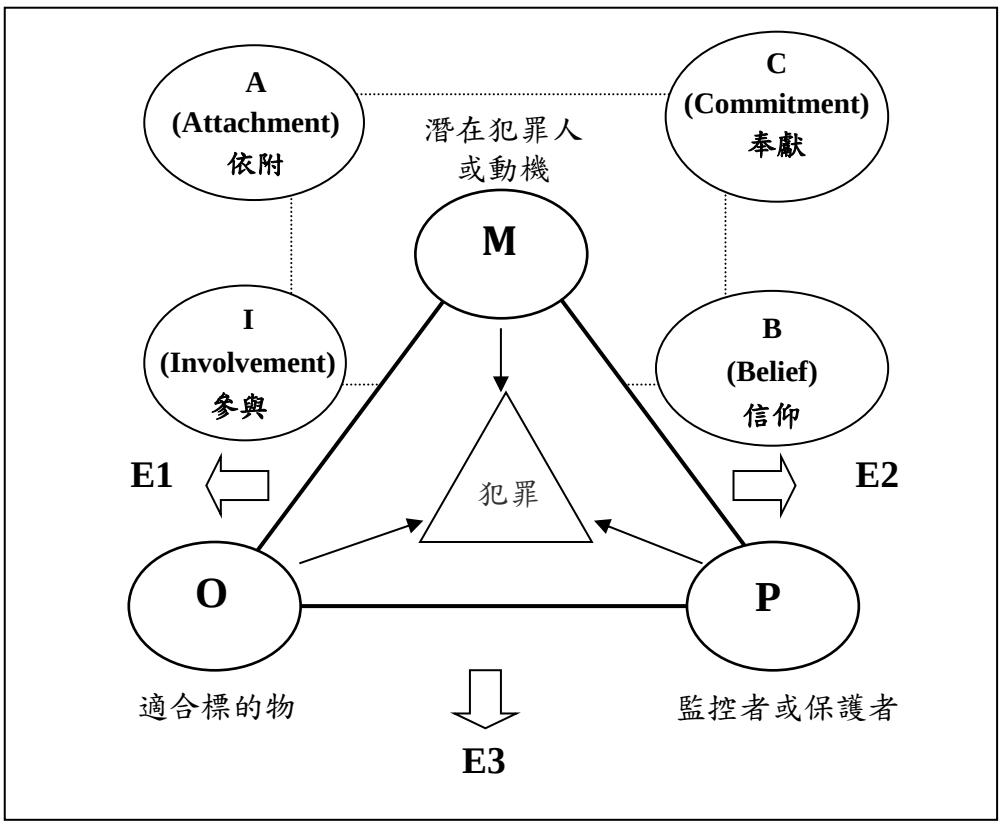

圖 3　整合日常活動犯罪理論之 M-O-P 與社會控制理論模式圖

資料來源：網路犯罪成因與防治對策之研究，2006，范國勇、林宜隆

五、網路空間治理

研究者粟斗南（2004）在「資訊安全與網路犯罪」之研究中引述了 1996 年 2 月約翰・派里・巴洛（John Perry Barlow）於網路上發表「**網路空間獨立宣言**」（A Declaration Of The Independence Of Cyberspace），文中提出反對既有的政府體制對網路空間進行任何形式的管制與掌控。強調現有的網路世界是由所有網路使用者自行建設、不受官方管制的全球性的社會空間（Global Social Space）。網際網路中的**網路治理（Cyber Governance）**應由網路本身所形成的社會契約（Social Contract）來做為主體，而不是由現有政府體制下

的法律或政府組織來對網際網路進行約束。此派論者多為**網路空間無政府主義（Cyberspace Anarchism）**者，其基本立場是不同意政府或國家的角色介入網際網路之管理，政府或國家也不應干涉網際網路中之任何活動，期待網路使用者有絕對的理性，也完全把國家的角色排除在外。

回顧 2016 年數位世界的兩件頭條新聞，剛好可以做為 2017 年網路治理展望之框架：一為 2016 年 10 月 1 日，美國政府將 IANA(Internet Assigned Numbers Authority, IANA）保管權責移交給全球多方利害關係人社群，一為 2016 年 11 年 2 日，中國政府宣布自 2017 年 7 月 1 日起實施新的「網路安全法(Internet Security Act)」：IANA 的移交，揭示多方利害關係人由下而上的政策發展流程；而中國的「網路安全法」，代表的是由上而下的政府強行介入網路治理。而新 ICANN(Internet Corporation for Assigned Names and Numbers, ICANN）章程，（ICANN 稱為網際網路名稱與數字地址分配機構，是美國加利福尼亞的非營利社團，主要由網際網路協會的成員組成，創建於 1998 年 9 月 18 日，目的是接管包括管理域名和 IP 地址的分配等與網際網路相關的任務）可能是最先進提供開放、自由及未分裂網路之多方利害關係人機制的最佳版本；而中國的網路安全法，則是一個國家在國土疆界內如何控制網際網路的最露骨版本。一方是多方利害關係人機制，一方是國家政府機制；而且不只中國政府強勢主導國家網路政策之立法，俄國、土耳其、伊朗、匈牙利、波蘭、巴基斯坦，甚至英國亦復如是。我們可以預見多方利害關係人機制，與國家型網路政策之新衝突型態嗎？

新的國家主義會開始裂解無疆界的網路空間（Cyberspace）嗎? 白宮華盛頓橢圓形辦公室的新總統之政治權力會踐踏集體智慧嗎？網路虛構（Cyber）會擊敗事實嗎？這些雖看似誇張的問題，但答案儼然是「Yes」。我們將即將會看到令人不寒而慄的新「網路冷戰（Cold Cyberwar）」時代的來臨；我們也會看到更多政府假借安全之名，限制諸如隱私、言論自由等基本人權；我們也會看到更多的政府，在全球網路空間築起疆界，將其國家化成為國家網路領地（即數位國土），以控制其人民、民營公司之個人資料、通訊內容之流通等。2015 年 7 月 1 日新版的《中國國家安全法》開始實施。該法的涵蓋面極廣，包括政治安全、軍事安全、經濟安全、文化安全、社會安全、網路安全、核安全，都一體適用於國家安全體系。其中第二十五條有關網路部分如下：

> 「國家建設網路與資訊安全保障體系，提升網路與資訊安全保護能力，加強網路和資訊技術的創新研究和開發應用，實現網路和資訊核心技術、關鍵基礎設施和重要領域資訊系統及資料的安全可控；加強網路管理，防範、

制止和依法懲治網路攻擊、網路入侵、網路竊密、散佈違法有害資訊等網路違法犯罪行為，維護國家網路空間主權、安全和發展利益。」

這段條文清楚揭露「**維護國家網路空間主權、安全和發展利益**」的法案主軸。

西方政府也開始出現傾向強勢之**網路治理規範（Cyber Governance Regulation）**，包括爭論網路安全是否比資料保護重要，並減少對包括網域名稱、IP 位址及網路協定等網路資源的多方利害關係人模式之承諾。另一方面中國政府包括習近平主席，已經認可及推進「**網路空間主權（Cyberspace Sovereignty）**」概念，同時也在考慮非政府部門的參與。2016 年 11 月浙江烏鎮第三屆互聯網世界大會中，發現已經出現中國版本的多方利害關係人模式，稱之為「**多黨（方）治理模式」（Multi-Party Governance）**，該會議亦邀集中國私營企業、技術社群甚至公民社群參與網路政策制定，雖然實務上仍值得再進一步觀察，但有趣的是其中仍然充滿意識形態的語言。

美國強化國家網路安全委員會（US Commission on Enhancing National Cybersecurity）主席 Tom Donilon，於 2016 年 12 月 2 日向美國總統歐巴馬提出報告指出，對其政權或關鍵基礎設施的嚴重網路攻擊，將會得到很強大的回擊，且建議其繼任者應嚴肅考慮委員會之建議。而 2016 年 12 月 29 日，中國網路空間管理辦公室（Cyberspace Administration of China）提出新的「**國家網路空間安全策略（National Cyberspace Security Strategy）**」，包括利用網路進行叛國、分離、反抗、顛覆破壞、偷竊或洩漏國家機密，將會受到懲處，也納入對國外勢力協助破壞、顛覆及分離提出警告之處罰。這是否意味著對抗即將到來？比較兩份文件，可以看出在 2017 年，美中的硬體及軟體武器競賽及網路衝突，有非常高的發生機率。但同時亦保留開啟對話及相互瞭解的一扇窗。兩份文件皆說明，要共同對抗網路恐怖份子及網路（數位）犯罪，而且兩國都亟需促進數位經濟之發展，換句話說，對抗及合作將會肩並肩而行；其中有相互不信任及利益與價值的衝突，但同時也準備好建立網路空間及國際法律討論之合作空間。

網路生態系統（Internet Ecosystem）會是一個分散式、多樣且無集中權威管理的機制，而其不同的子系統，會從單一或跨政府間所控制的階級架構，到基於非政府社群之自我規範機制；介於其間則由政府、民營企業、公民社群及技術社群等共同規範的發展。因此，**網路治理生態系統（Cyber Governance Ecosystem）沒有**一體適用的解決方案，特定形式的子系統，會依據特地需求及個別特質而設計；傳統的國家立法及跨政府間的協議，依然會持續扮演一定角色，但需要適切嵌入更廣泛的多利害關係人環境。不同管

理體制的競爭與共存，都可能會產生一些機會及風險。新機制、服務或平台之機會，將動態性引入政治策略、社會行動及市場發展。競爭的並存，可以刺激創新、產生新工作機會、擴大文化活動及強化一般大眾之言論自由。但不同體制的風險，是可能會產生更多爭議及嚴重衝突，包括威脅關閉創新、阻礙持續發展、減少個人自由，甚至污染、破壞或摧毀整個**網路治理生態系統**。

網路治理論壇（Internet Governance Forum, **IGF**）在 2005 年剛成立時，僅能扮演個網路治理政策制定後的議論場合；11 年後的今天，加上 IGF+（第二個 10 年）的新指令將其延伸至 2025 年之期程，儼然已經讓 IGF 成為一個對新興議題起始討論，或是決策組織對複雜問題尋求解決方案的絕佳場所。2016 年 12 月，在墨西哥瓜達拉哈拉（Guadalajara）的 IGF 會議，在網路治理與貿易協商方面，已經成為各利害關係深入討論的場合。沒有人會不同意，尤其是電子貿易（eTrade）是未來數位經濟最關鍵的元素，也必須進行跨國家間合作的必要安排；但至目前為止，全球網路協商與貿易協商，都是各自基於兩者非常特殊的政治文化而分別進行。開放的多方利害關係人討論方式，可以促進政府專家與各衝突團體坐在協商桌，共同尋求可以永續發展的正確妥協方案。**網路治理的相關討論是基於開放、透明**，藉由各利害關係人各自角色及立足點平等，由下而上的參與方式進行。傳統貿易協商則是關起門來，以跨政府間的相互協議方式進行，甚至給大企業私下遊說的機會。

IGF 已經逐漸成熟到可以做為型塑及設定新興議題及議題討論的一個平台。網路世界總是有不斷出現的新興與開放議題，如能將議題討論的框架予以結構化（Structuring of the Debate），就會非常有價值。將成堆的網路治理議題置於大框架下，可以歸納為「四**籃**」（**Four Basket**）**框架（第一籃：網路安全，第二籃：數位經濟，第三籃：數位人權，第四籃：數位技術）**，此框架可以協助不同利害關係人確認議題範疇，也可以提供應該與誰討論、在哪裡討論、如何討論等規劃之參考。過去全球 IGF 相關會議，已經幫網路治理議程提出參考框架，未來的網路安全、數位經濟甚至數位人權議題，都已經橫跨各領域。網際網路是經由技術協定網網相連，政策領域同樣需要不同群體、平台及機制的網路，經由各利害關係人協商而網網相連，**成為政治網路（Political Internet）**。展望 2017 年，我們必須盡速重新梳理出適合自己的網路治理討論協商機制，一種能夠讓新興議題快速解決的機制。到目前為止，**網路空間（Cyberspace）**仍然是無人領地，為創意及創新而開放，它仍屬全人類的公有財；**網路治理（Cyber Governance / Internet Governance）(**可參考 **ISO27014:2013 Governance of Information Security and COBIT 5.0 IT Governance）之**良窳，已成為各國國家發展的關鍵要素。

若依照社會控制理論來看它,「網路空間獨立宣言」倡導政府或國家不應介入網際網路之管理，這個理論恰好與「抑制理論」和「社會控制理論」唱反調，表面上是宣告網路使用者有絕對的理性能獨立自治，若依照這句話來解釋人類為什麼會藉由網路空間犯罪？就**網路空間治理（Cyberspace Governance）的理論**似乎應該被重新定義成：「**網路空間治理理論係為一項內化的自我控制（Reckless, Walter）亦是網路社群產出的道德標準（Hirschi, Travis），藉由自治來達到網路社會不當行為的抑制，但必須輔助外在之抑制力量的介入，內在與外在之抑制並行，才能使人趨向於不犯罪**」。此乃較能合乎網路空間治理的基本定義，也將是人類未來需要建構「**網路空間治理命運共同體**」。

肆、我國數位鑑識能量規劃與發展現況

一、設立我國數位鑑識實驗室

近年國內與電子化有關之犯罪案件大幅成長（如 2016 年 7 月第一銀行 ATM 盜領案、2016 年 5 月中華郵政商城網路個資外洩案、2017 年 2 月臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件、2017 年 5 月新型勒索病毒 WannaCry 重創臺灣、2017 年 6 月全球多個國家遭受新一輪 Petya 勒索病毒攻擊、2017 年 10 月遠東銀行 SWIFT 系統遭駭客入侵 18 億案、2017 年智慧型手機詐欺等犯罪案件），且犯罪手法不斷翻新，並逐漸朝組織化犯罪趨勢發展，即使是傳統犯罪案件如恐嚇取財或殺人案件等，常以電腦網路做為犯罪工具者,或為通訊設備(如電子郵件、即時通 LINE/Wechat/Juiker/FB Messenger、網路電話等通訊軟體之使用），取代傳統書信通訊方式，亦或被當成犯罪證物之儲存設備（如蠻牛千面人事件，犯嫌使用之毒物影像、勒索計畫書等均為電子化物證），再因偵查人員對於電子化物證認知不足，未進行搜索或扣押偵查作為，往往錯失破案契機。且電腦數位鑑識過程應注意數位證物證據能力，故鑑定時需依相關規定或 SOP 作業流程處理（**如符合國際標準 ISO27037、ISO27041、ISO27042、ISO27043 或 DEFSOP**），若有任何不經意之動作，將會污損物證原樣，破壞數位物證完整性。電腦數位鑑識絕非僅是解析犯罪檔案之能事，其中還需注意的事項包含如何確認證據本身的合法性（C）、完整性（I）、準確性（A）、一致性（C）及有效性（**CIAC 數位鑑識基本原則**）、如何確保證據檔案內容沒有被修改過、如何找出全部的證據資料等，然這些問題，早期尚未建立一套標準作業程序，以致於重要數位證據檔案常因處理不當而遭到破壞，但目前政府機關及研究單位已建立一套

標準作業程序（如 DEFSOP/ISO27037），甚至國內**台灣數位鑑識發展協會（ACFD）正積極規劃依 ISO27037/ISO27041/27042/27043/27050 等國際標準建立新版 DEFSOP**，且**符合 CIAC 數位鑑識基本原則**，進一步提升其數位證據之有效性及證據能力與證明力。

成立國家級數位鑑識實驗室（**如法務部調查局資安鑑識實驗室（Cyber Forensics Laboratory, CFL）2007 年成立，2013 年通過 ISO17025 認證**）已是各先進國家積極推動的數位鑑識發展目標之一，在對提升資通安全及數位證據鑑識能量的研究中，亦已成為重要的研究項目，而在國家級數位鑑識實驗室中，應有以下之工作目標：（如圖 4）

（一）充實數位鑑識軟、硬體設備，因應未來數位化科技犯罪案件趨勢所需，鑑定與解析各式各樣電子化物證，以取得科技犯罪案件關鍵證據與情資。

（二）建置符合 ISO17025 國際標準規範之數位鑑識實驗室與犯罪物證管理系統，嚴格控管犯罪證物保全，以確保證物本身之安全性及完整性，使鑑定結果具有證據能力。

（三）研發數位物證自動化數位鑑識軟體工具，快速有效解析犯罪有關之資訊，輔助偵查人員速迅掌握犯罪案件偵辦方向或釐清案情。

（四）提昇科技（數位）偵查能力，充實科技偵查蒐證設備，同時建構網路駭客攻防所需系統及工具，以有效防制與解決國內資安犯罪問題（如**科技建警與偵防並重**）

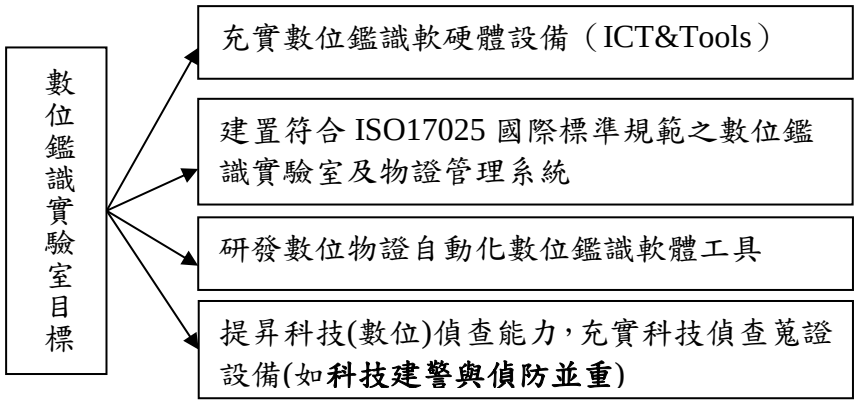

圖 4　數位鑑識實驗室工作目標圖

當專業之數位鑑識實驗室成立（如法務部調查局資安鑑識實驗室 2007 年成立，2013 年通過 ISO17025 認證），除因應法院、檢警等單位大量電子化物證檢驗所需外，亦有效解決當時國內警方尚無符合規範與專責處理數位

證據之實驗室窘境。且經由數位鑑識專業的訓練，大幅提升偵查人員對於數位鑑識工作的處理能力，以解決日益嚴重之數位犯罪問題（如司法機關 2015 年鴻海內部舞弊案破案及 2016 年 7 月 18 日第一銀行 ATM 盜領案破案）。並有助於強化對於駭客入侵等資安案件之偵辦能力，並有效防制此類網路犯罪之蔓延。

作者是臺灣第一位學者於 1999 年拜訪美國 FBI 加州聖地牙哥區域電腦鑑識實驗室（Region Computer Forensics Lab., RCFL）與研習（如圖 5 & 6）。RCFL 是 FBI 和其它聯邦、州和當地執法人員組成在一個地理領域內，RCFL 提供數位媒體的鑑識檢查與專業人才培訓，例如電腦，支援聯邦、州和當地犯罪的調查和/或起訴。

美國 FBI 第一個 RCFL 建立在加州聖地牙哥，它開始由 FBI 和其它聯邦、州和當地執法單位合作在南加州處理電腦證據，RCFL 最先建立時，這些單位經累積實際經驗可提供個別的資源來幫助處理電腦證據及數位鑑識。隨後其它的 RCFL 在北方的德州、芝加哥和堪薩斯城被建立。RCFL 是一個單一服務鑑識實驗室完全專心致力於數位證據的檢查、檢驗及鑑定以支援犯罪調查與專業人才培訓，例如：（http://www.rcfl.gov）

- 恐怖行動
- 兒童色情圖片
- 暴力行為的犯罪
- 智慧財產權的偷竊和破壞
- 行業秘密偷竊
- 金融犯罪
- 財產犯罪
- 網路犯罪
- 詐欺

圖 6　作者與美國 FBI 加州聖地牙哥 RCFL 主任合照（1999）

二、建構數位證據鑑識標準作業程序

制定一套合乎需求及符合 CIAC 數位鑑識基本原則之數位證據鑑識標準作業程序（Digital Evidence Forensic Standard Operation Procedure, DEFSOP）及規範，使檢、警、調偵查人員在處理數位證據時，能符合**一致性（Consistency, C）、完整性（Integrity, I）、準確性（Accuracy, A）及合法性（Compliance, C）**之原則（**CIAC 數位鑑識基本原則**），而提高數位證據之證據能力與證明力，並建立其數位證據有效性與公信力，這是在提升我國資通安全及數位鑑識能量規劃中不可或缺的一環，故透過國內外文獻整理分析與歸納，以及參考國內學者林宜隆教授所提出數位證據鑑識標準作業程序（DEFSOP），對數位證據鑑識標準作業程序做相關性的整理分析與建構具可行性及有效性的 DEFSOP。（如圖 7）

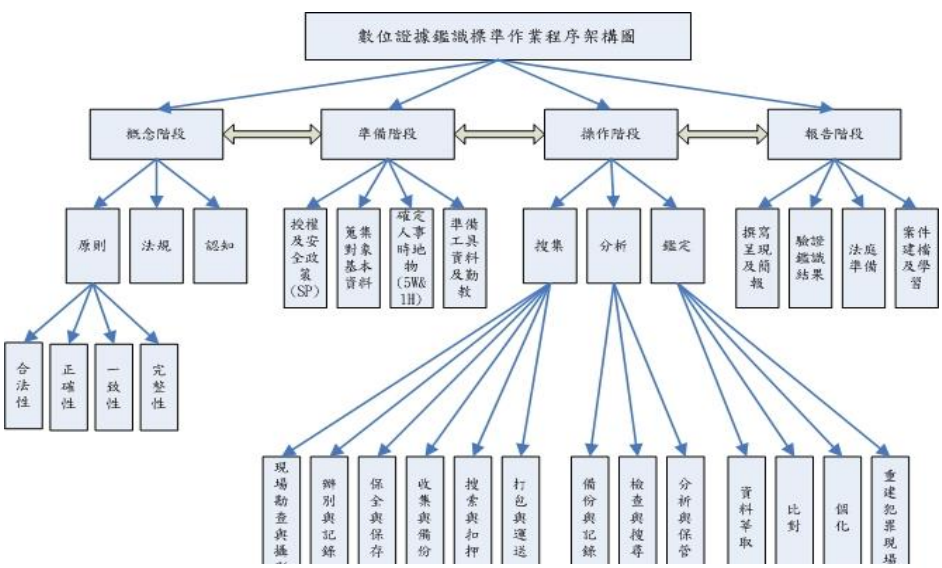

圖 7　數位證據鑑識作業程序（DEFSOP）架構圖

（一）概念階段

本階段分為原則、法規及認知三項規範，而在原則裡又可分為合法性（C）、準確性（A）、一致性（C）、完整性（I），在操作階段所執行的各程序及步驟，應該符合及遵守此概念階段之原則、法規及認知，方可使獲得之數位證據符合公正性、真實性及有效性，並提高其證據能力與證明力，以做為法官審判之依據。

（二）準備階段

1.授權及資訊安全政策

（1）授權：執法人員或系統管理人員在執行數位證據鑑識工作前，最好必須先獲得授權書（搜索票）或資訊安全政策規範的支持。

（2）資訊安全政策：能在合法之下合理的蒐集數位證據而不影響商業的運作。

2.蒐集對象基本資料

資訊犯罪事件的發生，當進入偵查的階段，根據資訊犯罪偵查流程圖，掌握重點資訊，以人、事、時、地、物及理由的角度，從各種管道，蒐集與案情相關的資訊，以發現嫌疑犯。

3.確定人、事、時、地、物及理由

當能發現可能之嫌疑犯，訪談與案情相關的人員，再深入瞭解案情，綜合所蒐集的資訊，以便掌握相關的人、事、時、地、物及理由之資訊。

4.準備工具、資料及勤教

根據案情的類型及特性，準備不同之軟硬體工具設備及資料，含犯罪現場鑑識工作必填之相關之表單及搜索票。任務出發前，依各人之專長，作好任務編組，建立指揮系統且讓彼此能相互溝通的管道，且勤前教育及演練，說明案情、搜索之任務、範圍、重點且對每人的任務宣達，並檢查相關之工具是否準備齊全，以期發揮最大的工作效能。

（三）操作階段

1.搜集

數位證據之搜集，係執法人員到達現達之首要工作，其工作項目，依本研究可分為（1）現場勘查與攝影，（2）識別與紀錄，（3）保全與保存，（4）收集與備份，（5）搜索與扣押，（6）打包與運送等六項工作。

2.分析

在數位證據搜集打包後，需要進一步鑑識的證據，應先送回相關警察機關保管，再或逕送數位證據鑑識實驗室，作進一步的分析，或因案情需要，須在其犯罪現場作初步的分析，其工作項目，依本研究可分為（1）備份及紀

錄，（2）檢查與搜尋，（3）分析與保管等三項工作，為確保分析資料的完整性及正確性。

3.鑑定

其數位證據資料還是很龐大時，就需要進一步鑑定證據，作進一步的分析，其工作項目，依本研究可分為（1）資料萃取，（2）比對，（3）個化，（4）重建犯罪現場等四項工作，為確保分析資料的完整性及正確性。

（四）報告階段

1.鑑識報告、呈現及簡報

（1）鑑識報告：鑑識報告，是必須要給法官、被告及偵辦人員等相關人員閱讀的，故內容不宜太深奧，且又必須呈現真實的內容。

（2）呈現及簡報：原則上可供證據的物品皆應作為呈堂證供，即具有證據能力及證明力之證物都要呈現及報告於法庭上。

2.驗證鑑識結果

鑑識結果的正確性,除遵守相關之原則外,其操作手冊及相關表格建立，鑑識工具的使用說明在電腦鑑識領域中是相當重要的一環。

3.法庭準備

數位證據鑑識應分類，說明符合證據監管鏈的流程，作好法庭交互詰問的準備工作，以最專業及最真實的呈現給法官裁判。

4.案件建檔及學習

每件案件應依案件類型分類，建立每件案件的卷宗及經驗、技術分享，最好應建立專家知識庫供下次他人偵辦案件參考與深度學習。

三、培訓資通安全專業人才

我國資安（網路）犯罪具有高犯罪黑數，許多企業組織甚至政府機關為保護信譽與秘密，就算損失重大亦多不願聲張報案，加上犯罪手法日新月益（如司法機關2015年鴻海內部舞弊案破案及2016年7月18日第一銀行ATM盜領案破案、2017 年 5 月 12 日爆發數萬起勒索網路攻擊事件、2017 年 10 月遠東銀行 SWIFT 系統遭駭客入侵 18 億案），檢警調執法機關對於數位鑑識及偵查人才有高度的需求，而國內目前專責偵辦網路犯罪案件僅內政部警政署刑事局偵九大隊、電信大隊及六個院轄市警察局刑事警察大隊科技偵查隊與法務部調查局資通安全處及六個院轄市調查處資安科，至於數位鑑識能量（或資安鑑識能量）目前僅有內政部警政署刑事局科技犯罪防制中心與法務部調查局資通安全處等專責單位。加上，經由數位鑑識標準作業程序與工具所蒐集的數位證據,也需要經由合格的鑑識人員來進行操作、執行與蒐集，

方能確保數位證據的證據能力，在考量各項層面之下，應針對國際標準作業程序中（ISO27037/ISO27041/27042/27043/27050 等）所提出數位鑑識與數位證據之人才培育、教育訓練計畫及能力評鑑認證的建議事項，以提升我國整體數位鑑識水準並與國際接軌。

近來政府機關及民間重要企業頻遭中共駭客入侵，有計劃、有系統的進行網路佈建，以「網軍」形式對我從事資訊戰操演，有鑒於此，我國必需培養資通安全攻擊及資安鑑識人才以確保國家安全，企業也需加強資安防護及資安治理工作，以防範駭客入侵，除此之外，國家更需培養資安教育及資安防護人才以提昇全民資安鑑識認知，以建立國家全面的資安防護體系與全民資安鑑識認知。

因此，本文研究參考國內學者林宜隆教授於 2004 年行政院國家資通安全會報資安學程專案報告中，規劃我國資通安全專業人才架構（包括資安防護人才、資安攻擊人才、資安鑑識人才、資安偵查人才、資安教育人才與資安治理人才等六大資安專業人才），必定是未來網路資訊社會發展的趨勢（如圖 8），說明如下：

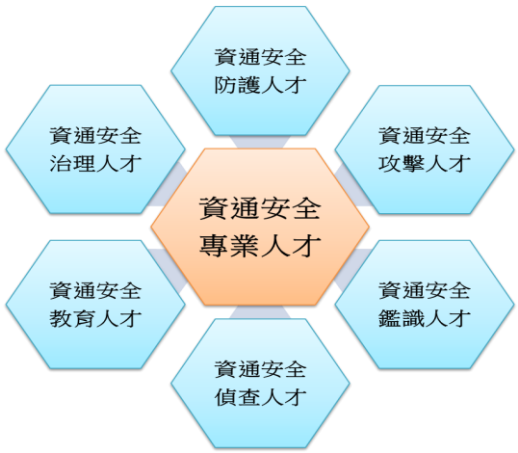

圖 8　我國資通安全專業人才規劃架構圖

（一）資通安全防護人才（如 CISSP）

主要是從事資訊安全及資產的防護，在面對不斷的資安威脅下，政府機關及民間企業都極需此種人才，其所涵蓋的領域也最廣，從資安政策及架構、病毒分析、修補程式（PT）、通報及危機應變、數位稽核、IDS、Firewall 及 VPN 等均屬資安防護的領域。

（二）資通安全攻擊人才（如 CEH）

主要是從事資訊作戰工作，入侵敵方的電腦網路系統以從事破壞、干擾、

或植入木馬竊取敵軍資訊，應相當熟練各種駭客工具及撰寫 exploit code，對於作業系統核心及網路架構相當清楚，應具備有相當深厚的電腦網路技術功力，這類工作大都屬機密工作，以國防部及中科院（舉辦資安攻防演練）最需此種人才，而我國舉辦資安攻防演練時，也需此種人才（我國行政院 2003 年舉行第一次資安演練作者曾擔任攻擊團隊隊長，負責攻擊方法、工具、訓練及策略規劃）。

（三）資通安全鑑識人才（如 ACE/EnCE/CFCE/UFED/CFE/ISO27041~43 LA）

主要是依據一套標準作業程序來從事數位證據的搜集、分析與鑑識，需對日新月異的電腦技術相當熟悉，且相當熟練的使用各種數位鑑識工具，以利網路犯罪的偵查，並於法庭上擔任專家證人，在實務上，國內僅內政部警政署刑事局科技犯罪防制中心與法務部調查局資通安全處有從事數位證據的鑑識，接受法院的請託代為從事資通安全數位鑑識工作，資安鑑識人才明顯不足，而企業方面也同樣需要此類人才。

（四）資通安全偵查人才（如 CFCE/CFE/UFED）

主要是從事電腦網路犯罪的偵查，不需對電腦技術相當熟練，但需了解刑事數位偵查及網路犯罪手法的概念，且需熟悉刑法三十六電腦罪章及刑事訴訟法等相關法律，在我國電腦犯罪偵查單位主要有檢察官、刑事局電信偵查大隊、刑事局偵九大隊、調查局資通安全處、各縣市警察局刑警大隊科技偵查（隊）組等。

（五）資通安全教育人才（如 ISO/IEC 27001/27011/ISO27017/ISO27018 LA）

資通安全教育人才，主要是由各專業領域之資安人才所組成，包含各大專院校相關科系或政府組織（機構）、部門之從事資安教育、資安治理及訓練工作，因此積極推廣全民資安（從基本教育做起）的認知，以符合我國資通安全政策，培養想要從事資安工作之專業人員。

（六）資通安全治理人才（如 ISO/IEC 27014/ISO27007/COBIT 5.0）

資通安全治理人才主要是從事資訊安全稽核及指導及控制組織資訊安全活動，在面對資訊安全管理漏洞與風險的評估，政府機關及民間企業都極需此種人才，所涵蓋的領域，可引入國際標準規範，依各級機關之資安管理運作情境，考量國際標準之資安治理實作框架（如 ISO27014/**COBIT 5.0**），以期強化資訊安全的稽核與防護的作業程序。目標在於確保資訊安全目標及策略承接組織營運的目標及策略。

我國資通安全專業六大人才架構，瞭解目前我國大學或其他研究機構，

仍有絕大部份比例是偏重於資通安全技術層面，包括資通安全教育人才、資通安全攻擊人才及資通安全防護人才。而**對資通安全鑑識人才、資通安全偵查人才及資通安全治理人才等三**方面仍略顯不足，因此為了提昇我國資通安全及數位證據鑑識能量，完整規劃我國資通安全六大專業人才的培育，加強學校、政府與民間之研究機構的配合，是當前刻不容緩的工作。

四、檢視推動科技警察之成效

檢視各縣市政府警察局在推動科技警察（Cyber Police）之成效，如下：

（一）各縣市「科技犯罪偵查專責組」編組：經調查目前各縣市警察機關將「科技偵查隊」納入組織規程並完成法制化者，計有臺北市、新北市、桃園市、臺中市、臺南市、高雄市等六都直轄市。至於各縣市警察局因囿於預算經費人力等不足因素，目前仍維持科偵組任務編組的型態，兼任網路犯罪偵查及一般刑案偵處。

（二）各縣市政府警察局科技偵查能量：依據警政署刑事警察局2014調查各縣市警察局科偵組，有關網路犯罪偵辦情形、勤業務運作狀況及科技警察專業學經歷等項目中，計10縣市科偵組，兼具內外勤性質；在偵辦案件類型方面，計13縣市科偵組偵辦案件類型，不限於網路犯罪，計13縣市科偵組業務範疇，以承辦刑事警察局科技犯罪防制中心業務為主，計14縣市科偵組，需負責管理科技偵防設備器材。在數位鑑識與蒐證能量方面，計5縣市尚未辦理，其餘15縣市中，以臺北市數位鑑識能量居冠，新北市、高雄市居次，再次為臺中市、臺南市、桃園市。在專業學經歷方面，各縣市科偵組人員，具資訊相關學歷者，僅占10%；五年以上科技偵查相關經歷者，僅占18.75%。因此為了提昇我國數位證據鑑識能量，完整規劃我國資通安全鑑識人才及資通安全偵查人才的培育，加強警察大學及警專學校、政府警察機關與民間之研究機構的配合，是當前刻不容緩的工作。

中央警察大學資訊管理研究所因此積極規劃相關課程來配合此趨勢，於2000 年 9 月特將資訊管理研究所分成二組（**2003 年 8 月 A 主任因個人因素取消資訊警察分組，是錯誤決策，非常遺憾，並傷害我國網路（科技）警察**人才培育**非常深遠**）：資訊管理組及資訊警察組，**資訊管理組**為一般資訊科技結合管理科學的相關課程研究，如何應用於警察機關及警察工作、協助警察辦案、並提昇警察組織效能及工作效率(如警察業務資訊化(I)、IEK Model)。而**資訊警察組**顧名思義為培育**網路（科技）**警察之墊腳石而設計的課程，課程內容著重於資訊網路（數位）犯罪打擊的相關新技術及新理論，運用最新的**資安鑑識及數位偵查（Cyber forensics and Digital Investigation）之**科技及

方法來探討當前資訊(數位)犯罪的新興模式與技術(如犯罪偵查工程化(E)及破案資訊知識化（K）、IEK Model），進而協助及考察實務單位偵查網路（數位)罪犯(如配合刑事警察局偵九隊成立與各縣市警察局刑警隊電腦(網路)犯罪偵查組設置），此課程設計為 2000 年當時我國最新首次創舉（2005 年華梵大學資訊管理研究所碩士在職專班成立資通安全組為國內第一所資通安全碩士學程（Master of Cyber Security Program）），相信其應用於警察打擊犯罪之範疇將更上層樓。以下為 2000 年當時資訊管理研究所資訊警察組的課程綱要規劃如表 2 所示：

表 2　89 學年資訊管理研究所資訊警察組課程一覽表

必修課程		
課程名稱	學分數	授課年級
研究方法論	3	一上
資料通訊與網路	3	一上
電腦網路犯罪偵防專題	3	一上
數位鑑識執法專題	3	一下
科技犯罪實務個案研究	2	一下
專題演講	0	一、二
選修課程		
課程名稱	學分數	授課年級
作業系統安全實務	3	上
網際網路與犯罪問題	3	上
資訊犯罪資料分析（BBA）	3	上
資通安全管理	3	上
資訊安全技術與管理	3	上
網路安全技術與管理	3	上
雲端安全技術與管理	3	上
資訊倫理與個資保護	2	上
資料保護及隱私權專題	2	上
網際網路與智慧財產專題	2	上
無線通訊與網路安全專題	3	上
網際空間與法律規範專題	3	上

（續下頁）

網際空間治理專題	3	上
電腦稽核與舞弊稽查	3	上
資通訊科技法論	2	上
網路犯罪分析與偵防實務	3	上
數位鑑識技術與反鑑識技術	3	上
資通安全管理相關國際標準專題	3	下
數位證據蒐證與鑑識	3	下
人工智慧與資訊社會學	2	下
網路入侵與偵測	3	下
電子交易犯罪與防制專題	2	下
高等資訊密碼學	3	下
資通安全鑑識	3	下
數位鑑識執法與鑑識實作	3	下
電信網路詐欺與政策分析專題	2	下
資訊戰與電腦病毒	3	下
資通安全管理法規專題	3	下
通訊保障與監察技術專題	2	下
電子商務法律專題	2	下
數位證據標準作業程序（DEFSOP）	3	下
駭客攻擊與防護技術	3	上
駭客攻擊與防護策略	3	下
IDS/IPS	3	下
數位內容過濾與偵測	3	下
雲端鑑識與行動鑑識	3	下
鑑識會計與舞弊稽核	3	下
數位偵查鑑識相關國際標準專題	3	下

伍、創新司法警察 IEK Model 智慧模型與未來趨勢

本文研究認為各縣市警察局刑警大隊科技偵查（隊）組以臨時編組方式運作的困境，係因司法警察人員經常遭調用支援其他勤業務，造成不確定性高、欠缺歸屬感、工作量龐雜及角色定位模糊等因素，導致司法警察人員無法累積數位鑑識專業知能與充實數位偵查專業技術。故本章將以建立司法警

察IEK Model（1.警察業務資訊化（Information, I）；2.犯罪偵查工程化（Engineering, E）；3.破案資訊知識化（Knowledge, K））智慧模型架構的參考依據，其創新司法警察IEK Model智慧模型芻議如下：

一、未來科技警察面臨新挑戰：

如新興駭客型詐欺集團、數位匯流與跨境犯罪、虛擬貨幣網路洗錢、網路犯罪高度分工及科技警察素質不足等。故本文研究植基於傳統犯罪學理論，並加入臺灣地區新興網路（數位）犯罪特性與手法，嘗試從建置未來科技警察與創新科技服務等面向，建立司法警察IEK Model智慧模型實務運作架構，以強化中央與地方網路（數位）犯罪偵防與技能雙向交流，擴大培育網路（數位）犯罪偵查專業人才，以提升各司法及警察單位之科技偵查能量，**進一步達成整合「科技建警」與「偵防並重」之警政新策略目標，最後達成預防及阻止<犯罪科技化，科技犯罪化>目標，完成<治安科技化，科技治安化>理想境界。**

二、司法警察 IEK Model 智慧模型架構：

本文研究提出 IEK Model 作為未來建立科技警察與創新偵查能量之決策參考，期使司法警政當局在防制網路（數位）犯罪時，與時俱進，更具有系統化及科技化的前瞻觀點與作法（如**治安科技化，科技治安化，預防及阻止犯罪科技化與科技犯罪化，行動犯罪化與犯罪行動化**）。因此，結合警政署刑事警察局剖析臺灣地區 2005-2015 年網路詐欺犯罪案例手法及演進過程，所提供網路犯罪特性與手法之統計數據，進行模擬模型的關聯性分析，以建立臺灣地區司法警察 IEK Model 智慧模型及案例分析（如表 3）。IEK Model 的主軸與範疇如前述：（1）警察業務資訊化（Information, I）；（2）犯罪偵查工程化（Engineering, E）；（3）破案資訊知識化（Knowledge, K）。

三、建立警政智慧三化 IEK Model：

（一）警察業務資訊化：如警政資訊管理系統 PIS，警政服務雲，交通違規處罰資訊系統，交通服務雲，犯罪監控系統，犯罪熱點警訊服務系統，交通塞車路段即時服務系統，婉君網路集會，社群傾聽民意，Facebook of NPA 等。

（二）犯罪偵查工程化：即犯罪偵查智慧工程化，如數位證據保全 SOP 及系統，數位證據鑑識 DEFSOP，行動鑑識工具及系統，DNA SOP，犯罪偵查專家系統，犯罪監控專家系統， 犯罪徵兆偵查資訊系統，網路蒐證分析系統，網路犯罪偵查專家系統，網路鑑識/鑑定系統，數位證據

雲端服務平台等。

（三）破案資訊知識化：如偵查破案知識庫系統，雲端破案知識管理系統，大數據犯罪分析資訊系統（Big data analysis cases IS），犯罪監控整合知識分析系統，犯罪破案決策支援系統，犯罪破案人工智慧系統，雲端鑑識分析平台，雲端鑑識人工智慧自動分析平台，雲端鑑識服務平台，DM、BDA、BI、KM、CC、IoT、IoP、IoM 等。

如此才能實現及落實整合「科技建警與偵防並重」之治安政策。綜上，鑑於網路（數位）犯罪偵查工作與數位偵查技術、網路資通訊技術及法律規範等三者息息相關，且互為因果關係。故本文提出有關「司法警察 IEK Model 智慧模型」之偵查策略雛型架構（如圖 9），即從**數位偵查、追訴處罰、法律規範、數位鑑識、資通安全等面向發展**，期能全面整合提升臺灣網路（數位）犯罪科技偵防技術與數位鑑識能量，並提供未來研究相關網路（數位）犯罪的方向與願景，**最後達成預防及阻止<犯罪科技化，科技犯罪化>目標，完成<治安科技化，科技治安化>理想境界。**

表 3　建立臺灣地區司法警察 IEK Model 智慧模型案例分析

類型	未來網路犯罪趨勢	科技警察策進作為	警察 IEK 智慧模型
網路犯罪企業化有組織經營	利基市場，上游研發病毒軟體、中游販賣惡意程式軟體、下游提供網路犯罪支援。	蒐集惡意軟體 APP 樣本及簡訊連結樣本，與民間資安公司合作破解入侵。	1. 警察業務資訊化(I)。 2. 犯罪偵查工程化(E)。 3. 破案資訊知識化(K)。
複合型駭客詐欺集團	詐欺集團結合駭客之網路複合犯罪類型，手法快速翻新。	刑事警察局研擬新興科技通訊監察技術，及時偵破網路指標性案件。	1. 警察業務資訊化(I)。 2. 犯罪偵查工程化(E)。 3. 破案資訊知識化(K)。
跨境網路犯罪	結合行動裝置、電信、網路，形成網路資通匯流跨國犯罪。	跨境網路犯罪多為同文同種之兩岸居民，繼續深化兩岸合作關係，並擴及其他鄰近東南亞國家。	1. 警察業務資訊化(I)。 2. 犯罪偵查工程化(E)。 3. 破案資訊知識化(K)。
虛擬貨幣	比特幣為加密電子貨幣，匿名交易、無銀行帳戶。	2014 年歹徒要求被害人購買游戲點數之案件，已超過 40%，加強 165 反詐騙宣導。	1. 犯罪偵查工程化(E)。 2. 破案資訊知識化(K)。

（續下頁）

零時差APT攻擊	利用新軟體程式上市漏動，進行網路惡意攻擊。	要求高資安風險企業改善網站資安防護能力，防止民眾個資持續外洩。	1. 犯罪偵查工程化(E)。 2. 破案資訊知識化(K)。
LINE加密協定	即時通訊軟體LINE，採加密協定，造成電信及網路路由追查的困難與瓶頸。	政府跨部會合作，邀過各類平臺會議請網路業者改善資安機制，進行阻斷封鎖。	1. 犯罪偵查工程化(E)。 2. 破案資訊知識化(K)。
IoT網路駭侵	IoT物聯網漏洞，未來將成為被駭之新興網路犯罪標的物。	警政署已核准2016年臺灣警察專科學校增設成立「科技偵查科」，招180名新血，畢業後投入網路犯罪科技偵防工作。	1. 警察業務資訊化(I)。 2. 犯罪偵查工程化(E)。 3. 破案資訊知識化(K)。

資料來源：本研究整理

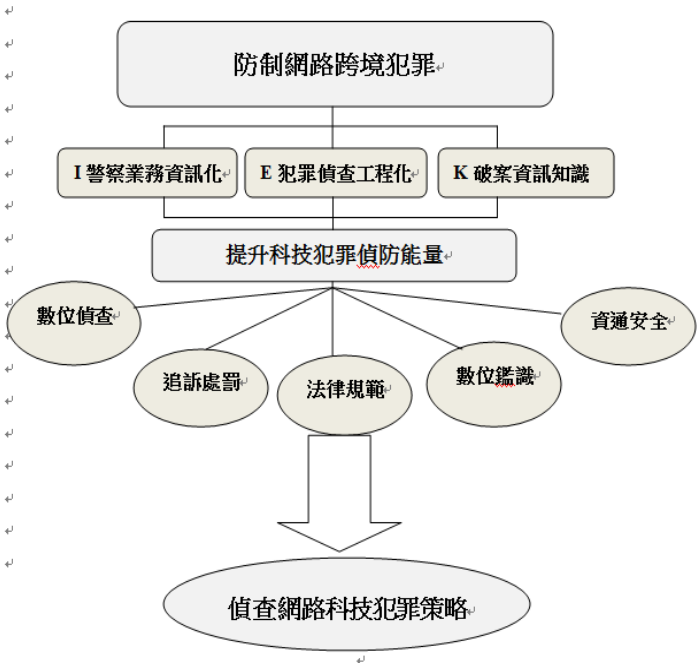

圖 9　警察 IEK 智慧模型架構圖（資料來源：本研究整理）

陸、結論與建議

一、結論

為提昇數位證據鑑識能量，需要眾多規劃建議事項及加強各單位之配合，惟限於現行制度，或限於人力、物力、經費等因素，並無法立即全面性地推動實施，可能需有先後次序之別，逐年逐項來付諸實行，為能提供政府相關單位能及早建置我國資通安全及數位鑑識機制，本文建議為解決目前我國在資通安全及數位鑑識工作方面衍生之問題，作者認為下列三項規劃及建置必要行動事項：

（一）國家級數位鑑識實驗室之設立：

數位證據具有易於修改、易於流失、難以蒐證等特性（如數位證據應法制化），因而造成國內各審、檢機關審判此類案件時，有誤判情事之發生，在此種因素下，除加強蒐證人員之專業訓練及正確之蒐證觀念外，數位證據應法制化，司法警察機關更應儘快建置國家級資通安全及數位鑑識實驗室以提昇之鑑識技術能量及確保鑑識品質。

（二）數位證據鑑識標準作業程序建構：

在目前警方偵辦移送的網路數位（數位）犯罪案件中，經過法庭裁判程序而判刑確定之案件寥寥可數，未有法定之證據處理程序及數位證據法制化（如符合 DEFSOP/ISO27037/ISO27041/ISO27042/ISO27043 等國際標準）就是其中一項重要之因素，故本文研究提出一套具可行性及有效性數位證據鑑識標準作業程序（DEFSOP），期望在數位鑑識上能有一套標準作業流程，以符合法定程序及法制化數位證據，使得數位證據能作為法院訴訟程序中的佐證資料，並提高其數位證據的有效性（符合 CIAC 基本原則）及公信力。

（三）資安專業人才培育：

資安事件發生的頻率增高，資安事件的發生似乎越來越難防範，因此完整規劃我國資通安全六大專業人才的培育，是當前刻不容緩的工作，唯有憑藉受過良好訓練的資安鑑識專業人才，才能有效做好資通安全防護，並可有效保障發生問題時受損的範圍與機率的減低，以減少衝擊。且有了資安鑑識及資安偵查專業人才，將可專責為我國未來有關資通安全及數位鑑識工作與研究發展(如行政院資通安全辦公室於 2016 年 8 月 1 日改制為行政院資通安全處），為打擊網路（數位）犯罪及研發資通安全及數位鑑識技術而努力。

以上三項所規劃之項目，不僅為我國資通安全及數位證據鑑識能量之重要建置項目，亦將對我國司法警察機關偵查網路(數位)犯罪工作大有幫助，

而且是非常迫切需要的，因此本文特別提出應列為資通安全及數位證據鑑識能量之三大架構；至於上述三項應建置之規劃項目，其設立之編制、人員、設備及法定程序等內容及詳細細節也需要集思廣益及深入規劃，因此應可做為我國台灣數位鑑識發展協會（ACFD）未來繼續深入研究的題目，亦可提供其他研究者作為未來研究之方向。

數位證據的取證鑑識過程對於證據能力有極大的影響，所以對於數位證據的蒐集、分析、保全與監管，每一環節都應由專業機構與專業人員執行。在操作階段透過先進Cellebrite UFED的擷取方法和分析技術,破解罪犯手機,對行動裝置的物理萃取、解碼、分析和報告，嚴格執行「數位證據保全」之安全控管及驗證機制，以確保各證物不會遭到污染或破壞，以確實達到數位證據鑑識之符合一致性（C）、完整性（I）、準確性（A）與合法性（C）等原則（CIAC Principle）。作者曾以市場上占有率最高 Android 智慧型手機當作實驗，使用鑑識工具 Cellebrite UFED 萃取相關的數位證據，透過交叉分析數位證據及完整結果的呈現，還原犯罪事實，提供事件調查鑑識人員可依循的工具選擇參考，進一步**達成整合「科技建警」與「偵防並重」之警政新策略目標**。

二、建議

（一）從「M-O-P 網路（數位）犯罪三角理論」進行網路（數位）犯罪偵查：

本文研究認同國內學者林宜隆教授經由「M-O-P 網路（數位）犯罪三角理論」之實證研究，主張結合日常活動理論與社會控制理論，針對有動機及能力的犯罪者，並利用社會控制理論的四個社會鍵來控制，進而形成網路數位偵防新對策。故未來司法警政工作的新思維和新挑戰，必須建立在「司法警察 IEK Model 智慧模型」的架構上，並導入「**網路犯罪生命週期**」（**Cybercrime SDLC**）系統管理之概念，將「警察業務資訊化（I）」、「犯罪偵查工程化（E）」、「破案資訊知識化（K）」等科技偵防面向，落實到未來防制網路犯罪或駭客的勤務作為，方能達成警政署整合「科技建警」與「偵防並重」之治安願景與警察目標。

（二）整合「科技建警」與「偵防並重」之警政新策略：

本文研究認為可先整合刑事警察與科技警察的勤業務功能，積極培訓科技警察專業人才(如警察專科學校於2016年7月開始招收科技偵查科學生)；強化警政署三位副署長的功能取向，其中至少一位應具備科技專業能力與智慧知能（如網路科技、數位偵查、數位鑑識）；推動以服務民眾為導向的智慧型警政科技策略，有效整合科技建警與偵防並重的創新策略。

（三）強化司法警察IEK Model智慧模型效益評估：

本文研究嘗試建構一個可以提升未來網路（數位）犯罪科技偵防能量之「司法警察IEK Model智慧模型」偵查策略雛型架構，期望對複雜多變的各種網路（數位）犯罪型態，從數位偵查、追訴處罰、法律規範、數位鑑識、資通安全等面向進行探討分析，以有效防範網路（數位）犯罪之發生。故該架構中每一階段之偵防績效仍需經過確認、驗證或測試，以有效提升網路（數位）犯罪科技偵防能量與效益評估。

（四）科技警察專責網路（數位）犯罪全球趨勢：

美國已將網路攻擊列為重要國家安全威脅，並將網路攻擊部隊人力由500人提升至4,500人，預算更由39億美元提高為47億美元，其目的在強化網路數位偵防能量。故本研究認為臺灣警政當局除在推動各項防制網路（數位）犯罪攻防策略時，亦應強化治安資訊系統的基礎建設，同時必須適時增加網路（數位）犯罪偵防警力的正式編制員額，才能有效打擊各類型科技犯罪，進而預**防及阻止**「**科技犯罪化與犯罪科技化**」，「**行動犯罪化與犯罪行動化**」**策略目標。**

（五）加強海峽兩岸跨境打擊網路（數位）犯罪：

臺灣跨國詐欺集團，將網路（數位）犯罪任務系統化、組織化、駭客化及產業化（如臺灣跨境網路詐欺黑色產業），已具企業規模黑色產業。因其組織結構完整周密，再納入資訊管理模式，使該犯罪組織更具高科技犯罪水準，除對國內危害程度更加嚴重，並影響臺灣在國際社會形象甚鉅。本文研究認為網路跨境犯罪多為同文同種之兩岸居民，故必須深化兩岸合作關係，建立網路跨境犯罪分析及分享雲端服務平台（如先分享網路金融詐欺案及電信詐騙案等），並擴及其他鄰近東南亞國家，以利共同打擊網路跨境犯罪。

參考文獻

林宜隆、藍添興，未來警察之新科技與新思維－數位證據與資訊鑑識，警光月刊，2005。

林宜隆，「建構數位證據鑑識標準作業程序」，司法新聲 101 期_第 4 篇，2012，1 月

林宜隆、陳映任，數位證據鑑識標準作業程序與犯罪現場程序模型(ACSPM)及 ISO27037 數位證據處理程序之比較分析，第二十七屆國際資訊管理學術研討會，ICIM 2016，靜宜大學，台中市，2016/05/21。

林宜隆、陳映任，行動裝置數位證據鑑識標準作業程序與案例驗證之探討，Cyberspace 2016 聯合研討會，大同大學，台北市，2016/11/18。

林宜隆、張文耀、劉耿旭，「建構個人資料保護之數位證據鑑識標準作業程序」，電腦稽核 27 期，2013 年 1 月。

林宜隆，2007，數位證據標準作業程序(DESOP)之建構，電腦稽核，第十六期。

林宜隆，2009，網路犯罪理論與實務第三版，中央警察大學出版，桃園。

林宜隆、顏雲生、吳柏霖、蕭勝方，2010，「VoIP 攻擊分析與數位證據鑑識機制之研究」，第二十一屆國際資訊管理學術研討會(ICIM 2010)，台南市：成功大學。

林宜隆等，2000 年第一屆「網際空間：資訊、法律與社會學術研討會」論文集序與成果報告，中央警察大學。

林宜隆等，2000 年第二屆「網際空間：資訊、法律與社會學術研討會」論文集序與成果報告，中央警察大學。

林宜隆等，2001 年第三屆「網際空間：資訊、法律與社會學術研討會」論文集序與成果報告，中央警察大學。

林宜隆等，2002 年第四屆「網際空間：資訊、法律與社會學術研討會」論文集序與成果報告，中央警察大學。

林宜隆等，2003 年「網際空間：科技、犯罪與法律社會學術研討會」論文集序與成果報告，中華民國資訊管理學會暨資通安全管理委員會。

林宜隆等，2004 年「網際空間：資安、犯罪與法律社會（Cyberspace2004: Cybersecurity, Cybercrime, Cyberlaw and Cybersociety）學術研究暨實務研討會，淡江大學。

林宜隆、薛明杰，我國資通安全專業人才規劃之初探，2005 犯罪偵查與鑑識科學研討會，中央警察大學。

行政院國家資通安全會報，建立我國通資訊基礎建設安全機制計畫（九十四至九十七年），民 93 年 3 月。

林宜隆，資通安全學程專案報告，行政院國家資通安全會報技術服務中心，民 93 年 11 月。

林宜隆、薛明杰、楊鴻正，我國資通安全鑑識實驗室建置之探討，2004 臺灣商管與資訊研討會，民 93 年 9 月。

楊鴻正，「我國資通安全鑑識科技能量規劃之研究」，中央警察大學資訊管理研究所碩士論文，2003 年 6 月。

黃志龍，「建構數位證據鑑識標準作業程序規範之研究」，中央警察大學資訊管理研究所碩士論文，2006 年 6 月。

林宜隆，楊鴻正，各國資通安全鑑識技術能量之研究，電腦稽核，第十三期，2005 年 8 月。

林宜隆、賀宙才，大學資安五大人才培育之探討-以資通訊安全聯盟課程為例，2007 年網際空間：資安、犯罪與法律社會學術暨實務研討會，2007 年 11 月。

林宜隆、閻瑣琳、陳受湛"我國資安鑑識實驗室建構與規劃之探討—以法務部調查局為例"，2005 年第七屆「網際空間：資訊，法律與社會」研討會，2005 年 11 月。

黃明達、林宜隆等，資通安全學程專案報告，行政院國家資通安全會報技術服務中心，2004 年 11 月。

林宜隆、邱士娟，我國網路犯罪案例現況分析，資訊科技期刊，2003。

林俊宏譯，未來的犯罪，木馬文化，2016。

黃啟賓，警政革新與犯罪預防：20 年來之警政發展，警學叢刊，2011。

黃明凱，網路犯罪輔助偵查專家系統雛型之建構，警察大學資訊管理研究所碩士論文，2002。

江守寰，以大數據探勘技術分析「視覺化管理」在監視錄影系統之運用，犯罪學期刊，第 18 卷，第 2 期，2016。

陳文生，台灣網路治理元年：2017 年全球網路治理發展與挑戰，2017。

Michael Knetzger, Jeremy Muraski，2008,"Investigating High-Tech Crime", Pearson

Eoghan Casey, 2000, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Academic Press.

Oliver, W.M., 2007, Homeland Security for Policing .NJ: Person Education. Rosenbaum, D.2006, The Limits of Hot Spots Policing. In Police Innovation: Contrasting Perspective, edited by David L. Weisburd and Anthony A. Braga.

New York: Cambridge University Press.

Simson., L Garfinkel, 2010,Digital forensics research: The next 10 years. Digital Investigation.P64-73.

Various. Eoghan Casey, 2009, Handbook of Digital Forensics and Investigation, Acadmeic press.

Hugh D Barlow.,1984, "Social Change Crime Rate Trends: A Routine Activity Approach", Boston: Little, Brown & Company Limited, pp.78.