出國報告(出國類別：進修)

跨境電腦犯罪之司法管轄與發展趨勢
～以網路詐欺犯罪為中心

服務機關：臺灣嘉義地方法院檢察署
姓名職稱：陳靜慧檢察官
赴派國家：美國史丹佛大學
Stanford University
出國期間：民國 105 年 12 月 9 日至 106 年 12 月 8 日
報告日期：民國 107 年 3 月 5 日

摘要

資訊科技的發展一日千里，網際網路的普及為現代生活帶來無窮的便利，卻也成為犯罪行為人的溫床，電腦犯罪成為新興活躍的領域，如何針對電腦犯罪態樣加以規制，早已是國際間關注的焦點。然而，法律的腳步永遠跟不上科技的變化，跨國電腦犯罪的樣貌早已脫離傳統的窠臼，朝向規模更大、速度更快、更隱密的方式轉變，而網路詐欺犯罪是始終猖獗的場域，各式各樣的詐欺類型在科技的輔助下應運而生，各國應如何對跨境電腦犯罪之網路詐欺進行有效的追訴？國際間的合作與司法互助是必然的模式。本文透過對美國 CFAA 等相關法規範之沿革探討，以及歐洲理事會網路犯罪公約之論述，期以對我國相關法制提出建議及方向。

目次

第一章　緒論

第一節　研究動機與問題意識

所謂「IT產業（information technology industry）」在過去半個世紀有巨大的變革，隨著處理器效能與記憶體容量持續快速進步，資訊科技不僅僅速度更快，且相關裝置變得更小、更輕、更容易使用；原始的資訊產業也逐漸由通訊產業匯集成通稱為「資訊通訊科技（information communication technology，簡稱ICT）」之綜合，此一科技無所不在，且可說已逐漸整合為現代社會的每一個面向。在過去幾年中，專家與政策制定者益發關切保護資訊通訊免於受到不法侵害的議題[1]，而在司法實務上，未經授權者故意入侵資訊電腦系統，往往係以竊盜、中斷、毀損資料或進行其他非法行為的目的，許多專家預期電腦攻擊的數量及嚴重性在未來幾年將會大量增加。舉例而言，在2014年10月，一位愛沙尼亞公民Sergei Tšurikov因其謀劃犯罪之行為造成超過900萬美元的損失，而在美國被判處十一年有期徒刑[2]，該犯罪行為發生在2008年，Tšurikov及其共犯駭入RBS WorldPay公司的電腦網絡，據稱是當時最複雜且相當組織化的電腦詐欺犯罪行為，犯罪行為人得以危害RBS WorldPay公司所使用的加密資料，並且提高了「薪資借記卡（payroll debit cards）」的帳戶限制，進而以偽造的薪資借記卡提供了一個提款網絡，在短短12小時內癱瘓了至少全世界280個城市、超過2100台的自動提款機，受影響的國家包括美國、俄國、義大利、香港、日本及加拿大等，Tšurikov及其他駭客得以在實際使用這些RBS電腦系統時監控這些提款情形；此外，發生在2014年11月Sony公司遭到自稱為「和平守護者（Guardians of Peace,GOP）」駭客攻擊，可說是駭客攻擊跨越國界之適例[3]。這些案例闡釋了諸多現代電腦犯罪的特徵與挑戰—它是組織化的、大多基於財務上的動機、具有科技複雜性、且是跨越國界的，在現代生活中透過數位科技廣泛散布，誠如「水可載舟、亦可覆舟」，對於人類生活有其積極正面影響，但也存在轉型的黑暗面。

---

[1] G. Press,CYBERCRIME, CURRENT CONTROVERSIES.GREEN HEAVEN PRESS（2016）,78.
[2] US Department of Justice,' International hacker sentenced', Press Realse(24 October 2014)
[3]https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?_r=0

根據趨勢科技提出 2018 年的資安報告[4]，人們透過不安全的網路進行連線和互動的情況日益嚴重，技術實作上的缺失使得駭客有機可乘；而在 2018 年，數位勒索將是網路犯罪集團獲利的主要模式，同時也將促使犯罪行為人朝各種可能帶來龐大獲利的詐騙手法。物聯網（Internet of Things，簡稱 IoT）裝置的漏洞將擴大犯罪行為人可利用的打擊面，而所謂「變臉詐騙」或「商務電子郵件入侵（Business Email Compromise，簡稱 BEC）將使更多企業受詐騙而蒙受財物損失。司法實務如何針對日新月異的電腦犯罪技術加以因應？首要問題涉及跨境犯罪的司法管轄權之認定，而在各種新興的電腦犯罪態樣中，其中又以網路詐欺行為所可能造成的危害更大，其影響層面更廣，美國法上 CFAA 法案即係對此一問題之回應。

第二節　研究方法與研究過程

本研究擬由「電腦犯罪」之概念論述出發，由電腦犯罪之意義、特性與類型加以分析。其次，在立法架構上，我國關於電腦犯罪的規範主要見諸刑法第三十六章「妨害電腦使用罪章」，以及刑法第 339 條之 3 關於電腦詐欺之規定；另外，「電腦處理個人資料保護法」於民國 101 年 9 月 21 日修法並更名為「個人資料保護法」，就個人資料之運用、保護及刑事制裁提供法制基礎；現行的規範體系是否足以因應實務上的電腦犯罪態樣？由「一銀 ATM 盜領案」的訴訟發展，即可窺見我國現行法規範關於電腦犯罪之規制仍有所不足，職是之故，本研究於第三章關於「電腦犯罪的司法管轄權議題」中，立基於「司法管轄權的基礎」，進一步闡釋在電腦犯罪領域之司法管轄權之運用情形；不可諱言地，司法管轄權之認定為犯罪追訴之第一步，而電腦犯罪之本質又使司法管轄權之界定呈現複雜之面貌，數位證據的取得往往需要國際合作，對於犯罪行為人的引渡更常是能否有效追訴犯罪的關鍵所在。

此外，日益盛行的網路詐欺行為態樣繁多，本研究第四章針對網路詐欺的類型予以析述，並論及特殊態樣之詐欺行為（如：網路釣魚、網址嫁接、側錄信用卡、身份盜用等）；電腦犯罪的規模超越想像，網路詐欺的手法隨著科技發展日新月異，國際間立法例如何針對電腦犯罪之網路詐欺行為加以應對？歐洲理事會網路犯罪公約的框架性規範可提供吾人清楚的規範模式，該公約第八條對於網路

[4]http://www.trendmicro.tw/cloud-content/tw/pdfs/security-intelligence/reports/trend_micro_2018_prediction_paradigm_shift.pdf

詐欺行為有十分明確之規範；再者，本研究第五章以「跨境電腦犯罪之追訴」為主題，分敘網路犯罪公約之相關規定與美國法上對於電腦犯罪之規制及其立法趨勢；最後，本研究第六章「跨境電腦犯罪之法制化趨勢」中，針對我國現行關於電腦犯罪之規範狀態，提出應朝向犯罪類型細緻化之方向邁進，同時必須強化國際合作與司法互助，建立因應機制，使能有效打擊電腦犯罪。

第二章　電腦犯罪之概述

第一節 「電腦犯罪」之意義

第一項　概念源起

在 1980 年代以前，並沒有詞彙用以形容非法入侵電腦系統的行為，因在當時，電腦尚未如同今日如此普及；1983 年 9 月，《新聞週刊（Newsweek）》刊登了一篇名為《小心！駭客就在你身邊》的文章，內容是關於 FBI 在美國威斯康辛州的都市 Wilwaukee 逮捕了一群被控入侵數台電腦的駭客；同樣在 1983 年，電影「戰爭遊戲（WarGames）」上映，這是一部關於一個年輕駭客無意中入侵五角大樓作戰計畫回應系統的科幻電影；由於相信這個系統是個遊戲，這個年輕駭客造成了核子導彈的恐慌並幾乎引起了世界大戰。從此以後，對於電腦安全的關注開始增加，立法機關也開始強調此一議題[5]。而隨著科技發展及連網裝置（Internet-enabled devices）愈來愈普及，對犯罪者而言則意味著利用該等科技遂行犯罪行為的機會迅速增加，電腦犯罪逐漸被認可為刑事法律的一環；然在概念上，關於「電腦犯罪」的定義性用語在早期即存諸多爭議[6]，1991 年 Martin Wasik 所撰寫的 *Crime and the Computer* 可謂係探討電腦犯罪之濫觴，而學者有主張所謂「網路犯罪（cybercrime）」應是「電腦犯罪（computer crime）」的一個子集（subset）

[5] G. Press, *supra note* 1, at 14.

[6] 相關用語如：”e-crime”, ”computer crime”, “hi-tech crime’, “digital crime.”等，Alisdair A. Gillespie, *Cybercrime: Key issue and Debates*. (Routledge Taylor & Francis Grou, LONDON AND NEW YORK, 2016), 1.

[7]，此一立論或可謂係正確的，因基本上，雖然有些電腦犯罪確實是與網路相關，但電腦非必然需連接到網路空間[8]，若僅著眼於「網路犯罪」，則其範圍將比「電腦犯罪」更為狹隘。另外，論者亦有認為，「數位犯罪」或「高科技犯罪」的用語涵蓋較廣，可解釋其非必然需要連結到網路乙節[9]。本研究將使用「電腦犯罪」一詞，以涵蓋網路與離線（off-line）情形的犯罪行為。

「電腦犯罪」的核心概念為何？凡是與保護資訊電腦系統及其內容相關的行為，即屬「電腦安全（cybersecurity）」之範疇，而對於電腦安全產生危害之不法行為，則係所謂之「電腦犯罪（cybercrime）」。在網際網路跨越國際藩籬之今日，電腦犯罪之態樣繁多，而在網際網路上對個人所產生的侵害類型更是多樣化的，析言之，網路可能是非法內容產生的場域，犯罪行為人可能透過詐欺或取得被害人同意的方式為之，如：利用數位相機的技術與照片分享散布兒少色情；此外，有其他方式可能侵害網路使用者，如網路騷擾（cyber-harassment）、網路追蹤（cyberstalking）及網路霸凌（cyber-bullying）」[10]等，電子通訊及社群網站的發展更挹注此一類型之電腦犯罪行為；再者，網路銀行及線上交易的便利使得金融詐欺更為盛行。另一方面，數位媒體的可近性則可能導致智慧財產權所造成的侵害擴大，現代生活對於電腦及數位網絡的過度依賴，使得科技本身成為一個具有吸引力的目標，對於犯罪行為者而言，科技可以是資訊的取得手段，也可以是作為造成分裂及損害的手段；職是之故，掌握電腦犯罪的發展趨勢，實為今日法律人的重要課題。

第二項　電腦犯罪之意義

所謂「電腦犯罪」一詞並無精確的定義，通常泛指透過網際網路或其他電腦網絡所導致之犯罪行為[11]；而隨著電腦的使用逐漸成為主流，多數學者認為應在傳統犯罪類型外，將「電腦犯罪」獨立成為一個特殊的犯罪類型；隨著科技的演

---

[7] T. a. Loader, *Computer Crimes and Digital Investments*. T. a. L. i. Walden, Ed., (Oxford University Press, 2007), 19.

[8]即"cyberspace",在此概念意義下即指「網際網路（internet）」

[9]使用"e-crime"或"cybercrime"則侷限在與網路連結之犯罪。P. Hunter, The growing phenomenon of crime and internet: A cybercrime execution and analysis model. *Computer Law and Security Review* (2009), 529.

[10]在概念上，所謂「網路霸凌」常指涉的被害人為兒童或青少年，而「網路騷擾」此一用語則指被害人為成人之情形, 與「網路追蹤」相同，惟亦有學者認為此一區分基準並無實益。Alisdair A. Gillespi, *supra note* 6, at 258

[11] J. Fairtlough, *Introduction To Cyber Crime Investigation*. (LawTech Publishing Group, 2014), 466-467.

化，與電腦犯罪相關的行為本質也隨之進化，在關於電腦犯罪的意義界定上，論者有分由下列角度切入：（1）傳統犯罪行為透過電腦的使用更為便利，如詐欺；（2）透過網際網路產生的電腦犯罪，如駭客；（3）完全以科技作為媒介的犯罪，如網路殭屍（botnet）[12]。此外，犯罪行為人的動機也逐漸演變，由好奇心及欲取得特定地位的犯罪意圖，轉變為主要基於財務動機，且其犯罪行為更為組織化、系統化[13]。

在電腦犯罪的範圍界定上，首要問題在於：是否所有侵犯或使用網際網路的犯罪皆屬電腦犯罪？這答案應是否定的[14]；事實上，「電腦犯罪」一詞已被濫用為涵蓋所有犯罪行為的用語，如何針對電腦犯罪妥適定義已成為當務之急；一個較為普遍的區辨是在「利用電腦進行犯罪」與「針對電腦資訊內容的犯罪」之間劃一界線，此一區分實益在於：前者係指利用電腦設備進行法律原本即已規範的犯罪態樣，典型的例子如竊盜或散佈兒少色情；然而，另一方面，網路空間允許犯為行為以新型態出現—如：網路釣魚（phishing）、駭客侵入銀行帳戶、或在網頁上散播非法訊息等，此即所謂「針對電腦資訊內容進行犯罪」，指以電腦資訊內容為標的所導致的犯罪行為，其典型的案例即為「駭客行為（hacking）」，在電腦出現之前，並無駭客犯罪行為，因駭客行為必須以攻擊電腦資訊內容為其成立要件[15]。

惟針對上開分類基準，有批評指出，無法預期的科技發展可能會混淆「利用電腦進行犯罪」與「針對電腦資訊內容的犯罪」兩者之間的差別，因此，亦有論者提出包含下列三類型的細微區別來對電腦犯罪加以定義[16]：（1）透過網際網路擴張或助長的傳統犯罪活動[17]；(2)因網際網路蔓延或更為激進的傳統犯罪活動[18]；(3)由網際網路所創造的犯罪活動[19]。此一判斷基準有助於理解在諸多案件中，電腦犯罪並非新的犯罪行為，而是以新的方式進行現存犯罪行為態樣，上開第一個類型「透過網際網路擴張或助長的傳統犯罪活動」之適例即屬「信用卡詐欺」，自從信用卡問世以來，信用卡詐欺即已存在（如藉由複製簽帳單收據或在自動提款機裡設置陷阱側錄資料等），但網際網路與電子商務的發展導致此一犯罪型態

---

12 D. S. Wall, *Cybercrimes: The transformation of crime in the information age*. (Cambridge: Polity, 2007), 44-48

13 R. G. Smith, in *Crime over time: Temporal perspectives on crime and punishment in Australia*. (Newcastle upon Tyne: Cambridge Scholars Publishing, 2010), 214.

14 Alisdair A. Gillespie *supra note* 6, at 3.

15 *Id*, at 4.

16 S. Furnell, in *Handbook on Internet Crime*, Y. a. Y. Jewkes, M., Ed., Willan Publishing(2010) , 46.

17 原文為”Traditional criminal activities that are expanded or enhanced by the internet.”

18 原文為”Traditional criminal activities that are generalized and radicalized by the internet.”

19 原文為”Criminal activities that are created by the internet.”

開始轉變，對於犯罪之追訴而言，即意味著更高技術層次的挑戰；上開第二種類型「因網際網路蔓延或更為激進的傳統犯罪活動」之適例如「網路霸凌」，霸凌行為始終存在，通訊科技的應用不僅助長此一類型犯罪，而且使得此等犯罪以損害性更高的方式蔓延，何以言此？傳統霸凌方式下的被害人尚可隱藏身分，但由於數位科技的使用，使得網路霸凌的被害人幾乎無處可躲藏。由上開說明可知，前兩類犯罪代表著現存犯罪藉由網路賦予新樣貌，但顯然有些類型的犯罪在網路出現前並不存在（典型例子如「駭客」），此即第三種態樣—由網際網路所創造的犯罪活動。亦有論者有認為不應該關注焦點放在科技面向，而應著重於犯罪行為人的行為[20]，而此種以犯罪行為人為基礎的方式具有不依賴科技的優點，因此無須嘗試將新科技套用在舊的定義上，然而，以犯罪者為基礎加以定義的缺點在於可能因此失去電腦犯罪的特殊性。因此，以前述三種區分方式對「電腦犯罪」一詞加以定義，毋寧較為切合電腦科技之發展與司法實務之規制需求。

在法律實務上，傳統對於日常生活中電腦犯罪的態樣，侷限在與電信服務相關之詐欺行為與電子資金相關之移轉及竊取行為[21]，而在接下來的數十年，電腦網絡與個人電腦的普及興盛，不僅使電腦犯罪類型轉變，也產生了電腦犯罪相關法律；而在對於電腦犯罪議題的探討方面，主要可說是圍繞在電腦的不正使用（misuse of computers）領域。析言之，早期的關注焦點在於對私人資訊的未經授權，擴展到電腦也可能作為從事經濟犯罪之手段。隨著電腦成為主流，關注的焦點則朝向保護未經合法授權的電腦資料、電腦及網路的遠端攻擊、傳統犯罪行為以新的態樣出現，如著作權的侵害、兒少色情的散布與全球化詐欺體系的出現等，近幾年來常聽聞的跨國詐騙案件，即屬新興的犯罪型態。

隨著快速的科技發展持續進行，電腦犯罪此一領域將繼續呈現新的挑戰，網路頻寬的快速增加允許使用者將其裝置持續與網際網路連接，使其進而對外來攻擊更為脆弱[22]；對於犯罪行為人而言，點對點（Peer-to-peer ，簡稱 p2p）科技不僅僅可使用在傳送非法內容，也可以用來整合阻斷式服務攻擊與散佈惡意軟體[23]。電信通訊的集中與電腦運算將行動電話轉化為縮小網絡的電腦（miniature networked computers）；在此發展趨勢之下，我們也看到網路與越來越多日常生

[20] 並認為應區分三類型：（1）駭客(hackers)及濫用科技者（phreak）;（2 交易資料及訊息的買賣雙方（information merchants and mercenaries）;(3)恐怖主義者（Terrorists）極端主義(extremists)者及失常主義者（deviant）。T. a. Loader *supra note* 7, at 20.

[21] M. D. G. a. S. W. Brenner, The emerging consensus on criminal conduct in cyberspace. *UCLA Journal of Law and Technology* 3, (2002), 12.

[22] S. Morris, "The future of netcrime now: Part 1-threats and challenges," *Home Office Online Report No. 4* (Home Office, 2004)S. Morris, 20.

[23] *Id*, at 21.

活的物件整合連結，這就是所謂「物聯網[24]」，有許多不同的用語被用來描述此一概念，如：IoT（Internet of Things）、ICS（Industrial Control System）、CPS（Cyber Physical Systems）、SCADA（Supervisory Control and Data Acquisition）等，這些用語均泛指透過科技的運用來控制特定的裝置；然而，對司法實務工作者而言，當特定的科技實質上改變了犯罪風險，於偵查過程及在法庭上支持控訴的區辨能力若涉及與物聯網相關的犯罪，則可能產生新的變革，此一趨勢可謂係電腦犯罪未來的挑戰。

第二節　電腦犯罪之特性

不論對電腦犯罪一詞採何立場，電腦犯罪大體上均具有下列特性[25]：規模性（scale）、可近性（accessibility）、匿名性（anonymity）、可攜性（portability）及可轉換性(transferability) 、全球性（global reach）與缺乏有效的監管(Absence of capable guardians)等。茲就此等電腦犯罪之特性敘述如下：

第一項　規模性（scale）

網際網路與傳統的通訊形式不同，其允許使用者以低成本且簡便的方式與其他人聯繫，根據 2014 年的統計，世界上大約有三億人使用網際網路，佔了世界人口的百分之四十[26]，這是潛在犯罪行為人與被害人最大的對象，並且以力量倍增的效能，造成傳統犯罪無法達到的犯罪規模。舉例來說，網路殭屍“Bredolab”預估可在其高峰時感染三千萬台電腦、每天產生三億電子郵件[27]；又例如透過網際網路散布兒少色情，其犯罪結果發生地可能遍及世界各處，其他類型之犯罪亦然；隨著使用網際網路的人口有增無減，此一規模性之特質日益鮮明，乃屬當然。

---

[24] I. G. Secretariat, "ITU Internet report 2005 : the Internet of things," *Internet reports* (International Telecommunication Union, (2005)

[25] Alisdair A. Gillespie *supra note* 6, at 8.

[26] I. T. Union, "ICT facts and figures : The world in 2014," (International Telecommunications Union,2015).

[27] Sophos, *Security threat report* (2013) , at 27.

第二項　可近性（Accessibility）

僅在數十年前，所謂的電腦在外觀上是體積巨大的，對政府機關、研究及金融機構而言，電腦並非主要的設備；在當時，能夠造成電腦犯罪大部份侷限於有途徑使用電腦者及相關專業人士。而今，科技無所不在，不論對於犯罪者與被害者而言，使用電腦變得越來越容易。根據統計，在 2012 年至 2013 年，在澳洲、加拿大有超過百分之八十的成年人得以使用網際網路，其中超過半數使用行動電話或手持裝置[28]。網際網路與手機的普及，使得電腦犯罪更為容易進行，尤在今日，智慧型手機的普及使得人們無時無刻不與網際網路相連結，此即電腦犯罪之可近性特徵。

第三項　匿名性（Anonymity）

對於犯罪行為人而言，匿名性是一個顯然的好處，得以隱藏真實身份以遂行犯罪行為，降低遭司法機關調查追訴的可能性與風險，不論在任何犯罪行為均是如此，而所謂電腦犯罪之匿名性特徵，則是透過數位科技的發展得到挹注，犯罪行為人可能故意在網路上透過代理伺服器（proxy server）、詐騙郵件（spoofed email）、網際網路協定（internet protocol, IP）或匿名寄件者（anonymous emailer）的使用隱藏其身份；再者，由司法實務工作者進行調查取證的角度觀之，現代通訊網絡的本質是相關數據資料會在抵達目的地之前可能會途經諸多司法管轄權領域，此一特質使其通訊之追溯變得格外困難與耗時。授權或未經授權而連接無線網路可能隱藏真實使用者的身份，即使其位置是可以被辨識的。資料可能故意被儲存在法規與調查較不嚴格的司法管轄權所在[29]，此一匿名性特性無疑是司法機關對真正電腦犯罪行為人進行追訴的最大困難所在之一。

---

[28] Australian Bureau of Statistics, *Household use of information technology, Australia 2012-13*, Cat. No. 8146.0(2014) Statistics Canada, Individual internet use and e-commerce,2012(28 October 2013)

[29] J. Clough, *Principle of Cybercrime 2nd ed*. (Cambridge University Press, Monash University, Victoria, 2015), 8.

第四項　可攜帶性與可移轉性（Portability and transferability）

數位科技的核心在於得以在微小的空間儲存大量的資料，並且以保持質、量的方式複製該等資料，儲存與處理所佔據空間甚微小，聲音或影像的複製可以以極低的成本傳送給數以百萬計的接收者。電腦運算與通訊科技的整合使得此一過程無縫接軌，讓人們可以在數秒內用行動電話拍張數位照片並上傳到網站，此即所謂的「可攜帶性與可移轉性」。此一特質對於司法機關在犯罪追訴的過程而言，則代表著調查證據的高度技術性與複雜性。

第五項　全球性（Global reach）

本質上，刑事法律傳統上被視為是具有地域性的，受限於犯罪行為所發生之領土司法管轄權；然而，誠如常言所道「網路無國界」，現代電腦網絡的全球性特質使得犯罪行為可能發生於世界上各個角落，只要是網際網路可及之處，犯罪行為人即可能觸及，犯罪行為地、結果發生地可能遍及不同刑事司法管轄領域，此即電腦犯罪之全球性特質，涉及跨境電腦犯罪之司法管轄權認定問題（詳後述）。

第六項　缺乏有效監管的特性（Absence of capable guardians）

根據「日常活動理論（routine activity theory）」，犯罪的三個必要要素包括：具有犯罪動機的行為者、從事犯罪活動的機會存在、以及有效監管者的缺席[30]。若將此一理論運用到網路環境，此三要素對於遂行電腦犯罪行為也是同樣重要。數位科技使得犯罪行為更容易發生，甚至阻礙了法律的執行；易言之，一個影響犯罪行為人是否決定從事犯罪行為的重要因素在於遭到偵查與追訴的風險。在此

[30] L. C. a. M. Felson, Social change and crime rate trends: A routine activity approach. *American Sociological Review* **44** (1979), 588-589.

一面向，數位科技使法律執行面對諸多挑戰；電子資訊之多變性本質需要複雜的法律技術來確保其在刑事審判中使用的可回復性、保全與有效性，然而，現代通訊的網絡本質使得有效的監督變得極為困難。許多基礎建設是私有的，意指法律執行機關必須處理許多不同的實體。另一方面，通訊往往途經複數司法管轄領域，產生與各地域法律執行機構相互協助的需求；然而，即使可以獲得該地有關當局的協助，關於資料的保留可能會受限或不存在。再者，若被告身處另一司法管轄領域，可否進行引渡程序？在缺乏有效監管之下，電腦犯罪面臨比其他犯罪更高之調查成本與高度複雜性。

第三節　電腦犯罪的類型（types of cybercrime）

關於電腦犯罪之類型，可依不同的區分基準加以分類，論者有將之區分為下列三個態樣[31]：

第一項　針對電腦或網路的犯罪（Crimes directed against the computer or network）

此為電腦犯罪最單純的類型，電腦及其內資料成為犯罪行為的對象；在此類犯罪類型之證據調查方面，網路的資料程式碼、操作紀錄與電腦是相關證據資料的來源。例如：駭客入侵、包括病毒或電腦蠕蟲的惡意程式攻擊、阻斷服務式攻擊（Denial of Service attacks）、智慧財產的竊取等，均屬以電腦及其內資料作為犯罪行為對象之犯罪類型。

第二項　使用電腦進行犯罪（Crimes committed using a computer）

幾乎每一個「書面」犯罪（paper crime）都會涉及電腦之使用，如透過電腦作為媒介進行猥褻或色情物品的散布，即屬適例；在此情形，「電腦」是工具，

[31] J. Fairtlough, *Introduction To Cyber Crime Investigation*. (LawTech Publishing Group, 2014), 276.

但並非犯罪行為之目的。常見之態樣包括：個人資料的竊取、網路詐欺（釣魚及其他網路詐騙）、網路性犯罪等。

第三項　在電腦內發生的犯罪行為（Crimes committed within a computer）

此為逐漸被承認的電腦犯罪類型，指在區域或系統網路內犯罪，亦可稱為「與內容相關的電腦犯罪（content-related cybercrime）」，此類犯罪主要目標為存在於網路內的活動及資料，並以其為槓桿發動攻擊。在類型上，資訊洩漏、仇恨言論性犯罪或其他與言語相關的犯罪活動形式都是此類犯罪之典型。

第四項　實務上常見之電腦犯罪態樣

論其實際，電腦犯罪最為普遍的特徵之一即為科技導向，其中最為人所知的即是「駭客行為（hacking）」，在類型上，駭客行為屬於前述第一種「針對電腦或網路犯罪」，在行為態樣上屬於「非法入侵電腦（unlawful accessing of a computer）」；隨著社群媒體的普及化，經歷過電子郵件遭駭客入侵或電腦被駭客入侵的人越來越多。公眾對於駭客行為的認知無疑是受到媒體的影響，甚有認為駭客已成為網路空間最為嚴重並令人害怕的威脅[32]，在了解法律體系如何處理駭客行為之前，首先必須了解何謂「駭客行為」？

事實上，“hacking”一詞可謂已經經過相當程度的質變，最初“hacker”一詞是擁有較優秀電腦能力者的自稱，當然，現在情況也許相同，有些駭客是透過駭客行為來宣示他們的技巧；然而，該用語出現分歧現象，是因為駭客最初並非從事未獲授權的違法行為，而僅是程式設計技巧的展現，但現今的駭客可能被認為是非法侵入電腦系統，因而導致隱私權遭侵犯的問題，有些甚至造成更嚴重的後果，其類型可再細分為[33]：（1）竊取電腦資源（包括在被駭客入侵的伺服器上儲存文件）、（2）竊取專有或機密資訊、（3）對於系統或文件進行破壞、改變

[32] S. Furnell, *supra note* 16, at,174.

[33] M. Yar, *Cybercrime and Society 2nd ed*. (Sage, 2013), 8-31

或重建、（4）阻斷服務式攻擊、（5）散佈惡意程式等。其中第一種類型，即電腦資源的竊取，此與資料的竊取不同，而係指涉駭客的目的是為了要利用被駭電腦的某些或全部資源，其可能包括非法物質在內，也可能包括竊取無線網路頻寬而使該網路所有者增加支出；此外，駭客亦可能透過竊取無線網路頻寬散布兒童色情圖片，當執法者介入調查時，其顯現者為該網路所有者的 IP 位址，而非駭客本身，此即電腦犯罪之匿名性特徵之體現。而論其實際，駭客行為並不受限於網路空間，駭客行為隨著網際網路革命性的發展而擴大，由於網際網路是連結的網絡，意味著人們可以利用這些連結去入侵電腦，不論該電腦為何人所有。

除駭客行為外，在實務上，常見的電腦犯罪態樣主要有三：

一、未經授權入侵電腦或電腦系統：（Unauthorized access to computer or computer systems）

基本上，未經授權入侵電腦可能僅是取得未獲許可而登入，而在更複雜的層次，則可能涉及駭客使用網際網絡去獲得遠端連線，有時跨越數個司法管轄權；軟體發展的速度使得程式缺陷與漏洞成為無法避免的問題，而駭客常尋求其被訂正前利用這些弱點[34]，所謂的「零時差攻擊（zero-day）」即是在修補前遭駭客利用。

二、惡意軟體（Malicious software）

所謂的「惡意程式（malware）」即係出於惡意目的而攻擊電腦的軟體，最明顯的例子即是電腦病毒（virus），學說上有對惡意軟體提出三種分類[35]：（1）病毒（Viruses）、（2）電腦蠕蟲（Worms）、（3）木馬程式（Trojans）。茲就此三種類型說明如下：

（1）病毒（Viruses）：

電腦病毒可謂係最古老的惡意軟體形式之一，其為可自我複製的程式，透過附加方式散佈於特定檔案或儲存媒介，而在有些情況，病毒的程式設計是為了要增加被打開的可能性，舉例而言，1999 年有一個名為「Happy 99」的病毒設計為若開啟即可在螢幕上施放煙火，使用者可能會誤以為這是某種問候而開啟檔案。

---

[34] A. H. T. C. Centre, *Malware: Viruses, worms, Trojan horses*. High tech crime brief no. 10 (Australian High Tech Crime Centre, 2006),1.

[35] Furnell, S. and Ward, J. 'Malware an evolving threat' in Kanellis, P., Kiountouzis, E., Kolokotronis , N. and Martakos, D. Digital Crime and Forensic Science in Cyberspace(2006, Idea Group), 28.

（2）電腦蠕蟲（Worms）：

電腦蠕蟲與病毒一樣可自我複製（self-replicating），但其係可自動傳播的（autonomous）[36]，換言之，病毒係透過附加於檔案或儲存裝置的方式散布，而蠕蟲則是利用網路的連結性，其來源代碼允許其接觸受感染機器的網際網路協定，進而利用連結到網路的電腦所存在的弱點，在區域性網路系統（如公司或大學），蠕蟲的問題性更大，因區域性網路系統的本質使其可在電腦間快速散播。

（3）木馬程式（Trojans）：

木馬程式（Trojan）則是病毒的變體，且常成為電腦病毒與蠕蟲的載體[37]。與病毒或蠕蟲不同點在於，木馬程式無法自我複製，這也是為何其常常附隨於病毒而發生；木馬程式允許一個人可以遠距控制電腦，使其得以複製電腦或檢視螢幕上發生什麼情形，這可能也包括網路攝影機之使用，亦即一個人可以透過木馬程式監控並記錄使用者，進而可據以勒索對方或取得色情照片。

另外，常見的「間諜軟體（spyware）」通常與其他惡意軟體各自獨立，其基礎雖然可能偽裝得有所差異，但均係以侵犯隱私權作為目的。與上開病毒、蠕蟲或木馬程式不同之處在於，間諜軟體著重於隱私權的侵犯，而非對於系統造成損害或直接竊取財務資訊，其可能是由公司所製造；舉例來說，許多資訊巨擘公司如 Google[38]、 Apple[39]都曾遭控訴使用間諜軟體。

三、阻斷服務式攻擊（Denial of Service attacks，簡稱 DoS attacks）

阻斷服務式攻擊係利用網絡相連的電腦相互聯繫，達到癱瘓網路進而拒絕服務的目的。當一個網站無法處理其所接收到的請求時，即可能係受到阻斷服務式攻擊。舉例來說，當一場受歡迎的音樂會票券在網站上特價售票時，該系統易被同時發出的請求所癱瘓；一個阻斷服務式攻擊故意複製此一效果，而且可以針對單一電腦、伺服器、網站或網路；有許多種方式可以達成阻斷服務式攻擊，最基本的類型是，個人可以發送數以千計的電子郵件或足夠數量的請求來癱瘓系統，阻斷服務式攻擊也可能肇因於病毒癱瘓網絡的複製程式，或因為使用暴力破解法（brute-force cracking）來破解密碼時造成系統需處理大量資料而癱瘓。在 *US v.*

---

[36] *Id*,.29
[37] S. Furnell, *supra note* 16, at 185
[38] Google 會利用「我的活動」搜集使用者資訊(http://3c.ltn.com.tw/news/25035)
[39] Apple 會搜集手機使用者的 UDID(Unique Device Identifier，裝置唯一識別碼)
(https://www.bnext.com.tw/article/19876/BN-ARTICLE-19876)

Phillips[40]一案中，被告使用暴力破解法程式傳送數千個請求到大學電腦，將通常每月大約 20000 個請求的數量，增加到每月 1200000 個請求數量，造成系統崩潰[41]。

再者，更為複雜的阻斷服務式攻擊利用網路協定（internet protocol）來癱瘓作為攻擊目標的電腦，網際網路之網絡系統依賴協定允許電腦間相互聯繫，並確保提出請求的資料達到目的地。其運作方式為：客戶端的電腦（the client computer）傳送請求到伺服器，進而回應並確認其身分。另一個變體是「網際網路控制訊息協議（internet control message protocol，ICMP）」。"Pings"是被傳送到其他電腦測試是否可使用或連結到相同網路的微小訊號，ICMP 攻擊行為即涉及傳送大量的偽造的 ping 訊息到第三當事人的伺服器，這些測試 ping 訊息會將有回應的當事人電腦網路位址回傳，攻擊程式就會立即以大量回應，進而塞爆伺服器與當事人電腦之間的網路頻寬，這可能會導致伺服器與當事人電腦同時癱瘓。在一個分散阻斷服務式攻擊（DDoS）裡，攻擊者即係以控制其他電腦來攻擊目標電腦或網路；於 2010 年，一個電腦程式設計者即因涉及感染數以千計的電腦，及使用殭屍程式來從事阻斷服務式攻擊而被判刑[42]。

近幾年來，透過惡意程式的使用取得密碼及其他個人資訊逐漸盛行，常見的方式是透過網路釣魚的方式引誘被害人在不知情的狀態下下載了惡意程式。也可能透過所謂的「勒索軟體」，造成被害人的電腦當機並發出使用者被發現觸犯刑事犯罪的警告，較為典型的例子是兒童色情法律或非法侵害著作財產權[43]，被害人接著會收到指示支付「罰金」給執法機關來解除電腦鎖定，惡意軟體會持續操作被駭的電腦，進而完成詐欺行為或其他電腦攻擊行為。

第四節　我國現行法律規範狀態及實務運作

第一項　刑法妨害電腦使用罪

[40] 477 F 3d 215 (5th Cir. 2007)
[41] J. Clough, *supra note* 29, at 43.
[42] *US v. Raisley,* 466 Fed Appx 135(3rd Cir, 2012)
[43] I. C. C. Center, "Internet crime report 2013,"　(Internet Crime Complaint Center, 2013),.13

關於電腦犯罪的法律規制狀態，我國刑法第 323 條原規定為：「電氣關於本章之罪，以動產論」；其後，於民國 86 年 10 月 8 日修正公布為：「電能、熱能及其他能量或電磁紀錄，關於本章之罪，以動產論」亦即將「電磁紀錄」增列為準動產[44]；嗣後，再於民國 92 年 6 月 25 日修正公布為：「電氣、熱能及其他能量，關於本章之罪，以動產論」，本次修法時立法理由載明為：「本條係 86 年 10 月 8 日修正時，為規範部分電腦犯罪，增列電磁紀錄以動產論之規定，使電磁紀錄亦成為竊盜罪之行為客體。惟學界及實務界向認為：刑法上所稱之竊盜，須符合破壞他人持有、建立自己持有之要件，而電磁紀錄具有可複製性，此與電能、熱能或其他能量經使用後即消耗殆盡之特性不同；且行為人於建立自己持有時，未必會同時破壞他人對該電磁紀錄之持有。因此將電磁紀錄竊盜納入竊盜罪章規範，與刑法傳統之竊盜罪構成要件有所扞格。為因應電磁紀錄之可複製性，並期使電腦及網路犯罪規範體系更為完整，爰將本條有關電磁紀錄部分修正刪除，將竊取電磁紀錄之行為改納入新增之妨害電腦使用罪章中規範。」

其後，民國 92 年新增刑法第三十六章「妨害電腦使用罪章」，其中刑法第 359 條即明定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金」。該條之立法意旨載明為：「電腦已成為今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害，鑒於世界先進國家立法例對於此種行為亦有處罰之規定，爰增訂本條。」學者有認為，「資訊」與「資料」為常使用之電腦術語，並被視為同義詞而交互運用，其實「資訊」（information ）一詞在西方源於拉丁語 "informatio"，指傳達思想之過程與內容；「資料」則係呈現資訊之材料，除有體物本身外，還包括有體物上之文字、圖畫或符號，凡是呈現資訊之素材，可被稱為資料。「電磁紀錄」本身僅係資料，用以呈現資訊，電磁紀錄之取得即係資訊之取得。舊刑法第 323 條電磁紀錄竊盜罪之侵害客體係電磁紀錄，所保護之法益其實係電磁紀錄上有財產價值之資訊，此乃因資訊具備無體性，並不適合作為行為客體。與此相關者，「營業秘密法」[45]所保護之營業秘密，其實即為「資訊」，

[44]然而，該次修法同時增訂刑法第 339 條之 1「不正利用收費設備詐欺罪」、第 339 條之 2「不正利用自動付款設備詐欺罪」及第 339 條之 3「不正利用電腦詐欺罪」等三罪，讓原先第 343 條的準用各罪規定出現「失誤」，僅能準用於第 339 條之 3、第 340 條、第 341 條及第 342 條之罪，故於民國 88 年刑法修正時修正第 343 條為：「第 323 條及第 324 條之規定，於前 7 條之罪準用之。」換言之，電磁紀錄視為動產之規定，在普通詐欺罪、不正利用收費設備詐欺罪、不正利用自動付款設備詐欺罪、不正使用電腦詐欺罪、常業詐欺罪、準詐欺罪及背信罪皆得準用之。參見廖宗聖、鄭心翰，科技法學評論，第 7 卷第 2 期，2010 年，第 69 頁。

[45]我國於民國 85 年制訂營業秘密法，其立法目的在於保障營業秘密，維護產業倫理與競爭秩序，調和社會公共利益。(參見該法第 1 條規定)

此由營業秘密法第 2 條有關「營業秘密」之定義，即為：「方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊。」即可窺知[46]；如電磁紀錄上承載著受著作權或營業秘密法所保護之資訊，則未獲同意無權複製他人電磁紀錄之行為，即會侵害電磁紀錄所呈現出無體資訊之「資訊之專屬性或排他性使用」（the exclusive of information），此種財產上利益侵害即為舊刑法第 323 條電磁紀錄竊盜罪所要規範者[47]。惟大多數電磁紀錄之取得皆以檔案複製或線上資料傳送、下載之方式進行，此種電磁紀錄複製行為並不符合傳統竊盜罪之「竊取」定義，因此有前述 92 年間刑法之修正。

析言之，立法者之所以在 86 年修正刑法第 323 條而增列「電磁紀錄」視為以動產論後，繼續於 92 年提出第 359 條（列為新增第三十六章妨害電腦使用罪章中條文之一），無非係因立法者認為並非所有應受刑法保護之資料皆具有財產價值，立法者對於電磁紀錄之保護，採取了不僅只是在保護財產之觀點，更著重於如電磁紀錄係未經同意而被無權取得時，由此導致刑法之保護法益可能遭致侵害之危險。

而就法益保護之觀點而言，刑法第 359 條之保護法益，除「資訊與資料之私密性、完整性、可使用性」外，同時還包含「實害」，因如僅意在保護「資訊與資料之私密性、完整性、可使用性」，則凡未經授權而取得他人持有中之未公開電磁紀錄，即已侵害資料隱私權，構成要件上毋須以「致生損害」為必要，立法者在該條文中添加「致生損害於公眾或他人」之構成要件，顯有意藉此限制本條之適用範圍[48]，以符刑法謙抑之要求，防止過度之處罰[49]。觀諸舊電磁紀錄竊盜罪係財產犯罪，刑法第 359 條無故取得電磁紀錄罪則係關於資料安全之刑法規範，92 年刑法修正公布後，舊電磁紀錄竊盜罪與舊電磁紀錄侵占罪均無法再被適用，只能依刑法第 359 條無故取得電磁紀錄罪代替；學者有認為，如此立法政策是否妥適，非無疑義；其理由在於，刑法第 359 條「無故取得電磁紀錄罪」既以「致生損害」為要件，即係要求有事實上損害始克該當，應屬結果犯之規定，相對於「足以生損害」或「有受損害之虞」等危險犯之規定，係只要求有發生損害之危險為已足之情形，並不相同。在此意義下，僅只單純「得知」電磁紀錄之資訊內容，尚非屬本條所謂之「取得」，還須持有電磁紀錄之備份，並造成損害，方構

[46]營業秘密法第 2 條規定:「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計 或其他可用於生產、銷售或經營之資訊，而符合左列要件者:一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」

[47]參見 蔡蕙芳，電磁紀錄無權取得行為之刑法規範，中正法學集刊第 13 期，第 109 頁至第 119 頁

[48]參見 蔡蕙芳，前揭文，第 156 頁至第 158 頁

[49]參見 李茂生，刑法新修妨害電腦使用罪章芻議【上】，臺灣本土法學雜誌第 54 期，第 243 頁

成刑法第 359 條之「取得」行為；學說上有認為，該條所謂之「無故取得電磁紀錄」，係以無權侵入系統為前提，由此而接觸、刺探到未獲授權存取之電磁紀錄，並將電磁紀錄予以複製而言[50]；至於依行為人身分原有接觸或控制電磁紀錄之權限，只是違反公司資訊安全規範將該等資訊帶回家工作時，因行為人並無洩漏之動機或目的，即不宜機械性使用刑法第 359 條保護，而應屬於民事訴訟範圍之營業秘密爭執，以免逸脫電腦或網路犯罪之立法原意[51]。

就資訊本身而言，營業秘密法所保護之「秘密」性質上亦屬「資訊」之一種，無論係 92 年刑法修正前之電磁紀錄竊盜罪，抑或修法後之刑法第 359 條無故取得電磁紀錄罪，此等規範之主要立法目的，均非意在為營業秘密提供保護，以處罰不正取得營業秘密之行為。由於現行營業秘密法未具有規定刑事處罰之條文，因此營業秘密之刑事保護，僅賴於依據具體情況之不同，援引適當之刑法條文為之。而從前述刑法之修法過程與構成要件解析，亦顯示刑法之修正與變化，將會影響營業秘密之刑法保護範圍，此種無意識之連動關係，從刑事立法政策而言並非妥適，如欲建立完善之營業祕密保護法制，根本之道應採取類似著作權法之立法模式，以營業秘密法為基礎，針對營業秘密之性質，制定各種不同行為態樣之刑事處罰規定，方屬妥適[52]。

刑事立法保護法益之核心內涵之一在於犯罪類型之建構，而犯罪類型之建構，又以規範與處罰之行為態樣最屬重要。以營業秘密為例，關於不法侵害營業秘密之行為，主要包括「取得」、「洩漏」與「使用」等三種。如再配合行為階段之發生順序與營業秘密取得之原因合法與否，則得組合為「合法取得營業秘密後之不法洩漏」、「合法取得營業秘密後之不法使用」、「不法取得營業秘密」、「不法取得營業秘密後之不法洩漏」、「不法取得營業秘密後之不法使用」等各種行為態樣。在我國現行保護營業秘密之刑事立法現狀下，除「合法取得營業秘密後之不法洩漏」、「不法取得營業秘密」有明文處罰外，其餘各種行為態樣是否或有無適當之規範與處罰依據，實仍有待立法補充。據此，為處理前述營業祕密保護之刑事法制困境，我國曾先後提出各種相應法案，包括刑法部分條文修正草案（新增妨害農工商罪之刑法第 255 條之 1、第 255 條之 2、修正妨害秘密罪章之刑法第 317 條及增訂第 317 條之 1）、公平交易法部分條文修正草案、科技保護法立法草案、敏感科學技術保護法立法草案及營業秘密法部分條文修正草案（增

[50]參見 蔡蕙芳，前揭文，第 163-165 頁；林山田，刑法各罪論【上冊】，第 555 頁
[51]參見 張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，第 89、90 頁
[52]參見 蔡蕙芳，同前，第 181 至第 182 頁。

訂第 15 條之 1、第 15 條之 2 ），終因各種因素而遲未能完成立法[53]。而作為我國民、刑事法規之主要法律被繼受國，並為營業秘密法立法時所參酌法制之一之德國，該國有關營業秘密保護之法律建制，係採取民、刑事立法同兼之方式，其中刑事立法係以「不正競爭防止法」（原名「不正競爭禁止法」， Gesetz gegen den unlaute ren Wettbewerb，簡稱 UWG ）內之規範為核心，並輔以刑法中之部分相關條文，共同築起有關營業秘密刑事立法保護之主要架構[54]。立法意旨係將營業秘密法定位為民法之特別法，該法所稱之「營業秘密」，並未等同於刑法保護之「工商秘密」，而刑法妨害電腦使用罪章原非以保護營業秘密為其規範意旨，致我國就營業秘密保護之刑事立法規範出現漏洞，刑法第 359 條無故取得電磁紀錄罪中所謂之「無故取得他人電腦之電磁紀錄」，係以無權侵入系統為前提，由此而接觸、刺探未獲授權存取之電磁紀錄，並將電磁紀錄予以複製而言。是以，論者有認為，基於憲法為保障人權意旨所肯認之罪刑法定原則，如行為人係合法取得他人營業秘密之電磁紀錄，其後加以不法使用或不法洩漏時，依其情節可能該當刑法第 317（洩漏業務上知悉之工商秘密罪）、318（洩漏公務上知悉之工商秘密罪）、318-1（洩漏電腦或相關設備秘密罪）、318-2（加重規定）、 335（普通侵占罪）、336（公務公益及業務侵占罪）、342 條（背信罪）等條文之構成要件或民事侵權行為責任。簡言之，刑法第 359 條之無故刪除他人電腦之電磁紀錄罪之成立，須以無故刪除他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人為要件，且揆諸該條文立法理由可知，該條文所保障者乃「電腦使用人」，而非「電腦中檔案所有人」；又所謂「刪除」乃指使電磁紀錄完全消失或使部分消失致不能再現電磁紀錄之意義而言。

再者，刑法所稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄，刑法第 10 條第 6 項定有明文；依此，刑法第 359 條之無故取得他人電磁紀錄罪主要是係為了因應電磁紀錄具有「可複製性」之特性而訂定，則在行為人取得電磁紀錄（即複製電磁紀錄）前後，因未必會同時破壞他人對該電磁紀錄之持有，則對被害人的整體財產總額並無影響，此與一般財產犯罪之態樣不同；而行為人取得電磁紀錄後，若只是單純的持有，也不會減少被害人的整體財產總額，而真正會使被害人整體財產總額產生影響者，應係行為人的後續的其他利用行為。是以，若認為所謂之「損害」係被害人整體財產之減少，亦即指減少被害人現有之利益，或喪失將來可得之利益，則真正致使此一「損害」

[53]參見 陳彥嘉，保護營業秘密之刑事立法，臺灣法與德國法的比較研究，國立東華大學財經法律研究所碩士論文，2006 年，第 113 至第 276 頁，關於各種有關刑事立法保護規範之比較與整理。
[54]參見 陳彥嘉，同前，第 278 頁。

者，當係行為人其他後續利用行為，而非「取得電磁紀錄」之行為，則亦不符合無故取得電磁紀錄「致生」損害之要件（因為行為人取得電磁紀錄後，不一定會有後續利用行為，故取得電磁紀錄與後續利用行為間，並無因果關係，則取得電磁紀錄與「損害」間亦無因果關係；至於後續利用行為，亦可能另構成犯罪）。故若認「損害」係指被害人整體財產總額之減少，則刑法第 359 條之無故取得電磁紀錄罪將少有構成的可能(亦即僅有取得電磁紀錄時同時破壞了被害人對於該電磁紀錄之持有時才會構成），此殊非立法之原意。

另依上開立法源由，亦可知立法者係希望以「無故取得」來取代「竊取」之概念，是以無故取得電磁紀錄罪所侵害財產利益之內容，乃是特定財產之所有權或持有權，故性質上屬於「侵害個別財產利益之犯罪」，學理上即認為此種犯罪被害人的整體財產是否減少並非重點。與此相較，刑法第 342 條背信罪，則屬於「侵害整體財產利益之犯罪」，故須以被害人整體財產價值產生減損為要件。刑法第 359 條之無故取得他人電磁紀錄罪既與刑法第 342 條之背信罪，在性質上完全不同，兩者之所謂「致生損害」自然亦不得為相同之解釋。論其實際，刑法 359 條乃是將之無故「取得」、「刪除」、「變更」電磁紀錄 3 種犯罪態樣併列，且此 3 種犯罪態樣均以「致生損害於公眾或他人」為要件，此 3 種犯罪態樣之「致生損害於公眾或他人」要件，自應為相同之解釋。而就無故「刪除」電磁紀錄而言，行為人一有「刪除」之行為，即已造成被害人被害人整體財產價值之減少，亦即造成「損害」，則「致生損害於公眾或他人」的要件，豈不是贅文？承上所述，法院實務判決有認為「致生損害於公眾或他人」乃係立法者為了達到立法謙抑之要求所設的要件，亦即行為人不僅有「刪除」電磁紀錄之行為，而且尚須該電磁紀錄對於公眾或他人有相當之財產價值或祕密性，在法律評價上可以認為行為人的刪除行為係「造成損害」時，才構成犯罪，以避免刑罰範圍過於擴張[55]；此外，立法者既已認識到電磁紀錄之可複製性[56]，並肯認「無故取得」電磁紀錄之行為具有可罰性，將之與「刪除」、「變更」併列，自然係將之為相同評

[55]參見最高法院 104 年度訴字第 2335 號刑事判決：「…刑法第 359 條所規定「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人」罪，屬於結果犯，必須該行為已致生損害於公眾或他人之結果，始構成本罪。否則，縱有無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄行為，倘未致生損害於公眾或他人之結果，因該罪無處罰未遂犯之明文，自不成立該罪。換言之，刑法第 359 條之罪，以「致生損害」於公眾或他人為構成要件，屬於結果犯，此與僅以「足以生損害」於公眾或他人為構成要件之罪，例如刑法第 210 條之偽造私文書罪，以有足生損害於公眾或他人之危險，即行成立，迥然不同。…」

[56]參見最高法院 104 年度台上字第 5295 號刑事判決：「…依刑法第 323 條修正理由說明，因電磁紀錄具有可複製性，與其他電能、熱能經使用後即消耗殆盡之特性不同，行為人於建立自己持有時，未必會同時破壞他人對該電磁紀錄之持有，對被害人整體財產總額並無影響，與竊盜罪構成要件有所扞格，改納入刑法妨害電腦使用罪章。依此，如果以侵害財產法益之觀點解釋刑法第 359 條不法取得電磁紀錄罪，將無故限縮其適用範圍，且違反該章保護電腦使用者免受侵害之本質不符…」

價，則在無故「取得」電磁紀錄之態樣，自然不能因為他人對該電磁紀錄之持有並無影響即認為「損害」並未發生，而也應認為該電磁紀錄對於公眾或他人有相當之財產價值或祕密性時，在法律評價上即可以認為行為人的「取得行為」係「造成損害」[57]；此為法院實務判決向來對於刑法第 359 條取得、刪除、變更電磁紀錄罪之見解。

然而，隨著對於資訊安全的重視日益提高，近期法院實務見解則認為妨害電腦使用罪之保護法益係在於維持電子化財產秩序，故並不以實際上對公眾或他人造成經濟上之損害為限。只要電腦中重要資訊發生得喪變更，已足導致電腦使用人發生嚴重損害，即足該當[58]，且就該條所稱「刪除」而言，最高法院 104 年度台上字第 3392 號判決甚至明確指出：「刑法第 359 條之破壞電磁紀錄罪，係指行為人無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人。所稱『刪除』，固係指反於電磁紀錄製成之方法，將電磁紀錄完全或部分消除之謂，惟是否必使之永久消除而無法回復，始得謂為『刪除』，在學理上非無爭議；然就該『刪除』係刑事法上之『構成要件』觀之，自應基於當代共通之學理，或本乎相關之法規，而為合乎立法本旨之闡釋。查 92 年 6 月 25 日修正公布新增刑法妨害電腦使用罪章所定之罪，其保護法益兼及個人及社會安全法益，並非僅 16 止於個人法益（參行政院會同司法院送立法院審議之原修正草案修正說明）；而刑法第 359 條規定之立法意旨，無非認「電腦已成為今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害，鑒於世界先進國家立法例對於此種行為亦有處罰之規定，爰增訂本條。」（參立法理由），顯見本罪之立法係鑒於電腦之使用，已逐漸取代傳統之生活方式，而所有電腦資料皆係經由電磁紀錄之方式呈現，電磁紀錄有足以表徵一定事項之作用（諸如身分或財產紀錄），則對電磁紀錄之侵害，亦可能同時造成身分或財產上之侵害關係，嚴重影響網路電腦使用之社會信賴及民眾之日常生活。參諸對電腦及網路之侵害行為採刑事處罰已是世界立法之趨勢，乃增訂該罪，對行為人科以刑事罰。故而本罪規範應係重在維持網路電腦使用之社會安全秩序，並避免對公眾或他人產生具體之損害。

[57]參見 臺灣臺北地方法院 94 年度訴字第 1561 號刑事判決。

[58]臺灣高等法院 104 年度上訴字第 1094 號刑事判決：「按「無故取得、刪除或變更他人電腦或其他相關設備之電磁紀錄，致生損害於公眾或他人者」，構成刑法第 359 條之罪。而電腦已成為今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害（參照該條之立法理由），足認本條犯罪之成立雖以對公眾或他人產生具體之損害為必要，然本項法益既係在於維持電子化財產秩序，故並不以實際上對公眾或他人造成經濟上之損害為限。只要電腦中重要資訊發生得喪變更，已足導致電腦使用人發生嚴重損害，即足該當。被告 OOO 未經告訴人同意，擅自將告訴人網站上之文章等電磁紀錄刪除，造成告訴人須另花費時間、人力始能將其網頁重建，並造成告訴人上開網頁文章之電磁紀錄之喪失，足認被告 OOO 上開行為業已造成告訴人之損害甚明。」

不論行為人所使用之破壞方式為何，祇要無故刪除他人電腦或其相關設備之電磁紀錄，即該當於刪除之構成要件。復因電磁紀錄本身具有可複製性，又不具有損耗性，縱被複製亦不致因此而消失，而依現行之科技設備，若要回復被刪除之電磁紀錄，亦非難事，故解釋上，應認電磁紀錄遭受無故刪除時，即已產生網路電腦使用之社會安全秩序遭受破壞之危險，至於該電磁紀錄事後得否回復，均無礙於『刪除』之成立。倘其刪除行為，又已致生損害於公眾或他人，本罪即已該當。否則，行為人於刪除電磁紀錄時，祇須先保留備份之電磁紀錄，俟東窗事發後再行提出，或事發後要求將電腦或其相關設備送由專門機構依現行之科技設備予以回復，即不構成刪除電磁紀錄之罪，則本罪之規範目的豈不落空。是本罪所稱『刪除』，顯不以使電磁紀錄永久消除而無法回復為必要。」

實務上亦具相當重要性之刑法妨害電腦使用罪章條文，當屬刑法第 358 條之無故侵入電腦或相關設備罪。刑法第 358 條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」由此規範內容可知，關於無故侵入電腦或相關設備之行為態樣分為兩個層次，其一為透過無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞等方式（第一層次之行為），其二為入侵他人電腦或其相關設備（第二層次之行為）[59]，當行為人以「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」或「利用電腦系統之漏洞」[60]入侵他人電腦或其相關設備，即屬違反無故入侵電腦或相關設備罪。

另外，鑑於電腦及網路已成為人類生活之重要工具，分散式阻斷攻擊（DDoS）或封包洪流（Ping Flood）等行為已成為駭客最常用之癱瘓網路攻擊手法，故於 92 年修法新增訂刑法第 360 條關於干擾電腦或相關設備罪：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金」。依該條立法理由之說明，本條之規範目的旨在以刑法保護電腦及網路設備之正常運作，且其處罰之對象乃對電腦及網路設備產生重大影響之故意干擾行為，為避免某些對電腦系統僅產生極輕

[59]依立法理由之說明，無故侵入他人電腦之行為以刑罰相繩已是世界立法之趨勢，且電腦系統 遭惡意入侵後，系統管理者必須耗費大量時間與人力進行檢查、修復，才能確保電腦系統的安全 性，因此，此種行為之危害性已經達到科以刑事責任之程度，為保護電腦系統之安全性，特增訂 無故入侵電腦或相關設備罪。參見 廖宗聖、鄭心翰，前揭文，第 72 頁。

[60]論者有認為，基本上僅有「無故輸入他人帳號密碼」之構成要件可被實務界加以使用，其他 兩個行為態樣之規定並無太大之用處，只要「無故輸入他人帳號密碼」之構成要件該當即可解決 電腦犯罪一半以上的問題。參見 張紹斌，刑法電腦專章及案例研究，軍法專刊，第 54 卷第 4 期，第 88 頁。

度影響之測試或運用行為亦被繩以本罪，故加上「致生損害於公眾或他人」之要件，以免刑罰範圍過於擴張[61]。再者，有鑑於電腦病毒、木馬程式、電腦蠕蟲程式等惡意之電腦程式，對電腦系統安全性危害甚鉅，往往造成重大之財產損失，致生損害於公眾或他人[62]，故亦於 92 年修法增訂刑法第 362 條關於製作專供犯本章之罪之電腦程式罪[63]。

由前揭說明可知，我國刑法關於妨害電腦使用罪之行為態樣包括有：無故侵入電腦或相關設備（刑法第 358 條）、無故取得、刪除變更電磁紀錄（刑法第 359 條）、干擾電腦或相關設備（刑法第 360 條）、製作專供犯電腦犯罪之電腦程式罪（刑法第 362 條），其中除刑法第 358 條外，其餘犯罪類型均明訂須以「致生損害於公眾或他人」為要件，在立法方式上採取實害犯而非危險犯之模式。此一修法實係考量電腦已成日常使用之工具，電腦使用安全、電磁紀錄支配權及電腦系統效能等已成為值得獨立保護之法益，故設專章予以保護該等法益[64]。

此外，在利用電腦進行詐欺行為方面，民國 86 年增訂刑法第 339 條之 3 規定：「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人之財產者，處七年以下有期徒刑(第一項)。以前項方法得財產上不法之利益或使第三人得之者，亦同（第二項）。」其立法理由為「以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，為電腦犯罪型態，為適應社會發展需要，爰增列處罰專條。」於民國 103 年 6 月 17 日修法，除在第一項增列「得併科七十萬元以下罰金」之處罰規定外，並增訂第三項之未遂犯規定。此一規定可謂係在電腦犯罪專章外之特殊電腦犯罪處罰規定，由此可知透過電腦犯罪方式進行詐欺行為，其可能造成之實害較傳統一般詐欺犯罪行為為鉅，此由其刑度較高之規範方式即可窺知。

第二項　個人資料保護法

[61]刑法第360條規定之增訂理由參照。
[62]1999年4 月26 日發作之 CIH 病毒造成全球約有六千萬台電腦當機，鉅額損失難以估計，即為著名案例。參見刑法第362條增訂理由。
[63]刑法第362條規定:「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」
[64]參見刑法第三十六章說明第二點。

就立法沿革而言，「個人資料保護法」之前身為「電腦處理個人資料保護法」，其立法目的在於保護人民之資訊自決權益，使個人人格權得到完善之防護，不需時時處於恐懼其個人資料遭竊之狀態，故在我國法制上針對個人人格完整性制訂專法規定，針對過度侵害人格權之行為施以刑事制裁。「電腦處理個人資料保護法」之立法目的雖在於保障人格權、促進個人資料之合理利用，然其保護客體僅限於經電腦處理之個人資料，若未經電腦處理之個人資料，即不屬該法所保障之範疇；基此立法疏漏，而有「個人資料保護法」之修法[65]。

個人資料保護法第 1 條即開宗明義規定：「為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」針對本條於（舊法之電腦處理個人資料保護法）84 年 7 月 12 日制定時，即於其立法理由內宣示：「電腦科技進步迅速，使電腦能大量、快速處理各類資料，且運用日趨普及，因而對國民經濟之提昇有重大貢獻。惟個人資料因濫用電腦而侵害當事人權益之情形日漸嚴重，亦引起民主先進國家之關切。故經濟合作暨發展組織（OECD）於 1980 年 9 月通過管理保護個人隱私及跨國界流通個人資料之指導綱領，歐洲理事會亦於 1981 年完成保護個人資料自動化處理公約，並提出 8 項原則以供遵守。迄今已有瑞典、美國、紐西蘭、德國、法國、丹麥、挪威、奧地利、盧森堡、冰島、加拿大、英國、芬蘭、愛爾蘭、澳洲、日本、荷蘭等 17 國制定相關法律以保護個人資料」。因此，就上揭法條及其立法理由相互參照之下，本法就個人資料保護之目的，乃是避免因濫用當事人之資訊而侵害其權益，故凡是針對個人資料之蒐集、處理及利用，必須在合理使用之範圍內始得為之，以避免造成個人人格權受到侵害；反面言之，若資訊之內容不足以造成個人人格權之侵害，甚至根本無法辨識、特定究係何人之資訊，自不在本法保護之範圍內。蓋以資訊之本身，若根本無法確定究係何一對象，自不會有個人人格權被侵害之問題[66]。按維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值，隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障，其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權（司法院大法官釋字第 585 號解釋理由、第 603 號解釋文參照）。是前揭釋字第 585 號解釋揭諸隱私權為受憲法第 22 條所保障之非列舉基本權之一，釋字第 603 號解釋文除指出隱私權為受憲法

[65]「電腦處理個人資料保護法」係於民國 101 年 9 月 21 日修法，更名為「個人資料保護法」。
[66] 參見台灣高等法院 104 年度上訴字第 1393 號刑事判決。

第 22 條所保障之非列舉基本權之一，且更進一步將隱私權擴展至人民得自主決定其個人資料之「資訊自主權」。而所謂隱私權，乃係基於人格尊嚴、個人之主體性及人格發展所必要，屬民法第 195 條規定所明定之人格權之一種，旨在保障個人在其私領域的自主，即個人得自主決定其私生活的形成，不受他人侵擾，及對個人資料自主控制，是隱私權侵害類型可分為：（1 ）私生活的侵入、（2 ）私事的公開、（3 ）資訊自主的侵害。隱私權之概念，逐漸演進至當前具有積極性之資訊隱私權，即「免於資料不當公開之自由」或「對自己之資料之蒐集、輸入、累積、流通、使用，有完全決定及控制之權利」[67]。

其次，就個人資料保護法之重要規範內涵論之，個人資料保護法第 6 第 1 項規定：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。三、當事人自行公開或其他已合法公開之個人資料。四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。」另關於非公務機關對於個人資料蒐集或處理之規範，依個人資料保護法第 19 條第 1 項規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。五、經當事人書面同意。六、與公共利益有關。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。」另依個人資料保護法第 20 條第 1 項規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、經當事人書面同意。」 23 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯；非公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於蒐集之特定目的必要範圍內為之，個人資料保

[67]參見 許文義著，個人資料保護法論，第 53 頁至第 54 頁。

護法第 5 條、第 20 條第 1 項本文分別定有明文。而個人資料保護法第 5 條、第 20 條所稱之特定目的「必要」範圍，其內涵實即指比例性原則。依憲法第 23 條「憲法所列舉之自由權利，除為防止妨害他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要者外，不得以法律限制之」之規定，此原則之衍生權，包括：合適性原則、必要性原則及狹義比例原則（即過量禁止原則）…合適性原則，乃指被告行使之手段須可達其目的；必要性原則，指在所有可能達成目的之方法中，被告應選擇對告訴人最小侵害之手段，即最小侵害原則；禁止過量原則，係指被告所欲完成之目的及使用手段，不能與因此造成之損害或負擔不成比例。又按非公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於蒐集之特定目的必要範圍內為之，但為防止他人權益之重大危害，得為特定目的外之利用，個人資料保護法第 20 條第 1 項但書第 4 款固有明文；惟揆諸舉重明輕之法理，縱係符合此款規定之「特定目的外之利用」，亦應受前開第 5 條揭諸之「誠實信用原則」、「正當合理關聯原則」（即須與「所要防止重大危害之權益保護」有正當合理關聯），以及第 20 條第 1 項本文規定之「必要」範圍之內涵即比例原則之規範，始符法體系解釋之意旨[68]。

在司法實務上，法院實務判決亦指出，個人資料保護法第 2 條第 1 款規定，所稱個人資料係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。又個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯，個人資料保護法第 5 條定有明文。再依同法第 20 條第 1 項前段之規定，因故取得他人個人資料者，原則上僅得於蒐集之特定目的必要範圍內，就該個人資料加以利用[69]。而針對違反個人資料保護法之主要刑責，規定於該法第 41 條：「違反第 6 條第 1 項、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。意圖營利犯前

[68]參見臺灣臺北地方法院 104 年度易字第 106 號刑事判決。

[69]參見臺灣臺北地方法院 104 年度易字第 325 號刑事判決：「…觀諸上開個人基本資料查詢結果、戶役政連結作業系統資料，乃法院為特定當事人之身分、審理案件所需，被告自其與告訴人之訴訟案件閱卷取得上開資料，自僅得於蒐集之特定目的必要範圍內，就該個人資料加以利用，而不得逾越特定目的之必要範圍，詎被告竟仍逾蒐集目的必要範圍，率爾將上開載有告訴人個人資料之文書張貼於該大廈之公布欄使不特定多數人得以見聞，且告訴人之個人資料實與社區公共利益無關，不得無故公然揭露之，此依被告之學經歷，自無不知之理，是被告此舉自屬濫用個人資料，且顯足生損害於告訴人之隱私權。是被告就上開個人基本資料查詢結果、戶役政連結作業系統資料之利用行為，已逾蒐集該個人資料特定目的之必要範圍，而足生損害於告訴人，其違反個人資料保護法第 20 條第 1 項之規定，而犯同法第 41 條第 1 項之罪，至為明確。」

項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」其處罰要件須以「足生損害於他人」為前提[70]，且若行為人係基於營利意圖而違反個人資料保護法相關規定者，即須加重處罰，此即我國目前關於個人資料保護之法律規制狀態。

第三項　由「一銀 ATM 盜領案」看我國司法實務之運作

近年來在我國喧騰一時的電腦犯罪案例，當數民國 105 年之「一銀自動提款機盜領案」[71]，該案係由拉脫維亞國籍之 Peregudovs Andrejs（譯為安德魯）、羅馬尼亞國籍之 Colibaba Mihail （譯為米海爾）、摩爾多瓦國籍之 Pencov Nicolae（譯為潘可夫）等 22 人，及其他不詳之成員，共同組成入侵銀行內部網路以盜領自動提款機（下稱 ATM）之國際犯罪集團。分工方式係由集團中之不詳成員，負責入侵銀行內部網路並製作、布署盜領 ATM 所需之電腦程式；由俗稱之「車手」負責依編組至 ATM 盜領款項兼為同組車手把風；俗稱之「車手頭」負責至 ATM 盜領款項並兼向各組車手收取贓款;該集團之不詳成員於民國 105 年 5 月 31 日前某日時，藉由網際網路，探知我國之第一商業銀行股份有限公司（下稱第一銀行）倫敦分行內，有一可同時連結網際網路及第一銀行內部網路之電話錄音主機（內部網路之虛擬 IP 位址 10.224.21.11）存在電腦系統之漏洞，並以不詳方式，探知第一銀行內部使用之 ATM，有多數為德國「Wincor Nixdorf」公司所生產（臺灣代理商為德利多富股份有限公司）之「ProCash 1500」型 ATM，並探知該型 ATM 內部吐鈔模組之運作與控制機制後，即分別為下列入侵第一銀行內部網路及盜領 ATM 犯行：（一）於 105 年 5 月 31 日晚間 10 時 36 分許，由上開集團內之不詳成員，在不詳地點，無故利用第一銀行倫敦分行電話錄音主機系統之漏洞，以與第一銀行倫敦分行電話錄音主機建立異常連線之方式，而入侵第一銀行倫敦分行電話錄音主機，以便作為日後入侵第一銀行其他電腦之跳板。（二）上開集團內之不詳成員，復於 105 年 7 月 5 日前某日時（105 年 7 月 5 日係集

[70]相較於電腦處理個人資料保護法刑事責任規範皆以「致生損害於他人」之實害犯形式加以制 訂，現行個人資料保護法的刑事責任要件則皆盡改為「具體危險犯」的規範類型，即無庸實際上 損害的發生，僅需「足生損害於他人」，即得以本條相繩，而依法院向來之實務見解「所謂足生 損害，固不以實已發生損害為必要，然亦必須有足以生損害之虞者，始足當之」...由此可知個人 資料保護法對於法益保護之程度顯然更為提高。參見葉奇鑫、李明臻，<打擊網路犯罪新紀元: 個人資料保護法施行下檢察實務的衝擊與挑戰>，檢察新論第 13 期，2013 年 1 月，第 70 頁。

[71]下述犯罪事實係參臺灣臺北地方法院 105 年度訴字第 426 號刑事判決。

團內之成員最早來台之日期），在不詳地點，製作專供犯無故干擾他人電腦與設備罪之電腦程式（包含：1.取得「ProCash 1500」型 ATM 內現鈔資訊之電腦程式「cnginfo .exe」；2.命令該型 ATM 執行吐鈔動作且限定僅能於 105 年 7 月間執行之電腦程式「cngdisp .exe」與「cngdisp_ new .exe 」），與專供犯無故刪除他人電腦之電磁紀錄罪之電腦程式(即「cleanup .bat」，犯案後可呼叫「sdelete .exe」，「sdelete .exe」之功能係針對欲刪除之檔案進行磁區抹除，使得刪除後之檔案難以透過專業軟體進行復原，以徹底刪除上開「cnginfo .exe」、「cngdisp .exe」之電腦程式）。（三）上開集團成員自 105 年 6 月 28 日起至同年 7 月 4 日止，在不詳地點，無故利用第一銀行倫敦分行電話錄音主機系統之漏洞，而入侵第一銀行倫敦分行電話錄音主機後，復以第一銀行倫敦分行電話錄音主機作為跳板，以不詳方式入侵第一銀行內部網路中負責「ProCash 1500」型 ATM 電腦程式更新派送暨監控之應用程式伺服器（下稱 AP 伺服器，內部網路之虛擬 IP 位址為 10.20.4.42），先後派送 33 個異常封裝檔至該型之 ATM 電腦，藉以探測該型 ATM 電腦執行環境並執行盜領前準備工作之相關電腦指令，如開啟該型 ATM 電腦之 Telnet（遠端登錄服務）功能，其中「00000000 .dms 」之異常封裝檔，無故變更該型 ATM 電腦之電磁紀錄，新增具有管理者權限之管理者帳戶。（四）上開集團成員於 105 年 7 月 5 日前某日時，在不詳地點，無故利用第一銀行倫敦分行電話錄音主機系統之漏洞，入侵第一銀行倫敦分行電話錄音主機後，復以第一銀行倫敦分行電話錄音主機作為跳板，以不詳方式，入侵第一銀行內部網路中負責針對第一銀行所使用另一系列由 NCR 公司生產之 ATM ，進行 ATM 電腦程式更新派送之 NCR 伺服器（內部網路之虛擬 IP 位址為 10.20.4.55）。將上開電腦程式(即「cnginfo .exe」、「cngdisp.exe」、「cngdisp_new .exe」、「cleanup .bat」)存放在該伺服器內，以便日後開始進行盜領時，供附表一所示之第一銀行 ATM 得以連線至 NCR 伺服器後以 FTP（遠端檔案傳輸）方式加以下載。（五）上述入侵第一銀行倫敦分行電話錄音主機、電腦程式、入侵第一銀行 AP 伺服器並變更 ATM 電腦之電磁紀錄及入侵第一銀行 NCR 伺服器佈署上開電腦程式等前期工作完成後，該集團內負責至 ATM 盜領款項之車手暨車手頭共 15 人，即自 105 年 7 月 10 日凌晨起開始分組犯案，渠等利用手機通訊軟體通知上開集團內不詳成員，該不詳成員旋無故利用第一銀行倫敦分行電話錄音主機系統之漏洞，入侵第一銀行倫敦分行電話錄音主機，復以第一銀行倫敦分行電話錄音主機作為跳板，以 Telnet（遠端登錄服務）之方式與 ATM 電腦建立連線，並輸入事先已建立在 ATM 電腦上之管理者帳號「support_000000a0」暨密碼後，操控 ATM 之電腦，再由 ATM 之電腦上以 FTP（檔案傳輸服務）之方式，自 NCR 伺服器下載取得上開「cnginfo .exe」、「cngdisp .exe 」與「cngdisp_new .exe」、「cleanup .bat」之電腦程式，隨即執行「cnginfo .exe」之電腦程式確認 ATM 之吐鈔模組狀態，

再執行「cngdisp .exe」或「cngdisp_new .exe 」之電腦程式，無故干擾第一銀行之 ATM 電腦及 ATM 內之吐鈔模組之設備，使 ATM 在未經 ATM 電腦與第一銀行帳務系統連線稽核之狀況下，直接由 ATM 之吐鈔模組吐出上開程式所指定數額之現鈔，並由守候在各該 ATM 前之車手或車手頭取款，而以此等不正方式，自各該具有自動付款功能之 ATM 盜取金額，共計達新臺幣 8327 萬 7600 元。

臺北地方法院於民國 106 年 1 月 25 日，以 105 年度訴字第 426 號判決，判處 Peregudovs Andrejs、Colibaba Mihail、Pencov Nicolae 共同犯無故變更、刪除他人電腦之電磁紀錄罪，均處有期徒刑伍年，均併科罰金新臺幣陸拾萬元。該案上訴後，臺灣高等法院於民國 106 年 5 月 18 日將原判決撤銷，改判 Peregudovs Andrejs 共同犯無故變更、刪除他人電腦之電磁紀錄罪，處有期徒刑肆年拾月，併科罰金新台幣伍拾萬元，Colibaba Mihail 共同犯無故變更、刪除他人電腦之電磁紀錄罪，處有期徒刑肆年捌月，併科罰金新台幣肆拾萬元，Pencov Nicolae 共同犯無故變更、刪除他人電腦之電磁紀錄罪，處有期徒刑肆年陸月，其理由為：按刑事審判旨在實現刑罰權分配之正義，故事實審法院對於被告之量刑，應符合比例、平等及罪刑相當原則，使輕重得宜，罰當其罪。又法律上屬於自由裁量之事項，並非概無法律性之拘束。自由裁量係於法律一定之外部性界限內（以定執行刑言，即不得違反刑法第 51 條之規定）使法官具體選擇以為適當之處理；因此在裁量時，必須符合所適用之法規之目的。更進一步言，須受法律秩序之理念所指導，此即所謂之自由裁量之內部性界限。再者，刑之量定，為求個案裁判之妥當性，法律賦予法院裁量之權，於科刑時則應審酌刑法第 57 條所列各款情狀，分別情節，為被告量刑輕重之標準。本件尚無積極證據證明就被告 3 人就涉及之「跨國駭客盜領集團」案件，居於主導、指揮地位，是原審對此部分未詳予審酌，而遽判處被告三人刑法第 359 條法定最高之重刑，即有期徒刑 5 年，併科罰金 60 萬元，稍嫌過苛，難謂符合比例原則及平等原則，量刑有所失入，於罪刑相當原則亦屬有悖，當非法之持平，難謂允洽。被告 3 人此部分之指摘原審判決量刑不當，為有理由；故審酌被告 3 人均為外籍人士，與其他真實姓名、年籍均不詳具電腦專長之成員，組成「跨國駭客盜領集團」，共同基於意圖為自己不法所有，利用銀行電腦系統之漏洞，入侵銀行內部電腦網路，製作、存放盜領 ATM 款項之惡意電腦程式，變更、刪除他人電腦之電磁紀錄，遠端操控，以盜領 ATM 內款項之犯行，於短時間內盜領金額總計高達 8,327 萬 7,600 元，嚴重擾亂我國金融秩序，危害我國社會治安，且本件僅查獲 7,754 萬 5,100 元，仍有 573 萬 2,500 元之贓款尚未查獲，且查獲之鉅款，若非員警即時查獲，當可能以地下匯兌之方式流通國外，被告 3 人在集團內乃負責贓款處理之關鍵性角色，有嚴懲之必要，兼衡被告 3 人犯後均坦承搬運贓物，飾詞否認其餘犯行等一切情狀，就被告安德

魯部分量處有期徒刑 4 年 10 月，併科罰金 50 萬元，罰金如易服勞役，以 2,000 元折算一日；就被告米海爾部分量處有期徒刑 4 年 8 月，併科罰金 40 萬元，罰金如易服勞役，以 2,000 元折算一日；就被告潘可夫部分量處有期徒刑 4 年 6 月，併科罰金 30 萬元，罰金如易服勞役，以 2,000 元折算一日，以示懲儆。並於判決末之「建議」欄提出兩點：「（一）從速修法提高刑度補破網：網路犯罪日新月異，電影手法成現實；以刑法第 339 條之 2「以不正方法由自動付款設備取得他人之物」為例，法定刑只 3 年以下有期徒刑、拘役或 30 萬元以罰金，當時此類犯罪頂多提款卡盜領，誰會想到，現在遠端遙控讓 ATM 吐鈔。（二）網路犯罪無國界，司法互助有必要性：網路犯罪無國界，以本件第一銀行 ATM 盜領案為例，只起訴處理贓款的被告 3 人，對於多數已潛逃出境車手及隱身幕後主腦，無法有效追查，國際司法互助有其必要性。」

其後，被告三人與檢察官均就二審判決提出上訴，最高法院於民國 106 年 8 月 29 日駁回上訴，本案即告定讞[72]。此一判決顯示出我國司法實務面對跨國犯罪進行調查取證之窘境，以及現行法規存在之缺失。（詳後述第六章）

[72]檢察官提出上訴理由被告 3 人與其他盜領犯罪集團成員盜領第一銀行不同分行之 ATM 內之款項，係侵害第一銀行各分行實際管領該 ATM 之人，所侵害者應為不同財產法益之人，且本件遭盜領款項之地點，不僅分散在臺北市、新北市及臺中市等不同城市（分屬 22 家分行），即使在同一城市內，亦橫跨數個不同行政區，衡諸社會一般觀念，每組車手在同一分行所設置之 ATM 盜領款項完畢後，其盜領行為之目的即已滿足，行為結果亦已完成，各行為間之獨立性甚為明顯，自應分論併罰。原判決認定被告 3 人與其他盜領犯罪集團成員各次盜領 ATM 款項之行為，均為接續犯之一行為，而均各論以一罪，於法不合云云。然最高法院指出，證據之取捨、事實之認定及刑罰之裁量，均為事實審法院之職權，倘其採證認事並未違背證據法則，而所量之刑既未逾越法定刑度範圍，亦無顯然違背比例、公平及罪刑相當原則者，自不得任意指為違法而執為上訴第三審法院之適法理由，所謂接續犯，係指基於單一之犯意，以數個舉動接續進行而侵害同一法益，在時間及空間上有密切關係，依一般社會健全觀念，難以強行分開，在刑法評價上，以視為數個舉動之接續實行，合為包括之一行為予以評價，較為合理，於此情形，即得依接續犯論以包括一罪。原判決已敘明被告 3 人與其他盜領犯罪集團成員，共同意圖為自己不法所有，利用銀行電腦系統之漏洞，入侵銀行內部電腦網路，製作、存放盜領 ATM 款項之惡意電腦程式，變更、刪除他人電腦之電磁紀錄，遠端操控，以盜領第一銀行 ATM 之現鈔，係在密切接近之時間所為，侵害同一被害人即第一銀行之財產法益，依前開說明，其等各行為之獨立性極為薄弱，在刑法評價上，以視為數個舉動之接續施行，合為包括之一行為予以評價，較為合理等旨，而駁回檢察官之上訴。

第三章　電腦犯罪的司法管轄議題(jurisdiction)

第一節　概述

關於電腦犯罪的挑戰之一，即在於其能穿越實體的邊界（transcend physical borders），而對於司法實務而言，困難之處在於有關司法管轄權的法律仍傾向於以領土邊界（territorial borders）作為劃分基礎[73]，如何調和其間差異進行有效的證據調查與追訴，無疑是當務之急。

第二節　司法管轄權的基礎（The basis of Jurisdiction）

凡提及司法管轄權，第一個必須加以考量的問題是：一個國家在什麼情況下可以宣示其司法管轄權？在學理上，關於國家能否行使司法管轄權，有兩個主要的基礎:「境內管轄(territorial jurisdiction)」與「境外管轄(extraterritorial jurisdiction)」；不論就內國法或國際法論之，領土可謂係管轄權的核心[74]，領土管轄權即國家對犯罪行為擁有管轄權之範圍，因該犯罪行為發生在該國家的地理疆界之內。然而，一個國家亦有實行境外管轄權之情形，亦即使其本國法律適用於境外發生之犯罪行為，普遍為各國所採取的境外司法管轄權有四項根據：

一、普遍管轄（Universal Jurisdiction）：此一依據指可由任何國家實行管轄權，通常適用於重大犯行[75] ，其立基點在於有些行為是如此罪大惡極，因此任何國家都應該能夠加以追訴，而不須引渡（extradite）罪犯至其國籍所屬國家或犯罪行為發生地。

---

[73] Alisdair A. Gillespie *supra note* 6, at .21
[74] M. Hirst, *Jurisdiction and the Ambit of the Criminl Law*. (Oxford University Press, 2003),45.
[75] A. Aust, *Handbook of International Law*. (Cambridge University Press, 2005).,46

二、**保護原則**（Protective Principle）：保護原則允許國家尋求境外管轄權以確保國家安全或重要的國家利益[76]，此一原則可能與網路空間的某些行為態樣相關，因其可能擴及在軍事基礎建設或位於世界各地的政府情報據點（government listening outpost）所發生的網路攻擊。

三、**積極屬人原則**（Active personality principle)：此一原則是以犯罪行為人的國籍為基礎。

四、**消極屬人原則**（Passive personality principle）：此一原則係以被害人的國籍為基礎，在某些情況可能延伸適用於經常性居住（habitual residence）。

第三節　電腦犯罪領域司法管轄權的概念（Concept of Jurisdiction）

儘管各國可對電腦犯罪行為制定相關刑事法規，但如何針對可能發生於世界任何地方的犯罪行為人主張司法管轄權，實乃電腦犯罪與其他犯罪類型的主要差異所在。早期有學者認為網絡空間（cyberspace）是一個獨特的地方，超越了基於地理位置的傳統規則[77]。然而事實並非如此，論者有認為，各國現在一貫將傳統的以地域為基礎的規則應用於網路行為，並且原則上拒絕將網際網路視為權限範疇以外的領域[78]，在刑事法律中此一立場尤其鮮明，認為有必要將網際網路視為是其領土之延伸。刑事管轄權如何在域外行使？在探討此一問題前，必須先就管轄權之內涵予以釐清，其主要議題包括：

1、國家是否有立法權來規範相關行為（涉及「規定性管轄權(prescriptive jurisdiction)」之概念）？
2、法院是否有權審理特定爭議（涉及「判決管轄權(adjudicative jurisdiction)」之概念）？

---

[76] *Id*, at 45
[77] J. Clough, *supra note* 29, at 475.
[78] U. Kohl, *Jurisdiction and the internet: Regulatory competence over online activity* (Cambridge University Press, Cambridge, 2007), 11-12.

3、國家是否有管轄權來執行法律（涉及「執法管轄權(enforcement jurisdiction)」之概念）？

茲就上開管轄權的內涵在電腦犯罪領域之運用分敘如下：

第一項　規定性管轄權（Prescriptive jurisdiction）

「規定性管轄權」也被稱為「立法管轄權（legislative jurisdiction）」。網路犯罪公約第 22 條為確定管轄權制定了若干基礎，但不排除一國根據其國內法行使其他形式的管轄權[79]。第一種情形是犯罪行為發生在其領土內，體現了所謂的「屬地原則（the Principle of Territoriality）」[80]，這也是行使刑事司法管轄權最普遍的基礎。原則上，一個國家對其主權領土內發生的犯罪行為得行使司法管轄權，但有其例外情形可使領土原則擴及域外行為。

首先，一個國家可以對在該國旗幟的船舶或已登記的航空器上發生的行為行使領土管轄權。電腦犯罪公約就此亦有相關規範[81]，亦即將領土管轄權的範圍擴大及於不在有關國家的陸地管轄範圍之內的船舶或航空器。其次，「客觀屬地原則（the Principle of Objective Territoriality）」允許對在管轄範圍以外發生的犯罪行為主張具備刑事司法管轄權，網路犯罪公約基於保障被害人處於該刑事司法管轄權領域之情況而肯認之，在這種情況下可適用的較為狹義的原則即所謂「保護原則（the Protective Principle）」，此一原則適用於犯罪行為的目的損及該國的根本利益之情形[82]。

網路犯罪公約承認的規定性管轄權的另一個基礎是「國籍原則（the Nationality Principle）」，要求當事人對其國民犯下的罪行確立管轄權，而不論其

---

[79] Cybercrime Convention, Art.22(4): This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5 When more than one Party claims jurisd

[80] Cybercrime Convention, Art.22(1)(a): Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory;

[81] Cybercrime Convention Art.22(1)(b)-(c): Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: …(b) on board a ship flying the flag of that Party; or(c) on board an aircraft registered under the laws of that Party…

[82] J. Clough, *supra note* 29, at 477.

發生在世界何處[83]。在後述美國 CFAA 法案中可以找到另一個表達域外管轄權的例子。許多規定適用於「受保護的電腦（protected computer）[84]」，其定義為包括「用於或影響州際或外國商業或通信的電腦」，包括位於美國境外的電腦，其作用是對於州際或對外貿易或美國的通訊產生影響[85]。事實上，電腦甚至不需要位於美國境內，僅須連接到網際網路，即可能對美國州際或外國通訊產生影響，進一步言之，凡是可以在商務條款下管理的全世界所有電腦都是 18U.S.C§ 1030 所涵蓋的「受保護的電腦」[86]。

在美國此一聯邦國家中，刑事司法管轄權的聯繫可能是聯邦刑事司法管轄權的先決條件。例如，許多美國聯邦條款從「州際商業（interstate commerce）」權力中取得管轄權[87]。在電腦犯罪案例中，網際網路本身通常被視為是州際商業的工具，舉例言之，透過網路傳送照片的方式等同於在州際線路上移動照片，從而構成州際商業運輸，而由於網絡犯罪通常涉及電信網絡的使用，因此聯邦刑事管轄權的可能性大大增加[88]。

由實然面觀之，一個主權國家固可制定關於規定性管轄的相關法律，但能否針對所制定之法律具體裁判與執行，實屬二事。此一原則同樣適用於網路空間，在訴訟實務上，關於此議題的典型實例即為雅虎訴訟（Yahoo! litigation）案件，雅虎公司（Yahoo!）經營一個類似 eBay 的網路拍賣網站，來自世界各地的人們都可以加以利用，其中有些販售的品項包括納粹大事記（Nazi memorabilia）在有些國家是立法禁止販售的，兩個遊說團體 LICRA 及 UEJF 反對納粹大事記陳列在網站上，並要求法國的雅虎網站移除陳列乾等物品的網站超連結，·雅虎公司則主張法國法院對該等事項並無審判權，此一議題隨即進入巴黎地方法院（the Tribunal de Grande Instance de Paris）；法院認為法國對此確有審判權，並要求雅虎公司禁止法國人民得以取得該網站之連結，並要求法國雅虎公司的使用者被告知該等品項是違法的；雅虎公司提出上訴主張該等要求在技術上是不可行的，且將侵害該公司設立基準法之美國憲法第一修正案（the First Amendment to the U.S. Constitution）所保障之基本權利；然法國法院在 2000 年 11 月駁回雅虎公司的上

[83] Cybercrime Convention Art.22(1)(d): Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: …(d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
[84] 18 USC § 1030(a)(2)(C)(4), (5), (7).
[85] 18 USC § 1030(e)(2)(B)
[86] J. Clough, *supra note* 29, at 479
[87] US Const. Art. I, § 8, cl. 3.
[88] J. Clough, *supra note* 29, at 480

訴。其後，雅虎公司向美國地方法院（District Court）提出訴訟，認為法國法院的裁判因違反美國憲法第一修正案而不具有執行力。美國地方法院同意受理，然隨後因技術上的理由而為第九巡迴上訴法院逆轉[89]，但該逆轉並未使得上開命令具有執行力。該雅虎公司的訴訟為一民事訴訟，但卻顯露出一個事實——當法國法院聲稱要以特定方式實行其司法管轄權時，並無法在外國領域執行其裁判。刑事訴訟的程序同樣立基於相同原則，當一個國家可以運用司法管轄權時，原則上僅能用以確保其領域內所及之犯罪行為。

第二項　裁決管轄權（Adjudicative jurisdiction）

一旦規定性管轄權已確立，問題即在於特定的法院對具體案件是否具有裁決權力，或對爭訟之主要案件是否具有管轄權；其強調的重點在於該犯罪行為與該國家之間存有一個「真實而實質的聯繫（real and substantial link）」即為已足，此一檢驗在國際公法和國際法中是普遍適用的[90]。在前述 Yahoo!, Inc v.La Ligue Contre Le Racisme et L'Antisemitisme 案件中，法國法院要求雅虎公司採取一切必要措施，使法國使用者無法獲得與納粹有關的訊息，該等訊息在法國是非法的。最初的確認判決根據第一修正案的理由而予以批准，儘管該裁決隨後在上訴中被撤銷，但在該案例清楚地說明了真正的全球通訊媒介所呈現的緊張局勢；詳言之，在一方面，使用者享有其在原國籍地傳播合法訊息的自由。另一方面，目的國是否有權不容忍其被定義為非法的活動，僅僅是因為可能影響到在該活動合法國家中生活的人[91]？此種矛盾與衝突，實為跨國犯罪之追訴所面臨的難題。

根據網路犯罪公約，在這種情況下，各當事國家需要透過磋商方式，以確定最妥適的刑事司法管轄權[92]，這反映出國際上需要相互尊重，即相互尊重其他國家的主權，以及不對這些國家的內部事務進行不公正的干涉。國際法的一般要求是行使管轄權必須是合理的，因此，徵求意見的要求並不是絕對的。例如，如果一方確認另一方不會採取行動，或者磋商可能會妨礙調查或程序，則協商在該等情況下可能是不恰當的[93]。析言之，諸多因素可能影響司法管轄權之決定，包括

[89] 433 F.3d. 1199(9th Cir, 2006)
[90] J. Clough, *supra note* 29, at 481
[91] *Id*,at485
[92] Cybercrime Convention, Art.22(5): When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.
[93] J. Clough, *supra note* 29, at 485

罪犯的地點、犯罪人和受害人的國籍、造成的傷害程度、證據的位置和處罰的程度等。電腦犯罪與傳統犯罪決定司法管轄權之聯繫因素存有本質上差異，例如，在非電腦犯罪中，犯罪行為通常只在一個地方實施，而電腦犯罪可能涉及多個司法管轄區；同樣地，在非電腦犯罪中，受害人和犯罪人通常會在同一管轄範圍內，但電腦犯罪的情況並非如此，犯罪者的地點可能與犯罪地點的關係不大。實際上，這些問題通常由下述之「執法管轄權」來解決，特別是引渡法之規範。

第三項　執法管轄權（Enforcement jurisdiction）

即使同時存在「規定性管轄權」和「裁決性管轄權」，論其實際，強制執行的能力對司法管轄權構成了最重要的限制；一般而言，一個國家只能對在轄區內的人行使執行管轄權。而國際法上所稱「引渡」則係一國要求強迫遣返被指控或定罪的人在請求國受審或服刑的正式程序」，性質上可說是國際禮讓問題，而非國際法規定的義務問題，並且通常透過各國的雙邊條約和國內立法方式確立。基此立場，網路犯罪公約亦承認引渡或起訴的義務[94]。

引渡往往要求提出請求的一方和該人所在國家之間存在「雙重犯罪（dual criminality）」；換言之，根據兩個司法管轄區的法律，這種犯罪行為必須是最低刑罰。在「愛情病毒（Love Bug）」的案例中，貼切地說明了這一要求所提出的困難。該病毒於 2000 年首先在香港出現，然後迅速在全球蔓延，據估計，該病毒在當時影響了超過 4,500 萬用戶，包括美國航空航天局（NASA）和美國中央情報局（CIA）等政府機構在內的二十多個國家，據稱造成了數十億美元的損失；根據調查，雖然能夠確定必須負起責任者是菲律賓一名電腦科學學生，但由於缺乏前述雙重犯罪之規範，因此無法將該實際行為人引渡至美國進行懲罰[95]。

當可引渡罪行的數量相對較少時，引渡條約通常列舉可引渡的罪行；即使可引渡罪的數量增加，這一傳統仍存在。舉例來說，1976年澳大利亞與美國之間的條約規定了二十九種可引渡罪，但這種規範方法在出現新的犯罪時會遇到特別的困難，因傳統上列舉引渡之罪行甚少適用於電腦輔助犯罪類型，並且未包含以電腦為犯罪目標的行為。故在立法趨勢上，國際條約已經從「列舉式」轉變為「消

94 *Id*, at486
95 *Id*, at487

去法」。例如，前述「澳大利亞－美國條約（the Australia－US Treaty）」隨後進行了修訂，將可引渡的犯罪定義為「根據締約雙方法律，剝奪一年以上的自由或更嚴厲的懲罰刑罰」。此一做法雖較具實益，但仍需要考慮是否可以在每個司法管轄區發現相對應之法律；例如，網路賭博和仇恨言論是常見只在一司法管轄權區域為非法的行為，在此情形下即無法滿足「雙重犯罪」之要件。此外，即使在技術上可引渡，引渡過程的複雜性和成本也確保了它通常被用於嚴重犯罪[96]。

第四節　電腦犯罪之司法管轄權

網際網路對於管轄權會產生什麼影響？這可能是在對於網路空間進行規制時最具有爭論的議題之一；論者有主張網路空間是個獨特的架構，應以一個新的法律層面加以規範，然而，持相反意見者則認為網際網路並無特殊之處，其僅係伺服器與電腦連結而成存在於國家的實體網絡，伺服器與電腦必然物理性地存在於某處[97]。

詳言之，當網際網路開始發展時，論者有認為其所展現新面向無法為國家法律所適用，可謂係創造了新的世界秩序，網際網路被宣稱創造了自由的空間，此一觀點在最初甚至試圖與國家統治權的傳統規範脫離[98]。將網路空間歸類為一個新面向背後的基本原理在於網際網路與其他空間不同，網際網路的結構與其內容可被複製、儲存的本質，在現代通訊科技的速度下，意味著犯罪行為人取得一個在澳洲的檔案，與取得一個在美國雲端伺服器上的檔案是一樣容易的。事實上，網際網路、特別是雲端科技（cloud technology）的運作使得資料得以不固定存在於某一地點，而係散佈於數個位置。論者即有認為爭論國家法律是否適用於散佈於全球的此一架構是不實際的。地理上的疆界通常被設定為管轄權的界線，然有三個現存的國際領域是沒有任何國家得以實行管轄權的：南極洲（Antarctica）、公海（high seas）及外太空 (outer space)，在此領域僅得適用國際法。國際法得以適用於網際網路，意味著國家法律之間的差異將逐漸消失[99]。

---

[96] *Id*, at488

[97] Alisdair A. Gillespie *supra note* 6, at 25.

[98] J. Reidenberg, *Technology and internet jurisdiction*. (University of Pennsylvania Law Review, 2005), 153

[99] M. R. Rahman, Khan, M.A., Mohammad, N and Rahman, M.O., Cyberspace claiming new dynamism in the jurisprudential *International Journal of Law and Management.*, (2009), 274-290

然而，法律將如何適用並非如此清楚，國際刑事法律是與侵害人類法益相關，無法同等適用於網路犯罪。現在法律並非針對網路犯罪而制定，因而產生制定新法律的需求。理論上，可透國際條約將網際網路建立為一個新的國際領域，法律可將條約內容包括其內。然而，縱使如此，依然無法改變網路空間與其他空間不同的事實。上述南極洲、外太空與其他國家的領土互不干擾而存在於所有的疆界之外，網際網路隨著落腳於國家的伺服器而存在，因此，關於網際網路的國際領域，則要求國家必須出讓發生在其自身國家領域內的主權[100]。

第五節　電腦犯罪之國際合作

跨國電腦犯罪應如何加以制裁？論者有提議應擴大國際刑事法院（International Criminal Court，ICC）的管轄權，使其得以裁定網路犯罪議題[101]，然論者有認為，國際刑事法院設立宗旨為裁決侵害人權的犯罪，而非如網路犯罪相對低層次的犯罪[102]。又論其實際，世界各地每天有成千上萬的網路犯罪正在發生，對一個單一國際法院而言，針對為數眾多的網路犯罪實行管轄權是客觀上不可能的；此外，國際法院被認定為可以與犯罪行為發生所在國家同時管轄犯罪，現實上也是存在困難的，換言之，主權國家何以需交出其對網路犯罪的管轄權力？在多數情況下，相關證據係存在於國家領土疆界之內，因此，由國家法院管轄該等行為是較合乎邏輯的。在解釋上，若每個國家對於刑事法律採取一致的標準，將會是較為理想的狀態，其優點在於無需國際刑事法院介入，亦將無「宣稱司法管轄權（jurisdictional claims）」的問題出現[103]。

然而，在現實上，要求每一個國家同意相同的法規範是難以想像的，因不同的國家對於刑罰與何等行為屬違法行為均存有差異；舉例言之，關於著作權侵害（copyright infringement）與何種行為構成兒童色情（constitute child pornography）？在多數國家間即存在主要差異[104]。值得注意的是，承前所述，網路犯罪條約（Convention on Cybercrime）並未試圖將法律標準化，而係制定最低標準而留給

---

100 Alisdair A. Gillespie *supra note* 6, at 25

101 R. Rahman, Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. *Computer Law and Security Review.* (2012), 407

102 Alisdair A. Gillespie *supra note* 6, at 26

103 舉例而言，若有多數國家宣稱其對特定犯行具有管轄權，亦無必要將犯罪嫌疑人由 X 國引渡至 Y 國，因在兩個國家的法律規定均相同，意味著引渡本身並無意義。

104 Alisdair A. Gillespie *supra note* 6, at 27.

締約國自由裁量空間，雖然該公約並未獲得一致性的同意，因有許多國家不願簽字同意[105]，但誠如由該公約之規範目的旨在達成下列三個方向[106]：（一）協調國內刑事實體法網路犯罪行為之構成要件，以及連結網路犯罪領域內之各項協議；（二）提供國內刑事訴訟法必要的權力，以調查和起訴此類型犯罪，以及其他有關於電腦系統或具有電子證據形式之犯罪；（三）建立一個快速且有效的國際合作制度；此一具有的妥協內容代表一個全球化的條約是不切實際的，縱然在理論上具有吸引力，然終究無法在現實上實行[107]。網路犯罪公約第 22 條即是關於管轄權的規定，顯然其係以領土原則（territorial principle）作為預設立場。簡言之，網路犯罪公約第 22 條要求締約國就發生在其領土內的犯罪行為採取措施，並鼓勵國家將此擴及至船舶國旗（ships flagged）及註冊之航空器(aircraft registered)，除在本國管轄領域外，並在主動國籍原則（active personality principle）的基礎下考量境外管轄，但此為選擇性，而非締約國之義務[108]。

基此，國內法適用於網際網路世界是基本原則，但管轄權認定的困難該如何解消？即使我們接受國家具有規範網際網路的權力，仍無法否定所謂「網絡邊界交錯與跨越國家邊界」的問題； 基此，跨越國界的網路犯罪該如何加以處理呢？

網際網路可以跨越國界，此即跨越國界犯罪（cross-border crime）的議題，當一個犯罪跨越國家的數個邊界，意味著數個國家可能對該犯罪宣示管轄權。舉例來說，X國的居民A傳送病毒侵入位在Y國的居民B所使用的電腦，以及位於Z國居民C所使用的電腦，可以想見的是，X國Y國及Z國君可能宣示其管轄權，X國宣示管轄權的基礎在於該病毒係在其領土內所創造，且係透過其邊界傳送，Y國與Z國亦可能會主張因其領土內的電腦遭受影響而主張有領土管轄權[109]。學者 Podgor 指出，在此等跨國犯罪案件中，並無整合性的系統來決定何國具有管轄權，而前開網路犯罪公約亦未強調此一問題[110]；詳言之，依該公約第 22 條第 5 款規定，當發生爭議時，所涉及之相關當事國應以最適合進行追訴的觀點來決定管轄權所在，然並未敘明應考量的因素為何？可推測的是，這是採取實用主義的方法（pragmatic approach），因該公約的起草人了解到要使犯罪追訴發生達成一

105 R. Rahman, *supra note* 102,at 411.

106 參見 林元裕，檢視電腦犯罪之刑法規制－兼論歐洲理事會網路犯罪公約，國立中正大學法律學研究所碩士論文，民國 99 年 6 月，頁 126。

107 Alisdair A. Gillespie *supra note* 6, at 27

108 Cybercrime Convention, Art.22(2): Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

109 Alisdair A. Gillespie *supra note* 6, at 28

110 E. S. Podgor, Cybercrime: Discretionary jurisdiction. *University of Louisville Law Review* **47**, 727-738 (2009)Podgor, E.S. 'Cybercrime: Discretionary jurisdiction' (2009) ,733.

致共識是有困難的[111]。在此所應探討的，是「多重管轄（multiple jurisdiction）」而非「共同管轄（concurrent jurisdiction）」。

在大部分的法律體系，包括國際法在內，通常有「禁止雙重侵害原則（the principle of double jeopardy）」，亦即一個人不得因相同犯罪被重複處罰。然而，此一原則在上開案例是無法適用的，因A並非觸犯單一犯罪，而係分別在ＸＹＺ國犯罪，故無是否因相同侵害行為而重複處罰之問題，而係不同的數次侵害行為。

然而，一個犯罪行為人不可能同時接受三個國家審判，要如何決定追訴權發生的順序？或許最顯然的因素是何國家對該行為人得以進行拘留。管轄權不僅僅指涉哪一個國家可以宣示管轄權，亦與得否實行該管轄權有關。對於該犯罪行為人可以進行拘留的國家較容易實行管轄權。舉例言之，設若D是居住在英國威爾斯的國民，使用網路聊天室對居住在英國的居民Ｘ，以及居住在美國的Ｙ進行霸凌，Ｘ因承受嚴重的霸凌結果產生焦慮而就醫，Ｙ同樣承受相同影響而企圖自殺，但在死亡前被發現；就法律層面而言，犯罪行為人Ｄ應就其對Ｘ所為的行為受英國法制裁，並就其對Ｙ所為的犯行受美國法律制裁，英國是基於整個犯罪行為都是在其領域內發生的基礎宣示管轄權，美國則是基於犯罪結果發生地之基礎宣示管轄權；假使英國警方逮捕Ｄ，則英國極有可能決定先對Ｄ進行追訴，美國可能會爭執有一個更為嚴重的犯罪結果在其境內發生，但因美國現實上無法拘留Ｄ，無法進行追訴，除非英國決定引渡Ｄ，但其結果會造成實質上必須暫停其在英國境內的追訴；若該案例中兩國均對Ｄ無法進行拘留，情況會更複雜—設若Ｄ是德國人，且在德國境內進行網路霸凌行為，此時德國也可能宣示其有管轄權，而英國或美國更可能基於其國家的國民為被害人而宣示管轄權，然不論是美國或英國都無法現實拘留該名犯罪行為人，亦即無法立即進行追訴，而需仰賴德國引渡該名犯罪者。

此一「多重管轄」可能造成何國應放棄其司法管轄權、交出對行為人拘留權的爭論。在近幾年最具有爭議性的網路犯罪案例之一是 McKinnon v. United States[112]， Gary McKinnon 是一個在英國的蘇格蘭居民，他聲稱要尋找外國證據而駭入美國五角大廈系統（the US Pentagon system），美國當局宣稱其不僅檢視了機密文件，並且還刪除為數不少使美國防衛網絡無法運作的文件，McKinnon 雖否認有刪除任何文件的行為，但承認其駭客行為；美國政府尋求引渡使其面對

[111] Alisdair A. Gillespie *supra note* 6, at 29
[112] http://lexisweb.co.uk/cases/2008/july/mckinnon-v-government-of-the-united-states-of-america

各式與電腦犯罪相關的指控，McKinnon 則尋求避免遭引渡，最初甚至指控美國當局對其提出不正當施壓與程序濫用的認罪協商（plea bargain），其後法院決定 McKinnon 可被合法引渡至美國。

在此一案件中，英國及美國均宣稱其有管轄權，但問題在於何國可先行使？McKinnon 的支持者認為其應在英國受審判而非美國，最顯然的因素可說是英國可對其進行拘留，McKinnon 身處英國較易接受審判；然而，反駁此一論點者認為在英國境內並無任何電腦遭受損害，受損害的電腦係位於美國，在適法性的爭論上，美國對於追訴 McKinnon 有較強的基礎。英國與美國的檢察官討論渠等相互競爭管轄的論點，最後決定美國是最適合管轄該案件的國家，其理由在於[113]：

1. 損害係在美國境內發生；
2. 美國已開始調查程序；
3. 該案涉及許多相關證人，大部分居住於美國；
4. 所有的物證均在美國；
5. 美國檢察官可以針對 McKinnon 所涉及之犯行提起最大程度之控訴；
6. 大量未使用的證據位在美國境內。

由上開說明可知，電腦犯罪的司法管轄權在法律體系是個困難的議題，實務上常見「重複宣稱有管轄權（overlapping jurisdictional claims）」的問題，而或許以雙邊立場（on a bilateral basis）來尋求解決之道是較容易的。質言之，在管轄權的實行上，最為重要的議題在於確保行為人的拘留，大部分的國家在損害發生於領域內時，會宣稱其有管轄權，但若對行為人無現實上的拘留可能性，該管轄權的宣稱在某種程度上是沒有意義的[114]，如果全世界在關於電腦犯罪的面向上採取相同的法律標準，無疑會是較簡單的情況，但現實上不可能發生，國際條約、特別是全球性的條約，甚少提供足夠的細節來確保全球一致性，以國際刑事法院為例，針對戰犯的形式規定即無法達成全球一致的標準，電腦犯罪此一較為低層次，通常涉及言論或內容的犯罪，當然無從達成一致標準。職是，在此一範疇，引渡及確保嫌犯的拘留在管轄權的實踐上即屬重要。

[113] Alisdair A. Gillespie *supra note* 6, at 30
[114] *Id*, at 32

第四章　網路詐欺行為（Fraud online）

第一節　概述

網路詐欺行為可謂係電腦犯罪中最為常見且日益猖獗的類型，而談及「網路詐欺」，最具有象徵意義的網路詐欺案例即是所謂「奈及利亞詐欺（Nigerian mail fraud）」（又稱為「419 詐欺」），性質上是一種「預付費（advance fee）」詐欺，未經同意的訊息內容典型地要求接收者幫助訊息傳送者將一筆大數目的金錢非法地移到國外，為了達成此一目的，他們需要接收者的銀行帳戶資料明細，網際網路可以說是犯罪行為人尋找易受騙、貪婪的以及脆弱被害者的天堂；何以言之？首先，網際網路提供了通往無數被害者的途徑，舉例來說，奈及利亞電子郵件詐欺最初是透過傳統的信件方式進行，網際網路的來臨使行為者得以在虛擬世界毫不費力地接觸數以百萬的潛在被害者，可以接觸越來越多的人們，即意味著透過詐騙方式可以獲取的機會更大；其次，網際網路是一個巨大的市場，越來越多的網路使用者在網路上購買商品與服務，而使用網際網路進行轉帳亦成為趨勢；根據統計，在 2013 年，在美國有 61%的成年人透過使用網際網路方式處理金融事宜，在此同時，透過行動電話上網轉帳的比例也從 2011 年的 18%提高到 2013 年的 35%[115]。此一趨勢呈現出許多金錢在網路進行移轉，如比特幣（Bitcoin）之虛擬貨幣（virtual currencies）也成為詐欺犯罪移轉刑事所得的重要媒介。商業與金融領域網路交易的蓬勃發展提供了一個人們可能較疏於謹慎回應電子郵件或透過網站提出資訊的環境，也提供給詐欺犯偽裝成合法正當組織的機會；在網路環境中，我們常與向來會尋求的真實與信賴感脫離，而在網路交易中似是而非地存有一種助長詐欺的立即直接性，缺乏傳統的認證工具似乎未讓人們更加警惕，反而助長了信賴而非存疑的態度[116]。再者，網路提供了匿名性，行為者不僅僅可以隱藏其真實身份，也能夠採取使用替代身份的方式。此外，網路詐欺的多重司法管轄權本質（the multi-jurisdictional nature of online fraud）使調查與追訴變得更為困難，特別是涉及相對微小的數額，這就是所為的「微型詐欺（micro-frauds）」[117]，各該犯行所獲取的犯罪所得可能甚微，達到難以調查的程度，但對行為人來

---

115 J. Clough, *supra note* 29, at 210

116 E. Finch, 'The problem of stolen identity and the internet' in *Crime Online*, Y. a. Y. Jewkes, M, Ed. (Willan Publishing, 2007), 38.

117 D. S. Wall, *Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age*. T. H. a. B.

說，從來自數以千計的被害人所獲得的利益可能是極高的，在此等誘因下，與其他電腦犯罪的許多類型相同，詐欺犯罪不僅僅逐漸跨越國界，也逐漸邁向組織化[118]。

第二節　網路詐欺之類型

網路詐欺行為的態樣繁多，可大致區別為下列類型[119]：

第一項　網路銷售詐騙（Fraudulent sales online）

網路購物帶來極大的便利性，但對買賣雙方都存在著風險，賣方希望確認收款後再出貨，但買方希望在收到貨物後再付款，在網路交易方面往往需要更高的信賴：貨物必須事實上如所預定地送達，款項必須如期支付。在現實生活中，拍賣詐欺可說是網路詐欺最為常見的類型；由消費者的觀點來看，拍賣網站的風險在於事先支付款項，商品可能不會遞送，或可能會與廣告內容不同或品質低劣。另外的風險在於商品可能是竊盜所得，或是贗品。而由賣方的觀點來看，風險在於必須確認款項收取前遞送物品，這與非網路交易的情形相同，雖然第三方交易媒介（如 PayPal）機制逐漸興盛，但信用卡與借記卡（credit and debit cards）仍然是網路交易的主要機制，此等交易媒介即常成為網路銷售詐騙之對象。

第二項　預付費詐欺（Advance fee frauds）

最為常見的網路詐騙類型之一為「預付費詐欺」，被害人被說服在預期接受某些服務或利益時支付費用，但最後落空，如：快速致富機制（“get rich quick” scheme）、商業機會（business opportunities）、教育資格認證（educational qualifications）、

Schell, Ed., Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (Hershey: IGI Global, 2011), 69.

[118] R. G. Smith, in *Handbook of transnational crime and justice, 2nded*, P. R. a. J. Albanese, Ed. (California: Sage Publishing, 2014), vol. Ch7.

[119] J. Clough, *supra note* 29, at .212

樂透詐騙（lottery scams）以及財物顧問詐騙（financial advice scam）等，另有所謂「租賃詐騙（rental scam）」，是以在網路上廣告虛假的租賃物件，藉以獲取個人資料以及財務資訊（financial deposit）；近年來，主要的兩種詐欺類型則屬「約會詐欺（“dating”or“romance”scams）」以及「電腦支援中心詐欺（“computer support center”scams）」。

所謂的「約會詐欺」通常在合法約會網站或社群網站的聊天室（chat rooms）尋找被害人，透過使被害人相信其身處愛情關係中獲取利益與信任，一旦建立起信賴關係，即以各式各樣的藉口尋求金錢援助，在 2012 年，「網路犯罪投訴中心（the Internet Crime Complaint Center）」收到大約 4500 件約會詐騙的投訴，損失金額超過 5 千 5 百萬美金[120]；除了財務上的損失，被害人也可能暴露自身於遭到勒索的風險中，甚至危害人身安全。再者，所謂「電腦支援詐欺(Computer support scams)」則是指被害人接到聲稱來自知名軟體公司的電話，來電者給予被害人忠告，其內容為在他們的電腦內偵測到惡意程式，必須支付特定費用始能移除，被害者進而被導引到某個網站進行費用支付程序，除了被詐取金錢外，被害人也暴露在被惡意程式攻擊的風險中，如詐欺行為人可能取得對電腦的遠端控制途徑。而不論係何種預付費詐欺類型，均可能導致個人資訊的洩漏與財物損失。在某些案例中，被害人甚至可能被利用作為「錢騾（money mules，指非法財物運送者）」而協助非法洗錢，典型的例子就是宣稱可以「在家工作（work from home）」的電子郵件，被害人被要求提供銀行帳戶，進而被用來作為洗錢的工具。雖然這些非法財物的運送者也許會拿到一些佣金，他們還是可能會因協助犯罪而被控以反洗錢法等罪嫌[121]。

第三項　點擊詐欺（Click frauds）

另一網路詐欺的形式是所謂的「點擊詐欺」，這是利用線上廣告的費用通常是基於訪客瀏覽次數或是網站點擊次數來計算，網站所有者可能因此以僱用廉價勞力的方式增加所收取的費用，或是以自動化軟體虛增網站服務的使用者流量[122]，假網站（false website）也可能被用來吸引訪客，進而將訪客引導到客戶網站（client site），或在瀏覽時被一堆廣告所干擾。

---

120 I. C. C. Center, "Internet crime report 2012," (2012), 16

121 J. Clough, *supra note* 29, at 215

122 AAustralian High Tech Crime Centre, *Money mules*, High Tech Crime Brief No. 16(AIC, 2007), 2.

舉例來說，在 Facebook, Inc. v. MaxBounty, Inc.,一案[123]中，Facebook 聲稱 MaxBounty 使用其附屬公司創造了虛假的臉書網頁，進而達到將臉書使用者引導連結到第三個商業性網站的目的。這些網頁可能使用「限時優惠（limited time offers）」的廣告來吸引註冊者，例如禮物卡或是如平板電腦的科技產品等優惠；一旦註冊之後，使用者可能被導引到第三方的商業性網站，進而被要求必須完成更多步驟才能得到該優惠，據稱 MaxBounty 可以透過其導引到第三方網站的流量得到報酬，此即點擊詐欺之適例。

第四項　電子金融轉帳犯罪（Electronic funds transfer crime）

在財產犯罪領域，實體金錢的竊盜案件固然始終存在，但今日，大部分的金錢都是以無形的形式存在，與實體貨幣最大之不同點在於，虛擬現金得以大量被移轉，可能跨越不同司法管轄權而較不易立即被察覺，駭客可能自外部取得未經授權的機會，或內部人逾越權限而達成此一目的。隨著網路金融的盛行，其也成為具有犯罪吸引力的目標，因在竊取者與資金間僅有使用者名稱與密碼，此即電子金融轉帳犯罪日益興盛之緣故。前述我國「一銀 ATM 盜領案」即屬此一類型之詐欺犯罪。。

第五項　詐欺性投資（Fraudulent investments）

網際網路提供了散播詐欺投資機會的絕佳機會，毫無疑問的，對於犯罪行為人而言，透過架設一個看起來可信真實的網站，承諾高投資報酬率並誘惑投資的網站是輕而易舉的；再者，由於許多人在網路世界尋求投資機會，關於詐欺性投資的資訊得以極為快速地散布。此種詐欺性投資的適例如：使用網路散布資訊達到影響股價的目的，這就是所謂的「哄抬股價（pump and dump/trash and cash）詐騙機制」，這可以包括簡單地在網路論壇中談論股價的漲跌，或較嚴重地在媒體上釋放假消息[124]。

---

[123] 274 FRD 279(ND Cal. 2011)

[124] S. Morris, "The future of netcrime now: Part 1-threats and challenges," *Home Office Online Report*

第三節　特殊態樣之網路詐欺模式

第一項　網路釣魚（Phishing）

所謂「網路釣魚」是科技發展與社交工程（social engineering）的綜合性產物，可廣泛性地定義為「犯罪行為人透過電子郵件與網站的創造與使用，企圖蒐集個人性,財務及敏感性資訊[125]，典型的網路釣魚是從看似正當的網站（如銀行網站）寄送，並要求收件者對於其帳戶資料進行認證；舉例言之，通常會聲稱帳戶遭盜用，銀行必須確認其安全性細節，收件者容易受詐騙而提供相關資訊，該等資訊即被用來進行身份犯罪。

另外，所謂「針對性網路釣魚（Spear phishing）」一詞被用來描述針對特定人或團體的網路釣魚攻擊[126]，舉例來說，臉書與 LinkedIn 等社群網站是個人資訊豐富的源頭所在，可能被用以作為針對特定個人或組織傳送看似更可信網路釣魚訊息的媒介。網路釣魚多被用在獲取金融財務資訊，也可能被用來蒐集對於犯罪行為人有用的帳戶資訊，透過網路釣魚郵件獲取個人資訊的方式有許多種，最單純的態樣是要求收件人立即回應，例如：電子郵件可能附加顯示來自稅務單位的檔案，要求收件人必須填寫其資料並在七天內寄回，否則即無法獲得相關租稅優惠[127]，網路銷售詐欺也可能使用此一計謀來誘使消費者提供帳戶資訊。較為複雜的態樣則是提供一個複製合法單位的假網站連結，通常使用偽造的網域名稱，進而獲取使用者的個人資訊。除了複製商業性與財務機構的網站外，詐欺行為人亦逐漸利用社群媒體網站，例如在臉書上張貼提供免費禮物卡得文章，被害人進而會被導引到假網站並被要求必須提供個人資訊始能獲得優惠。另外一個態樣則是在郵件中合併使用連結或附件，一旦點閱即會下載如鍵盤記錄（keyloggers）或木馬程式（Trojan）等惡意監控軟體。

No. 4 (Home Office, 2004), 17

125 Binational Working Group on Cross-Border Mass Marketing Fraud, *Report on Phishing: A report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States*(2006), 4.

126 *Id*, at 8-9

127 F. Paget, Identity Theft, White Paper(McAfee, 2007), 8.

第二項　網址嫁接（Pharming）

除了以電子郵件或其他網路通訊形式誘使使用者連結至釣魚網站外，亦有其他態樣，例如：網站的網域名稱可能是常見正當網站的錯誤拼法，或不同的網域名稱（如以”com”代替”org”），使得使用者誤會而連結至假網站。更為複雜的態樣即是所謂的「網址嫁接（pharming）」。

所謂的「網址嫁接」性質上是一種重新導向的詐騙技巧，由網路釣魚衍生而來，藉由入侵使用者電腦植入木馬程式（Trojan），或是利用域名伺服器（Domain Name Server， DNS Server）的漏洞，將使用者錯誤地引導到偽造的網站，進而伺機竊取重要資料。當使用者在瀏覽器輸入一個文字的網址時（例如：www.google.com），會被轉換成一連串數字的位置（例如：74.125.198.94），這就是所謂的「DNS 轉譯」，由 DNS 伺服器達成此服務。萬一這個 DNS 伺服器上面的檔案被修改時，當使用者輸入一個金融網站的網址，卻被導向一個惡意的釣魚網站，且該釣魚網站完全仿冒得跟正牌網站一致，導致使用者以為是原本的網站，進而輸入個人的機密資料。要修改 DNS 伺服器上面的檔案也許不容易，但修改電腦裡面的 DNS 快取檔案就相對簡單多了，木馬程式即可以做到這樣的效果。更狡猾的是，這些木馬程式還會等使用者先造訪過正牌網站後，才跳出來要求使用者輸入機密資料的對話視窗，並將使用者輸入的資料傳送到惡意的駭客手中，類似的事件發生於 2006 年的美國運通網站上[128]，駭客透過讓域名伺服器（DNS）中毒，而將本來應導向 ABC、American Express、 Citi and Verizon Wireless 等一千多個網站的查詢，轉向偽裝的假主機[129]。

第三項　側錄信用卡（Credit card skimming）

側錄信用卡是正常使用的信用卡遭到非法地攔截或複製，通常是透過電子化方式為之[130]，此一技術是利用在許多信用卡、儲金卡及其他交易卡片上磁條科技

[128] J. Clough, *supra note* 29, at .224
[129] https://www.networkworld.com/article/2313049/lan-wan/how-to-prevent-pharming.html
[130] Model Criminal Code Officers Committee, *Model Criminal Code: Chapter 3, Credit card skimming*

的弱點，由於允許快速容易地將卡片資料程式化，同時意味著該等資料也可以容易地被複製；除了常見的信用卡側錄外，該技術也適用於以磁條儲存資料的任何卡片。遭側錄的資料也可能被傳送到海外並製作偽卡，因此，即使在引進晶片認證技術以提高安全性的司法管轄地區，也可能在沒有這些技術的國家生產複製卡。再者，在海外使用卡片也可能使詐欺的偵測及報告延誤，進而使相關調查的困難度提高[131]。

第四項　身份盜用（Identity Theft）

在現代社會生活中，人們常常需要證明自己的身份以出入工作場所、使用信用卡購物或出示駕照等，當犯罪行為人得以偽裝成他人身份，即可能取得原本不應享有的權利，此種使用虛偽身份進行犯罪的類型泛稱為「身份犯罪（identity crime）」，可謂係詐欺行為之特殊態樣之一。

關於「身份犯罪」此一概念並無單一的定義性內涵，亦有稱之為「身份詐欺（identity fraud）」或「身份盜用（identity theft）」；若細究其概念差異，所稱「身份犯罪（identity crime）」是用來指被告使用假身份進行犯罪的普遍通稱，可能包括洗錢、運輸毒品、逃漏稅、非法移民或恐怖主義，也可能包括較為輕微的犯罪，例如未成年人使用假證件購買含酒精飲料；而「身份詐欺（identity fraud）」是較為特定的身份犯罪類型，在此一類型中，假身份被用來獲取金錢、貨物 、利益或服務；至於「身份竊取（identity theft）」則是使用既存的個體身份[132]。析言之，身份犯罪與身份詐欺的是透過使用假身份進行現存犯罪行為，執法機關通常著重主要犯罪類型的追訴而忽略針對個人身份的冒用，數位科技的發展無疑有助於以假身份遂行犯罪，但目前法律的缺陷在於無法針對身份盜用的初步行為進行處罰[133]。此為與「身份竊盜」此一用語的區別實益所在。

然而，論其實際，「身份盜竊」一詞是有問題的，原因有很多。首先，該人的身份不是「被盜」的，而係這種身份的某些方面被犯罪分子所利用，通常是為

---

offences, Final Report(2006), 1.

131 *Id*, at 5.

132 Australasian Centre for Policing Research and the Australian Transaction Reports and Analysis Centre, Standardisation of definitions of identity crime terms: A step towards consistency, Report Series No. 145.3(Australasian Centre for Policing Research, 2006),9-10.

133 Model Criminal Code Officers Committee, *Identity Crime*, Final Report(2008), 12.

了犯下另一種罪行。其次,「身份盜用」通常用來指那些現有身份被盜用的情況。然而,「虛假身份」的使用還可能包括創建虛假身份(「身份構造(identity fabrication)」或改變現有身份(「身份操縱(identity manipulation)」)[134]。

在對「身份盜用」科以刑事責任時,首先需要針對「身份」一詞進行明確定義,論者有認為,法律身份關心的不是涉及到一個人的自我意識的內在化的身份觀點,亦非關於一個人被他人看待的方式的外部觀點,而是關於透過資訊累積使得該個人得以與其他人加以區辨的方式[135]。此一識別過程可被描述為「數據與特定人之間的關聯」,這通常是由一個人展示他們知道的東西來完成的,例如密碼;或是呈現他們擁有的東西,比如駕駛執照;或者通過展示身體特徵,如指紋;雖然我們的身份證明可以通過多種方式進行驗證,但是可以用於此目的的信息基本上屬於三類之一[136]:

1、生物特徵識別(biometric identity):個體特有的物理特徵,如指紋、聲音、DNA特徵、視網膜等;
2、歸屬身份(attributed identity):我們在出生時獲得的身份方面,如姓名、出生日期和地點、父母的姓名和地址;;
3、傳記身份(biographical identity):我們隨著時間的推移獲得的各種身份,包括:資歷、工作經歷、執照、護照、銀行帳戶等。

在此一分類下,為了實施身份盜竊,違法者需要獲取或偽造身份資訊。基於文件及資訊可能被盜、非法購買或偽造的可能性,歸屬身份和個人身份識別是最容易被盜用的。因此,大多關於身份盜竊都是圍繞著「身份文件檔案」和「身份資訊」的概念。

對於犯罪行為人而言,數位科技使得獲得身份資訊更為便利,社群網站的使用有助於詐欺犯罪行為人獲取潛在被害人的特定資訊,許多預付費用機制的科技也要求接收者提出個人資訊,身份犯罪最主要的元素—偽造—也透過數位科技而轉變,隨著桌面排版(desktop publishing)、影像軟體(imaging software)與彩色掃瞄便捷快速的時代來臨,對於犯罪行為人來說,可以十分容易地偽造虛偽的身份證明文件,此種特殊態樣之詐欺類型,亦朝向日漸興盛之途。

---

134 J. Clough, *supra note* 29, at 240
135 E. Finch, The problem of stolen identity and the internet. *Crime online*, (2007),30.
136 J. Clough, *supra note* 29, at 242

第四節　網路詐欺犯罪行為之規模

網路詐欺的精確規模是難以估量的，其理由繁多，首先，關於定義的爭議使得精確的紀錄成為問題，「詐欺」一詞本身即難以定義，雲端科技的發展使得此一問題更為困難；舉例言之，關於付款方式的詐（(payment card fraud)究應歸類於身份盜用或應被通稱為「詐欺」即存有爭論[137]，在相關的犯罪統計上，調查詢問受訪者關於「身份詐欺」的問題可能存在問題，因該用語涉及不確定法律概念，且可能與其他形式的詐欺行為重疊[138]。其次，關於犯罪統計的紀錄通常未對違犯方式加以區別；再者，相關調查常是以被害人的反應作為基礎，而非以真正的犯罪統計。此外，網路詐欺的實際程度往往未被報導，這是因爲有些「被害人」對於自身處境渾然不知，而有些被害人不願提及此一負面經驗，特別是商業性組織擔憂失去消費者的信心，常常不願意公開遭詐欺的事實[139]，此等原因均使網路詐欺的數量難以精確計算。

第五章　跨境電腦犯罪之追訴

第一節　網路犯罪公約（the Convention of Cybercrime）

電腦犯罪無國界，而國際間關於網路犯罪之法律規制，即屬2001年11月由歐洲理事會的26個歐盟成員國以及美國、加拿大、日本和南非等30個國家的政府官員在布達佩斯所共同簽訂的國際公約—「網路犯罪公約（the Convention of

[137] Canadian Internet Policy and Public Interest Clinic, Identity theft: Introduction and background, CIPPIC Working Paper No.1, ID Theft Series(2007), 1

[138] M. McGuire and S. Dowling, Cyber crime: A review of the evidence, *Research Report No. Chpt2* (Home Office, 2013),8.

[139] J. Clough, *supra note* 29, at 229

Cybercrime）」。事實上，經濟合作暨發展組織（Organization for Economic Co-operation and Development，OECD）自1983年起即著手進行關於網路犯罪之立法研究，對各國網路犯罪之立法進行分析比較，同時評估提出國際統一立法之可能性，於1986年發表了「電腦有關犯罪:法律政策分析」之報告，其主要內容在於針對各國共通之網路犯罪類型（如:詐欺、偽造、修改電腦程式或資料、未經授權進入電腦、侵害著作權、竊取營業秘密等）均應施以刑事制裁；其後，歐洲理事會於1989年發表 No. R.(89)9 電腦犯罪相關建議[140]，繼於1996年設立研究網路犯罪之專家委員會，並於1997年4月設立「網路空間犯罪專家委員會(Committee of Experts on Crime in Cyber-space)，負責研擬網路犯罪公約，並於2000年12月31日完成初稿，稱為「歐洲理事會網路犯罪公約草案」經歐洲理事會通過後，「網路犯罪公約」成為全世界第一部針對網路犯罪行為所制訂的國際公約。而「網路犯罪公約」制定的目標之一，旨在期望使國際間對於網路犯罪的立法有一致共同的參考標準，同時希望國際間在進行網路犯罪 偵查時有一個國際公約可供遵循、支持，而得以有效進行國際合作。

網路犯罪公約代表國際間對於網路犯罪問題廣泛的回應。該公約序言內容說明「網路犯罪公約」的功能、目標[141]，本文區分為四章，涵蓋實體法與程序法，第一章為定義性規範（Use of terms），說明公約內相關術語之使用內容，亦即對網路犯罪涉及的術語進行名詞定義，包括：（1）電腦系統：係指任何設備或一組或多組相互連結或相關連的設備，按照電腦程式執行數據之自動處理[142]；（2）電腦數據：指將任何事實、資訊或概念之表示於電腦系統中，依適當之形式進行處理，包括適當的電腦程式，俾利電腦系統執行功能[143]；(3)服務提供者：指任何

[140]Recommendation No. R.(89)9 of the Committee of Ministers to Member States on Computer-related Crime.

[141]網路犯罪公約的前言旨在闡述該公約之宗旨，包括以下 8 點:(1)網路犯罪公約之會員國均須慮及歐洲理事會之目標在於達成會國國間之一致和諧;(2)網路犯罪公約之會員國均承認與該公約非歐洲理事會會員國合作之價值;(3)網路犯罪公約會員國均認可追求打擊網路犯罪、保護社會共通犯罪政策之要求，尤指透過適當立法與國際合作之進行;(4)網路犯罪公約會員國均意識到電腦網路數位化、匯流化與全球化之深遠影響;(5)網路犯罪公約會員國均關注電腦網路與電子資訊可能被利用於犯罪之風險，同時關於該等犯罪之證據可能會被儲存或傳輸於電腦網絡當中;(6)網路犯罪公約之會員國認可會員國與私人企業合作共同打擊網路犯罪之必要性，以及保護使用、發展資訊科技之正當利益需求性;(7)網路犯罪公約會員國均相信有效打擊網路犯罪將有賴持續增加、快速及運作良好之國際合作模式;(8)網路犯罪公約會員國均確認該公約旨在制止破壞、濫用電腦系統、網際網路，以及資料之保密性、完整性與可使用性之必要，該制止係藉由將侵入行為予以犯罪化，同時加強國內外偵查、起訴之權限，期以有效打擊網路犯罪，進而提供快速、可靠的國際合作協議供遵循。參見 Cybercrime Convention, supra note 1, pmbl ; See also Jay Fisher, The Draft Convention on Cybercrime: Potential Constitutional Conflicts, 32 UWLAL. REV. 339, 343-44(2001)

[142] "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.

[143] "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.

公共或私有之實體提供給用戶具備通訊能力電腦之服務，以及任何其他實體代理此類通訊服務或此類服務之使用者為電腦數據之處理或儲存者[144]；(4)數據傳輸：指任何電腦系統用以通訊之電腦數據，由電腦系統產生以片段之方式形成通訊鍊，指引通訊之來源、目的地、路徑、時間、日期、大小、持續期間，或其下位服務之型態[145]。

網路犯罪公約第二章為關於國家層級必須採取的措施（Measures to be taken at the national level），又細分為第一節「刑事實體法（Substantive criminal law）」、第二節「刑事程序法」與第三節「管轄權」三個部分，實體刑事法部分為要求各簽約國於各國國內應採取的措施，程序法部分則是規定有關電子證據調查的特殊程序法制度；值得注意者為，在規範非法擷取 (Illegal access)的行為方面，「網路犯罪公約」要求各國應立法明定非法擷取為犯罪行為並應予處罰。第三章為國際合作章節，包括一般原則和特殊規定兩個部分，在一般原則中包含規範引渡及相互合作等相關問題，而特殊規定則係有關電腦證據取得的問題，其規定簽約國應建立一周七天且一天二十四小時皆能聯絡合作機制的網路[146]，各國也要對於相關人員加強訓練，並配給必要的裝備以配合各國合作事項的進行；第四章為「最後條款」，主要規定該公約的簽訂、生效、加入、區域應用、公約的效力、聲明、聯邦條款、保留、保留的法律地位和撤回、修訂、爭端處理、締約方大會、公約的退出和通告等程序性事項。

在刑事實體法的規範中，電腦犯罪公約主要規範四種類型的犯罪行為，第一種犯罪類型規範在第一條，即妨害電腦資料檔案與電腦系統之機密性、完整性與

---

144 "service provider" means : (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

145 "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

146 Article35: Each Party shall designate a point of contact available on a twenty-four hour, seven-daya-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice;b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

可使用性之犯罪[147]，該等犯罪行為是發生於電腦中，或係以電腦資料作為犯罪行為之目標，進一步可再區分為下述三種態樣：

一、 非法接觸存取（Illegal access）[148]

二、 非法擷取或干擾數據資料、系統

1. 非法擷取(illegal interception)[149]： 攔截資訊在最近幾年受到許多關注，政府部門攔截資訊也屬此範疇之議題，本規定特別強調資訊之攔截，其目的是為了保護通訊的隱私[150]。
2. 干擾數據資料(Data interference)[151]
3. 干擾系統（System interference[152]）

三、 濫用裝置（misuse of devices）[153]

---

147 Offenses against the confidentiality, integrity and availability of computer data and systems

148 Article2: Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed internationally, the access to the whole or any part of a computer system without right. A party may require that the offences be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

149 Aricle3: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system

150 Clough, J. *Principles of Cybercrime*(2010, Cambridge University Press)p.137

151 Article 4: 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

152 Article 5: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

153 Article 6: 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in

其次，在「與電腦相關的犯罪行為（Computer-related Offences）」方面，指的是電腦被用以作為促成犯罪結果的所有犯罪行為，雖然在現實上可能涵蓋大範圍的犯罪行為，但在電腦犯罪公約中僅將之區分為兩個類型，即「使用電腦相關的偽造（computer-related forgery）[154]與「使用電腦相關的詐欺行為（computer-related fraud）[155]。而在與內容相關的犯罪行為（content-related offences）方面，大部分著重於兒童色情（child pornography）之典型類型[156]。最後，則涉及與著作權侵害及其相關權利有關的犯罪行為（Offences related to infringements of copyright and related rights）[157]。此等犯罪行為之列舉明文，可謂係國際間對於網路犯罪問題之共識所在。

---

paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

[154] Article 7: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

[155] Article 8: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

[156] Article 9: 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:
a a minor engaged in sexually explicit conduct;
b a person appearing to be a minor engaged in sexually explicit conduct;
c realistic images representing a minor engaged in sexually explicit conduct. 3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d. and e, and 2, sub-paragraphs b. and c.

[157] Article 10: 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the

茲加以說明者，乃網路犯罪公約關於詐欺行為之規範；詐欺的預防涉及複雜的面向，網路犯罪公約第 8 條[158]即指出：「各參與本公約之成員國應採取下列內容作為相關必要的立法及其他措施，以對犯罪行為進行懲罰，並作為建立其內國法之參考，當其係非法存取全部或一部之電腦系統，且係以故意或無權方式為之，並具備為自己或他人無權取得之經濟利益意圖而有詐欺或以不正方式獲取之故意，其行為係以下述方式造成他人財產損害：

（1）任何『輸入』、『修改』、『刪除』或『去連結化[159]』電腦數據之方式、

（2）任何「干擾電腦系統功能」之行為。」

此一規定之規範目的主要針對資料的輸入或修改，以及針對意圖造成財產非法移轉，進而在資料傳輸過程中不正操控之行為予以犯罪化，第一部分涉及數據的任何「輸入、修改、刪除或者去連結化」，這一規定旨在擴展到廣泛的行為範圍，包括任何「干涉電腦程序或系統的功能」，亦即涵蓋硬體操控、抑制、打印輸出和影響數據記錄、傳輸的行為，或程序運行的順序[160]。

---

infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

[158] each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

(a) any input, alteration, deletion or suppression of computer data;

(b) any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

[159]此處之原文為"suppression"，關於"data suppression"係指"the process of withholding or removing selected information—most commonly in public reports and debates—to protect the identities, privacy, and personal information of individual students, teachers, or administrators. Data suppression is used whenever there is chance that the information contained in a publicly available report could be used to reveal or infer the identities of specific individuals.（see：https://www.edglossary.org/data-suppression/）基此意涵，本文參考「人體生物資料庫管理條例」第 3 條第 7 款規定「指於生物檢體、資料、資訊編碼後，使其與可供辨識參與者之個人資料、資訊，永久無法以任何方式連結、比對之作業。」故將該用語翻譯為「去連結化」。

[160] J. Clough, *supra note* 29, at 232

所稱「財產損害」的範疇廣泛，包括有形和無形財產的損失；詳言之，除包括從事相關行為的意圖，也包括具體的詐欺意圖，目的是允許未經授權使用網路取得軟體以獲得有關競爭對手的資訊，雖然這可能會造成經濟損失，但並非條文所述係基於以不誠實的意圖為之。

此等犯罪行為通常出現在電腦不正使用的規定中，其中大多處罰基於詐欺的意圖而取得或修改相關數據的情形。更為典型的是，網路詐欺通常在一般詐欺行為類型下進行追訴，以及任何一種特定的犯罪行為，包括偽造、虛假聲明以及交易護照和信用卡號碼等具體資訊。例如，在美國，據估計，「身份盜用罪防制法（the Identity Theft and Assumption Deterrence Act）」涵蓋的行為也可能規範在其他約 180 個聯邦刑事法規[161]。對於立法者而言，考慮將傳統詐欺條款應用於網路環境中出現的一些具體挑戰，可謂係有助益的方向。

以資金的流轉為例，數位形式的金錢流動可能對最初在有形商品背景下設想的犯罪構成挑戰。雖然這種犯罪行為通常適用於對於無形財產的侵害，但其他犯罪要素也必須予以考慮。例如，向來認為收到電子資金會構成基於竊盜意圖而獲取資金，同樣地，在美國一直認為電子轉移資金構成電匯詐欺法規的中的「運輸」[162]。其次，關於詐欺行為之犯罪構成要件之一為「被害人受詐欺」，而在許多電子詐欺的案例中，被告會輸入未經授權使用的資料，藉以獲取不屬於其自身的財產，舉例來說，在自動提款機使用竊取而來的 PIN 碼，或是在網路交易中使用盜取而來的信用卡號碼，在此種案例中，交易並非透過個人進行，而係電腦處理數字的過程，確認其正確性及認可其請求，設若欺騙是指控詐欺的核心，電腦是否有被詐騙之可能呢？論其實際，詐欺的本質包括被害人「相信假的東西是真的」，且實施詐欺者明知或相信其為虛假，因此，在技術層面，電腦本身不可能遭到詐欺，因電腦僅係單純就所提供的指示做出回應[163]。基此電腦犯罪之特質，有些法律將其詐欺之定義規定為「某人未經授權之行為，致使電腦、機器或電子設施做出回應[164]。

而在與電腦相關的偽造行為（Computer-related forgery）方面，偽造文件的製作向來是身份犯罪的主要內容；然而，傳統關於偽造的概念是以具體形式進行偽

---

161 J. Lynch, Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks. *Berkeley Technology Law Journal* **20**, (2005) ,259-294

162 18 USC$2314. It has been held that computer time is a 'thing of value' for the purposes of this Act: *US v. Seidlitz*, 589 F 2d 152 at 160(4th Cir. 1978)

163 J. Clough, *supra note* 29, at 235

164 'conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorized to cause it to do.' See s. 480.1(1)Criminal Code(Cth)

造文書，而未慮及如在網站上竄改電子數計或產生虛假的電子文件檔案[165]，網路犯罪公約第 7 條針對此一問題規定如下：「各該參與本公約之成員國家應可採取下列作為相關立法考量或其他措施，以對犯罪行為進行處罰並作為內國法規制之之參考，當其係以故意或未經授權的方式非法存取全部或一部之電腦系統行為，並使用「輸入」、「修改」、「刪除」或「去連結化」電腦數據資料之方式導致產生可理解為如具備可信性之法律意義，或效力不真實之數據資料，不問該等數據資料是否可讀取或可理解。」[166]

在施加刑事責任之前，當事人必須是具備詐欺或類似的不誠實的意圖， 此一規定的目的是為偽造有形文件創造相類的犯罪行為，其重點在於在合法交易過程中可能依賴的儲存數據的創建或修改。條文所稱未經授權「輸入（input）」正確或不正確的數據會導致與製作偽造文件相對應的情況，隨後的變更（修改、變化、部分變更），刪除（從數據介質中刪除數據）和去連結化（扣回、隱藏數據）通常與偽造真實文件相互對應。與電腦詐欺相關的案例一樣，這種行為可以為電腦不正使用的侵害行為所涵蓋，其處罰範圍包括針對數據的取得或修改，從而實施進一步的違法行為[167]。

網路犯罪公約第三章章名為「國際合作（International cooperation）」，第一部分為一般性原則（General principles），其中第 23 條係關於國際合作一般性原則之規定，其內容為：「各方應根據本章的規定並通過適用有關刑事事項國際合作的國際文書，在統一或相互立法的基礎上進行磋商，期使國內法得以被廣泛地運用於與電腦和數據有關的刑事犯罪之調查或訴訟，或蒐集電子形式的刑事犯罪證據。」[168]。而在引渡規範上，公約第 24 條第 1 項指出，該規定適用於締約方之間對刑事犯罪的引渡，依本公約第 2 條至第 11 條所定之雙方的法律，透過剝奪犯罪行為人最高限度為一年的有期徒刑，或受到更嚴厲的懲罰[169]，且根據約定

---

[165] Model Criminal Law Officers Committee, *Identity crime*(2008), p.15.

[166]each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

[167] J. Clough, *supra note* 29, at 237

[168]Article 23 – General principles relating to international co-operation
The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence

[169]This article applies to extradition between Parties for the criminal offences established in accordance

的安排適用不同的規範，其依據可為統一或相互的立法或引渡條約，包括歐洲引渡公約（ETS 第 24 號）在內，適用於兩國之間或更多的締約方，此等規範即屬最低刑罰或條約適用[170]。本條第 1 款所述的刑事犯罪應被視為在各締約方之間，或任何締約方之間存在的任何引渡條約中被列為可引渡的犯罪。雙方承諾在任何引渡條約之間締結可引渡的罪行等犯罪[171]。如果以訂有條約為引渡條件的締約方收到未與其訂有引渡條約的另一締約國的引渡請求，則可依據本文之規定，將該公約視為任何刑事罪引渡的法律根據[172]。不以條約的存在作為引渡條件的當事國間，應承認本條第 1 款所述的刑事犯罪為相互之間可引渡的罪行[173]。而在程序上，引渡應遵守被請求國法律，或適用的引渡條約規定的條件，包括被請求國可拒絕引渡的理由[174]。如果本條第 1 款所述的刑事犯罪的引渡僅僅因被請求者的國籍而被拒絕，或被請求國認為其對該罪行具有管轄權，被請求方應將案件提交給請求方，向其國家當局提出起訴的請求，並應在適當的時候向請求方報告最終結果。該當局並應根據該締約方的法律，以與其他類似性質的犯罪相同的方式作出決定並進行調查和訴訟[175]

在相互協助的一般性原則方面，網路犯罪公約第 25 條規範了相互協助的基本原則（General principles relating to mutual assistance），包括下列五點：

---

with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

[170]Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply

[171]The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

[172]If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

[173]Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

[174]Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition

[175]If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

1. 雙方應就在涉及電腦系統和數據的刑事犯罪之調查或訴訟程序，或以電子形式蒐集之證據方面，彼此提供最大程度的互助[176]。

2. 各方也應採取必要的立法措施和其他措施，履行本公約第 27 條至第 35 條規定的義務[177]

3. 在緊急情況下，各方可以透過快速通訊手段，包括傳真或電子郵件，提出相互協助或通訊相關請求，只要這種手段提供適當的安全和認證級別（如有需要時包括使用加密之情形），並在被要求方要求時提供正式確認。被請求方應以任何快速通訊手段接收，並回應請求[178]。

4. 除本章條款另有明確規定外，互助協議應符合被請求方法律或適用互助條約規定的條件，包括被請求方可拒絕合作的理由。被請求方不得以該請求涉及其認為屬於財政犯罪的罪行為理由，而行使拒絕就第 2 條至第 11 條所述罪行提供互助的權利[179]。

5. 如果按照本章的規定，被請求方被允許在雙重犯罪存在的情況下提供互助條件，則該條件應被視為已滿足，而不問其法律是否將該罪行置於同一類別的犯罪之列，或如果尋求協助的犯罪行為的行為在其法律下屬於刑事犯罪，則以與請求方相同的術語界定犯罪行為[180]。

---

[176]The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

[177]Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

[178]Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

[179]Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

[180]Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

第二節　美國法對於電腦犯罪之相關規制與立法趨勢

美國法上關於電腦犯罪的立法沿革方面，美國國會在 1984 年的「綜合犯罪管制法案（Comprehensive Crime Control Act）」納入了關於美國特勤局（US Secret Service）在信用卡詐欺及電腦詐欺領域管轄權的規定。其後，在 1986 年，美國國會通過了「電腦詐欺與濫用法(Computer Fraud and Abuse Act, 簡稱 CFAA)」，可謂係針對當時電腦詐欺法律[181]的修正，該法已被納入前述綜合犯罪管制法案，其擴大了保護電腦的範圍，並且明文使入侵電腦系統行為構成犯罪。詳言之，CFAA 規範了八個重點，除預備犯的規定[182]、刑事犯罪的科刑[183]、美國特勤局（US Secrete Service）之介入調查[184]、法律執行與情報機構之除外規定[185]、民事訴訟(civil cause of action)[186]及向國會報告之程序[187]外，主要包括行為態樣的禁止類型與定義性規定，茲分敘如下：

第一項　七種禁止的行為態樣[188]（offenses）：

一、**禁止間諜行為（Espionage prohibitions）**[189]：在未經授權或逾越權限的情況下故意入侵電腦，並透過此類行為獲得美國政府根據行政命令或法規所決定的資訊，因國防或外交關係或任何受限制的數據而需要防止未經授權的披露…

二、**未獲授權或逾越權限之資訊獲取**[190]：故意未經授權入侵電腦或逾越授權範圍，從而獲得特定金融機或發卡機構存放的財務記錄，或來自美國任何部門或機構的資訊，或來自任何受保護電腦之資訊等。

---

181 18 U.S.C. §1030，see: https://www.law.cornell.edu/uscode/text/18/1030
182 18 U.S.C §1030(b)
183 18 U.S.C §1030(c)
184 18 U.S.C §1030(d)
185 18 U.S.C §1030(f)
186 18 U.S.C §1030(g)
187 18 U.S.C §1030(h)，
188 18 U.S.C §1030(a)
189 18 U.S.C §1030(a)(1)
190 18 U.S.C §1030(a)(2)

三、侵入政府系統（Trespass on government system）[191]：故意未經授權入侵任何美國政府部門或機構的非公用電腦，入侵該部門或機構專用於美國政府的電腦，或者若該電腦不是僅供美國政府使用或由美國政府使用，但其行為影響美國政府使用或由美國政府使用者。

四、基於詐騙之意圖（With intent to defraud）[192]：明知且基於詐欺之意圖，未經授權而入侵受保護的電腦，或逾越授權範圍，並透過此方式為進一步的詐欺行為，以獲取任何具有價值的東西，若該詐欺行為之對象和犯罪所得僅與受保護電腦的使用有關，且該使用行為的價值未逾一年 5000 美元，即不在處罰範圍。

五、造成損害（Causes damage）之行為[193]，包括下列三種態樣：

（一）故意造成程式、資訊、代碼或命令的傳輸，並且由於此類行為，故意對受保護的電腦造成未經授權的損害；
（二）未經授權故意入侵受保護的電腦，並由於此類行為而魯莽地造成損害。
（三）未經授權故意入侵受保護的電腦，並由於此類行為導致損害和損失。

六、密碼之交易（Password trafficking）[194]：明知而意圖詐騙任何密碼或類似資訊的特定流量，以便在未經授權的情況下入侵電腦，包括此類流通影響州際或外國商業活動，或此類電腦由美國政府使用或由美國政府使用之情形。

七、狹持電腦與資料進行勒索（Extortion threat to a computer/data）[195]：意圖向任何人索取任何金錢或其他有價物品，在州際或外地商業中傳送任何包含下列資訊：

（一）對受保護的電腦造成損害的威脅；
（二）威脅在未經授權或超越授權的情況下從受保護的電腦獲取資訊，或在未經授權或逾越授權範圍而入侵的情況下損害從受保護電腦獲得的資訊的機密性；
（三）對於受保護的電腦造成損害，進而要求支付金錢或其他有價物品，而該損害之造成足以促成勒索。

[191] 18 U.S.C §1030(a)(3)
[192] 18 U.S.C §1030(a)(4)
[193] 18 U.S.C §1030(a)(5)
[194] 18 U.S.C §1030(a)(6)
[195] 18 U.S.C §1030(a)(7)

第二項　定義性規定[196]

一、所謂「**電腦（computer)**」係指執行邏輯、算術或儲存功能，具有電子、磁性、光學、電化學或其他高速數據處理設備，並且包括與數據儲存設備或通信設施直接相關之此等裝置，但是該用語不包括自動打字機或排字機、攜帶式手持計算機或其他類似裝置。

二、「**受保護的電腦(protected computer)**」一詞是指下列電腦：
（一）僅供金融機構或美國政府使用，或者如果該電腦非專供該使用，而係由金融機構或美國政府使用，而該行為對於金融機構或政府構成犯罪行為;

（二）用於或影響州際或外國商業或通訊活動，包括位於美國境外的電腦，且其使用方式會影響美國的州際或外國商業或通訊活動。

三、「**國家(States)**」一詞包括哥倫比亞特區、波多黎各聯邦和美國的任何其他聯邦、財產或領土;

四、「**金融機構(financial institution)**」一語是指：
（一）由聯邦存款保險公司提供保障的機構；
（二）美國聯邦儲備或包括任何聯邦儲備銀行在內的美國聯邦儲備會員；
（三）由國家信用社管理局提供保障的信用聯盟帳戶；
（四）聯邦房屋貸款銀行系統和任何房屋貸款銀行的成員；
（五）1971 年農業信貸法案下的任何農場信用體系機構；
（六）根據 1934 年證券交易法第 15 條向證券交易委員會註冊的經紀商；
（七）證券投資人保護公司；
（八）外國銀行的分支機構或代理機構（該用語定義見諸 1978 年國際銀行法案）；
（九）根據「聯邦儲備法案」第 25 條或第 25 條（a）款成立之組織。

五、「**財務記錄（financial record）**」一詞是指從金融機構基於其與相關客戶間之關係所持有的記錄中獲得的資訊。

---

196 18 U.S.C§1030(e)

六、「**逾越權限取得**（exceeds authorized access）」一詞是指經授權使用電腦，並透過該使用行為進而獲取或更改電腦中使用者無權獲取或改變的資訊。

七、「**美國部門**（department of the United States）」一詞是指政府的立法或司法部門，或特定行政部門。

八、「**損害**（damage）」一詞是指對數據、程式、系統或資訊的完整性或可用性所造成的任何損害;

九、「**政府實體**（government entity）」一詞包括美國政府、美國的任何國家或政治分區、任何外國，以及任何外國的州、省、市或其他政治分區。

十、「**定罪**（conviction）」一詞應包括根據任何國家的法律定罪的罪行，其指因未經授權或逾越權限入侵電腦而被判處一年以上有期徒刑之情形。

十一、「**損失**（loss）」一詞是指任何關於被害人所支出的合理費用，包括應對犯罪行為的成本、進行損害評估以及在回復其犯罪行為前狀況的數據、程式、系統或資訊，以及由於服務中斷而導致的任何收入損失、產生的費用或其他間接損失

十二、「**人**（person）」一詞是指任何個人、公司、公司、教育機構、金融機構、政府實體或法律或其他實體。

另在 1987 年，美國國會通過了「電腦安全法案（the Computer Security Act）」，改善了聯邦電腦系統的資訊安全，建立了基礎的安全措施。該法案旨在提高聯邦電腦系統中關於機密資料的隱私性及安全性，並為此類系統建立最低限度可接受的安全措施。然而，立法機關僅使美國國防部管理有關國防的電腦安全，而保留私人領域的範疇[197]。

在實務上著名的案件即是 1989 年的「Morris 電腦蠕蟲」案件[198]，這是第一起透過網路散佈的電腦蠕蟲，其事實略為：1988 年 10 月，Robert Morris Jr.散布電腦蠕蟲到到全國電腦機網絡，最終導致各教育機構和軍事基地的電腦當機或停止

197 G. Press, *supra note* 1,at14
198 928 F.2d 504

運行，而在訴訟發展上，1990 年，法院認定 Robert Morris Jr.因製造惡意軟體感染了在美國軍事學術及研究機構超過六十萬台電腦，而應依 CFAA 定罪，他被判處１萬美元罰金並判處三年緩刑及義務勞務，這是 1986 年 CFAA 立法後第一個重罪判決，該案經陪審團審判後判定他違反前述 18 USC §1030（a）（5）（c）所稱「未經授權而入侵電腦」。

CFAA 歷經數次修正，在 1994 年，針對散布電腦病毒的刑期更為嚴苛，在 1996 年，CFAA 修正為不論是否有犯罪所得，允許起訴未經授權而檢視電子資訊者[199]。該次修正擴大了對所有聯邦電腦系統資訊所為犯罪行為，並擴大對州際或國外商業所有私人電腦系統獲取資訊的犯罪，並增列對於「損害（damage）」的定義。隨後在 2001 年，CFAA 再經修正，除了增列對於「損失（loss）」的定義性規定外，同時提高了對於電腦犯罪的刑度，擴大對於境外電腦系統的保護等。而在 2008 年，CFAA 的修正涉及增加刑事沒收與處罰規定，並擴大在美國境內（即商業條款的外圍）對任何私人電腦系統資訊的犯罪行為等[200]。

必須進一步說明者，為針對電腦犯罪所導致的「損害（damage）」或「損失（loss）」如何加以認定，此部分涉及犯罪行為人的刑事責任。承前所述，CFAA 分別在 1996 年及 2001 年的修正中針對「損害（damage）」及「損失（loss）」增列定義性規定；詳言之，所謂的「損害」是指破壞任何資料程式系統或資訊的完整性或可近性[201]，而「損失」則是指這些破壞對被害人修復時所需的合理成本，包括回應攻擊或處理損害評估的成本[202]。在 1030(a)(5)(A)的規定及指出，該法所禁止之行為包括有意地對受保護的電腦或網路，其程式串、資訊、程式碼或命令進行異動，基此行為所生之損害，即可在請求賠償之列。

另一方面，在身份盜用方面，美國國會於 1998 年頒佈「身份盜用罪防制法（the Identity Theft and Assumption Deterrence Act）」作為其基礎規範，聯邦法律亦規範了「與身份識別文件，驗證特徵和資訊有關的詐欺和相關活動」[203]，該條文針對「身份資訊」做了如下四種分類：

---

[199] G. Press, *supra note* 1,at 15

[200]https://www.gpo.gov/fdsys/granule/USCODE-2010-title18/USCODE-2010-title18-partI-chap47-sec1030/content-detail.html

[201]the term" damage" means any impairment of the integrity or availability of data, a program, a system, or information.

[202]the term "loss" means any reasonable cost to any victim, including the cost of responding an offense, conducting a damage assessment and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service

[203] 18 USC§1028(fraud and related activity in connection with identification documents, authentication

1、由「指定的美國、外國政府或準政府組織提供或由其授權的文件」，或「由特定個人提供的信息」構成的文件。目的在識別個人，為普遍接受的類型[204]。

2、認證特徵：是指任何全息圖、水印、認證、符號、代碼、圖像、數字或字母序列或其他特徵，單獨或與其他特徵組合使用，由發證機構在識別文件製作時附於文件以做為識別手段，以確定該文件是否為偽造[205]。 “

3、虛假的身份證明文件：指不是由政府實體或非在政府實體的授權下，為了識別個人所製作能被普遍接受的文件類型；欺騙方式是讓人以為這些文件是由指定的美國，外國政府或準政府組織所頒發或授權的[206]。

4、身份識別手段：指可以單獨使用或與任何其他資訊一起使用的任何名稱或號碼，以識別特定的個人[207]。

何種侵害身份資訊的行為構成犯罪行為？美國聯邦法律規定下列可以概括地描述為識別資訊的「交易」而屬違法行為：

1、使用明知沒有法律效力的生物識別文件、認證特徵或者虛假身份證明文件[208]；

2、知情轉移證件、認證標誌，或者知道這些文件為虛假身份證明，文件被盜或了解身份文件沒有合法權限[209]；

3、在無合法授權的情況下，明知而轉移或使用識別文件，意圖犯下或協助或教唆違反聯邦法律，或構成違法行為的任何活動或與之相關的手段；包括在任何州或地方法律有關的申請亦屬重罪[210] “;

---

features, and information.）

[204] 18 USC§1028(d)(3):An identification document is a document made or issued by or under the authority of’ specified US or foreign governmental or quasi- governmental organisations which, ‘when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals’

[205] 18 USC§1028(d)(1)An authentication feature is ‘any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document- making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified

[206] 18 USC§1028(d)(4): A false identification document is ‘a document of a type intended or commonly accepted for the purposes of identification of individuals’ that ‘was not issued by or under the authority of a governmental entity’ or was so issued but was ‘subsequently altered for purposes of deceit’ and appears to be issued by or under the authority of a specified US or foreign governmental or quasi-governmental organisation.

[207] 18 USC§1028(d)(7) Means of identification is ‘any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual’

[208]18 USC § 1028(a)(1). ‘Produce’ is defined to include ‘alter, authenticate, or assemble’: 18 USC § 1028(d)(9). :knowingly and without lawful authority ‘produce an identification document, authentication feature, or a false identification document

[209]18 USC § 1028(a)(2). knowingly transfer an identification document, authentication feature, or a false identification document ‘knowing that such document or feature was stolen or produced without lawful authority

4、明知但仍使用虛假或實際的身份驗證、偽造身份證件、文件製作工具或身份證件[211]。

由上開規定可知，關於涉及資訊的犯罪行為態樣繁多，論者有將涉及資訊相關的侵害行為區分為四種態樣[212]：（1）破壞資訊（Destroying data）；（2）無正當理由取得資訊(Inappropriate access to data)；(3)非法揭露資訊(Unlawful disclosure of data)；（4）攔截資訊（Interception of data）。前三種類型在態樣上較為相似，析言之，所謂「破壞（destory）」可透過兩種途徑達成，包括「利用(access)」或是「揭露(disclosure)」，第一種情形是非法入侵電腦系統並且破壞、利用或揭露其所獲得的資訊（包括以惡意軟體影響電腦系統的破壞情形），第二種情形則是未經授權入侵電腦進而在無合法授權的情形下破壞或是揭露資訊。在與前述第一種類型相關的侵害行為上，責任基礎在於非法途徑或惡意程式的創造；第二種犯罪則與「授權（authorized）」的概念相關。而關於所謂「授權」此一概念應如何定義？依 U.S.C§ 1028 的規定，將「未獲授權（unauthorized）」定義為：
(1)個人本身並沒有資格控制存取此等程式或資料[213]
(2)個人本身並沒有取得任何有資格控制存取此等程式或資料權限的人的同意[214]

凡透過上開方式取得資訊，即可能構成對於個人資訊之侵害行為。

此外，由日益興盛的社群媒體使用者條款規範方式，亦可窺見司法實務對於行為人主觀要件的要求趨勢。在 United States v. Drew 一案[215]中，則涉及違反使用者條款（Terms of service violation）的概念，亦即指非授權之使用（unauthorized access)。谷歌之使用者條款(Google Terms of Service)即指出：「若未達法定年齡，可能無法使用這些服務；也無權接受這些服務條款以與谷歌公司建立有約束力之合約」[216]，而臉書（Facebook）的使用者條款則是「你同意在網站上任一註冊表格中，提供你本身正確，完整，與即時的資訊（註冊資料）.. 並即時維護與更新這些以及任何您提供給公司的資訊，以維護這些資料的正確性、即時性、與完整

[210]18 USC § 1028(a)(7). knowingly transfer or use, without lawful authority, 'a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law'
[211]knowingly trafficin 'false or actual authentication features for use in false identification documents, document-making implements, or means of identification'. 18 USC § 1028(a)(8).
[212] Alisdair A. Gillespie *supra note* 6, at 75.
[213]原文為："he is not himself entitled to control access of the kind in question to the program or data."
[214]原文為："he does not have consent to access by him of the kind in questioning to the program or data from any person who is so entitled."
[215]259 F.R.D. 449
[216]You may not use the Services and may not accept the Terms if you are not of legal age to form a binding contract with Google.

性...」[217]，另 Match.com 之使用同意條款「你必須至少年滿十八歲，且為單身或已與配偶分居，方能登記為 Match.com 的會員或使用其網站」[218]。在後續的立法改革上，從 Aaron’s Law 及「資料洩露公告與制裁網路犯罪法案（Data Breach Notification and Punishing Cyber Criminals Act,DBNPCCA）」可以看出立法者降低非惡意違規責任，增加惡意犯罪罰責的趨勢，詳言之，Lofgren/ Wyden/ Paul 法案（Aaron’s Law）[219] 主要在確認人們即使違反使用者條款或其他單純定型化合約，並不會導致刑事責任，而 Kirk/ Gillibrand (D-NY)的「資料洩露公告與制裁網路犯罪法案（DBNPCCA）」[220]則增加了「針對沒有得到授權的情況下，自受保護的電腦取得資訊」的處罰。

在 911 恐怖攻擊後，國會通過了將「電腦安全強化法案（Cyber Security Enhancement Act）」作為國土安全部法案的一部分，「電腦安全強化法案」給予執法部門更大的權限可透過網路服務提供者取得個人資訊，其目的在於提供持續的，自願的公私合作夥伴關係 改善網絡安全，並加強網絡安全研究 發展，勞動力發展和教育以及公眾意識 準備和其他目的[221]。而在 2002 年，國會通過了「聯邦資訊安全管理法案（TheFederal Information Security Management Act of 2002,，FISMA)」，成為美國 2002 年電子化政府法案的一環；該法案肯認資訊安全對美國經濟和國家安全利益的重要性，要求每個聯邦機構制定、記錄和實施綜合性計劃，其適用對象包括政府機構、承包人及其他組織所用之資訊與資訊系統，可謂為政府資訊科技系統建立起高度安全性需求標準。然雖自 2002 年起，關於電腦犯罪與電腦安全的關注持續成長，美國國會並未在這議題上通過新的立法。在 2011 年，眾議院通過了「電腦訊息分享與保護法案（Cyber Intelligence Sharing and Protection Act）」，但未獲參議院通過。這個法案允許美國政府與私人企業間分享網路流量資訊，其目的在確保網路攻擊的安全性。這個法案在 2013 年再度提出，也再度經眾議院通過而未獲參議院表決通過。關於電腦訊息分享與保護法案的爭議反映出圍繞著提案立法關於打擊電腦犯罪的爭議：有些隱私在安全性名義

---

[217][Y]ou agree to… provide accurate, current and complete information about you as may be prompted by any registration forms on the Site (“Registration Data”) . . . [and] maintain and promptly update the Registration Data, and any other information you provide to Company, to keep it accurate, current and complete ….”

[218]You must be at least eighteen (18) years of age and single or separated from your spouse to register as a member of Match.com or use the Website.”

[219]在 2015 年 4/21，U.S. Senators Ron Wyden (D-Ore.) and Rand Paul (R-Ky.) Representative Zoe Lofgren (D-Calif.)以跨黨派、跨參眾兩院的方式提出了 Aaron's Law 以改革 CFAA，以便將刑事起訴的重心，放在嚴重的網路犯罪上，而非對電腦或網路非惡意的違規行為。
https://www.wyden.senate.gov/news/press-releases/wyden-lofgren-paul-introduce-bipartisan-bicameral-aarons-law-to-reform-abused-computer-fraud-and-abuse-act-

[220] Senators Kirk (R-Ill.) 及 Gillibrandgd (D-NY)提出 Data Breach Notification and Punishing Cyber Criminals Act（DBNPCCA），希望提高特定電腦網路犯罪的罰責。
https://www.eff.org/deeplinks/2015/04/aarons-law-reintroduced-cfaa-didnt-fix-itself

[221] https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

下是被犧牲的，但並非所有人都同意安全性永遠優先[222]，即使是在著重隱私權保障的美國，亦面對相同的兩難處境。

[222] G. Press, *supra note* 1,at 16.

第六章　跨境電腦犯罪之法制化趨勢~心得與建議

第一節　概述

資訊科技的發展日新月異，法規範進行修改或增訂，往往是因應實務上的需求，不可諱言地，傳統法律體系處理電腦犯罪的規範方式，已無法滿足千變萬化的電腦犯罪手法，尤其在跨境電腦犯罪的議題上，各該主權國家除需檢視其內國法的規範是否足以有效打擊電腦犯罪態樣外，更需進一步的國際合作，包括引渡與相關司法互助，始能有效地遏止電腦犯罪之蔓延。

第二節　我國現行法規範之缺失

關於電腦犯罪的行為程度，可能從低技術性到技術複雜者，基此，研擬電腦犯罪相關法律最大的困難之一即是確保得以因應層出不窮的新型態威脅，我國刑法關於電腦犯罪雖設有專章即第三十六章「妨害電腦使用罪章」加以規範，而關於透過電腦犯罪方式實行詐欺行為，利用電腦進行詐欺行為方面，民國 86 年增訂刑法第 339 條之 3 規定：意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人之財產者，處七年以下有期徒刑（第一項）。以前項方法得財產上不法之利益或使第三人得之者，亦同（第二項）。」，其立法理由為「以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，為電腦犯罪型態，為適應社會發展需要，爰增列處罰專條。」於民國 103 年 6 月 17 日修法，除在第一項增列「得併科七十萬元以下罰金」之處罰規定外，並增訂第三項之未遂犯規定。然上開規範體系卻有下列缺漏尚待立法修正：

第一項　缺乏定義性規範

美國 CFAA 法案針對電腦犯罪之相關用語設有專條為定義性規範[223]，包括「電腦」、「國家」、「財務紀錄」、「逾越權限取得」、「美國部分」、「政府實體」等，且就所謂「受保護的電腦」、「金融機構」之定義更以列舉規定方式明定其範圍，而在其後修法中，更增列了對「損害」與「損失」的定義性規定，以因應司法實務上之需求；網路犯罪公約中，則針對「電腦系統」、「電腦數據」、「服務提供者」、「數據傳輸」之定義設有明文；然觀諸我國刑法妨害電腦使用罪章及相關規定中，除於刑法總則第 10 條第 6 項設有「電磁紀錄」之定義性規定[224]外，其所使用之「無故」、「電腦」、「保護措施」、「電腦程式」、「損害」等概念，究竟應如何加以界定？而刑法第 339 條之 3 所稱「不正方法」、「虛偽資料」、「不正指令」、「財產權之得喪、變更紀錄」之具體內涵為何？立法機關就此等法律規定用語應予以明文定義，俾使司法實務運作順暢，此部分之立法技術顯有疏漏。再者，對於電腦犯罪的規制圍繞在「電腦或其相關設備」、「電磁紀錄」此等概念，而忽略實務上常見的勒索軟體、駭客攻擊、惡意程式、阻斷服務式攻擊等犯罪型態，其規範用語實已遠遠落後科技應用之趨勢。

第二項　犯罪類型過於簡略

關於電腦犯罪之類型，我國刑法中規範之態樣除刑法第 339 條之 3 所定之電腦詐欺罪外，於第三十六章專章之刑法第 358 條至第 362 條設有相關條文以資規範，即刑法第 358 條「無故侵入他人電腦罪」、刑法第 359 條「無故取得、變更、刪除電磁紀錄罪」、刑法第 360 條「無故干擾他人電腦罪」、刑法第 361 條「公務機關電腦之加重規定」及刑法第 362 條「製作惡意程式電腦病毒程式罪」，而前述美國 CFAA 法案中，針對犯罪類型之規定則有七款規定[225]，包括：禁止間諜行為、禁止未獲授權或逾越權限之資訊獲取行為、禁止侵入政府系統、禁止基於詐欺意圖之行為、禁止造成損害之行為、禁止密碼之交易行為與禁止對電腦、資

[223] 18 U.S.C1030(e)
[224] 刑法第 10 條第 6 項規定：「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方法所製成，而供電腦處理之紀錄。」
[225] 18 U.SC1030(a)

料進行勒索之威脅行為，除其規範態樣貼近司法實務常見之犯罪態樣外，在關於基於詐欺意圖進行電腦犯罪之規定部分，CFAA 規定禁止行為人明知且基於詐欺意圖，未經授權而入侵受保護之電腦，或逾越授權範圍，並透過此一方式為進一步之詐欺行為，從而獲取任何有價值之物品；但若該詐欺行為之對象和犯罪所得僅存在於該電腦之使用，且該使用之價值未逾一年 5000 美元，即不在處罰範圍[226]，此一除外規定可謂係基於追訴成本考量之角度，在司法資源有限之情況下，若要求執法機關不區分犯罪所得之多寡，一律花費追訴成本進行調查取證，實無可能針對所有犯罪窮追猛打，尤其在電腦犯罪相較於其他傳統犯罪，更易達成犯罪結果、損害之發生更快更廣，其規模性遠非傳統犯罪可比，如何在司法成本之考量與有效追訴犯罪之間取得平衡，可謂係現代法律人的新課題。

其次，由前揭說明可知，以「未經授權或逾越授權範圍而入侵電腦系統」之規範方式可謂係我國刑法體系及美國 CFAA 所採取之基本模式，然除此一態樣外，關於隱藏真實身份進行電腦犯罪的駭客行為（包括：竊取電腦資源、竊取專有或機密資訊、對於系統或文件進行破壞、改變或重建、阻斷服務式攻擊、散佈惡意程式），立法機關應如何克服立法技術上的難度，區分不同的行為態樣、損害程度加以明文規範？凡此均值深究。

另一方面，在關於身份盜用的議題方面，隨著線上交易對於人們相互往來扮演著越來越重要的角色，有效的身份認證就顯得更加重要。舉例言之，網路銀行帶來諸多便利，雖然能夠不必出門、透過上網方式即可處理個人金融財務往來，但個人和使用這些資金的其他人之間的所有密碼都是數字符號之組合，若犯罪行為人可以取得這些密碼，即可能取代實際所有人的身份。接收這些訊息的電腦僅係單純回應，因為它已被編碼程式化。論者有提出在現實上，對「身份盜用」之行為有必要刑事犯罪化，理由是因為一般刑法對非法使用身份的處罰存有困難。雖然有許多犯罪行為可能適用身份資訊的詐欺使用，但這些行為通常在懲罰資訊的使用行為，而非處理資訊本身[227]。

關於「身份盜用」的違法行為如何論處，涉及涉及身份犯罪的連續行為。詳言之，行為的第一階段是獲取身份資訊的行為。在網絡犯罪的情況下，這通常是依據電腦濫用條款起訴的，在第三階段則是為犯罪目的而使用身份資訊，可能會

---

[226] 18 U.SC1030(a)(4)

[227] M. C. L. O. Committee, "Identity crime : final report / Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General," (Australian Government, Attorney-General's Dept., 2008), 14

受到一系列詐欺和相關違法行為的追訴。而第二階段關於擁有或傳遞該資訊的行為，即所謂「身份盜用」。此一議題雖然被廣泛認為是全球性的挑戰，但很少有國家製定了具體的身份盜竊規定。歐洲理事會網路犯罪公約也沒有涉及這個問題，表面上是因為它側重於犯罪行為，而不是具體的技術或技術，但此一身份盜用的犯罪行為將隨資訊通訊科技的發達而日愈便捷，國家刑罰權應在何階段介入？我國現行個人資料保護法之規範採取實害犯之立場[228]，然該等「損害」之定義為何？實務上盜用身份可能衍生的犯罪行為繁多，擁有或傳遞個人資料的行為在何種情形下應科以刑事制裁？前述美國聯邦法律關於違法交易個人識別資訊的規範，或可作為未來修法之參考。

第三項　刑度過輕

實務上針對電腦犯罪的法定刑度過輕，多所批評；舉例言之，前述臺灣臺北地方法院 105 年度訴字第 426 號、臺灣高等法院 106 年度上訴字第 593 號、最高法院 106 年度台上字第 2603 號關於「一銀 ATM 盜領案」之刑事判決號乃近五年來唯一在判決內提及「惡意軟體」之實務判決[229]，惟該案據以論罪科刑的條文為刑法第 359 條「無故刪除、變更他人電腦之電磁紀錄罪」及刑法第 339 條之 2 第 1 項非法由自動付款設備取財罪，其最高刑度分別為三年、五年有期徒刑，檢察官雖於起訴書就被告三人所觸犯之 12 罪各具體求刑有期徒刑 12 年[230]，然在訴訟過程中，法院認定被告 3 人與其他盜領犯罪集團成員各次盜領 ATM 款項之行為，均為接續犯之一行為，而均各論以一罪，法院判決僅能在法定刑度內為之，然前開二審判決末提出建議「從速修法提高刑度補破網」，並指出：「網路犯罪日新月異，電影手法成現實；以刑法第 339 條之 2「以不正方法由自動付款設備取得他人之物」為例，法定刑只 3 年以下有期徒刑、拘役或 30 萬元以罰金，當時此類犯罪頂多提款卡盜領，誰會想到，現在遠端遙控讓 ATM 吐鈔」，法官僅能依法判決，當法院判決的結果與人民期待、社會觀感落差太大時，即須思考法律規範是否已然落後實務需求之可能。此一司法實務判決之見解，實值吾人深省。

以網路詐欺為例，承前所述，其基本態樣包括「網路銷售詐騙」、「預付費詐欺」、「點擊詐欺」、「電子金融轉帳犯罪」、「投資性詐欺」，以及特殊型

[228]個人資料保護法第 41 條規定參照。
[229]資料來源：司法院法學資料檢索系統 http://jirs.judicial.gov.tw/Index.htm
[230]參見臺灣臺北地方法院檢察署檢察官 105 年度偵字第 15086、15087、18019、19141 號起訴書。

態之「網路釣魚」、「網址嫁接」、「側錄信用卡」、「身份盜用」等，此等詐欺行為與傳統詐欺行為最大的差異在於，其被害人的數目可能甚多、所造成的損害可能甚鉅，若未慮及網路詐欺行為透過電腦犯罪方式進行所導致之規模，僅以傳統的詐欺犯罪論罪科刑，或僅以提高刑度方式增列電腦詐欺條款（如我國刑法第 339 條之 3 規定），實屬忽略網路詐欺行為可能造成的損害程度。由前述美國法上關於電腦詐欺犯罪之相關法規修正亦可知，加重刑度乃無可避免的趨勢，惟我國相關電腦犯罪規範自明文立法至今，刑度未見類型化、幅度化調整，實屬缺漏。

第三節　國際合作與司法互助之重要性

隨著跨境犯罪日益增多，為追訴犯罪而需要在其他國家或地區蒐集證據之情形也隨之增加。根據法務部之統計，累計至 2016 年 10 月底，我國與美國進行司法互助的請求案件計 191 件，已完成 167 件；兩岸間相互提出調查取證之請求計 1,995 件，已完成 1,418 件[231]。由此一統計數據可知，國際合作與司法互助已然成為追訴犯罪的重要途徑，尤其在天涯若比鄰的網絡空間，跨國犯罪所面臨的司法管轄權爭議、調查取證的困難，實有賴國際間通力合作、無縫接軌的司法互助，始能掌握調查證據的時效性，避免相關證據（尤其是數位證據）遭湮滅而無法有效打擊電腦犯罪。

我國針對跨國盜領銀行存款之案件偵辦成效雖引起國際矚目與認同，但誠如法院判決所提及，該案被告三人並非跨國駭客盜領集團首腦，在欠缺國際合作與司法互助下，無法繼續追查該詐欺集團之首腦及其他共犯，對於遏止跨國犯罪集團進行網路詐欺犯罪行為而言，實屬缺憾；此種電子金融犯罪之跨國犯罪橫行，無疑是自恃透過橫跨不同司法管轄權之領域進行詐欺行為，層層分工、組織細密，綿密的犯罪網絡實難僅憑單一主權國家得以有效攻破；誠如網路犯罪公約第三章「國際合作（International cooperation）」所規範之相關原則，對於司法實務工作者而言，擴展國際合作關係、強化司法互助，是必須持續努力的方向。

[231] 參見　陳文琪，跨境取證之證據能力，檢察新論第 21 期，2017 年 1 月，第 183 頁。

第四節　心得及建議

我國關於電腦犯罪之相關法規範，對於涉及犯罪行為之用語，包括：「無故」、「電腦」、「保護措施」、「電腦程式」、「損害」、「不正方法」、「虛偽資料」、「不正指令」、「財產權之得喪、變更紀錄」等概念，缺乏定義性規定，而關於個人資料可能遭侵害的方式，個人資料保護法之規範亦嫌簡略；美國 CFAA 針對電腦犯罪之定義性規範、列舉式禁止行為態樣之規定，以及網路犯罪公約實體法規範中關於犯罪態樣之規制方式，可作為我國未來修法時之參考。

隨著電腦犯罪類型如雨後春筍地出現，駭客行為、病毒、電腦蠕蟲及木馬程式、勒索軟體等，早已成為實務上常見之犯罪態樣，而刑法妨害電腦使用罪章條文的刑度過輕，在司法實務傾向認定詐欺集團行為人的犯罪行為不構成數次犯行的情況下，往往造成法院判決的刑度與實際造成的損害顯然輕重失衡之結果。與美國法上針對電腦犯罪之規制屢屢修正，並傾向加重刑度之趨勢相較，我國現行法規範實有與時俱進之必要。

再者，網際網路的全面性發展，使得政府企業及個人越來越容易成為具有威脅性攻擊的對象，然由美國法對電腦犯罪之規制發展可知，如何在個人隱私與商業利益甚或國家安全中取得平衡，實為針對電腦安全進行法制規劃之重要課題。

最後，電腦犯罪所具有的可近性、可攜帶性與可移轉性等特質，使得犯罪行為人遂行犯罪的成本降低，透過電腦犯罪可享有的匿名性及客觀上缺乏有效監管的情況，除了提高了犯罪的誘因，使得犯罪規模擴大外，對於司法機關而言則意味著調查取證的複雜性、困難度提升，而電腦犯罪之規模性、全球性則使其可能造成的影響無遠弗屆，在跨國詐欺犯罪行為有增無減、態樣趨於精細化、組織化的今日，國際合作與司法互助必然是時勢所趨，如何建立因應跨國詐欺犯罪之模式，乃能否有效打擊此等犯罪之關鍵。

參考書目:

1. A. Aust, *Handbook of International Law*. (Cambridge University Press, 2005).
2. N. F. Authority(UK), "Annual fraud indicator," (National Fraud Authority, UK, 2013).
3. M. D. G. a. S. W. Brenner, The emerging consensus on criminal conduct in cyberspace. *UCLA Journal of Law and Technology* **3**, (2002).
4. S. Canada, "Individual internet use and e-commerce, 2012," (2013).
5. I. C. C. Center, "Internet crime report 2012," (2012).
6. I. C. C. Center, "Internet crime report 2013," (Internet Crime Complaint Center, 2013).
7. A. H. T. C. Centre, *Malware: Viruses, worms, Trojan horses*. High tech crime brief no. 10 (Australian High Tech Crime Centre, 2006).
8. A. H. T. C. Centre, in *High Tech Crime Brief*. (AIC, 2007).
9. *UNITED STATES V. RAISLEY* (2012 https://casetext.com/case/united-states-v-raisley).
10. C. I. P. a. P. I. Clinic, "Identity theft: Introduction and background," *CIPPIC Working Paper, ID Theft Series* (2007).
11. J. Clough, *Principle of Cybercrime 2nd ed.* (Cambridge University Press, Monash University, Victoria, 2015).
12. R. a. CNBC, US attorney general confirms probe of Target data breach. 2014.
13. M. C. C. O. Committee, in *Final Report*. (Model Criminal Code Officers Committee, 2006).
14. M. C. L. O. Committee, "Identity crime : final report / Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General," (Australian Government, Attorney-General's Dept., 2008).
15. *Judgments - Mckinnon V Government of The United States of America and Another* (2008 http://www.bailii.org/uk/cases/UKHL/2008/59.html).
16. M. M. a. S. Dowling, "Cyber crime: A review of the evidence," *Research Report No. Chpt2* (Home Office, 2013).
17. J. Fairtlough, *Introduction To Cyber Crime Investigation*. (LawTech Publishing Group, 2014).
18. L. C. a. M. Felson, Social change and crime rate trends: A routine activity approach. *American Sociological Review* **44**, (1979).

19. E. Finch, The problem of stolen identity and the internet. *Crime online*, (2007).
20. E. Finch, in *Crime Online,* Y. a. Y. Jewkes, M, Ed. (Willan Publishing, 2007)
21. B. W. G. o. C.-B. M. M. Fraud, "Binational Working Group on Cross-Border Mass Marketing Fraud," (2006).
22. B. W. G. o. C.-B. M. M. Fraud, "Report on Phishing: A report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States," (2006).
23. S. Furnell, in *Handbook on Internet Crime,* Y. a. Y. Jewkes, M., Ed. (2010)
24. S. a. W. Furnell, J. , in *Digital Crime and Forensic Science in Cyberspace,* P. Kanellis, Kiountouzis, E., Kolokotronis , N. and Martakos, D., Ed. (Idea Group, 2006)
25. A. A. Gillespie, *Cybercrime: Key issue and Debates*. (Routledge Taylor & Francis Grou, LONDON AND NEW YORK, 2016).
26. M. Hirst, *Jurisdiction and the Ambit of the Criminl Law*. (Oxford University Press, 2003).
27. P. Hunter, The growing phenomenon of crime and internet: A cybercrime execution and analysis model. *Computer Law and Security Review* **529**, (2009).
28. U. Kohl, *Jurisdiction and the internet: Regulatory competence over online activity* (Cambridge University Press, Cambridge, 2007).
29. T. a. Loader, *Computer Crimes and Digital Investments*. T. a. L. i. Walden, Ed., (Oxford University Press, 2007).
30. J. Lynch, Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks. *Berkeley Technology Law Journal* **20**, (2005).
31. S. Morris, "The future of netcrime now: Part 1-threats and challenges," *Home Office Online Report No. 4* (Home Office, 2004).
32. U. C. B. News, "Quarterly retail e-commerce sales 3rd Quarter," (US Department of Commerce, 2014).
33. F. Paget, "Identity Theft," *White Paper* (2007).
34. E. S. Podgor, Cybercrime: Discretionary jurisdiction. *University of Louisville Law Review* **47**(2009).
35. G. Press, *Cybercrime (Current Controversies)*. (Greenhaven Press, 2016).
36. M. R. Rahman, Khan, M.A., Mohammad, N and Rahman, M.O., Cyberspace claiming new dynamism in the jurisprudential *International Journal of Law and Management*(2009).

37. R. Rahman, Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. *Computer Law and Security Review.* (2012).
38. J. Reidenberg, *Technology and internet jurisdiction.* (University of Pennsylvania Law Review, 2005).
39. *International hacker sentenced* (2014 https://www.justice.gov/usao-ndga/pr/international-hacker-sentenced).
40. A. C. f. P. Research, "Standardisation of definitions of identity crime terms: A step towards consistency," *Report Series* (Australasian Centre for Policing Research and the Australian Transaction Reports and Analysis Centre, Australia, 2006).
41. R. Richardson, "2010/2011 Computer Crime and Security Survey," (Computer Security Institute, 2011).
42. B. Sandywell, in *Handbook of Internet Crime,* Y. a. Y. Jewkes, M., Ed. (Willan Publishing, 2010).
43. I. G. Secretariat, "ITU Internet report 2005 : the Internet of things," *Internet reports* (International Telecommunication Union, 2005).
44. R. G. Smith, in *Crime over time: Temporal perspectives on crime and punishment in Australia.* (Newcastle upon Tyne: Cambridge Scholars Publishing, 2010).
45. R. G. Smith, in *Handbook of transnational crime and justice, 2nded,* P. R. a. J. Albanese, Ed. (California: Sage Publishing, 2014), vol. Ch7.
46. Sophos, "Security Threat Report 2013," (2013).
47. A. B. o. Statistics, Household use of information technology. Australia 2012-13, (2014).
48. I. T. Union, "ICT facts and figures : The world in 2014," (International Telecommunications Union, 2015).
49. D. S. Wall, *Cybercrimes: The transformation of crime in the information age.* (2007).
50. D. S. Wall, *Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age.* T. H. a. B. Schell, Ed., Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (Hershey: IGI Global, 2011).
51. M. Yar, *Cybercrime and Societ, 2nd ed.* (Sage, 2013).
52. Furnell, S. and Ward, J. 'Malware an evolving threat' in Kanellis, P., Kiountouzis, E., Kolokotronis , N. and Martakos, D. Digital Crime and Forensic Science in Cyberspace(2006, Idea Group),
53. 林山田，刑法各罪論【上冊】. (2012).

54. 張紹斌， 刑法電腦專章及案例研究. 軍法專刊 54, (2008).
55. 許文義，個人資料保護法論. 法學叢書 (三民書局股份有限公司, 2001).
56. 葉奇鑫、李明臻，打擊網路犯罪新紀元：個人資料保護法施行下檢察實務的衝擊與挑戰. 檢察新論第 13 期， (2013).
57. 廖宗聖、鄭心翰， 科技法學評論 (2010), vol. 7.
58. 蔡蕙芳，電磁紀錄無權取得行為之刑法規範. 中正法學集刊 13,（2010）
59. 陳文琪，跨境取證之證據能力，檢察新論第 21 期（2017 年 1 月）
60. 林元裕，檢視電腦犯罪之刑法規制—兼論歐洲理事會網路犯罪公約，國立中正大學法律學研究所碩士論文，（2010）
61. 陳彥嘉，保護營業秘密之刑事立法，臺灣法與德國法的比較研究，國立東華大學財經法律研究所碩士論文，（2006）
62 李茂生，刑法新修妨害電腦使用罪章芻議（上）臺灣本土法學雜誌 54, (2004).

附錄：18 U.S.C§ 1030

(a) Whoever—
(1)having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2)intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
(A)information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B)information from any department or agency of the United States; or
(C)information from any protected computer;
(3)intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4)knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A)knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B)intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C)intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[2]

(6)knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A)such trafficking affects interstate or foreign commerce; or

(B)such computer is used by or for the Government of the United States; [3]

(7)with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A)threat to cause damage to a protected computer;

(B)threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C)demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)

(A)a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B)a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offenseunder subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A)except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B)a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i)the offense was committed for purposes of commercial advantage or private financial gain;

(ii)the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii)the value of the information obtained exceeds $5,000; and

(C)

a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this

section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A)a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B)a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),[4] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)

(A)except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

(i)an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(I)loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(II)the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III)physical injury to any person;

(IV)a threat to public health or safety;

(V)damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI)damage affecting 10 or more protected computers during any 1-year period; or

(ii)an attempt to commit an offense punishable under this subparagraph;

(B)except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i)an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii)an attempt to commit an offense punishable under this subparagraph;

(C)except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—

(i)an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii)an attempt to commit an offense punishable under this subparagraph;

(D)a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i)an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii)an attempt to commit an offense punishable under this subparagraph;

(E)if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F)if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G)a fine under this title, imprisonment for not more than 1 year, or both, for—

(i)any other offense under subsection (a)(5); or

(ii)an attempt to commit an offense punishable under this subparagraph.

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.
(3)
Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—
(1)the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2)the term "protected computer" means a computer—
(A)exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
(B)which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States

that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3)the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4)the term “financial institution” means—
(A)an institution, with deposits insured by the Federal Deposit Insurance Corporation;
(B)the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
(C)a credit union with accounts insured by the National Credit Union Administration;
(D)a member of the Federal home loan bank system and any home loan bank;
(E)any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F)a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
(G)the Securities Investor Protection Corporation;
(H)a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
(I)an organization operating under section 25 or section 25(a) [1] of the Federal Reserve Act;
(5)the term “financial record” means information derived from any record held by a financial institution pertaining to a customer’s relationship with the financial institution;

(6)the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7)the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8)the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;

(9)the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10)the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11)the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12)the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses [5] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computersoftware, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)
(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—
(A)such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and
(B)any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.
(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section.