出國報告(出國類別:進修)

有關打擊網路犯罪(CYBER CRIME)法制及國際合作之研究

服務機關:臺灣桃園地方檢察署

姓名職稱:戎婕檢察官

派赴國家:美國哈佛大學

出國期間:民國 106 年 8 月 9 日至 107 年 8 月 8 日

報告日期:民國 107 年 11 月 6 日

摘要

本文分為三大部分，首先概述現行美國電腦犯罪法制，中段探討關於美英等國網路犯罪法制之發展趨勢，第三部分則介紹打擊網路犯罪之國際司法合作現況。法制研究中實體法部分，研究對象為美國聯邦刑法典中電腦犯罪專章及透過電腦遂行之傳統犯罪，包含商業間諜、侵害營業秘密罪、兒童色情罪 ； 程序法部分，則介紹依美國聯邦刑事訴訟法，對電腦中內容性訊息及非內容性訊息之取證程序。其次介紹現今英美等國，在面對新興網路犯罪型態時，帶領風向之判決、社會議題及衍生之法制演變。最後研究歐洲、美國及亞洲等區域，在進行國際司法合作時所依據之法源、組織及相關案例，並評析亞洲國家及我國在跨國網路犯罪防治上當有之態度及應擔負之責任。

壹、前言

筆者自 106 年 8 月至 107 年 8 月，有幸受法務部選送至美國哈佛大學法學院進修。在桃園地檢署服務期間，曾處理一件跨境違反藥事法案件，主嫌透過網路販賣壯陽藥，犯罪地以大陸及臺灣地區為主，惟網站伺服器註冊在加拿大等境外第三地，金錢則透過西聯匯款流通。偵辦過程首先遇到的困難是無法特定被告身分，因行為人刻意隱匿登入位置、難以與境外伺服器提供者取得聯絡，而縱曾思及尋求司法互助，但在考量被告恐隨時關閉舊網站、成立換湯不換藥新網站，案件於是逐步走往傳統式的偵查方向——調閱路口監視器、比對貨運車輛車牌、守株待兔的跟監、挨家挨戶的訪談、大量戶役政及聯徵資料的比對;該案最終不負苦心特定出主嫌五名，然而對原本以科技偵辦跨境網路犯罪的胸心壯志，卻化為檢警週週加班熬夜的苦工合作。數年過去，再次回想起當時選擇以最傳統的方式處理，除了本於當下手中卷證做出判斷外，也因為對偵辦跨境電腦犯罪的不熟悉，潛意識避開了從電腦、境外取證著手之管道。面對過去不足之時，也激起了筆者探索電腦犯罪、跨國案件偵辦領域的意念。

在美國哈佛大學進修期間，筆者選修了由前麻州、紐約郡助理檢察官、現任 Nutter, McClennen & Fish in Boston 法律事務所合夥人 Seth Berman 教授所開設之「電腦犯罪實體與程序法」課程。Berman 教授在擔任檢察官時期，均專責於打擊電腦犯罪中心（New England Electronic Crimes Task Force; New York Electronic Crimes Task Force），並在擔任檢察官後數年即轉而至私部門服務，領導了跨華盛頓特區、紐約、波士頓及倫敦地區的跨境科技犯罪與鑑識顧問公司（Boston, New York, Washington and London offices of Stroz Friedberg）。課程中 Berman 教授除了電腦犯罪實體及程序法，及現行電腦犯罪跨境取證規則外，也帶領學生討論了多個現在美國及歐洲的新興案例，包括：Microsoft vs People，Playpen 案及高爭議之美國 CLOUD 法案之英國偵查權力法案（Investigatory Powers Acts）等，這些現正進行中的案件及新興誕生的法案，呈現了當前司法單位在打擊電腦犯罪、跨境偵查、司法合作上的困境，而此些個案與法案的判決及運用，亦將影響未來此領域犯罪偵查的發展，本文將會一一介紹。除了課堂修習外，筆者亦利用寒假進修期間，前往夏威夷州檢察署刑事偵查部（State of Hawaii Department of the Attorney General, Criminal Investigation Division）見習。見習期間，夏威夷州檢察署刑事偵查部將打擊網路犯罪列為重點偵查案件，尤以網路兒童色情犯罪（Online Child Pornography）為打擊目標，筆者於 21 天的見習期間，有幸參與相關案件的討論及網路犯罪防治宣導工作的籌備，親身理解了美國檢察單位在打擊電腦犯罪時的態度與方法。

筆者進修期間，適逢哈佛法學院創校兩百週年，校方以舉辦各類學術研討會之方式進行長達數週的校慶活動，其中多場研討均與國際電腦犯罪相關，各方學者專家以不同的方式切入此一廣大的議題，使之討論充滿正反論辯、利益交鋒。

作為一個第一線的實務工作者，在面對個案時，我們大可輕鬆地避開繁複的理論、立法背景不談，依法操作，然而身為一個法律人，將實務經驗應證於理論之上，刺激制度之精緻

化，更是不可躲避的責任。筆者受法務部選送，期許在這篇論文中，淺入深出，能同時對於個案操作及法制建立上有所貢獻。

貳、美國電腦犯罪法律簡介[1]

一、實體法

（一）美國聯邦刑法電腦濫用罪章

美國聯邦刑法第 1030 條，又稱電腦詐欺及濫用罪章（Computer Fraud and Abuse Act, CFAA)。此條文包含七種電腦犯罪類型，中心思想是環繞在未經授權之侵入電腦行為（unauthorized access），類型如下：

1.「未經授權或超越授權侵入電腦取得機密資料損害國家或協助外國政府罪」（18 U.S.C. 1030(a)(1)）—本項犯罪規定幾乎沒有被使用過。

2.「未經授權或超越授權侵入電腦獲取資訊罪」（18 U.S.C. 1030(a)(2) ）：

（1）條文內容：

「未經授權或超越授權意圖（intentionally）登入電腦，以此方式取得（Ａ）商業組織、信用卡發行者、消費者報告機構中消費者之商業紀錄;（Ｂ）美國官方機構或部門之資訊;（Ｃ）所有受保護之電腦。」

（2）構成要件介紹：

本條犯罪在 1986 年修法時，將原本的犯意從「明知」（knowingly）修正為「意圖」（intentionally)，要求被告必須以獲取訊息為意圖，未經或超出授權侵入電腦。[2]目的是為因應電腦使用中，授權與未授權區域之分野並不如實體世界如此明顯，使用者經常會有意識地進入某個區域，但無法在進入時明確確認是否因此闖入他人之管領範圍內，因此如果採用「明知」之犯罪標準，很容易使得誤入他人領域之使用者構成犯罪，是以立法者將主觀要件之門檻提高為「意圖」（intentionally)，即必須以竊取資訊為目的行動，才可能構成本條犯罪。[3]

本條犯罪保護之法益為「隱私」，引此儘管法條用語為「取得」（obtaining）他人資訊，但檢察官並無需證明行為人有使用積極行為拿取該等資訊，單純之觀看（mere observation）也已經構成犯罪。又包括本條在內之電腦詐欺及濫用罪中，所指「電腦」非常廣泛，依照 18 U.S.C. 1030(e)(1)之定義， 為「以電子或其他方式進行邏輯、算數演算

[1] 本章法條之介紹順序及重點，參考自 Kerr, Orin S. Computer Crime Law. 3rd ed., West Academic Publishing, 2012.
[2] Id. at 78
[3] Id.

或有儲存功能之高速資料處理器」。[4] 依此，從電腦、智慧型手機、MP3 播放器到微波爐或電子烤箱，均可被列入本條所稱電腦，是否能與網際網路連結，並非判斷標準。[5]

（3）加重規定：

18 U.S.C. 1030(a)(2)、1030(a)(3)、1030(a)(6)等罪原則上為最重刑責一年以下之罪（規範可見 18 U.S.C. 1030(c)(1)(A)）。然就 1030(a)(2)之未經授權或超越授權侵入電腦獲取資訊罪，該法則於 18 U.S.C. 1030(c)(2)(B)增訂加重規定，將刑期提高最重刑責 5 年以下。加重事由如下：

「(i) 為商業利益或個人獲利而犯罪;

(ii) 犯罪係用以達成對美國政府或各州政府進行之刑事犯罪或侵權行為;

(iii) 所獲取之資訊價值超過 5,000 美元。」

就獲取之資訊價值之計算標準為何，聯邦上訴法院第六巡迴法院於 2011 年在 United States v. Batti, 631 F 3d. 371(6th Cir. 2011)案中，對此作出解釋：

（4）United States v. Batti[6]

被告 Luay Batti 為 Campell-Ewald 廣告公司之資訊室員工， Batti 超越授權進入由公司 CEO 的保管的機密檔案夾裡，取得包括一 Campell—Ewald 公司為 GM 汽車公司所製作的廣告母帶。Batti 表示其取得該等資料的目的，只是要警告公司其電腦保密設施有漏洞，然 Campell—Ewald 公司最後則將 Batti 開除。數週後，Campell—Ewald 的機密檔案外流至網路，經 FBI 調查後，確認是 Batti 所為。檢察官則以 18 U.S.C. 1030(a)(2)(C)超越授權意圖登入電腦，以此方式取受保護電腦資訊罪起訴，並依(c)(2)(B)(iii)之規定，以獲取利益超過 5000 美元加重之。

最高法院維持地院見解，首先認為本罪之成立，並不以損害發生為要見，即便 Batti 將廣告母帶公布，並未影響 Campell—Ewald 與 GM 公司之廣告合作，仍可成立犯罪。其次，法院認為，因應網路犯罪之特性，眾多被竊取之資訊係無形資產，與傳統竊盜或贓物犯罪不同，難以衡量市場價值，故加重規定中「所獲資訊價值」之判斷，除以市場價值（market value）外，製造成本(cost of production)亦可作為計算標準。以本案為例，廣告母帶因並未在市場上流通，並無固定市場價值，但 Campell—Ewald 在製作該廣告時，花費 305,000 美元，被認為是一可為法院接受之標準。

3. 18 U.S.C. 1030(a)(3)「未經受權或超越授權侵入美國政府電腦獲取資訊罪」。

4. 18 U.S.C. 1030(a)(4)「未經授權或超越授權侵入電腦，進行電信詐欺罪」—又稱聯邦電腦詐欺罪：

（1）條文內容：

[4] Id. at 81.
[5] Id.
[6] Id. at 82-87

「明知且意圖詐欺，未經授權或超越授權侵入受保護之電腦，以遂行詐欺，並獲取財產利益。但利益價值僅止於電腦之使用或未超過一年美金 5000 元者，不在此限。」

（2）構成要件介紹：

本條係上開 1030(a)(2)與 18 U.S.C. 1343 電信詐欺規定之綜合。[7]犯罪之構成要件有四：詐欺意圖、侵入他人電腦（或超越授權）、遂行詐欺行為、獲利 5000 美元以上。又在參議員國會報告（Senate Report）中，明確表示本罪欲排除單純使用電腦遂行犯罪之傳統犯罪手段，如：使用電腦為犯罪所得作帳、透過電腦聯絡共犯等，將被歸類在傳統電信詐欺即 mail fraud or wire fraud 中。本條犯罪之成立，以「侵入他人電腦」為要件。[8]再者，立法者也強調本罪成立必須行為人透過侵入手段，實際獲得利益，若侵入電腦所獲取之資訊並未被用在詐欺獲利行為上，僅會成立單純 1030(a)(2)(C)侵入電腦犯罪，而非本條要處罰的電腦竊盜行為（computer theft）。[9]就電腦侵入行為與電腦竊盜行為之分野，聯邦上訴法院第一巡迴法院於 1997 年在 United States v. Czubinski, 106 F 3d. 1069 (1st Cir. 1997)案中，對此作出解釋。

（3）United States v. Czubinski[10]

Richard Czubinski 受僱於國稅局波士頓辦公室納稅義務人服務處，被允許為工作所需，進入國稅局之整合資訊系統，查看納稅義務人申報資料。然 Czubinski 為滿足自己私慾，接連查看了數個政治人物、地方政府官員甚至其前女友之稅務資訊。地院判處其涉犯 18 U.S.C. 1030(a)(4)「未經授權或超越授權侵入電腦，進行電信詐欺罪」。

高等法院推翻地院判決，認定本條犯罪之成立，必須被告在侵入電腦或超越授權取得其內資訊後，實際用以詐欺並且獲利。然而本件並無證據可認 Czubinski 除查看該等資料外，有更進一步複製、列印或使用該資訊，因此其行為可能僅是在滿足好奇。因此 Czubinski 可能僅涉犯侵入電腦的輕罪，而非 1030(a)(4)之電腦竊盜重罪。

5. 18 U.S.C. 1030(a)(5)「未經授權或超越授權侵入電腦，致生損害罪」—又稱聯邦電腦損害罪：

（1）條文內容：

「(A) 明知而進行程式、資訊、密碼、指令之傳輸，未經授權，故意導致受保護之電腦損害(damage);

(B) 未經授權意圖進入受保護之電腦，因而重大輕率(recklessly)造成損害（damage）;

(C) 未經授權意圖侵入受保護電腦，導致損害及損失(damage and loss)。」

（2）構成要件介紹：

(A)款所規範之行為，係排除他人使用電腦之行為，譬如散布病毒、癱瘓電腦，導致電腦無法使用; 又本項將「未經授權」置放在「損害」前，係欲排除經授權之傷害電腦型為，

[7] Id. at 90.
[8] Id. at 90-91.
[9] Id.
[10] Id. at 92-98.

如公司員工經指示將電腦資訊加密阻止外人查看之行為。[11](B)款則規範意圖侵入未經授權進入之電腦（排除超越授權之行為），並因為重大輕率行為造成之損害。[12](C)款乍看與(B)極為相似，但(B)係無過失責任，一旦未經授權之侵入行為，同時造成損害（damage）與損失(loss)時，犯罪即成立。[13]就「損害」電腦之定義，聯邦上訴法院第六巡迴法院於 2011 年在 Pulte Homes, Inc. v. Laborers' International Union of North America, 648 F 3d. 295(6th Cir. 2011)案中，作出解釋：

(3) Pulte Homes, Inc. v. Laborers' International Union of North America[14]

北美勞工國際聯盟（Laborers' International Union of North America, LIUNA)對 Pulte Homes 公司進行了與勞工權益相關之抗議行動，其手法是動員聯盟成員以打電話、寄發電子郵件到 Pulte 公司，使得該公司無法使用電話，電子郵件信箱也因此爆滿，無法正常接收、發送信件。 Pulte 公司向提出告訴，認為該聯盟涉犯 1030(a)(5)「未經授權或超越授權侵入電腦，致生損害罪」。然聯盟辯稱其所做係「間接性攻擊」，並沒有對電腦設備造成損害。

上訴法院維持地院認定，對「損害」（damage）在第 1030(e)(8)條中之定義作出解釋。第 1030(e)(8)條明定：「損害」係指「任何對某數據、程式、系統、資訊之完整性（integrity）、可用性造(availability)成減損(impairment)者」。而法院則進一步根據字典對上「完整性」、「可用性」、「減損」闡釋，認為「完整性」係指「原初的完美狀態」、「可用性」係指「可發揮做用的能力」、「減損」則指「退化、弱化」。而該案被告所做的以大量電話、信件癱瘓 Pulte 公司電信、電腦系統之行為，使得該公司之電話、電腦設備喪失原本之功能，符合法條「損害」之定義。

(4) 加重規定：

1030(c)(4)(A)(i)規定了關於 1030(a)(5)「未經授權或超越授權侵入電腦，致生損害罪」之加重規定，如下：

「(I) 損害發生於 1 人或超過 1 人以上，在 1 年間累計超過 5,000 美元;

(II) 導致 1 人或超過 1 人之醫療檢查、診斷、修復過程被損害或因而有修正必要，或有損害及修正必要之可能;

(III) 對人造成身體傷害;

(IV) 對公共健康及安全造成威脅;

(V) 對美國政府司法、國防、國安系統之電腦造成傷害;

(VI) 行為導致 10 台以上電腦在 1 年內期間受損者。」

就「損害」之計算及加重規定中被告之主觀犯意為何，聯邦上訴法院第九巡迴法院分別於 2000 及 1996 年在 United States v. Middleton, 231 F 3d. 1207 (9th Cir. 2000)案及 United States v. Sablan, 92 F 2d. 865 (9th Cir. 1996)案中，作出解釋：

---

[11] Id. at 100-101.
[12] Id.
[13] Id.
[14] Id. at 108-109.

(5) United States v. Middleton[15]

Nicholas Middleton 曾受僱於 Slip.net 網路服務公司，為公司之網路技術人員。Middleton 離職後，公司仍允許其保留一公司之電子郵件帳號; Middleton 卻使用了一「Switch User」軟體程式，將自己的帳號更換為另一公司員工之帳號，進而操作該帳號，新增或刪除其他帳號。此後，Middleton 又透過一測試帳號，進入公司主要電腦中，新增數個帳號，登入公司用以進行內部管理、經營客戶網站及設有公司帳單系統之重要電腦中，將管理員密碼變更、更改電腦設定、刪除帳單系統及資料庫。被告的破壞行為遭發覺後，Slip.net 公司進行了下列行動：配置新密碼、重新安裝遭刪除之帳單系統軟體、重建遭刪除之資料庫，公司員工共花費超過一百小時修復損害，Slip.net 並僱請了外部資安專家，防範未來破壞再度發生。因上開 Slip.net 所為之價值超過 5000 元，被告被起 1030(c)(4)(A)(i)及 1030(a)(5)之加重毀損電腦罪。然而被告認為，法院拒絕依其請求，對陪審團進行下列指示：「損害之計算，不包括將電腦修復為比原本更良好、更安全之設備」，導致判決結果不公。

巡迴法院駁回了被告之主張，並認為地院原本給陪審團之指示係正確的—「損害之計算，包括各種犯罪後自然會發生且可以想見之結果（natrual and forseeable result）」。因此，Slip.net 公司所羅列的各項後續處理行為，包括加強其資安層級，均可認為係一公司電腦系統遭侵入破壞後，可能採取的舉措，可被列入損害之計算中。

6. 18 U.S.C. 1030(a)(6)「電腦設備密碼竊取罪」:

「明知且以騙取交易為意圖，使用透過侵入未經授權之電腦而取得之密碼或其他類似資訊遂行騙取犯罪者，且須符合下列兩情形之一：(A)所為交易會影響跨州或外國經濟者; 或(B)受侵入電腦係美國政府所使用者。」

7. 18 U.S.C. 1030(a)(7)「恐嚇毀損電腦設備罪」：本條主要所保護之對象為政府機構之電腦或銀行。[16]

「意圖恐嚇取財跨州或跨境間通訊，包括下列內涵者：

(A)威脅損害受保護之電腦者;

(B)威脅將不經授權或超越授權，自受保護之電腦中取得機密資訊或將損害該等資訊者;

(C)索取和損害電腦相關之財物，而該種損害係為遂行恐嚇犯罪而致。」

(二) 美國聯邦刑法典下利用電腦遂行之傳統犯罪

[15] Id. at 113-119.

[16] Charles Doyle, cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, 2 CRS Report for Congress 2008).

侵害著作權、竊取商業機密或兒童色情等等傳統犯罪，無需電腦之參與亦可遂行犯罪，但因為有電腦之使用，該等犯罪對被害人或社會將造成數倍巨大且迅速的損害，以下介紹三種美國重要之利用電腦遂行之傳統犯罪。

1.商業間諜及竊取營業秘密罪：規範在美國聯邦刑法典第 1831 條至第 1839 條，又稱 1996 商業間諜法(Economic Espionage Act of 1996, EEA)。

(1) 重要條文內容：

A.「經濟間諜罪」（18 U.S.C. 1831）：

「(a) 意圖或明知行為將使外國政府、單位、機構獲利，而為下列行為者：

(1) 竊取或未經授權掠奪、取得、攜離、隱藏，或以詐欺、詭計或欺瞞之方式取得營業秘密;

(2) 未經授權複製、重製、素描、作畫、攝影、下載、上傳、改變、銷毀、影印、再製、傳輸、運送、寄送、郵寄、通訊或傳送營業秘密;

(3) 收受、購買、擁有明知為遭竊取、掠奪、取得或侵佔之營業秘密;

(4) 上開三行為之未遂;

(5) 共謀為(1)至(3)行為者;

最高處罰金 500 萬美元或最重 15 年以下有期徒刑。

(b)組織犯上開罪者，最重處罰金 1 千萬美元或所竊營業秘密價值之 3 倍，價值計算包含研發、設計及重置遭竊秘密之支出。」

B.「竊取營業秘密罪」（18 U.S.C. 1832）：

「(a) 明知或意圖所為將損害他人，仍意圖侵佔用於跨州或跨境商業產品或服務之營業秘密，以牟利非秘密擁有者之他人，而為下列行為者：...（(1)-(5)均同商業間諜條文），最重處有期徒刑 10 年。(b)組織犯上開罪者，最重處罰金 500 萬美元或所竊營業秘密價值之 3 倍，價值計算包含研發、設計及重置遭竊秘密之支出。」

(2)美國面臨之商業間諜及營業秘密犯罪現況：

商業間諜犯罪的跨國性，使其與電腦犯罪難以分割，犯罪者包括受外國政府支助之企業、受僱為他人行竊之網路駭客、外國同業競爭對手等，均透過電腦達成犯罪目的。又對美國（或各國）政府而言，現今之尖端營業秘密幾乎均與科技相關，包括 IA 人工智慧或物聯網(Internet of Things, IoT)等，均成為商業間諜犯罪之目標，因此要有效防範、打擊商業間諜及竊取營業秘密罪，必須從嚇止網路犯罪開始。[17]美國政府認為，其現今面對商業間

[17] Dni.gov. (2018). Foreign Economic Espionage in Cyberspace, at 5. [online] Available at: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf [Accessed 24 Oct. 2018].

諜及營業秘密遭竊威脅之來源集中於三個國家：中華人民共和國、伊朗及俄羅斯，此等國家為了制定科技、經濟、軍事等國家政策，亟欲得知美國在此等領域之發展，因此暗中支持企業及個人進行間諜行為，攻擊目標則為商業網絡遍及全球之美國大型國防、電子及通訊業者。[18]

(3) USA v. Xu

Xu Jiaqiang 於 2010 至 2014 年間，在美國 IBM 公司任職軟體研發人員，因而得以接觸 IBM 所研發之某軟體（群集檔案系統，clustered file system）及該等軟體之原始碼，此等軟體經 IBM 公司使用且販賣至世界其他國家，具有高度商業價值。因此，該軟體遠始碼被放置在防火牆後，而 IBM 公司內僅有少數人可接觸之。[19]FBI 循線追查，Xu 向臥底之 FBI 探員表示，其擁有該軟體之原始碼，可複製該軟體後，販售給 FBI 臥底探員，Xu 展示了原始碼並且將複製之軟體上傳與 FBI 探員供其測試，甚至在交涉過程中 Xu 也表示該等原始碼係未經 IBM 公司授權攜出。大陪審團將 Xu 起訴，共 6 項罪名，包括：(1) 竊取並侵佔（stole and converted, count one）、(2) 複製（copied, count two）、(3) 接收並擁有（received and possessed, count three），將該軟體原始碼提供給中華人民共和國國家健康及家庭計畫委員會使用(National Health and Family Planning Commission, NHFPC)等商業間諜及妨害營業秘密。[20]Xu 在紐約南區地方法院審理中認罪，法院判處 5 年有期徒刑。[21]

2. 網路兒童色情犯罪（child pornography）

網路兒童色情犯罪在美國受到高度受重視，且刑罰極為嚴峻——部分犯罪手段，為五年以上有期徒刑，法院無裁量權（mandatory minimum sentence）。立法者重處此等犯罪，係基於受害兒童承受之身心傷害將長期存在，而受侵害影片也在其一生中均有可能再度對之造成傷害，且此等色情影片，將有提高實際兒童性犯罪發生之可能。

網路兒童色情犯罪之規定係在美國聯邦刑法典第 2252 條，內容摘要如下:

(a)(1) 將兒童性行為之影像在跨州、跨境經濟中傳輸、運送(transports or ships);

(2) 接收、散佈(receives or distributes)透過跨州或跨境傳送之兒童色情影像，或為跨州、跨境散佈該影像而重製(reproduces)之;

(3) 販賣(sells) 透過跨州或跨境傳送之兒童色情影像;

(4) 意圖觀看而登入或持有(accesses with intent to view or possesses)透過跨州或跨境傳送之兒童色情影像。

---

[18] id.at 4.

[19] Justice.gov. (2018). Chinese National Sentenced for Economic Espionage and Theft of a Trade Secret From U.S. Company. [online] Available at: https://www.justice.gov/opa/pr/chinese-national-sentenced-economic-espionage-and-theft-trade-secret-us-company [Accessed 27 Oct. 2018].

[20] USA v. Xu, Superseding Indictment, Sl 16 Cr. 10 (KMK) (2016).

[21] Justice.gov. (2018). Chinese National Sentenced for Economic Espionage and Theft of a Trade Secret From U.S. Company. [online] Available at: https://www.justice.gov/opa/pr/chinese-national-sentenced-economic-espionage-and-theft-trade-secret-us-company [Accessed 27 Oct. 2018].

(b)(1)涉犯(1)-(3)款罪之最輕刑度為5年以上有期徒刑，最重不超過20年; 若有同類犯罪前科者，最輕刑度為15年以上有期徒刑，最重不超過40年;

(2)涉犯(4)款罪之最重刑度不超過10年; 若有同類犯罪前科者，最輕刑度為10年以上有期徒刑，最重不超過20年。

(c)就(a)(4)之持有兒童色情影像罪，有下列情況者，經被告主張，可不予起訴：

(1) 所持有之影像未超過三個

(2) 即時處理：(A)已銷毀該等影像;或(B)報告權責單位，交出兒童色情影像與該等單位處理。

二、程序法

當跨境電腦犯罪發生，外國政府核發令狀，向美國人民、企業、政府調取證據，美國資訊擁有者原則無須配合。但在相關法制不斷發展下，電腦犯罪專章逐步修正、增添立法，依索取資訊之不同，分別許可範圍：

(一) 元數據（metadata）之索取

現行法律規範對於個人持外國令狀向美國服務提供者—指電磁通訊服務（electronic communication service provider）、網路服務提供者（remote computing service provider）索取元數據（不涉及資訊實質內容，用以顯示實質資訊之儲存位置、歷史資料、資源尋找、檔案記錄等功能），不承認該令狀之強制力，但允許持有者出於自願提供。美國聯邦刑法典2702條第(c)項第(6)款（18 U.S.C. §2702(c)(6)）規定：

電磁通訊及網路資訊提供者於下列情形可提供與用戶相關之非內容性資訊：

（1）第2073條授權者（詳後述）;

（2）經使用者同意、授權者;

（3）為保護用戶之財產或權利所需;

（4）服務提供者合理認為為預防可能造成生命及身體重大損傷之緊急事件時，經將受警急事件威脅者要求者;

（5）提供予失蹤兒童與兒童剝削防範中心相關資訊或;

（6）提供給非政府機構之個人。

(二) 內容性資訊（contents）之索取

現行法規範禁止美國服務提供者配合外國令狀提供內容性資訊予請求者。要求內容性資訊的索取必須配合第2073條規定之要件。美國聯邦刑法典2073條（18 U.S.C. §2703）規定：

(a) 暫時性或備份性儲存之電信（electronic storage）[22]通訊內容：
政府機關要求電信業者提供其電子通訊系統中之 180 日內通訊內容，但所持令狀必須為經美國認定合格之司法權內法院，依聯邦刑事訴訟程序或州訴訟程序所核發。若超過 180 天以上之通訊內容，要求調取之機關，聲請程序同本條(b)款所定之程序聲請。
（b）遠端電腦設備[23]內電子通信內容
若未經通知用戶，政府機關欲調取遠端電腦設備內電子通信內容者，必須持經美國認定合格之司法權內法院，依聯邦刑事訴訟程序或州訴訟程序所核發之令狀。若已通知用戶，則可使用由大陪審團核發之行政傳票(administrative subpoena)、訴訟傳票（trial subpoena）或依本條(d)款聲請美國法院核發令狀。
（c）政府機關要求索取儲存於遠端電腦設備之非內容性資訊：
必須符合下列標準之一：
(A)取得經美國認定合格之司法權內法院，依聯邦刑事訴訟程序或州訴訟程序所核發之令狀
(B)依本條(d)款聲請美國法院核發之令狀
(C)取得用戶同意
(D)針對電信詐欺案件，可提出書面請求，其上記載資訊擁有對象之年籍資料
(E)若僅是調取使用者之基本資料，可使用由大陪審團核發之行政傳票或訴訟傳票即可

依據上開美國刑法典第 2701 條至第 2712 條（即儲存通訊法, Stored Communication Act, SCA）之規範，關於外國令狀對美國網路及電信服務業者之效力，可分別如下：（1）就非內容之用戶資訊方面：所稱「政府機構」係指「美國之政府單位或政治附屬單位」，明確排除外國政府。故外國政府無法持外國令狀，強制美國網路或電信服務提供者提出與用戶相關之非內容性資訊，僅能仰賴業者自願性配合;（2）就內容性資訊方面：上開法條推定性的禁止個人或政府機構對網路電信服務業者索取內容性資訊。

面對複雜且嚴格之證據取得規則，當外國政府欲自美國業者索取內容性資訊時，通常會透過四種方式[24]：

1. 司法互助程序（Mutual Legal Assistance Treaties, MLAT）:

2009 年美國聯邦政府將司法互助訂入在聯邦刑法典中（18 U.S.C. §3512），並同時將儲存通訊法之令狀（SCA warrant)羅列於得請求協助之範圍。美國聯邦刑法典第 3512 條（18 U.S.C. §3512）規定：
(a)請求與協助之執行—

---

[22] 18 U.S. Code § 2510 (17) “electronic storage” means—
(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.
[23] 18 U.S. Code § 2711(2) the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system.
[24] Orin Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 409-10(2014).

(1)總則—
經（外國政府之國家律師）請求，並經美國司法部權責人員核准後，聯邦法官可核發令狀已執行外國政府請求之事項，以利外國政府進行刑事偵查、沒收、刑之執行及補償程序。
(2) 令狀範圍—
(B) 第 2703 條所規範之標的為已儲存之電信、電子通訊或與該等通訊相關資訊之搜索令或令狀 。
2. 請求美國官員（通常指檢察官）展開國內之刑事調查程序，並在該程序中，向法院聲請相關令狀。然此必須以調查事實在美國亦構成犯罪為前提。且實質面上，因美國檢察官對於是否偵辦某案件，具有較大之裁量權，經常將辦案資源之分配作為是否開啟案件偵查之考量重點，因此外國政府必須說服美國檢察官願意將辦案資源使用於國際協助事宜上，而非用於偵辦其他國內性案件。
3. 透過政策、行政手段，促使美籍網路服務公司在外國政府之分公司，在提供網路服務時，將資訊備份儲存在當地儲存設備中，如此便可避免境外取證之需要。然而此種處置方式，因為儲存地點分散且規模較小，易為駭客攻擊對象，在資訊安全上存有疑慮。
4. 規避法規的灰色地帶方法—請求美國電信服務提供者，將資訊輸出境外，交由第三人，再由第三人交予外國政府。然此部份之合法性遭質疑，認為僅係將原本不法之取證手段，分拆為兩階段型之，並無法治癒其不法。然而美國政府直至 2014 年，並未有判決直接認定此種手段之非法性。

面對 SCA 混亂而複雜的標準，學者倡議應修法，將某一案件能否使用外國令狀調取美國業者所保存之資訊之標準，建立在網路、電信使用者之所在地，而非僵化於資訊儲存地或內容、非內容之分。亦即，若使用者使用電信、網路服務時，係在美國境內，則調取與其相關資訊，無論係非內容或內容性，均應依美國法為之; 反之，若使用者使用服務時，所在位置在國外，則美國業者可以選擇自願配合外國令狀（permissive disclosure），而此不分非內容性或內容性資訊。此種分野方式，可以保護美國境內使用者之隱私權，而外國使用者，因為對受美國法隱私保護並無期待，自然無需強加美國法程序保障之要求於資訊之調去上，反而係偏重給予美國業者判斷權限，由其決定該外國令狀之合法性、對隱私保護之足夠性等因素，選擇是否配合外國政府。如此亦可免除外國極權政府依其國家令狀強迫美國業者協助侵害使用者隱私之問題。[25]學者此一修法之倡議，與美國最高法院微軟案中之意見類同（詳後述）。SCA 之規範並在 Cloud Act—雲端法案之通過後遭到修正（詳後述）。

參、美國網路犯罪新興議題、案例與修法發展

一、 Google 公司對現行跨境取證、司法互助模式的評論與建議

[25] Id. 416-18.

為了打擊犯罪，以美國為首的各國政府持續向 Google 公司要求與其使用者相關之資訊[26]，在 2016 年時，來自政府請求的件數達到高峰，使 Google 對使用者隱私的保護受到輿論質疑，Google 公司夾在配合政府防範、偵查犯罪的壓力與使用者信心動搖的威脅中，在 2016 年 4 月發出聲明，表達其對網路服務提供者協助司法調查此一議題之觀點。

Google 公司首先表達了對現行法規的不滿，其認為現行法規：美國電子通訊隱私法（The U.S. Electronic Communications Privacy Act, ECPA），同時阻礙了政府執法及隱私保護。Google 認為，第一，在現行法律下，跨進資料的調取必需透過 MLAT，依據資訊顯示，平均一次司法互助，請求方需費時 10 個月方能獲取資訊; 第二，為了順利獲取資訊，部分國家開始訂立法律，形式上係規範內國公司，但實質卻產生境外蒐證效力，在執行該法律的同時，很可能違反了證據儲藏國之法律，使得被執行之網路服務提供公司陷於兩難。為求解套，部分國家開始要求網路服務公司將資料儲存於國內，以避開跨境取證的必要，然而此一作法卻對資訊儲存的安全性造成威脅。係因，單一地點的資訊儲存其資安防護能力較弱，容易成網路安全攻擊的對象，對於經營者來說，更提升了營業成本，增加額外支出。第三，現行法對於美國政府所核發之搜索令是否具有「境外」取證的效力，並未清楚界定，導致法院法律上詮釋的困擾，由此從 US v. Microsoft 案件及中及可見一斑（詳後述）。[27]

為此，Google 提出了一個新立法藍圖:應篩選出合格之國家—以該國家對正當法律程序、隱私及人權之保障標準為判斷依據，允許該等國家兼可以相互直接請求資訊之提供，而不需經由傳統司法互助程序。而內國之搜索令效力範圍，應以受搜索人所在地及國籍為準，而非以資訊儲存地為準，例如：若受搜索人為美國人且亦居住於美國境內，則即便與其相關的資訊儲存在愛爾蘭，美國法院所核發的搜索令亦可強制網路服務提供者交出該資訊。在篩選出符合基本權保障標準的國家後，美國與該等國家應該簽訂雙邊協議，將此種司法協助的替代方案法制化。[28]

Google 公司對於現行制度、司法互助模式的臧否，點出了存在已久的問題，其所提出的建議，也預言了制度修正的走向，包括給予特定「合格」國家直接索取證據之可能、雙邊協議之簽訂，均與美國政府在 2018 年最告法院對微軟案作出判決後之立法內容相似。

二、 US v. Microsoft[29]

1. 背景事實介紹

[26] Justice.gov. (2018). Chinese National Sentenced for Economic Espionage and Theft of a Trade Secret From U.S. Company. [online] Available at: https://www.justice.gov/opa/pr/chinese-national-sentenced-economic-espionage-and-theft-trade-secret-us-company [Accessed 27 Oct. 2018].
[27] Walker, K. (2018). Digital security and due process: A new legal framework for the cloud era. [online] Google. Available at: https://www.blog.google/outreach-initiatives/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/ [Accessed 12 Sep. 2018].
[28] Id.
[29] United States v. Microsoft Corp., 584 U.S. (2018).

微軟公司在西元1997年設立了一以網站為基地的電子郵件服務，向公眾提供服務，也就是Outlook.com。用戶透過該電子郵件服務所登記、傳送、接受的資訊，分別儲存在微軟母公司或子公司的數據中心內，微軟公司的母公司總部位於美國，惟其眾多子公司則散佈在世界各地。

微軟美國母公司在2013年收到來自美國司法部向法院取得之搜索票，要求其提出某一Outlook.com使用者的電子郵件相關資訊。微軟母公司僅向司法部提供了該用戶電子信箱的通訊錄，此外則拒絕提供諸如註冊資料、電子郵件收發對象及內容等資料，理由為：儲存相關電磁紀錄的伺服器係為在美國境外—愛爾蘭的都柏林，而司法部所持搜索令是由美國地方治安法院核發，無權要求微軟公司提供境外資料;其認為微軟公司若要取得該等位在都柏林伺服器的資料，必須要遵循司法互助管道，由司法部向都柏林司法部門提出互助請求，取得都柏林司法單位之許可後，才能伸手進入微軟公司都柏林分公司的伺服器，拿取資料。然而地方治安法院則駁回了微軟公司撤銷該搜索票之請求; 法院認為，依據Stored Communications Act（SCA，儲存通訊法），法院得核發搜索票，准許執法人員搜索儲存在外國伺服器的電磁紀錄，蓋因當執法人員取得電子紀錄時，審視電磁紀錄之地點將是在美國境內，至於資料取得地點，並非管轄權判斷的準據。

微軟公司對地方治安法院判決向地方法院提起上訴，地方法院再重新審理案件後，維持地方治安法院的裁定，甚進而對微軟公司拒絕提供電磁紀錄之行為以藐視法庭為由做出裁罰。然而，上訴法院及第二巡迴法院則撤銷了地方法院的判決，其認為Stored Communications Act並未授權地方治安法院對儲存在外國伺服器中之資料發出搜索票，藐視法庭的裁罰被撤銷，案件被發回地院。

2. 法律爭議

(1) SCA是否可以作為境外搜索之授權依據？

結論是否定的。依循判例，若國會沒有明確定授權某法律具有境外效力，則該法律之適用僅限於內國事務（“absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application.”）。而從SCA法條文字中，並無法看出立法者有授予之境外效力之意，因此當某搜索行為是在美國國土以外發生時，SCA所核發的搜索令即無法做為搜索之依據。

檢察官很早即放棄了此一論點，轉而爭執要求微軟公司提出愛爾蘭伺服器內所儲存資料的行為，並不構成搜索，而即便構成搜索，也是一境內搜索行為。

(2) 請求微軟提出愛爾蘭伺服器之資料，是否為搜索行為？或僅為傳票調取資料(subpoena)行為？

檢察官為了避開「依據SCA所核發之搜索令僅能對內國發生效力」的限制，將其要求微軟公司提出資料的行為，詮釋為傳票調取資料(supeona)行為。檢察官將首先界定了傳票調取資料(supeona)行為所針對的是紀錄(record)，例如公司的商業紀錄等資料，有別於搜索行為（search and seizure)所針對的是內容(content)；而政府要求微軟交出來自愛爾蘭伺服器的行為中，包含了兩階段：資料的傳輸(transferring of record)及內容的揭露(disclosure of content)，如此一來，若將前半部資料傳輸行為是透過傳票拿取，即便涉

外，亦不在受 SCA 第 2703 條搜索令僅對內生效的限制，而後半部，當微軟公司交出電子郵件內容時，政府才算是取得了資料之內容，而構成搜索，但此時搜索地點已在美國境內，符合 SCA 規範。

微軟公司反對此種切割，認為檢察官的論點明顯在規避依 SCA 所核發之搜索票無法境外搜索之規範。微軟公司認為，前半段由愛爾蘭傳送電子郵件返回美國之行為，所涉及之資訊，就是電子郵件的「內容」，並非單純之「紀錄」，而 SCA 中也將政府索取涉及通訊「內容」者，視為構成搜索行為，排除於「傳票」所得拿取的「紀錄」外。而且搜索包含複製欲索取之資訊的階段，並不只限於打開、閱覽、揭露該資訊時，因此當微軟公司在愛爾蘭端複製資料以利傳輸回美國公司交出予政府時，搜索行為即發生在愛爾蘭，檢察官的行為顯然在進行境外搜索。

(3) 執法地點是否在境外？

假設法院認定政府要求微軟交出資訊的行為是搜索行為，則執行搜索地點究竟在何處？檢察官認為，SCA 第 2703 條所針對的(focus)是「係爭資訊曝光時」(disclosure as the "focus" of § 2703)。因此，即便部分取證行為發生在海外，只要資訊遭揭露地點係在美國境內，即可認為是一般的境內搜索。

微軟則認為，SCA 第 2703 條所針對的(focus)是「隱私權被侵犯時」(privacy as the "focus" of § 2703)。很明顯的，政府已將手伸入微軟公司秘密保護、放置在愛爾蘭伺服器的資訊，即便政府尚未將之打開來閱覽，該秘密的隱私已經受到入侵(intrusion)，如果依照政府狹隘地將搜索限於資訊揭露時，排除資訊的「複製」、「傳輸」階段，則無法全面保障隱私權。

3. 法院審理結果

案件在 2017 年排入最高法院審議期程中，引起各界高度爭議與關注，然而眾議院於 2018 年 3 月 22 日，通過了一項法案—Clarifying Lawful Overseas Use of Data Act（釐清電磁資料海外合法使用法，又稱 CLOUD Act)，因為此法案係針對本案搜索令核發所依據的 Stored Communications Act 作出解釋與修正，對於類同於本案之事實，提供了明確的取證程序規範，司法部僅需依據該新法案對微軟公司提出取證要求，若能滿足該法規所設要件，微軟公司即應提出其放置在海外伺服器內的電磁資料。此一新法案的誕生對本案的法庭審理產生根本性影響。美國司法部在法案經眾議院通過後，便以「案件為虛擬」（moot，即爭議已解決，審理無實益）為理由，請求法院不再審理此案，可預期的是，最高法院則在 2018 年 4 月 17 日做出判決，撤銷上訴法院之判決，將案件發回第二巡迴法院，指示其撤銷地院之本案判決及藐視法庭裁罰。

三、 釐清電磁資料海外合法使用法（CLOUD Act）

1. 法案介紹

該法案為針對美國聯邦刑法典中儲存通訊法之修訂，目的在於改善執法單位對於跨境資料收取的機制。法案分為兩部份，第一部份規範美國自外國取證之行為，第二部份則規定外國向美國的取證行為。以下就此兩部份，則要簡介：

(1) 美國執法單位自外國取得資訊：

「電子通訊或遠端電腦服務之提供者，當其擁有、持有、控管屬於其服務使用者之電信、電磁紀錄時，依本法負有保存、備份及揭露該等資訊之義務，至於該等資訊存放地點係在美國國境內，或保存在境外他國，不在所論。」[30]該法案就美國執法單位欲自他國取得電磁紀錄資訊時，開章明義的確認了美國網路服務提供者，必須配合執法單位提供存放在境外之資訊的義務。這個定性，係針對最高法院對微軟案的判決而生，以「業者必須配合執法單位提出資料」為原則。而必須注意的是，此原則適用的對象限於與美國訂有行政協議的合格外國政府（qualifying foreign government）。要成為合格外國政府，必須該政府對於電磁紀錄之取得，亦設有符合美國標準的實體及程序規範，以防止對人民隱私的不正侵犯。

當然，有原則必有例外。該法案給予業者聲請法院撤銷或修改提供資訊命令的權力，並且為法院訂立了一套是否撤銷或修正的判斷準則(comity analysis)[31]：

(A)美國執法單位透過此取證程序可以確保的偵查利益;

(B)合格外國政府拒絕提供證據可以獲得之利益;

(C)業者若配合提供證據後，因為兩國間法律規範的落差，而受到的刑事制裁或其他裁罰的可能性、受處罰性質及嚴重性;

(D)資訊將遭搜取的服務使用者所在位置、國籍，該使用者與美國或與資訊存放國之關係;

(E)資訊提供者與美國之聯繫因素及所在地是否在美國;

---

[30] "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

[31] COMITY ANALYSIS.—For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate—

"(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;

"(B) the interests of the qualifying foreign government in preventing any prohibited disclosure;

"(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

"(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;

"(E) the nature and extent of the provider's ties to and presence in the United States;

"(F) the importance to the investigation of the information required to be disclosed;

"(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

"(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

(F)調查該將受揭露資訊之重要性;
(G)是否有其他侵害較小之手段可以獲取該資訊;
(H)若係在司法互助下，代表外國國家透過本法進行資料調取，該外國國家所受有的偵查利益。

在考量上開各點後，如果法院可以撤銷或修正境外取證的准駁，以維護司法之利益(the interests of justice)。

美國執法單位取得業者儲存在外國之資訊時，業者原則上必須同意，但例外可以向法院提出禮讓請求(comity claim)，已如上述。然而，此種境外取證實際上要發生與外國法律牴觸、對外國司法主權或人民隱私造成不利影響，且該等影響大過於取證利益的情況，依照以往司法互助的經驗，實難想像。但這個狀況，在歐盟於 2018 年 5 月施行資料保護法後(General Data Protection Regulation)，產生些許變化。歐盟的資料保護法就歐盟成員國將所掌握之資訊交給非歐盟國，設有多項限制，且要求此種資訊傳送，必須是以兩國之協議作為基礎 ; 然而，非常明顯的，美國與歐盟間並沒有一個協議，同意美國持其內國法院之令狀，不透過司法互助，直接索取存放在歐盟國資訊之協議。但該資料保護法對此等限制也設置了例外條款，即：當為保護重要公益而有必要時(necessary for important reasons of public interest)，及迫切的合法利益存在時(compelling legitimate interests)。[32] 當歐盟的資料保護法與美國的 CLOUD 法案發生衝突時，美國法院要如何依據上開標準審視資料調取許可的合法性、歐盟法院又要如何解釋資料保護法的兩項例外，都是兩法案開始施行後的未定數，歐盟與美國間或許會透過簽訂新的協議來處理此灰色地帶，也有可能是靠兩地法院判決的累積，形成慣例。

(2) 外國執法單位向美國業者索取資訊：

依照 SCA 規定，國外執法單位若欲取得儲存在美國境內之資料時，即便是外國政府欲調取對於其本國人在本國所犯犯罪，都必須要透過司法互助規定(the mutual legal assistance treaty, MLAT)，然而這對於外國執法單位來說，無疑是案件偵查過程中重大的負擔，因為司法互助機制必須透過層層申請、聲請，曠日廢時，嚴重阻撓外國政府打擊犯罪的效能。CLOUD 法案針對此部分大刀闊斧地做出了改變。

依據該法規定，美國檢察總長及國務卿有權，認證外國國家，允許該等國家跳過司法互助程序，直接透過 CLOUD 法，向美國業者索取資訊。然而要成為此等受認證之國家，必須符合 CLOUD 法所列之實體、程序標準，並與美國簽立行政協議。其羅列眾多標準，茲介紹重要者如下：

A. 外國政府必須要訂有堅實的程序及實體法規，在相關資料調取程序中，保障人民隱私等基本權利。在此所說的程序法及實體法，包含了與電腦反罪相關之程序及實體法，可以

[32] Jennifer Daskal, J. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. Stanford Law Review, [online] 71. Available at: https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/ [Accessed 16 Sep. 2018].

2001 年 11 月 23 日在布達佩斯鎖定立之電腦犯罪公約為本，審視某外國政府之立法品質。且外國政府之立法亦須符合法治精神及遵守世界人權保護原則。

B. 外國政府採取了必要措施，盡量降低取證、留置證據及傳播資訊之需求。

C. 外國政府所核發的取證命令，必須明確且特定，即應列出對象人別、帳戶、地址、資訊存放設備，並且必須以預防、偵查、追訴重大犯罪為目的。

D. 該外國取證命令，必須是由職司審判之獨立機關依法核發。

E. 如果欲對正在通訊之電磁資訊做攔截，必須要載明特定期間。

F. 取證命令必須有助於目標之達成，且並無其他更小侵害之替代方式存在。

G. 外國政府必須同意美國政府對該資訊是否受到妥適使用進行期間性的監督。

必須注意的是，CLOUD 法案所授權的外國政府向美國業者取證，僅限於資訊擁有者為「身處美國境外之外國人」。反之而言，如若該人為美國公民、美國合法居留者或其他身處美國境內之人，外國政府仍需透過傳統之司法互助機制，向美國業者索取電磁資訊。[33]這樣的分野，建築在美國政府對於美國人及美國境內之人採取高度之隱私保護，且其認為其有權介入管理資訊流通向外國之事，而對於外國政府從美國業者手中拿取屬於外國人之資訊，美國政府則採取較保守、限縮之姿態，給予外國政府較大自由與權限。

CLOUD 法案若通過後，除將對美國與他國就電腦犯罪跨境取證之互動模式產生根本性之影響，更有可能導致各外國就其關於強制力取證之內國法加以修正，以符合 CLOUD 法案中所要求之程序及實體標準，方能滿足與美國簽訂行政協議之前提。事實上，英國已經受到 CLOUD 法案的影響，修正其內國法中關於強制取證之規定，可以預見的，其他國家也將跟進，確保其對隱私、人權之保護能達成 CLOUD 法案之期待。這是一個透過內國法案影響國際性執法標準的標準案例，因訂立法案者為美國，為刑事司法互助之重要樞紐國，因此其立法所生之影響，更為顯著而巨大。

我國因應於此，同樣必須檢視我國之相關取證規定，是否尚有不足之處。譬如 CLOUD 法案中要求外國政府必須同意遵循與美國簽訂之行政協議中證據使用之方式，並定期受美國政府的檢視與監控。則我國內國法關於協議條件遵循之方式、監督證據使用之機關及於美國對證據使用進行審查時之對口機關為何，均有加以研議之必要。

2. 對雲端法案之批評

然而雲端法案通過在及，批評聲浪仍未停歇。數個反對該法案之團體，對於法案提出兩項主要批評：(1)法案通過後，將危害各國對其國境內所持有之資訊之隱私保護 ；(2)外國將透過該法案，對第三國人民進行監聽或獲取該第三國人民之資訊，而無需第三國司法單位之把關。[34]

上開批評並非空穴來風，針對第一項批評，可以體現在歐盟之資料保護法與美國雲端法之衝突上，其背後即反應了兩國、不同法治系統對隱私之保護時，跨境諮詢應如何被保護及

[33] Id.

[34] Ruiz, D. (2018). Responsibility Deflected, the CLOUD Act Passes. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes [Accessed 19 Sep. 2018].

揭露。因應美國雲端法之制定，歐盟內部及有聲浪表示必須從嚴全是可以向美國雲端法妥協之例外情況，否則即是違反了該資料保護法為提升歐盟內資訊保障強度之立法目的。[35]而針對第二項批評，最令人憂心者是，美國與外國僅需透過行政協議，即可允許該國獲取對存在於第三國之資訊，何國具有資格可與美國訂立行政協議，選擇權繫於檢察總長與國務卿所隸屬之行政權，欠缺有力之權力分立監督，且資料遭掠取之第三國在程序中亦無置喙餘地，無異大開隱私權保護大門。[36] 面對 CLOUD 法案通過後可能造成的隱私威脅，我國是否也有訂例如歐盟資料保護法相關章節之必要、當我國境內之資訊面臨遭掠奪之危機時，應由何機關為危機處理者、相關機制為何，及當資料已被擷取，負責提出救濟之機關、救濟途徑為何，均是必須考量之問題。

四、 反駭偵查行動(hacking back)

1. 基本定義

政府使用駭客行為蒐取情報，進行間諜工作或反制他人對政府之傷害，譬如俄羅斯政府僱用駭客入侵美國民主黨委員會之電子信箱，竊取與 2016 年總統選舉相關資訊、美國與伊拉克政府據稱駭入伊朗政府電腦以阻止其進行核分離行為、北韓政府駭入 SONY 音樂位在美國總部，報復其嘲弄北韓領導人之行為...等等，向來存在。然而這種由政府所進行的駭客行為，其實係建立在合法與非法的灰色地帶上，而勉強由國家安全為由將之正當化。

在電腦犯罪日益猖獗的今日，司法單位面對隱藏於網路世界中的罪犯及證據，是否可以採取更積極的蒐證手段—即反駭偵查行動，即不斷被討論。美國聯邦調查局在 2014 年進行了大規模的反駭偵查行動，其使用一名為「網路調查科技」（Network Investigative Technique, NIT）之電腦病毒，植入某非法網站使用者之電腦內，索取如 IP 位置等使用者資料，特定犯罪嫌疑人。[37]

數個問題在學術及實務界爭執不斷：1.反駭行為之法律地位，係資料調取？或搜索扣押行為？2.搜索令之核發是否符合明確性及合理懷疑門檻？3.反駭目標若在海外，是否構成境外搜索，而有侵害他國司法權領域之虞？

2. 案例介紹—FBI 查緝 Playpen 網站案件

美國聯邦調查局收到來自境外之資訊，一架設在美國之網站 Playpen 涉嫌刊登兒童色情影像供使用者觀賞。該網站為了躲避追緝，使用洋蔥式迴路（onion router network, Tor network)，即透過在多個伺服器間轉跳上網路徑，隱藏使用者之位置，同時也將登入路徑加密，雙重確保隱密性。

[35] Id.
[36] Id.
[37] Kerr, O. (2017). 2017 statutory and case supplement to Computer crime law. 3rd ed. pp.214-215.

聯邦調查局在 2014 年時，佔領了該網站，但為追蹤涉嫌違反兒童色情罪之使用者之身分，並未將其關閉，開始經營該網站達數星期，目的是為了展開反駭偵查行動。聯邦調查局首先向法院取得了一張搜索票，將 NIT 安裝至 Playpen 網站中，待使用者輸入帳號密碼登入該網站時，NIT 便會侵入使用者之電腦，將使用者之 IP 位置等相關資訊回傳給聯邦調查局。在數個禮拜內，調查局便以此方式入侵了一千台電腦，資料遭劫取之使用者，或稱犯罪嫌疑人，遍及全球，使該案成為一跨國之司法執行。[3839]

3. 搜索合法性爭議

美國刑事訴訟程序要求法院核發搜索票時必須檢視是否具有犯罪的可能理由（probable cause）及明確性（particularity）。挑戰 Playpen 令狀合法性者認為，聯邦調查局持一張由東維吉尼雅區聯邦治安法官所核發之搜索令即對全美國、全球登入 Playpen 之電腦進行搜索，不但無法證明受搜索登入者均有犯罪嫌疑，也沒有特定搜索對象，形同一張空白搜索票（general search warrant）。受起訴者向各州法院提出控告，多數法院均採用下列邏輯，肯認該搜索票、搜索行動之合法性：

(1) 犯罪的可能理由：在眾多可以顯示登入者之主觀犯意之事證中，Playpen 之首頁即顯示了明顯的兒童色情影像，因此登入者主觀上必然知道即將登入之網站涉及兒童色情，由此便可以支持搜索對象可能違法。[40]又，Playpen 使用者必須配合網站，經過重重審核，因此可以排除偶然登入該網站之可能性。由此兩點，多數法院均認為有合理理由可以支持該搜索行為。[41]

(2) 明確性：法院認為，明確性並不因搜索標的數目龐大而受到影響; 依循犯罪的可能理由之判斷，所有登入該網站之人，均有涉嫌犯罪嫌疑，則每台電腦均有被搜索之理由。法院搜索票將搜索扣押對象特定於「登入 Playpen 網站之電腦」及「與透過網站觀賞、使用兒童色情影像之證據」，具有明確性。[42]

4. 政府反駭行動使用在跨國網路犯罪之合法性、可行性探討[43]：

論者有謂，使用電腦病毒駭入犯罪嫌疑人電腦之反駭偵查手段，因為搜索之目的即在特定犯罪嫌疑人，本質上無法在搜索前確認搜索對象所在位置及身分，因此極有可能發生境外搜索及扣押之結果，是一侵犯他國司法主權之行為，將對國際關係造成威脅，也有違國際習慣法，不得為未經他國同意進行境外執法行為之原則，更可能致執行搜索行為之美國執法人員遭外國司法追訴責任之風險。[44]

---

[38] Id.

[39] Rumold, M. (2016). Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation [Accessed 20 Oct. 2018].

[40] Supra Orin S. Kerr, note 37 at 215-216.

[41] Id.

[42] Supra Orin S. Kerr, note 37 at 216-217.

[43] Orin S. Kerr; Sean D. Murphy, Government Hacking to Light the Dark Web: What Risks to International Relations and International Law, 70 Stan. L. Rev. Online 58 (2017-2018)

[44] Ghappour, A. (2016). Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. SSRN Electronic Journal, 69, p.1075.

支持反駭偵查手段之論者認，儘管反駭偵查手段的使用，可能造成執法界線的爭議，然隨著網路犯罪之發展，相關爭議在實際運作上，並不會在國家間產生問題，並且也可透過跨國合作模式的發展，逐漸被解決。[45]舉例來說，在打擊刑事之司法互助領域，各國間依循公約、協定、或備忘錄等的簽署，已經發展為一綿密的互助網絡，而國際性組織，如國際刑警組織或歐洲刑警組織等，也長期致力於跨境合作。再以，各國政府間均設有涉外事務之聯繫窗口，可以及時提供或掌握他國就跨境犯罪之偵查進度，適時予以協助。跨境網路犯罪更是國際合作最為密切的案件類型之一，以 Playpen 網站案件為例，侵害兒童性自主權犯罪之可罰性普世皆然，各國政府間目標一致，自然對於外國政府之反駭搜索行為持支持態度，歐洲刑警組織更以「重要之國際合作案例」稱之。同樣使用 NIT 反駭入犯罪網站，追索犯嫌身分之案例，包括全球最大毒藥網路黑市「絲路」網站（Silk Road)之破獲：在美國聯邦調查局採取反駭手段確認網路經營者身份及位置係為在冰島後，向冰島政府發出合作請求，而後由冰島執法單位依其國內程序扣押相關證據後，交給美國調查局使用。值得注意的是，採用反駭偵查手段的國家並不僅止於美國，歐洲刑警組織也曾使用 NIT 駭入登入兒童色情網站 The Giftbox Exchange 之使用者電腦[46]，澳洲警方也使用網路誘騙方式（phishing）駭入另一兒童色情網站 The Love Zone 之使用者電腦[47]。這些遭駭入之電腦，許多係為在美國境內，但並未遭到美國政府之反對。 由此等案例，均顯示出各國現有機制足以處理反駭偵查中發生之跨境執行結果，並實質有助於國際合作之發生。

批評者亦有認，使用 NIT 進行偵查破壞了國際司法互助方式，不符合國際習慣法，亦將導致蒐證行動違法，譬如美國政府使用 NIT 自外國電腦中取證之行為，違反了美國法律機構 1987 年的法律釋義（American Law Institute in a 1987 Restatement）—即美國執法單位未經他國同意，不得跨境執法[48]。支持論者則認為，從文義解釋，該 1987 年之法律釋義所描述的係實體的進入他國境內進行執法行動，與執法者身處美國境內，使用軟體透過網路取得他國電腦內資訊不同;再以，從立法歷史進程解釋 1987 年之規範，應認為該法律釋義在編纂時無從考量到網路科技對犯罪手段及偵查方式之影響，因此其詮釋對象並不包括此種反駭偵查手段，自然不能據以認定反駭偵查手段違法。從另一方面，對英美法系國家而言，習慣法的生成本就與時空變遷有所呼應，當世界各國均接受反駭偵查手段知識，此種偵查行為也將成為國際習慣法之一部分。末以，要求使用如 NIT 類之反駭偵查前，必須依循傳統司法互助方式、取得他國政府同意，在實際上並不可行，蓋因 NIT 之存在目的即是特定難以特定之

[45] Supra Orin S. Kerr, note 43 at 61-62.
[46] Cox, J. (2017). The Strange Case of a Hacked Dark Web Child Porn Site Just Got Stranger. [online] Available at: https://motherboard.vice.com/ en-us/article/the-strange-case-of-a-hacked-dark-web-child-porn-site-just-got-stranger. [Accessed 18 Oct. 2018].
[47] Cox, J. (2016). AustralianAuthoritiesHacked Computers in the US. [online] Available at: https://motherboard.vice.com/en-us/article/australian-authorities-hacked-computers-in-the-us [Accessed 28 Oct. 2018].
[48] Supra Ghappour, note 44 at 1117-18.

犯罪行為人身份及位置，在未特定身分位置前，要求執法單位事先取的他國許可，便如同雞生蛋蛋生雞之問題，陷入循環。[49]

反對者認為NIT，反駭偵查手段必須被限縮且被制度化。限縮方式包括：1. 進行反駭手段前，必須先特定受搜索人（電腦）之IP位置，若位在國外則必須依循司法互助方式取得他國同意; 2.必須將犯罪類型限縮在可以特殊類型，經常需要進行跨境偵查之類型上，如反恐、兒童色情、組織犯罪等。[50]本文認為，反對論者提出之反駭偵查手段規範架構過於保守，因為若將反駭的使用限縮在涉及境外電腦時，必須取得他國同意，減損了反駭偵查中重要之功能—找尋犯罪者位置，而此功能在打擊現金重大網路犯罪，扮演重要角色，更可認為是反駭偵查的核心功能。因此如果同意反駭偵查之採用，必須面對的是傳統司法互助模式是否可以被改變，例如對特定犯罪開放跨境執行，且允許先執行後，後請求互助。

然而，支持者之論點則對於國際司法合作之狀況，有流於過於樂觀之嫌。首先，在司法互助現況上，並非所有國家均有良好之互動關係。支持論者所描述之美國及歐盟、或歐盟各國間互助之順暢，係建立在該等國家、區域在堅強之經濟及政治實力、文化及歷史背景的關聯、長年以來累積的互助案例及政府間之信任感上。然而，令人挫折的現實是，此種背景狀態，並不必然存在於美國與世界其他國家、或歐美以外其他國家間。譬如，若今日是由開發中或未開發國家警方對歐盟或美國境內電腦植入NIT惡意軟體，搜取資料，則歐美政府是否仍對於該搜索行為持支持態度，甚而繼續協助後續偵查，實存有疑問。再以，Playpen網站使用者涉嫌之犯罪行為係兒童色情犯罪，可罰性普世皆然，然若當電腦使用者涉嫌之犯罪，係竊取商業機密、著作權、商標權、國家機密等罪，美國或歐美政府，是否也樂於將遭指控之本國公民所擁有之資料，交予外國政府，更令人感到懷疑。又或者，即便發動偵查之國家並非開發中或未開發國家，當受搜索之標的係美國重要商業機構，甚至政府機構，當企業與政府機關代表向法院提出搜索合法性之質疑，實難想像美國法院能夠毫無疑慮的肯認該等證據的證據力。

反駭偵查將會成為打擊電腦犯罪之主流議題，正如同英國之偵查權力法案，其立法之原因之一，即是要正視執法單位的蠢蠢欲動，與其強硬禁止反使執法單位走向偏鋒，不如呈現在檯面上討論，將之制度化。在保守與開放間，可以想像的合作方式似仍以條約、協議或備忘錄的簽訂為基礎為宜，即在國家間達成概括性的協議，允許他國對本國境內電腦進行反駭偵查手段，在協議中規範執行之門檻，如：必須取得本國法院之令狀，及事後審查機制，如：完成後必須陳報兩國法院，並賦予受執行國家反對之權利。若執行後發現受執行電腦並非簽約國，內國法針對此亦應該建立一審查機制，由法院依比例原則執行之必要性與侵害之程度。

肆、英國打擊網路犯罪修法趨勢——2016 調查權力法

[49] Supra Kerr, note 43, at 66-68.
[50] Supra Ghappour, note 44 at 1117-18, 1128-1131.

在打擊犯罪的過程中，跨境取證的難題同樣困擾著英國。面對司法互助的費時費工，英國早在 2016 年時，便開始了一個領先全球的立法——2016 調查權力法(Investigatory Powers Act 2016, IPA 2016，又稱窺伺者法案，snooper’s charter)。該法大規模的修正了調查權立法的內容，賦予執法機關調取海外電信通訊內容及相關資訊的權利。以下針對該法案對於跨境取證之規範，進行介紹。

一、實體內容[51]

調查權力法第六部分第一章第 136 條規定，政府通信局(Government Communications Headquarters, GCHQ)可以透過「概括性攔截令狀」（bulk interception warrant），進行對海外電信資料的搜索。所謂「概括性攔截令狀」係指對於傳輸中之電磁紀錄（communication）及與之相關之資訊（secondary data)進行監控與擷取。同法第六部分第三章第 176 條規定，政府亦可透過「概括性設備侵入令狀」（bulk equipment interference warrant）進行對海外電信資料的搜索。所謂「概括性設備侵入令狀」即係俗稱之「駭入電腦設備」(the process of hacking)之行為，包括：使用設備駭入或感染他人電磁設備、遠端遙控電磁設備、入侵電腦內之資料夾、窺看加密電磁訊息、取得私密之密碼或加密之鑰匙、即時監看他人網路活動、毀壞電磁設備等等。依照本法案第 138 條、第 178 條規定，概括性設備侵入令狀」，搜索標的為：(i)海外通訊內容(overseas-related communications); (ii) 海外資訊(overseas-related information); (iii)海外可供個特定資訊來源之相關資訊(overseas-related equipment data)。而上開兩種令狀之目的，在於確保下列事項之必要性: (i) 國家安全、(ii)預防及偵查重大犯罪、(iii)保障英國之經濟利益，例如：反恐、反核武、維護經濟發展、反網路攻擊、維護國家情治單位及盟友之運作、國家維安及打擊重大犯罪。

二、程序要求[52]

同法第 138 條、第 178 條對於令狀的核發程序作出規定，將之訂為「雙重審查機制」(double lock mechanism)，實施通訊監察、調取資訊之機構，必須向國務卿(the Secretary of State)提出申請，國務卿在審查核發令狀之必要性後，可決定准駁。國務卿允准後、令狀核發前，必須接受司法委員會委員(Judicial Commissioners)之審查。

三、外界批評

[51] 2016 Investigatory Power Act, Article 136.
[52] 2016 Investigatory Power Act, Article 138, 178.

英國政府在立法後，稱該法是一獨步全球之立法，是將政府對於通訊監察及取證行為透明化、制度化，然而隱私及人權倡議人士則認為這是將過度的政府監控行為合法化的荒謬立法。反對該法案人士的批評主要包括三個面向：第一，透過本法案可以獲取資訊之政府機關過多，上從司法單位、情治單位下至稅務機關，均可成為請求令狀之機構[53]；第二，依據該法所核發的令狀，可以針對整個種類的資訊或某財產範圍內的資訊進行大規模的搜索與扣押，即所謂的主題性搜索令(thematic warrants)，違反了搜索令必須具有明確、可得特定性(particularity)之法律原則[54]；第三，令狀的審核繫於行政權力國務卿手中，司法審核僅能進行形式審查，難以推翻國務卿之決定。而法案中關於令狀核發必要性之規範，用語非常模糊，充滿解釋空間，很容易包含各種使用用途，難以質疑該令狀之合法性，所謂的「雙重審查機制」淪為形式[55]。第四，本法案允許英國政府搜索、扣押境外電磁資料，有可能與外國法律規定、司法程序發生衝突；而單方的授權，在執行上也可能因為與外國規定扞格，而在執行時遭受阻礙。

四、法院態度

英國高等法院在 107 年 4 月 27 日，在 The National Council for Civil Liberties 訴 Secretary of State for the Home Department (Liberty v. SSHD) 案件中作出判決，認定 2016 調查權力法第四部分與歐盟法及歐盟人權公約 (European Union law and the European Convention on Human Rights, ECHR)扞格。

調查權力法違反歐盟法規及歐盟人權公約處有二：1. 依據該法規可以對電信業者或私人企業進行概括性電磁紀錄之攔截與駭入電腦設備之發動是由包山包海，已經超出了歐盟法規中，將發動原因限縮於偵查及預防重大犯罪之範圍。2. 取得經留置之電磁資訊之授權，並未受到法院或具獨立性之行政機關之事前審查。在上訴法院審理過程中，被告及英國內政部也承認調查權力法就此部分確實與歐盟法規及人權公約有扞格。上訴法院遂於判決中宣布，英國內政部必須在 107 年 11 月 1 月前就該法案之第四部分加以修正。然而，法院並未同意原告 Liberty 所稱：「調查權力法授權了籠統、無區別的資訊的留置與獲取」，只保守的要求修法以符合歐盟規範。[56]

五、英國跨境取證法制之未來走向

[53] 2016 Investigatory Power Act, Article 18.
[54] Medium. (2017). The UK Investigatory Powers Act: A Bad Example for the World. [online] Available at: https://medium.com/privacy-international/the-uk-investigatory-powers-act-a-bad-example-for-the-world-4e51b0d126b0 [Accessed 18 Sep. 2018].
[55] Ryk-Lakhman, I. (2016). The Investigatory Powers Act and International Law: Part I | UCL UCL Journal of Law and Jurisprudence Blog. [online] Blogs.ucl.ac.uk. Available at: https://blogs.ucl.ac.uk/law-journal/2016/12/26/the-investigatory-powers-act-and-international-law-part-i/ [Accessed 21 Sep. 2018].
[56] Liberty v SSHD, [2018] EWHC 975 (Admin)(27 April, 2018).

原告對調查權力法案的挑戰並不止步於此，其正發動募款，預計下一次的司法訴訟中，將挑戰該法第六部分所規定的概括性電磁紀錄攔截與案入電腦設備之規。[57] 若依照上訴法院在 Liberty v. SSHD 邏輯，調查權力法對於與擷取、駭入電腦以獲取海外電磁記錄相關之第六部分，同樣具有廣泛的發動原因，並不僅限於對於重大犯罪的預防與偵查，而法院之角色也僅在於國務院同意核發令狀後，進行程序性、形式審核，於 Liberty v. SSHD 案件中被法院指出不合於歐盟法律與人權公約之狀況如出一徹，其合法性恐將遭到法院同樣的質疑。[58] 其次，該法案第六部分授權為獲取海外電磁資訊，可以對電腦設備進行干預，即駭入電磁設備行為，搜索行為主動、範圍廣大且難以監督，對隱私權之侵犯極大，亦有可能造成不可預期的經濟損害，恐需有極正當之公益目的賴以維護，且課予極嚴密之審查程序，方有合法之可能。觀諸調查權力法在第六章之規範，能否滿足此種審查標準，實有疑慮。再以，第六章內所稱之「海外」資訊，僅以「收發通訊資訊之人位處英國國境之外」為其定義，允許將此等資訊列為搜索扣押範圍，似未區分受搜索電磁設備之持用人國籍、網路通訊服務公司國籍等區別，一律認為可對之搜索扣押，則於受搜索之人、服務提供公司事後發現，而主張依其所屬國法規或區域性規約（如歐盟規約），英政府單位係進行違法之隱私權侵害行為，英政府機關是否能依據調查權力法案為駭客行為依據，阻卻違法，恐將造成英國與他國間之矛盾。

調查權力法雖合法化了英國政府機關對境外公司或個人索取資訊之行為，而不論外國單位係因為理解到此一蒐證係英國政府之合法行為、或因擔心不加以配合將被英國法院認為藐視法庭，故而主動願意配合蒐證，但畢竟仍只具有英國內國之單方法律效力，執法上仍然很有可能受到阻礙。傳統法學概念上，各國均有其不可侵犯之審判權，境外執法受到嚴格的限制，以往多半是發生在間諜案件中，各國才會相對允許他國的跨境執法行為。如果僅是單以內國法允許本國機關進行境外執法行為，其適法性恐將受到國際社會之質疑。[59]

面對此一困境，英國政府樂見美國雲端法案之施行，而在雲端法案的架構下，與美國達成行政協議，以此確保外國資訊擁有者的配合程度。而不僅僅是透過雲端法案與美國達成相互獲取資訊之協議，歐洲理事會也著手討論關於跨境電磁紀錄取得之議題，極有可能創建出一個歐盟內各國相互允許他國，不經傳統司法互助程序，擷取本國業者儲存之電磁資訊之架構。[60]

---

[57] Theregister.co.uk. (2018). High Court gives UK.gov six months to make the Snooper's Charter lawful. [online] Available at: https://www.theregister.co.uk/2018/04/27 high_court_ip_act_unlawful_november_deadline/ [Accessed 16 Oct. 2018].

[58] Supra Ryk-Lakhman, note 55.

[59] Ryk-Lakhman, I. (2017). The Investigatory Powers Act and International Law: Part II | UCL UCL Journal of Law and Jurisprudence Blog. [online] Blogs.ucl.ac.uk. Available at: https://blogs.ucl.ac.uk/law-journal/2017/01/09/the-investigatory-powers-act-and-international-law-part-ii/ [Accessed 21 Sep. 2018].

[60] Scl.org. (2018). The CLOUD Act: Cross-border Law Enforcement and the Internet. [online] Available at: https://www.scl.org/articles/10183-the-cloud-act-cross-border-law-enforcement-and-the-internet [Accessed 20 Sep. 2018].

伍、打擊網路犯罪之跨國合作

一、全球現況與難題

網路犯罪之跨境合作，分為各國內國法制之一致化及國際執法合作兩個面向。

在內國法制方面，因經濟、社會發展狀態不同，各國間網路犯罪的界定不一，例如，在A國構成犯罪的，在B國則否，或是同樣均為犯罪的行為，在A國可能是重大犯罪，在B國則為輕罪。以亞洲國家為例，台灣、日本及新加坡擁有較相近的科技及經濟發展狀況，尤其在IT產業之發展迅速，相較於其他以農業、觀光、代工業為主之國家，對於網路犯罪相應立法即較為綿密。[61]又若比較亞洲國家與歐洲、美國，其等面對恐怖攻擊之威脅顯著不同，因此亞洲國家對於恐怖攻擊之相應刑罰及無法和歐美國家相提並論。然而，實體法律規範的落差，將助長罪犯以立法較疏漏之國家為犯罪基地，透過無遠弗屆之網路科技，在其他國家遂行犯罪，則受害國即便擁有嚴格、健全之刑罰處罰，在追訴犯罪過程中，亦將因地理距離、文化語言差異、審判權界線等障礙，阻礙偵查、起訴、審判及執行之有效性。

立法的不一致必須透過國家、審判權間的協調，方式包含國際協議的訂立或非官方組織的運作，以下將介紹現今國際社會間重要合作模式：

二、 歐洲合作現況

(一) 官方協議

歐盟（European Union)在過去，關於電腦犯罪之司法互助，主要倚賴歐洲理事會（Council of Europe）所簽訂之 刑事案件司法互助公約 （Convention on Mutual Assistance in Criminal Matters）及申根公約中關於刑事案件司法互助之規定（Schengen Convention），而這兩個規定均非常古老，無法滿足電腦犯罪司法互助所需的時效性。 因此在2003年，歐盟採用、增添了新的互助規定，即規範成員國，對於他國所核發凍結命令之應予承認，以防止證據之滅失[62]; 至2008年，歐盟進一步針對跨境取證的司法互助方式作出修正，要求會員國間，對於他國司法機關所核發、取得證據以供司法程序使用之取證命令，必須加以承認，然而該修正僅解決部分問題，即其所針對只僅限於現存在司法程序中之可知證據，對於尚未受司法掌控之其他可能證據，各國間之司法單位如何運作則未為規定。[63] 於2009，歐盟在斯德哥爾摩計畫（Stockholm Programme ）中嘗試就刑事司法

[61] Tonya L. Putnam, David D. Elliott, International Responses to Cyber Crime, DP5 HPCYBE0200 06-25-:1 11:57:25 rev1, 35.

[62] Council Framework Decision 2003/577/JHA of 22 July 2003 on the Execution in the European Union of Orders Freezing Property or Evidence, OJ L 196, 2.8.2003, para. 1.

[63] European Union, "The Stockholm Programme - An Open and Secure Europe Serving and Protecting the Citizen 2010/C 115/01" (Council of the European Union, December 2, 2009), OJ C 115 4.5.2010.

互助作出積極且全面性的修正，意圖建立一個全面性刑事司法決定的相互認可機制。直到2014年，歐盟再度針對此一領域加以修正，訂立：歐洲刑事案件調查命令執行方針（Directive on the European Investigation Order in criminal matters），透過此一執行方針，歐洲會員國間，被要求必須同意他國執法單位在本國司法權內進行特定刑事偵查型為，並且也允許、鼓勵會員國間成立聯合調查團隊（Joint Investigative Teams ）。歐盟就刑事案件司法互助的發展，從1958年訂立之刑事案件司法互助公約開始迄今，在起初的數十年，突破並不顯著，直至2000年後方有較活躍之積極性變革，可見犯罪模式的改變、犯罪組織的擴大，如：電腦犯罪之發達，使歐盟各國間體認到確保司法互網絡之全面性與有效性的重要。然而，歐盟組織本身並沒有針對跨境電腦犯罪之司法互助作出個別之規範。

歐洲理事會針對電腦犯罪，訂立了專屬之電腦犯罪公約（Convention on Cybercrime，又稱 Budapest Convention on Cybercrime），該公約在2004年生效，其目標有三：一、一致化簽約國間內國法對各類型電腦犯罪的規範；二、提供各國在偵查電腦犯罪時，可使用之刑事偵查、審理、執行手段；三、建立一快速且有效的國際合作場域。[64]

在實體方面，其針對五大類犯罪，要求各簽約國依公約健全其內國法律。此五大類犯罪包括：1.妨害電腦資訊及設備之保密性、健全性與可用性罪章（Offences against the confidentiality, integrity and availability of computer data and systems）；2.電腦相關犯罪章(Computer-related offences)—指透過電腦完成之傳統犯罪；3.非法內容罪章（Content-related offences），如兒童色情內容(child pornography)；4. 侵犯著作權等權利罪章（Offences related to infringements of copyright and related rights）；5.輔助規定(Ancillary liability and sanctions)，如未遂犯、幫助犯、法人犯罪等規範。[65]

在程序方面，公約則針對：1. 加速已儲存通訊紀錄之保存（Expedited preservation of stored computer data）；2. 提出電磁資訊命令之立法Production order；3. 對已儲存通訊紀錄之搜索與扣押（Search and seizure of stored computer data）；4. 即時擷取電磁紀錄（Real-time collection of computer data）。[66]

在國際合作方面，公約規定：1. 各國間必須盡最大能力協助他國，且在情況急迫時，可以使用最速之方式（Expedited Communiction）請求他國協助，如：電子郵件、傳真等（第25條）；2. 各國可以在未經他國請求之情況下，主動提供予外國其認為可能對該外國之電腦犯罪案件之處理有助益之「自發性資訊」（Spontaneous information）（第26條）；3. 若請求國與受請其國間並未簽訂司法互助協定，該公約及為兩國間互助程序之法律依據，公約並概括性的規定合作雙方之權利義務等基礎架構（第27條）；4. 為了未來司法互助之必要（包括可能之搜索、扣押行動），可請求他國快速地保存「已儲存之電腦證

[64] Convention on Cybercrime, Preamble.
[65] Convention on Cybercrime,Chapter II, Section 1.
[66] Convention on Cybercrime, Chapter II, Section 2.

據」（Expedited preservation of stored computer data）、「電磁通訊歷程紀錄」（traffic data）（第 29 條、第 30 條）; 5. 可請求他國在迅速之時間內，採用搜索、扣押或類同之證據保全方式，取得儲存在受請求國司法權範圍內之電磁證據（第 31 條）; 6. 可不經外國允許，在本國取得儲存在外國之電磁資訊，只要符合下列情況：（1）公開之訊息，（2）在本國經有權同意揭露資訊之人同意，從本國及可拿取儲存於外國之電磁資訊者。（第 32 條）; 7. 應協助他國進行即時電磁資訊之搜集、通訊內容之攔截; 8. 各國均應設立全年無休之司法互助聯絡窗口（24/7 Network），其提供之協助包括：a.技術支援、b.「已儲存之電腦證據」及「電磁通訊歷程紀錄」之保存、c.其他非電腦相關證據之搜集、法律資訊之提供、鎖定嫌犯所在位置（第 35 條）。[67]

（二）打擊犯罪組織

1. 歐洲網路犯罪中心 （European Cybercrime Center, EC3）[68]

歐洲網路犯罪中心成立於 2013 年，是一個架設在歐盟、更準確的來說—歐洲刑警組織（Europol）下的單位。旨在維護歐盟內居民、企業及政府免於各類與網路相關之犯罪。歐洲網路犯罪中心在處理電腦犯罪時採取，從三個面向下手：1. 預防與控管策略（Strategy）：包括與其他單位之合作、風險控管及策略之分析、政策之制定及風險控管訓練; 2. 科學鑑識（Forensics）：設置電腦鑑識組及一般鑑識組; 3. 打擊行動（Operations）：針對兒童網路色情犯罪、網路詐欺犯罪及其他倚賴電腦進行之犯罪行為進行調查。

和歐洲刑警組織類同，歐洲網路犯罪中心之主要角色與功能為：1.對歐盟會員國就跨境網路犯罪資訊之提供者及資訊交換平台、2.協助會員國進行犯罪調查活動、策略分析及提供專家或專業技術諮詢、3.提供網路犯罪偵辦及預防策略分析、4.公部門與非官方網路犯罪預防、學術機構及其他非執法性質之相關私人團體之連結、5.對於會員國提供各式相關犯罪預防、調查訓練之需要、6.提供高度技術之電腦鑑識專家、設備、7.代表歐盟執法機關和其他單位進行刑事執法令域外之共同領域（如網路風險管理及政策發展等）的對話。

值得注意的是，歐洲犯罪中心下，設有聯合打擊網路犯罪小組（Joint Cybercrime Action Taskforce, J-CAT）。[69]其角色及功能為：以資訊獲取為起首，在各參與國家間，協調就犯罪之發現、調查準備及展開跨境犯罪偵查共同合作，針對高科技網路犯罪、網路犯罪之預防、網路詐欺及網路兒童色情 4 大項目，進行努力。此聯合打擊網路犯罪小組的成員，來自歐盟會員國之官員、非歐盟但與歐洲刑警組織有合作關係國之官員及歐洲網路犯罪中心

[67] Convention on Cybercrime, Chapter III.
[68] Europol. (n.d.). European Cybercrime Centre - EC3. [online] Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [Accessed 6 Oct. 2018].
[69] Europol. (n.d.). Joint Cybercrime Action Taskforce (J-CAT). [online] Available at: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce [Accessed 7 Oct. 2018].

人員；這些成員均在同一個辦公室內工作，如此可以確保合作關係之密切及時效性。而Eurojust（詳後述）之專家，每週均會與此小組人員開會，進行個案討論或政策之擬訂。

聯合打擊網路犯罪小組對於案件的選擇，也是透過集體開會決定，會議中將討論：1.被提出案件之重要性即與組織目標之關聯性、2.交換重要情資、3.案件執行計畫（通常由提出請求國負責擬訂）、4.執行步驟之推演，包括：涉及不同司法權時相關法律問題之諮詢、偵辦過程中所需資源之獲取、責任分配等。[70]

2. 歐洲司法組織（Eurojust）與歐洲司法網路犯罪網絡(European Judicial Cybercrime Network, EJCN)

歐洲司法組織係一歐盟機構，歐盟會員國於1999年10月時，在芬蘭Tampere舉行歐洲理事會會議時，達成必須就重大組織性犯罪之國際司法互助做進一步的安排與規劃，後續於2000年12越，先行設立了歐洲司法組織之前身—Pro-Eurojust，進行該組織之試營運。美國911恐攻事件的發生，催化了歐洲司法組織的正式運作，該組織於2002年正式設立。[71]

歐洲司法組織的組成員，為來自各會員國之檢察官、法官（或地方治安官）、警官，也包括非歐盟會員國的參與國所指派的聯絡官。依其目前之組織架構及運行方式，可被定位為一國際司法合作之協調平台，其功能包括：1. 要求各會員國、參與國，指派權責機關參與案件之偵辦、相互協調、就何國為主辦單位達成共識、組成聯合調查小組並由各國提供歐洲司法組織相關案件偵查資訊，以利協調任務的達成；2.確保各國承辦單位相互提供案件偵辦資訊；3.確保各國間合作之順；4.與歐洲刑警組織合作，依據歐洲刑警組織對案件策略之分析，對承辦國家提供支持與協助；5.與歐洲司法網絡（European Judicial Network, EJN）合作並向之諮商，並將從案件中所獲得之資訊提供予之做成儲存資料；6.將個合作單位所提出之對他國之請求轉達；7. 提供翻譯、資訊解讀服務及舉辦、招開國際會議。[72]

隸屬歐洲司法組織之下，一專門針對電腦犯罪、網路犯罪之網絡，於2016年創立—歐洲司法網路犯罪網絡（European Judicial Cybercrime Network, EJCN）。同樣具有跨國資訊交換、協調合作功能，歐洲司法網路犯罪網絡提供予各國偵辦網路犯罪所需之專業人員，並且將資安風險承擔者，包括企業等加入合作場域，以預防網路犯罪的發生。[73]

然而，與其他國際組織類似，歐洲司法組織亦面臨無實際執行權力之困境，該組織面對此問題，期待能透過2007年簽署、2009年生效之里斯本條約解決。該條約第85條肯認了該組織之宗旨在於加強國際間就重大跨國犯罪預防、偵查之協調與合作，第86條則進一步授與歐洲理事會，依循相關立法程序，在該組織中成立「歐洲檢察官辦公室」（European

[70] Id.
[71] Eurojust.europa.eu. (n.d.). History of Eurojust. [online] Available at: http://www.eurojust.europa.eu/about/background/Pages/History.aspx [Accessed 9 Oct. 2018].
[72] Id.
[73] Eurojust.europa.eu. (n.d.). European Judicial Cybercrime Network. [online] Available at: http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx [Accessed 8 Oct. 2018].

Public Prosecutor’s Office），可為跨境司法互助由資訊分享到常態性合作之正向發展。[74]

3. 國際刑警組織（Interpol）

國際刑警組織以之前身「國際刑事警察委員會」（International Criminal Police Commission, ICPC）成立於 1923 年，於 1956 年成為 Interpol，現今總部設置在法國里昂，聯合國將之界定為一「跨政府組織」（intergovernmental organization）。該組織共有 192 個會員國，遍及全球，組織宗旨包括：1.作為全球刑事司法互助之資訊提供中心：此為該組織最主要之存在目的，及建立全球刑事資料資訊庫、安全的資訊交換管道及協助各國建立可與該組織連結之資料庫，以提供即時之刑事調查資訊; 2. 作為國際警力交流平台，致力於警察專業技能之訓練、交換、培育工作; 3.作為全球警政策略研究及發展中心; 4.作為跨領域合作之平台，以提升全球安全為終極目標。[75]

在資訊分享上，國際刑警組織建立有全球性的刑事資料庫（I- 24/7），各國之中央單位（National Central Bureau）可以迅速地從資料庫中取得各式刑事資訊，包括：國際通報（Interpol Notice）、失竊文物、失竊車輛、失竊旅行文件、信用卡資訊、指紋及相片、恐怖份子名單、DNA 資料、走私及人口販運資料等，成為各國追蹤、打擊犯罪行動之重要支援。[76]

上述提及之國際通報功能是一對人之協尋系統，依不同協尋目的進行不同顏色之通報，例如，紅色通報（Interpol Red Notice）係某人遭通緝時，Interpol 即可受發布通緝之國家要求，將該人在系統中列為紅色通報人口。然而，國際刑警組織並不與內國警察享有相同之警察權，實質上無法執行逮捕行動之結果，使得該通報並無強制性，而各國司法對於紅色通報效力之認定亦有所不同，部分國家要求表面證據的呈現（prima facie evidence），部分要求就現存證據提出說明(summary of evidence)，部分則不要求出示證據(no evidence)。 而國際刑警組織對於發布通報之審核，亦曾遭質疑，批評者認為該審核篩選功能不彰，部分國家利用刑事通報系統處理民事案件，且要求發佈通報之國家，亦多集中於司法體制較不穩定之國家，甚至時而論為政治、軍事或宗教之操縱對象。則在通報中立性遭質疑，又無實質拘束力之情況下，國際刑警組織此一通報功能之效力，即產生問題。[77]

(三) 策略交流平台

國際電信通訊聯盟(International Telecommunication Union)成立於 1865 年，是一例屬在歐盟下的跨政府組織，在創設之初，是預期作為公私部門間，與先進通訊設備，如電話、衛星等相關科技的對話平台，限期總部則設立在瑞士日內瓦。隨著網際網路及電腦科技發展，國際電信通訊聯盟成為歐盟下守護全球網路安全的重要機構。此聯盟涵蓋之面向頗為

[74] Supra note 71.
[75] Interpol.int. (n.d.). Priorities / About INTERPOL / Internet / Home - INTERPOL. [online] Available at: https://www.interpol.int/About-INTERPOL/Priorities [Accessed 7 Oct. 2018].
[76] **黃文志**, (n.d.). Interpol **發布紅色通報之困境與挑戰**, International Forum on Police Cooperation Combating Transnational Telecommunication Fraud Program.
[77] Id. at 25.

廣泛，舉凡資訊教育的發展、全球氣候變遷、資訊技術之普及等等均受到其關心，而於2003及2005 年，二度資訊社會世界高峰會議（the World Summit on the Information Society, WSIS)，確立了該聯盟近年發展之方向，及確保網路安全，隨後於2007 年該聯盟即因應網路資安之需求及網路犯罪的發展，訂立了保護網路安全及懲罰犯罪之規範—全球網路安全計畫（the Global Cybersecurity Agenda），目標是透過計畫建立全球就網路安全維護的軟硬體設備，制力在修補國際間相關法律漏洞、連結網路世界中之個人與群體、政府與公司、學術界與實務單位，創建在各國間協調之程序與實體機制、並且針對未來科技犯罪發展走向作出前瞻性的政策規劃。[78]此組織所訂立之規則，對各國並無拘束力，亦無協助各國執法單位進行情資交換之功能，但在政策之擬訂上，則扮演著顧問型的角色，並且定期舉辦國際性資安及網路犯罪防治研討會，對於一致化各國法制有著重要影響。

三、美國合作現況

（一）官方協議

「美國正在與世界各洲合作，透過改善訓練計畫、建立正確的法治架構、資訊分享及公眾參與，強化政府防範網路犯罪之能量。而其中，最好的國際合作方式，就是透過布達佩斯電腦犯罪公約。我的國家強烈的倡議各國參與該公約，因為沒有比其更好的途徑可以有效的防止、追訴電腦犯罪。」—美國前國務卿 John Kerry 在2015 年在韓國大學中以題為「開放但安全的網際網路：我們兩者均要」之演講如是道。

布達佩斯電腦犯罪公約雖為以歐盟國家為主要成員，然而美國因其強大之經濟政治地位，在簽署該公約後，即扮演著透過該公約，與其他國家進行網路犯罪預防與打擊的樞紐角色。此公約迄今已有61 國家簽署、批准，然而中華人民共和國、俄羅斯及我國則並未加入，[79]該公約因無法涵蓋全部國家，產生有效性之缺口。

（二）官方組織

(1) 美國司法部電腦犯罪及智慧財產組（the Computer Crime and Intellectual Property Section, CCIPS）

該組織隸屬美國司法部之下，職司預防、調查及起訴電腦犯罪。其合作對象包括美國政府的其他部門、私人組織、學術機構及外國單位。部門內的檢察官致力於內國及國際法治的建構、程序的制定及技能的提升，追求有效打擊網路犯罪。而包括著作權、商標及專利等在內的智財犯罪也因為常利用網路、電腦技術作為犯罪實施手段，而成為該部門防治的目標。

(2) 聯邦調查局(FBI)

[78] Itu.int. (n.d.). Key Areas of Action. [online] Available at: https://www.itu.int/en/action/Pages/default.aspx [Accessed 13 Oct. 2018].

[79] Treaty Office. (2018). Full list. [online] Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=EvogrdRV [Accessed 15 Oct. 2018].

面對網路犯罪威脅，美國聯邦調查局下設有數個處理網路犯罪之單位，包括：A. 網路組（Cyber Division）：設置在聯邦調查局總部，負責協調、調配警力; B. 網路犯罪特勤小組：設置在全美 56 個地點，內有幹員及分析師調查非法入侵電腦、智慧財產及個資之竊盜、兒童色情圖片及性剝削，以及網路詐欺等重要網路犯罪;C. 新打擊網路行動隊（New Cyber Action Teams）：處理世界各地發生之非法侵入網路案件，並搜集情資，供調查局維護國家安全及商業機密; D. 打擊網路犯罪小組(Computer Crimes Task Forces)：在國內連結新科技與聯邦、州及地方合作單位之行動，打擊網路犯罪。[80]

當涉外案件發生時，聯邦調查局同時與美國其他單位合作，如國土安全局及美國司法部，密切和國際刑警組織、外國執法單位配合。負責處理聯邦調查局國際合作之部門為國際行動部（International Operations Division），方式係設置聯絡武官，與各國之主要執法單位建立聯絡管道，確保打擊包括網路犯罪之跨境犯罪食，可與外國執法單位保持密切且迅速的聯繫。武官與外國單位之合作係建立在司法互助之行政命令、法律條文、國際條約、檢察機關守則、調查局政策及跨單位之協議等規範上，在恐怖攻擊、電腦犯罪日益嚴重之今日，為兩國間之司法互助，提供重要的協助。[81]

四、其他跨國合作——G7 24/7 Cybercrime Network

G7 是 Group of 7 的縮寫(2014 年俄羅斯退出，而由原本之 G8 變為 G7)，係指美國、日本、德國、英國、法國、義大利、加拿大等七國及歐盟，該等國家與組織間，每年會舉辦一高峰會，就國內外重要政治及經濟議題進行討論。[82]嚴格來說，G7 並非一組織，但該等國家在每次開會後，所達成的共識，將影響其各參與國未來政策之擬定，也因為該等國家均具有一定經濟實力，其政經局勢受到會議影響後，也間接影響國際政經局勢之演變。[83]

G7 24/7 Cybercrime Network 系統係在 1997 年 12 月，因應日益興盛的跨國通訊而建立，致力於打擊網路犯罪，其手段是「保存證據，並透過法制化之管道提供證據，以利後續偵查進行」並且在各國設立聯絡窗口(contact points)，至 2014 年參與之會員國共 70 國。[84]

五、歐美國際合作案例— GameOver Zeus Botnet 案

(一) 背景資訊[85][86]

[80] Federal Bureau of Investigation. (n.d.). Cyber Crime. [online] Available at: https://www.fbi.gov/investigate/cyber [Accessed 23 Oct. 2018].
[81] Federal Bureau of Investigation. (n.d.). International Operations. [online] Available at: https://www.fbi.gov/about/leadership-and-structure/international-operations [Accessed 24 Oct. 2018].
[82] CCDCOE. (2018). G7. [online] Available at: https://ccdcoe.org/g7.html [Accessed 15 Oct. 2018].
[83] Id.
[84] Id.
[85] Hkcert.org. (2014). GameOver Zeus Botnet Detection and Cleanup in Hong Kong. [online] Available at: https://www.hkcert.org/my_url/en/blog/14061302 [Accessed 22 Oct. 2018].

GameOver Zeus Botnet 係以公司及金融機構為目標，將惡意軟體置入網際網路，癱瘓網路運作（即「殭屍網路」）。犯罪者經常藉由此方法，竊取金融機密資料，成為網路詐欺、商業間諜犯罪者之工具。GameOver Zeus Botnet 的攻擊對象為微軟系統，最初係在 2011 年 9 月間被發覺。當個人或企業電腦使用者點開誘騙電子郵件時，可能就同時下載了惡意軟體。GameOver Zeus Botnet 有各種竊取商業機密之手段，譬如使用 man-in-the-browser (MITB)擷取電腦使用者間訊息的傳輸，或是製造虛偽的網路帳戶認證機制，騙取帳戶資訊，或再誘騙電子郵件中置入惡意軟體，癱瘓使用者電腦，帶使用者支付費用後才予解鎖，以此獲利。譬如 GameOver Zeus Botnet 的惡意軟體夥伴—CryptoLocker 即會使誤下載該惡意軟體之電腦內檔案遭鎖定，再威脅使用者付費解鎖。

在查緝 GameOver Zeus Botnet 方面，因是殭屍網路的變異體，其採用點對點通訊傳輸工具(Peer-to-Peer communication, P2P) ，改變原本使用 IRC 通訊協定演變成不易被發現的 HTTP/HTTPS 檔案傳輸方式，更容易隱藏路徑，同時採用動態網域產生演算法(DGA, Domain Generation Algorithm)，使得網域清單動態不斷更新，混淆查緝者視聽，提升追查困難。而幕後主使者之身份亦緩慢隨調查過程中揭露，其中主使者之來源包括俄羅斯、烏克蘭。

GameOver Zeus 殭屍網路的受害者遍及全球，依據美國聯邦調查局統計，至 2014 年，全球有超過一百萬台電腦受到感染，其中百分之 25 的受害電腦集中於以美國境內，而從微軟公司控告法院時所提交的文件可見，惡意網路架構更擴及英國、德國、伊朗、香港，甚至寮國再至澳洲。全球經濟損失至 2015 年達 6 千 9 百萬美元。

(二) 偵辦合作模式

面對全球性的網路犯罪，美國境內除了聯邦調查局（FBI）、美國司法部電腦犯罪及智慧財產組（CCIP, DOJ）及國防部的刑事犯罪調查單位(the Defense Criminal Investigative Service of the U.S. Department of Defense)聯手合作外，更有國家安全局下國家網路安全及通訊整合中心之電腦緊急解讀小組（Computer Emergency Readiness Team, DHS National Cybersecurity and Communications Integration Center, US-CERT）及時提供全球受害者諮詢、停止網路遭癱瘓情況之蔓延並協助增強受害者之資安層級。

除了受害者遍及全球外，經調查主謀者係俄羅斯籍之 Evgeniy Mikhailovich Bogachev。與美國合作之他國執法單位包括：澳洲聯邦警察（Australian Federal Police）、荷蘭國家警察高科技犯罪小組（the National Police of the Netherlands National High Tech Crime Unit)、歐洲網路犯罪中心（European Cybercrime Centre,

[86] Scribd. (2012). Microsoft complaint against Zeus botnet operators | Malware | Email Spam. [online] Available at: https://zh.scribd.com/document/86715736/Microsoft-complaint-against-Zeus-botnet-operators [Accessed 7 Oct. 2018].

EC3)；德國聯邦警察局（Germany’s Bundeskriminalamt）；法國司法警察局（France’s Police Judiciare）；義大利郵政及通訊警察（Italy’s Polizia Postale e delle Comunicazioni）；日本國家警察局（Japan’s National Police Agency）；盧森堡大公領地警察局（Luxembourg’s Police Grand Ducale）；紐西蘭警察（New Zealand Police）；加拿大皇家騎警（the Royal Canadian Mounted Police）；烏克蘭內政部打擊網路犯罪小組（Ukraine’s Ministry of Internal Affairs – Division for Combating Cyber Crime）及英國國家犯罪機構（the United Kingdom’s National Crime Agency）。美國執法機關也尋求了來自私部門的協助，其中包括微軟及 Dell SecureWorks 在內的十數家科技、網路、軟體、資安公司都加入偵查工作中。[87] 就跨國資訊傳遞協調之平台部分，美國執法單位則與歐洲刑警組織（Europol)下的歐洲網路犯罪中心 （European Cybercrime Center, EC3）合作，以該網路犯罪中心作為聯繫歐洲執法單位及各國間資訊交換平台。[88] 在跨國、跨法律及科技、跨傳統及新偵查技巧之合作下，GameOver Zeus Botnet 及勒索軟體 CryptoLocker 於 2014 年被取締及關閉，然而主嫌 Evgeniy Mikhailovich Bogachev 則據稱居住在俄國境內黑海地區，受到俄羅斯政府保護，美國聯邦調查局雖向全球發出 Evgeniy Mikhailovich Bogachev 之懸賞令，但相關執法單位仍因而無法將之引渡回國，接受調查。[89]

六、亞洲合作現況

（一）犯罪概況

根據新加坡大學國際資訊整合中心之研究，亞太地區的企業在 2014 年花費近 2300 億美元之金費在網路犯罪防治及資安維護上，領先全球。[90]即便如此，亞洲地區中有八個國家，仍名列全球前 10 名最易受到網路攻擊之國家。[91]

---

[87] “These companies include Microsoft Corporation, Abuse.ch, Afilias, F-Secure, Level 3 Communications, McAfee, Neustar, Shadowserver, Anubis Networks, Symantec, Heimdal Security, Sophos and Trend Micro.” U.S. Leads Multi-National Action Against “Gameover Zeus” Botnet and “Cryptolocker” Ransomware, Charges Botnet Administrator, DOJ Justice News, U.S. Leads Multi-National Action Against “Gameover Zeus” Botnet and “Cryptolocker” Ransomware, Charges Botnet Administrator.

[88] Europol. (2014). International action against 'Gameover Zeus' botnet and 'CryptoLocker' ransomware. [online] Available at: https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware [Accessed 13 Oct. 2018].

[89] Whigham, N. (2017). The mastermind behind arguably the most sophisticated cybercrime network ever. [online] NewsComAu. Available at: https://www.news.com.au/technology/online/hacking/the-russian-hacker-with-a-4-million-bounty-on-his-head/news-story/e5c363e260e25c0a09641d39e1d37636 [Accessed 13 Oct. 2018].

[90] Marsh.com. (n.d.). Cyber Crime in Asia: A Changing Regulatory Environment. [online] Available at: https://www.marsh.com/content/dam/marsh/Documents/PDF/asia/en_asia/Cybercrime%20in%20Asia%20A%20Changing%20Regulatory%20Environment.pdf [Accessed 5 Nov. 2018].

[91] Id.

根據 Europol 於 2016 年製作的「2015- 2016 網路犯罪全球熱區分部」報告顯示：中國大陸地區近年來開始使用快速訊息及廣告之方式刺激消費市場，這些市場提供眾多產品與服務，狀態就和西方社會之地下市場類似，提供支付工具（如信用卡）犯罪之工具，如提款機或讀卡機等，滋長利用電腦設備遂行財產犯罪的發生。[92]整個亞洲地區，在多項網路犯罪類型中，均被認定是高風險地區。例如，從被害角度出發，中國大陸與台灣有全球最高的殭屍病毒等惡意病毒感染率，其中手機惡意軟體的中毒率，僅次於非洲地區; 從加害角度出發，在阻斷服務攻擊（DDoS attack）上，超過全球件數的百分之 50 以上件數攻擊之來源為亞洲，這些來自亞洲的攻擊中，百分之 25 來自大陸，韓國、印度泰國、日本亦提供了可觀來源;大陸、越南、台灣、印度、日本則產生全球最最多的惡意郵件。[93]歐洲共 16 個國家在亞洲地區曾進行刑事調查行動，其中 12 個發生在大陸，另外香港及印度也有相對較高之網路刑案發生。[94]

（二）合作現況

從世界幾個與打擊網路犯罪重要公約，包括：非洲聯盟網路安全及個資保護公約（African Union Convention on Cyber Security and Personal Data Protection）、俄聯邦獨立國家協議（Commonwealth of Independent States Agreement）、歐洲理事會網路犯罪公約（Council of Europe Cybercrime Convention）、阿拉伯國家聯盟公約（League of Arab States Convention）、上海合作組織協議（Shanghai Cooperation Organization Agreement）等來看，亞洲國家參與公約締結之比例明顯偏低，譬如歐洲理事會網路犯罪公約中，非歐盟會員國者共 25 國締約，其中僅有日本及菲律賓為亞洲國家;而即便是上海合作組織協議，會員國及觀察員國僅 12 國，並未涵蓋多數亞洲國家。[95]

從非正式組織，如：國際刑警組織、歐洲刑警組織、歐洲司法組織、G7 24/7 Cybercrime Network 之會員組成來看，國際刑警組織 Interpol 中共有 52 個亞洲國家[96]，歐洲檢察官組織則在數個亞洲國家設有聯絡點，其餘組織或合作平台亞洲國家參與比例偏低。

聯合國毒品及犯罪辦公室於 2013 年就全球網路犯罪狀態及合作進行調查，該報告指出，當歐美國家經常性的使用電子郵件、傳真等迅速之資訊交換方式（Channels for urgent MLA requests）進行司法互助時，僅百分之 20 之亞洲國家表示其等也有此種管道。[97]

---

[92] Europol.europa.eu. (2016). The Geographic Distribution of Cybercrime. [online] Available at: https://www.europol.europa.eu/iocta/2016/distribution.html [Accessed 24 Oct. 2018].
[93] Id.
[94] Id.
[95] UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime Draft (2013), at 197-199.
[96] Interpol.int. (n.d.). Asia & South Pacific / Member countries / Internet / Home - INTERPOL. [online] Available at: https://www.interpol.int/Member-countries/Asia-South-Pacific [Accessed 28 Oct. 2018].
[97] Id. supra note 95, at 207-208.

數個原因使亞洲國家間在締結公約或組成非官方合作平台上困難於歐洲及某州國家：一、國家數眾多、二、國家法治發展狀態差異大、三、政治局勢衝突。亞洲地區發生之電腦犯罪，往往不僅肇因於經濟誘因，更來自區域或國家間不同之意識形態。譬如南韓政府聲稱其銀行及政府網路多次受到來自北韓的駭客攻擊，類似緊張關係也存在與台灣與中國大陸、印度與巴基斯坦等其他國家間。在社會經濟、法治基礎建設懸殊的狀態差異，已經使亞洲國家間的合作先天不利，持續不斷的政治、經濟衝突，更使得包括官方協議之簽訂、非官方合作組織或平台之發展難以推進。

然而，打擊網路犯罪的國際合作本就困難。根據前開聯合國調查報告指出，即便是歐洲網路犯罪公約之參與國，亦表示多半的跨境合作是倚賴兩國間的雙邊協議或互惠協議，該份報告中超過百分之 60 受訪國家為國際協定之參與國，但實際案例之運作上，僅百分之 25 之國家，係以國際公約中司法互助之規章作為互助基礎。[98]由此可見，國際型的公約之存在，相對於實際案例之使用，更可謂是各國擬定相關政策之上位依據，對於亞洲國家來說，即便未能參與歐洲網路犯罪公約或自行簽訂類似之國際公約，在內國法之制定、甚與他國簽訂雙邊互助協定時，仍可將之引為參考，實質參與公約之規範。

上開調查報告又顯示，在非官方合作方面，歐洲、亞洲及美洲地區國家，在提供非官方協助上，均有達百分之 70-90 高配合度之表現。[99]這些國家指出，非官方之互助活動，仍必須建立在國家間或區域間各種形式之協議上，透過國際或區域性組織或機構作為互動平台，同時還必須仰賴外交單位之協助，時而執法人員間之私人網絡亦有對合作所助益。由此可窺見亞洲國家間，在個案處理時，為各自偵審所需，仍然積極地進行合作，各國間亦普遍存有互助之協議，只是亞洲幅員廣大、國家眾多，仍亟需創立一能取得各國配合之整合平台，方能有效打擊網路犯罪。

陸、結語

打擊電腦犯罪之困難在於犯罪型態之日益全球化，然而打擊此種犯罪之容易處也在於此一全球化現象。當跨境電腦犯罪成為世界公敵時，各國形成共識，將內國法一致化、在同一個架構下進行跨國偵查之可能性便大幅提升，此由本文所介紹之美國關於電腦犯罪法條之規範即可理解，類似之犯罪行為，在我國也同樣成立犯罪，並無明顯差距; 因此實體法之一致性，應為全球打擊電腦犯罪合作之起點，實質挑戰則在於國際間如何合作。

談及偵辦跨境電腦犯罪之合作，論者往往提及歐洲理事會之電腦犯罪公約及國際刑警組織、歐洲刑警組織、歐洲司法組織等國際合作平台，然而此等以部分國家為主之公約及平台的有效性，仍必須依賴在其全球網絡路佈局之綿密性上。蓋因，當亞洲成為高比例電腦犯罪之來源、攻擊目標，但卻未被囊括在上開公約之下或合作平台中時，犯罪打擊即產生破口。面對亞洲國家間相對複雜之地理、歷史、政經情勢，倡議形成多邊互助協定、成立受信賴之

[98] Id. supra note 95, at 210.
[99] Id. supra note 95, at 211.

半官方之合作平台，絕非新穎，然無疑是所有參與網路犯罪打擊者一致的期待。亞洲司法合作之發展起步較晚、問題複雜而沈重，但卻是維持世界法律秩序的關鍵。台灣作為亞洲國家法制之典範，理應在困境中帶領亞洲各國，建立優良之法律機制，遏止跨境電腦犯罪之蔓延。