特稿

網路犯罪與資訊安全的未來
——從網域名稱扣押談網路治理

陳昱奉*

要　目

DOI：10.6460/CPCP.202208_(32).05

* 臺灣嘉義地方檢察署檢察官，國立政治大學商學院智慧財產研究碩士，前哈佛大學柏克曼－克萊恩網路與社會研究中心訪問學者。

摘　要

網路犯罪已然成為現階段最重要的犯罪型態，從影音串流侵權、投資詐欺至兒少性剝削等，無一不是廣泛而即時的法益侵害。但從犯罪偵查角度言之，此類犯罪的行為人本身，以及用以實施犯罪的網站伺服器等所在位置，經常不在我國境內。對於用以作為犯罪工具的網域名稱，美國以扣押、沒收的方式處理，肇因於美國就網域名稱管理的各個層面，具有其他國家無法匹敵的刑事管轄權。然而，對於含有.tw頂級域名以外的網域名稱，我國執法機關並無法比照美國模式進行實質扣押，而是援引刑事訴訟法第133條之1，向地方法院聲請域名扣押裁定，以停止域名解析方式，限制使用者接取不法網站。展望未來，對於網路犯罪與資訊安全，應轉變既有思維：一、防治重於查緝；二、維持刑法謙抑性；三、善用民事及刑事手段；四、加強國際合作；五、強化網路治理，方能因應日後來自虛擬世界的各種挑戰。

關鍵詞：網路治理、網域名稱扣押、域名停止解析、網域名稱系統回應政策區域、網站屏蔽命令、域名濫用

The Future of Cybercrime and Information Security – On Internet Governance from Domain Name Seizure

Yu-Feng (Harris) Chen *

Abstract

Cybercrime has become the most important type of crime at this stage, from video streaming infringement, investment fraud to child sexual exploitation, etc., all of which are widespread and immediate violations of legal interests. However, from the perspective of criminal investigation, the perpetrators of such crimes, as well as the location of the website server used to commit the crime, are often not located in our country. For domain names used as criminal tools, the United States has treated them with seizure and forfeiture, because the United States has criminal jurisdiction that is unmatched by other countries in all aspects of domain name management. However, for domain names other than the .tw top-level domain, Taiwan's law enforcement agencies cannot follow the American model,

* Prosecutor of Chiayi Prosecutor's Office; MBA of Institution of Intellectual Property, National Chengchi University; former Fellow of Berkman Klein Center for Internet and Society, Harvard University.

but to invoke Article 133-1 of the Criminal Procedure Law to apply to the court for domain name seizure warrant to disable domain name resolution and restrict user's access to unlawful websites. Looking forward to the future, regarding cybercrime and information security, the existing thinking should be changed to: 1. Prevention is more important than investigation; 2. Maintaining restraining of criminal law; 3. Making good use of civil and criminal means; 4. Strengthening international cooperation; 5. Strengthening internet governance can we respond to various challenges from the virtual world in the future.

Keywords: Internet Governance, Domain Name System (DNS), Domain Name Seizure, Disabling DNS Resolution, DNS RPZ, Website Block Order

壹、前　言

人類歷史發展至今，截至目前為止，除了實體世界之外，尚有由電腦設備及網際網路所構築而成的虛擬世界。自從英國科學家伯納李（Tim Berners-Lee）爵士在1989年的3月12日，在歐洲核子研究中心（CERN）工作的，成功傳出第一則透過網路發送的訊息開始，人類有史以來第一個網站info.cern.ch.，就架設在他自己的桌上型電腦[1]。因此，這一天被譽為「全球資訊網絡」（World Wide Web）的誕生日。從此以降，各式各樣的大量電腦等數位設備，藉由網際網路串連起來，以「網域名稱系統」（Domain Name System, DNS）為架構，傳遞來自世界各地的數位資訊，為人類帶來鋪天蓋地的改變。預料至2025年，全球儲存在私有和公共IT基礎設備、公用事業基礎設備、私有和公共雲端數據中心、個人計算設備（PC、筆記本電腦、平板電腦和智慧型手機）以及物聯網（IoT）設備上的數據，將可達200ZB[2]。

自犯罪偵查角度而言，網際網路已然成為相當重要的

---

1 有關伯納李爵士（鑑於發明網際網路此一功勛，經英國女王授與爵士）與網際網路的濫觴，詳見CERN, A Short History of the Web, https://home.cern/science/computing/birth-web/short-history-web (last visited: Oct. 10, 2021).

2 Steve Morgan, The 2020 Data Attack Surface Report, https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/ArcserveDataReport2020.pdf (last visited: Oct. 2, 2021). ZB為「澤」位元。

犯罪管道，基於網路世界「無遠弗屆」、「無時無刻」、「無所不包」的「三無」特性，致使犯罪行為跨越難以數計的司法管轄區域之外，犯罪時間為24/7全天候型態，犯罪行為人躲藏何處，復至難查緝，有時甚至達到「無計可施」的地步。根據美國聯邦調查局「網路犯罪申訴中心」（Internet Crime Complaint Center, IC3）[3]統計，2020年IC3收到的美國民眾投訴案件達數量，達到創紀錄的79萬1,790件，損失總計超過41億美元。與2019年相比，總投訴量增加69%。其中，「商業郵件詐騙」（Business E-mail Compromise, BEC）詐欺案件受害為最，計有1萬9,369起投訴，調整後損失約為18億美元。網路釣魚詐騙（online-phishing）案件也相當令人矚目，計有24萬1,342起投訴，調整後損失超過5,400萬美元；勒索軟體（ransomware）[4]案件的數量也在繼續增加，2020年據報計有2,474起[5]。除此之外，從全球觀點而言，網路犯罪於

3 美國聯邦調查局所轄，參見FEDERAL BUREAU OF INVESTIGATION, Internet Crime Complaint Center IC3, IC3 Mission Statement, https://www.ic3.gov/Home/About (last visited: Oct. 22, 2021).

4 為目前最嚴重資安問題之一，擴及全球主要產業。2021年發生在美國的「殖民油管」網路勒贖案件，廠商被迫支付贖金即屬適例。參見THE UNITED STATES DEPARTMENT of JUSTICE, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside, Department of Justice, June, 7, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (last visited: Sept. 13, 2021).

5 2020 Internet Crime Report, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited: Oct. 12, 2021).

2021年估計在全球造成總計6萬億美元的損失，成為僅次於美國和中國的世界第三大經濟體產值。而且未來五年內全球網路犯罪成本將以每年15%的速度增長，到2025年達到每年10.5萬億美元，高於2015年的3萬億美元。網路犯罪成本包括數據毀損和破壞、被盜資金、生產力損失、智慧財產權被盜、個人和財務數據被盜、挪用公款、詐欺、攻擊後對正常業務過程的破壞、鑑識調查、恢復和刪除被駭客入侵數據和系統，以及聲譽損害等等，不容小覷。

隨著網際網路進入現今每一個人生活當中，我們所謂「網路犯罪」（Cybercrime）一詞的定義，在學界中存在不同的見解。而歐洲理事會（Council of Europe, COE）於2001年11月23日在布達佩斯簽署之「網路犯罪公約」（Convention on Cybercrime）[6]第一章的定義中，對於該公約所規範的內容，認定網路犯罪仍屬於與電腦相關之犯罪行為（Computer-related crime）。[7]本文探討重點側重於網際網路，故以下均以「網路犯罪」一詞代表cybercrime。而網際網路係以「網域名稱」（Domain Name）為基礎的「網域名稱系統」所構築，以下為敘述簡便起見，「網域名稱」一詞或以「域名」代之，「網域

6 因簽署地在匈牙利布達佩斯，故一般亦稱為布達佩斯公約（Budapest Convention）。

7 陳昱奉，跨境電腦犯罪偵辦之未來走向——從「電腦犯罪公約（Convention on Cybercrime）」暨「In Our Sites行動」出發，台灣國際法學刊，15卷2期，2019年6月，頁95-105。公約內容請參見 Convention on Cybercrime, Budapest, Nov. 23, 2001, https://rm.coe.int/1680081561 (last visited: May 5, 2022).

名稱系統」一詞，則以英文縮寫DNS稱之。

除了傳統類型網路犯罪之外，更重要的是，在「資安即國安」的前提下，臺灣因為身處美中對立第一島鏈的關鍵地位，主要產業跟隨全球科技製造業連動，「地緣科技」（Geo-science and technology）讓臺灣也成為全球駭客活動熱區。根據行政院國家資通安全會報「109年國家資通安全情勢報告」[8]顯示，包括臺灣在內，全球所面臨的資安威脅，可分為下列六大項：一、個資與帳密頻遭大量竊取；二、社交工程郵件助長勒索軟體散布；三、物聯網設備資安漏洞擴大蔓延；四、進階持續性威脅攻擊鎖定能源產業；五、供應鏈資安威脅激增；六、關鍵基礎設施遭駭風險升高等。因此，如何有效防範資安威脅，實為執法單位日後所需面對的嚴峻問題。除此之外，我國近來從「楓林網」違反著作權法案件[9]、SWAG網站違反妨害風化案件[10]，均曾由執法機關嘗試藉由扣押網域名稱方式，暫停其網路活動。尤有甚者，臺灣網紅「小玉」藉由「深

8 行政院資通安全處，109年國家資通安全情勢報告，2021年6月29日，https://nicst.ey.gov.tw/Page/7AB45EB4470FE0B9/7234b46b-fe52-4295-8bae-41d9ea36d447（最後瀏覽日：2021年10月22日）。

9 蘇文彬，刑事局破獲盜版影音網站楓林網，每月獲利估至少400萬元，iThome，2020年4月8日，https://www.ithome.com.tw/news/136848（最後瀏覽日：2021年10月2日）。

10 林郁萍，號稱亞洲最大成人平台SWAG被抄　負責人夫妻檔等5人遭送辦，中時新聞網，2021年4月2日，https://www.chinatimes.com/realtimenews/20210402004244-260402?chdtv（最後瀏覽日：2021年9月12日）。

偽」技術，以名人臉像製作色情影片[11]，韓國「N號房事件」[12]，受害人眾多，甚或有兒童及少年在內，更凸顯出此舉之必要性。簡言之，如何在網路世界中，建立優質、衡平、合憲的數位偵查（digital investigation），甚或數位扣押（digital seizure）、數位沒收（digital forfeiture）作為，已然是世界各國執法及立法單位急需努力的方向。再進一步言，有關網路不法行為防治，究竟是否均須法官保留取得令狀始得為之？得否單純以「停止域名解析」（Disabling DNS Resolution）方式，截堵臺灣網域的出入訊號？抑或是某種程度得以由行政機關以行政處分方式為之？是否必須倚賴刑事程序，或者民事程序亦得更迅速獲得救濟？政府是否需另立專法因應？

雖然，網路世界的發展從初期開始，即非奠基於政府所創制的平臺，而是遵循「網路自治」原則，以開放、自律、平等為宗旨，由多方利害關係人漸次營造而成。但是伴隨著網路蓬勃發展，網路世界占據人類大半生活，無可諱言地，無論是網路犯罪，亦或是民事網路侵權，甚至是

---

11 許伯崧、董容慈，網紅小玉DeepFake換臉謎片　YouTube官方宣布：無限期停止營利資格，公視新聞網，2021年11月3日，https://news.pts.org.tw/article/552248（最後瀏覽日：2021年11月29日）。

12 周子馨，南韓N號房主嫌終審定讞！至少關34年、公開個資10年，TVBS新聞網，2021年11月11日，https://tw.news.yahoo.com/%E5%8D%97%E9%9F%93n%E8%99%9F%E6%88%BF%E4%B8%BB%E5%AB%8C%E7%B5%82%E5%AF%A9%E5%AE%9A%E8%AE%9E-%E8%87%B3%E5%B0%91%E9%97%9C34%E5%B9%B4-%E5%85%AC%E9%96%8B%E5%80%8B%E8%B3%8710%E5%B9%B4-055734593.html（最後瀏覽日：2021年11月29日）。

違反行政規範之網路違規案件，均跳脫不了對於「網路治理」（Internet Governance）的範疇。「網路治理」一詞則可追溯至「網路治理工作小組」（Working Group on Internet Governance, WGIG）；此小組因應2003年聯合國世界資訊社會高峰會（World Summit on Information Society, WSIS）日內瓦階段會議發表的「原則與行動宣言」而成立[13]。次而，WGIG在2005年6月發表WGIG工作報告，將網路治理工作定義為：「網際網路的國際管理應該是多邊的、透明的和民主的，政府、私營部門、民間社會和國際組織的充分參與（The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations.）」，以達到兼顧各方利益衡平的網路治理。該宣言內容於今視之，仍然適用無礙，亦為本文立論的張本。

貳、網域名稱扣押：從美國實務出發

一、網域名稱系統簡介

在DNS架構下，網域名稱，如www.harvard.edu（哈

[13] Building the Information Society: a global challenge in the new Millennium, Declaration of Principles, World Summit of the Information Society 2003, Dec. 12, 2003, https://www.itu.int/net/wsis/docs/geneva/official/dop.html (last visited: Sept. 21, 2021).

佛大學網站）、www.amazon.com（亞馬遜購物網站）等，係供網路使用者於連結網際網路時辨識之用，以使用者所熟知之英文名稱所組成，為使用者端的辨識模式；而該網域名稱相對應於電腦端，則為四組號碼連串所組成之IP（Internet Protocol）位址，以作為供電腦判讀之用[14]。

鑑於網域名稱涉及廣大網路使用者之利益，為有效並公平統籌分配網域名稱，並且維護網際網路運行之穩定性及競爭之公平性，「網際網路名稱與號碼指配組織」（Internet Corporation for Assigned Names and Numbers, ICANN）於焉成立，透過此一非營利組織的運作，掌理全球網際網路IP位址的分配、通用頂級網域名稱（gLTD）系統的管理，以及根伺服器（root server）系統管理[15]。

目前，ICANN進而將不同的頂級網域名稱，委由不同之「註冊管理機構」（registry）管理，如「.net」、「.com」等頂級網域名稱，係由Verisign負責[16]；「.org」

---

14 限於篇幅，有關網域名稱、DNS及IP位址的架構與基礎理論，請參見以下說明：Beginner's Guide to INTERNET PROTOCOL (IP) ADDRESSES, ICANN, Mar. 4, 2011, https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf (last visited: Oct. 2, 2021); How the Domain Name System (DNS) Works, VERISIGN, 2021, https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml (last visited: Oct. 2, 2021).

15 參見Welcome to ICANN!, https://www.icann.org/resources/pages/welcome-2012-02-25-en (last visited: Oct. 23, 2021); 愛范兒，全球網路的新「波瀾」：美國正式交出域名管理權，數位時代，2016年10月4日，https://www.bnext.com.tw/article/41205/icann-domain（最後瀏覽日：2021年10月29日）。該組織位於美國洛杉磯，成立於1998年。

16 Verisign的主要業務有管理世界13台根伺服器中的2台（A與

頂級網域名稱則由The Public Interest Registry（PIR）負責[17]。而一旦註冊者（registrant）欲使用網域名稱，則需向網域名稱註冊管理機構轄下之「受理註冊機構」（registrar）申購註冊服務，再由註冊管理機構依照ICANN之規定，予以分配網域名稱。在美國，截至目前為止，在眾多的受理註冊機構中，最著名應屬GoDaddy[18]。簡而言之，就網域名稱註冊服務產業而言，註冊管理機構就如同「批發商」，僅負責「批發」其所掌管之網域名稱，不直接面對消費者；而受理註冊機構就如同「零售商」，受理網域名稱使用者之申請，並提供註冊服務。

從而，就扣押、沒收網域名稱之法律面及執行面而言，對於涉犯侵權網站之網域名稱，只要其頂級域名為「.com」、「.net」或「.org」，則行為人為犯罪行為，如傳遞盜版數位內容訊號，或傳輸仿冒產品之網頁頁面訊息

J），.com、.net和.name通用頂級域名以及.cc和.tv國家代碼頂級域名的註冊，另包括.jobs、.gov和.edu頂級域名後端系統營運，同時提供管理型DNS服務（MDNS）、分散式阻斷服務（Distributed Denial of Service，DDoS）防禦，以及網路威脅報告等服務。VeriSign公司總部於2011年遷移至美國維吉尼亞州之Reston。What Does Verisign Do?, VERISIGN, https://www.verisign.com/en_US/company-information/index.xhtml (last visited: Oct. 2, 2021).

17 About PIR, the new, 2021, https://thenew.org/org-people/about-pir/ (last visited: Oct. 22, 2021)公司總部位於美國維吉尼亞州之Reston。

18 GoDaddy是目前全球最大的受理註冊機構，截至2017年為止，旗下管理7,500萬筆網域名稱，擁有1,700萬名客戶，總部設於美國亞利桑納州 Scottsdale。參見History & Milestones, GoDaddy, 2019, https://aboutus.godaddy.net/newsroom/history-and-milestones/default.aspx (last visited: Oct. 3, 2021).

時，必然會透過Verisign或PIR等網域名稱註冊管理機構之伺服器。因此，縱然該等侵權網站之伺服器係架設於美國境外，行為人亦未具有美國國籍，甚或不知孰為行為人時，因該等網站所使用之頂級網域名稱之持有管理者，如Verisign等公司係在美國境內，執法單位因之對於此等網域名稱之沒收，享有管轄權。準此，執法機關僅需將法院核可的扣押令狀，提示予Verisign等公司執行，即可達到沒收網域名稱之效果，無須再透過司法互助或在境外提出訴訟之方式為之。

二、背景簡介

所謂「域名扣押」（domain name seizure），係指自2010年左右開始，美國政府開始針對販售仿冒品及侵犯著作權的網站所展開的打擊犯罪行動。美國國土安全部（Department of Homeland Security）轄下的「移民及邊境執法局」（Immigration and Customs Enforcement）（下稱「ICE」），及其他相關執法機構，透過民事程序「對物」（*in rem*）沒收[19]的方式，認為系爭網站之域名，係嫌犯遂行侵犯智慧財產權犯行所使用之犯罪工具，遂以該域名為「被告」，向管轄法院提出相當合理之證據與說明，

[19] 迥異於傳統對人（*in personam*）的沒收，亦即無需確定被告人別，可將系爭標的物列為「被告」而沒收之。詳請參見陳昱奉，數位時代之犯罪偵查與網路自由及隱私權之保障——從網域名稱（Domain Name）之扣押、沒收談起，臺灣嘉義地方檢察署研究報告，2014年12月，https://www.cyc.moj.gov.tw/media/136016/551410383574.pdf（最後瀏覽日：2021年9月12日）。

聲請扣押（seize）該域名。

在此，值得探討的是，網域名稱係為IP位址相對應之代號，並非有體物，是否得成為沒收之客體？域名是否可以成為形式強制處分制度下的扣押標的？對此，美國尚無成文法以資規範，然自從2002年Kremen v. Cohenu一案後，實務上已普遍接受域名為「無形財產」（intangible property）的一種形式[20]，而與其他財產權一樣，得成為扣押之標的，核與財產權之特性並無相違。事實上，網域名稱之轉賣或拍賣在商業上數見不鮮，具有特殊意義或辨識性高的網域名稱，其價值更以百萬美元計[21]。再者，在ICE歷次Operation In Our Sites行動中，各法院並未將網域名稱排除在沒收之客體外，而予以拒絕核發令狀，足見目前各聯邦地區法院咸認為網域名稱乃得成為沒收之客體，核無疑義。此外，另值得注意的是，域名之扣押，雖然現實上並未發生物之占有移轉，但尚未脫逸美國憲法第四修正案[22]所賦予之扣押定義範疇。在United States v. Jacobsen,

20 Kremen v. Cohen, 337 F.3d 1024,1030 (9th Cir. 2002).

21 如域名Cars.com，其價格即達8億7千2百萬美元之譜，參見Joe Styler, The top 25 most expensive domain names, GoDaddy, 2022, https://www.godaddy.com/garage/the-top-20-most-expensive-domain-names/ (last visited: Oct. 6, 2021).

22 THE FORTH AMENDMENT: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

466 U.S. 109, 113 (1984)一案中，最高法院認為：「對於系爭財產個別的占有利益，有意義地加以干涉（some meaningful interference with an individual's possessory interests in … property），亦可謂之為扣押。」準此見解，將欲沒收之網域名稱登記資料納為國家控管，並將網址指向國家指定之網頁，亦屬扣押之態樣。

以近年來著名的WeLeakInfo.com一案[23]為例，該網站聲稱為其用戶提供搜索引擎，用於非法取得的個人資訊，其中包含超過120億則，包括姓名、電子郵件地址、用戶名、電話號碼和密碼等紀錄。該網站藉由訂閱制度營利，任何用戶都可以透過該網站查知遭洩露的個人資料。此次查緝行動是FBI、美國哥倫比亞特區檢察官辦公室、司法部電腦犯罪和智慧財產權科以及包括英國國家犯罪局在內，國際執法部門所採取的全面執法行動的一部分。荷蘭國家警察總隊、德國聯邦刑事警察局和北愛爾蘭警察局也參與此次行動。為有效迅速防止損害擴大，WeLeakInfo.com之網域名稱被扣押之後，上網瀏覽該網站之網路使用者，將會看到網頁被轉向至美國政府相關執法單位網站，並暫停該網站營運，透過網頁告知原有網站之網域名稱已遭扣押（如下圖1）。

23 WeLeakInfo.com Domain Name Seized, Department of Justice, Jan. 16, 2020, https://www.justice.gov/usao-dc/pr/weleakinfocom-domain-name-seized (last visited: Sept. 29, 2021). 讀者可以在網址欄鍵入WeLeakInfo.com之後，即可看到該警示網頁。

圖1

域名遭扣押後所顯示之警告頁面（WeLeakInfo案）[24]

三、法律依據

在實體法層面，以智慧財產權案件為例，侵犯智慧財產權網站之域名沒收，係以Title 18 U.S.C.第2323條為基準條文開展。Title 18 U.S.C.第2323條第(a)(b)項規定：任何用以交易第2319條所禁止標的之物品，或是任何用以，或意圖用以犯罪或幫助全部或一部犯罪之財產，均應沒收[25]。Title 18 U.S.C.第2323條第(a)項第2款進一步陳明，

24 同前註。

25 本條為美國沒收法制下之重要條文，其地位相當於我國刑法第38條。

Title 18 U.S.C. § 2323. Forfeiture, destruction, and restitution

(a) Civil Forfeiture.—

(1) Property subject to forfeiture.— The following property is subject to forfeiture to the United States Government:

(A) Any article, the making or trafficking of which is, prohibited under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title.

(B) Any property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense referred to in subparagraph (A).

(C) Any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense referred to in subparagraph (A).

(2) Procedures.— The provisions of chapter 46 relating to civil forfeitures shall extend to any seizure or civil forfeiture under this section. For seizures made under this section, the court shall enter an appropriate protective order with respect to discovery and use of any records or information that has been seized. The protective order shall provide for appropriate procedures to ensure that confidential, private, proprietary, or privileged information contained in such records is not improperly disclosed or used. At the conclusion of the forfeiture proceedings, unless otherwise requested by an agency of the United States, the court shall order that any property forfeited under paragraph (1) be destroyed, or otherwise disposed of according to law.

(b) Criminal Forfeiture.—

(1) Property subject to forfeiture.— The court, in imposing sentence on a person convicted of an offense under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90 section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title, shall order, in addition to any other sentence imposed, that the person forfeit to the United States Government any property subject to forfeiture under subsection (a) for that offense.

(2) Procedures.—

(A) In general.— The forfeiture of property under paragraph (1), including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed

第46章與民事沒收有關的條文，均得適用於該條所稱之沒收[26]。換言之，在Title 18 U.S.C第2323條所示之各項罪名，其射程範圍含括各種形式之扣押及民事沒收。此外，Title 18 U.S.C第981條第(b)項(1)款復規定，民事沒收得藉由檢察總長之指揮，透過檢察機關執行之[27]。

在違反著作權法案件部分，侵權網站之域名之所以得

---

by the procedures set forth in section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), other than subsection (d) of that section.

(B) Destruction.— At the conclusion of the forfeiture proceedings, the court, unless otherwise requested by an agency of the United States shall order that any—

(i) forfeited article or component of an article bearing or consisting of a counterfeit mark be destroyed or otherwise disposed of according to law; and

(ii) infringing items or other property described in subsection (a)(1)(A) and forfeited under paragraph (1) of this subsection be destroyed or otherwise disposed of according to law.

(c) Restitution.— When a person is convicted of an offense under section 506 of title 17 or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title, the court, pursuant to sections 3556, 3663A, and 3664 of this title, shall order the person to pay restitution to any victim of the offense as an offense against property referred to in section 3663A (c)(1)(A)(ii) of this title.

26 參見前註Title 18 U.S.C. § 2323(a)(2).

27 Title 18 U.S.C. § 981(b)(1)
Except as provided in section 985, any property subject to forfeiture to the United States under subsection (a) may be seized by the Attorney General and, in the case of property involved in a violation investigated by the Secretary of the Treasury or the United States Postal Service, the property may also be seized by the Secretary of the Treasury or the Postal Service, respectively.

成為扣押、沒收之標的，乃係依據Title 18 U.S.C第2319條第(a)項規定，即任何人違反美國聯邦法典第17編（Title 17 U.S.C）「著作權」（Copyright）第506條[28]，均屬涉犯

[28] Title 17 U.S.C. § 506
(a) Criminal Infringement.—
(1) In general.— Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed—
(A) for purposes of commercial advantage or private financial gain;
(B) by the reproduction or distribution, including by electronic means, during any 180–day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000; or
(C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.
(2) Evidence.— For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright.
(3) Definition.— In this subsection, the term "work being prepared for commercial distribution" means—
(A) a computer program, a musical work, a motion picture or other audiovisual work, or a sound recording, if, at the time of unauthorized distribution—
(i) the copyright owner has a reasonable expectation of commercial distribution; and
(ii) the copies or phonorecords of the work have not been commercially distributed; or
(B) a motion picture, if, at the time of unauthorized distribution, the motion picture—
(i) has been made available for viewing in a motion picture exhibition facility; and
(ii) has not been made available in copies for sale to the general public in the United States in a format intended to permit

刑事責任。Title 17 U.S.C第506條第(a)項規定：「故意以下列方式侵犯他人之著作權者，依Title 18 U.S.C第2319條之規定處罰之：(a)基於商業利益或個人財獲……。」而在違反商標法案件部分，在歷次所查獲的案件中，多屬在網站上販賣仿冒商品之類型。對此，美國聯邦商標法，即美國聯邦法典第15編（Title 15 U.S.C）第22章「商標」（Trademark）中，並未另設有特別法之刑責規定，而係回歸普通刑法即Title 18 U.S.C第2320條，作為處以刑事責任的依據。依照該條第(a)項規定，明知為仿冒商標之商品而販賣之者，得處以徒刑或科或併科罰金。復依同條第(c)項規定，涉犯同條所稱之刑事責任者，適用Title 18 U.S.C

---

viewing outside a motion picture exhibition facility.

(b) Forfeiture, Destruction, and Restitution.— Forfeiture, destruction, and restitution relating to this section shall be subject to section 2323 of title 18, to the extent provided in that section, in addition to any other similar remedies provided by law.

(c) Fraudulent Copyright Notice.— Any person who, with fraudulent intent, places on any article a notice of copyright or words of the same purport that such person knows to be false, or who, with fraudulent intent, publicly distributes or imports for public distribution any article bearing such notice or words that such person knows to be false, shall be fined not more than $2,500.

(d) Fraudulent Removal of Copyright Notice.— Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than $2,500.

(e) False Representation.— Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than $2,500.

(f) Rights of Attribution and Integrity.— Nothing in this section applies to infringement of the rights conferred by section 106A (a).

第2323條有關沒收之規定，再經由Title 18 U.S.C第2323條指向適用Title 18 U.S.C第981條所示之民事沒收程序。

綜上，由於侵犯著作權或商標權之域名，係行為人用於施行或幫助侵害智慧財產權之工具，並為佐證該犯行之證據，遂得成為沒收的客體。執法單位爰依Title 18 U.S.C第981條之規定，向法院聲請令狀，扣押系爭域名稱後予以沒收之。對此，ICANN為讓扣押、沒收程序得以順遂進行，遂制訂「網域名稱命令指引」（Guidelines for Domain Name Orders）[29]，供執法機關或其他民事案件當事人據以遵循。執法機關欲執行法院令狀，進而對系爭網域名稱進行扣押、沒收，需就下列問題提出說明：聲請人為何？聯絡人為何？執行命令性質為何（如：法院令狀、因著作權或惡意程式所衍生之第三人請求（third party request for action）？所欲執行日期為何？是否需要同時取得網域名稱之相關資訊？網域名稱紀錄要如何變更（如：變更網域名稱登記人等）？網域名稱之現況要如何變更（如：禁止系爭網域名稱移轉、禁止網域名稱更新登記資料、刪除網域名稱）？網域名稱是否需轉移至其他登記人？網域名稱是否要停止解析等等。在美國諸多案例中，

[29] Dave Piscitallo, Thought Paper on Domain Name Takedowns, ICANN Blog, Mar. 8, 2012, https://www.icann.org/en/blogs/details/thought- paper-on-domain-seizures-and-takedowns-8-3-2012-en (last visited: Sept. 7, 2021); Dave Piscitallo, Guidance for Preparing Domain Name Orders, Seizures and Takedowns, ICANN Security Team, 2012, https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf (last visited: Sept. 7, 2021).

ICE等執法單位於取得令狀之後，隨即通知Verisign等註冊管理機構，將令狀所列之網域名稱轉向至指定之IP位址，使網頁瀏覽者得以看見如圖1所示之網頁，進而知悉其所造訪之網站網域名稱已遭扣押；註冊管理機構並應要求受理註冊機構，將個別網域名稱之「技術聯繫窗口」（Technical Contact）及「管理聯繫窗口」（Administrative Contact）等記錄資料，轉至執法機關所指定之聯繫窗口，以此法將該網域名稱至於國家之實力支配之下。

值得注意的是，網域名稱扣押除了智慧財產權相關侵權行為得以使用之外，在於其他透過營運網站以遂行犯罪之情況，尤其是需要即時停止或減低犯罪所生之損害時，已可獲得相當實益。其中，在資訊安全方面，除了上述WeLeakInfo網站大量販售他人個資案件之外，2018年之Sofacy Group殭屍網路一案[30]，即以民事對物沒收方式扣押網域名稱.toknowall.com，以阻止損害擴大。本案波及甚廣，由數十萬受感染的家庭和辦公室（SOHO）路由器和其他物聯網設備組成全球殭屍網路，名為Sofacy Group，至少從2007年或大約在2007年開始運作，針對政府、軍隊、安全組織和其他被認為具有情報價值的目標。由於本案係以VPNFilter模式運作[31]，為了識別受感染的設

30 Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices, DEPARTMENT OF JUSTICE, May 23, 2018, https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected (last visited: Oct. 24, 2021).

31 VPNFilter惡意軟體是一個多階段的模組化平臺，具有多種功能，可

備並進行補救，美國賓州西區檢察官辦公室因此向法院申請並取得令狀，授權FBI取得屬於惡意軟體所命令和控制基礎設施的部分區域。而就網域名稱部分，在美國賓州西區聯邦法院所核發的扣押命令中，係採取民事對物沒收方式，將toknowall.com此一域名列為被告，認定該網域名稱，是犯罪嫌疑人涉犯美國聯邦Title 18 U.S. Code第1030條[32]「利用電腦設備詐欺罪」所使用之工具，爰指示受理註冊機構Verisign公司執行該網域名稱之扣押，執行方法及細節參照前述ICANN所制訂「網域名稱命令指引」為之。

支持情報蒐集和破壞性網路攻擊操作。在第1階段，惡意軟體通過重啟持續存在，使其與大多數其他針對物聯網設備的惡意軟體區分開來，因為惡意軟體通常無法在設備重啟後存活。此外，第1階段的主要目的是獲得持久的立足點，並啟用第2階段惡意軟體的部署。第1階段利用多個命令和控制（C2）機制來發現當前第2階段部署服務器的IP位址，致使該惡意軟體非常強大，並且能夠處理不可預測的C2基礎設施變化。參見William Largent, New VPNFilter malware targets at least 500K networking devices worldwide, TALOS CISCO, May 23, 2018, https://blog.talosintelligence.com/2018/05/VPNFilter.html (last visited: Dec. 30, 2021).

32 Title 18 U.S. Code § 1030 — Fraud and related activity in connection with computers.

圖2
Sofacy Group殭屍網路一案，扣押域名toknowall.com之法院令狀[33]

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEIZURE OF THE DOMAIN NAME, **toknowall.com**	WARRANT OF SEIZURE *IN REM* PURSUANT TO 18 U.S.C. §§ 1030(i) AND 1030 (j) AND 21 U.S.C. §§ 853(e) AND 853(f) AND SEALING ORDER Magistrate No. 18-665 [UNDER SEAL]

WARRANT OF SEIZURE AND SEALING ORDER

TO: VERISIGN, INC., 12061 BLUEMONT WAY, RESTON, VA ("REGISTRY")

ANY AUTHORIZED LAW ENFORCEMENT OFFICER

An Affidavit having been made before me by MICHAEL J. McKEOWN, a Special Agent with the Federal Bureau of Investigation, United States Department of Justice, that he has reason to believe that the above-captioned domain name is subject to seizure and criminal forfeiture pursuant to 18 U.S.C. §§ 1030(i) and 1030(j) and 21 U.S.C. §§ 853(e) and 853(f), and as I am satisfied that there is probable cause to believe that the property so described is subject to seizure and criminal forfeiture pursuant to 18 U.S.C. §§ 1030(i) and 1030(j) and 21 U.S.C. §§ 853(e) and 853(f);

YOU ARE HEREBY COMMANDED AND AUTHORIZED to seize, within fourteen (14) days of the date of the issuance of this warrant, by serving a copy of this Seizure Warrant and Order, upon the REGISTRY, the domain name described below pursuant to the seizure procedure contained in Attachment A to this Seizure Warrant and Order:

toknowall.com

33 參見同前註。

YOU ARE FURTHER COMMANDED AND AUTHORIZED to prepare a written inventory of the property seized and promptly return this Seizure Warrant and Order and inventory before this Court as required by law.

THE REGISTRY IS HEREBY COMMANDED to comply with all terms of this Seizure Warrant and Order pursuant to the seizure procedure set out in Attachment A to this Seizure Warrant and Order pending further order of the Court.

THE COURT FINDS that there is reason to believe that notification of the existence of this Seizure Warrant and Order will result in destruction or tampering with evidence and flight from prosecution, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is ordered that this Seizure Warrant and Order, including Attachment A to the Warrant, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Seizure Warrant and Order on the REGISTRY; provide copies of the Affidavit or Seizure Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: May 22, 2018

[redacted]
HONORABLE LISA PUPO LENIHAN
UNITED STATES MAGISTRATE JUDGE

參、網域名稱扣押在我國司法實務之實踐：兼論DNS RPZ之運用

一、背景簡介

相較於網域名稱扣押在美國已行之有年，在我國司法實務上仍可說是相當陌生的概念。誠如前述，美國實務上有關域名扣押制度之開展，係奠基於歷史悠久的「民事對物沒收制度」，然我國因欠缺此一機制，而且諸如

ICANN、Verisign、GoDaddy等與頂級域名相關的組織或公司，並非位在我國境內，欠卻管轄聯繫因素，因此網域名稱扣押機制是否得以在我國執行無礙，尚有疑義。對此，網域名稱扣押原本即重在防止訊號繼續傳接，防止一般大眾得以不斷造訪侵權網站，也因此，向來在網域管理上已經發展相當成熟的機制：Response Policy Zone，中文稱之為「回應政策區域」（下稱「DNS RPZ」），在查緝網路相關犯罪上提供了一套因地制宜的解決方案。

為了因應網路犯罪與網路安全威脅增加，「財團法人台灣網路資訊中心」（Taiwan Network Information Center, TWNIC）[34]整合國內網路關鍵基礎設施提供者（Internet Servie Provider, ISP），共同建構DNS RPZ[35]。簡言之，DNS RPZ是域名系統服務器所提供的功能之一，

34 財團法人台灣網路資訊中心（TWNIC）是一非營利性之財團法人機構，在交通部電信總局及中華民國電腦學會的共同捐助下，於1999年12月29日完成財團法人設立登記事宜，2017年12月22日完成主管機關變更為「國家通訊傳播委員會」。捐助章程中規定，TWNIC為我國國家級網路資訊中心（National Network Information Center），其服務宗旨如下：一、非以營利為目的，以超然中立及互助共享網路資源之精神，提供註冊資訊、目錄與資料庫、推廣等服務。二、促進、協調全國與國際網際網路（Internet）組織之間交流與合作，並爭取國際網路資源及國際合作之機會。三、協助推展全國各界網際網路應用之普及，以及協調資訊服務之整合、交換。四、協助或支援政府辦理各項事務，並推動網路資訊相關公益事務。參見TWNIC，成立宗旨，2021年，https://twnic.tw/about.php（最後瀏覽日：2021年10月2日）。

35 黃勝雄，DNS RPZ摘要說明，TWNIC，2020年9月23日，https://blog.twnic.tw/2020/09/23/15311/（最後瀏覽日：2021年10月2日）。

亦可稱之為「DNS防火牆」，發揮阻擋外來攻擊。由於在網路世界，有愈來愈多惡意程式及殭屍網路，利用DNS查詢C&C伺服器（Command and Control Server），RPZ允許遞歸解析器（recursive resolver），透過自定義的資訊修改解析結果後，再回傳給DNS客戶端，藉由修改查詢結果的方式，以防止駭客攻擊，或避免使用者訪問惡意網站。

目前，DNS RPZ機制採取主從架構，如將不當網域名稱或IP位址寫入主節點DNS RPZ時，所有參與DNS RPZ的次級節點，會同時限制接取此不當網域名稱或IP位址。一般而言，TWNIC主要負責臺灣國家網域名稱.tw的註冊與營運，另外，為提升網路空間安全，TWNIC與國內網路關鍵基礎設施提供者共同合作建構全臺DNS RPZ服務架構，透過全臺DNS RPZ服務架構，將DNS RPZ限制接取的網域名稱範圍擴大，不限於.tw國家頂級網域名稱，作為境內或境外惡意網域名稱第一線的防護措施。

二、法制概述

由以上論述可知，美國法上的網域名稱扣押，其前提需要取得法院的令狀始得將系爭域名扣押，將該域名的連結轉到司法單位所指定的警示頁面；如果是採行DNS RPZ的防火牆機制，也需要有法院的判決、裁定，或者行政處分，我國TWNIC才能據以執行。那麼，對於網路盜版等網路犯罪案件，在我國司法審判權範圍內，是否也能夠以網域名稱扣押及DNS RPZ等機制來處理呢？這裡將牽涉到二

個問題：我國刑事訴訟法所規定的「扣押」態樣，是否包括網域名稱扣押呢？如果答案是肯定的，那麼在取得法院令狀之後，實務面又應如何執行？

我國刑事訴訟法有關扣押之相關規定，最基本的條文為第133條第1項：「可為證據或得沒收之物，得扣押之。」另外，「非附隨於搜索之扣押，除以得為證據之物而扣押或經受扣押標的權利人同意者外，應經法官裁定。」「偵查中檢察官認有聲請前條扣押裁定之必要時，應以書面記載前條第三項第一款、第二款之事項，並敘述理由，聲請該管法院裁定。司法警察官認有為扣押之必要時，得依前項規定報請檢察官許可後，向該管法院聲請核發扣押裁定。」刑事訴訟法第133條之1第1項、第133條之2第1項分別定有明文。亦即，若非以搜索為前提的扣押，亦得以循上開規定，向法院聲請裁定獲准後執行扣押。再者，扣押為強制處分之一種，刑事訴訟法並未限定其執行態樣，因此，以扣押之意思而對欲扣押之標的執行扣押，即產生扣押效果。簡言之，一旦扣押之意思達到扣押標的之持有人或所有人，並將應扣押標的移至公權力之下，扣押行為即告完成，法律上即為國家所占有，其原有運作之功能亦即因扣押而中止。例如：扣押刀子一把後，即不得再持之用以傷人；扣得挖土機一部後，即不得再用以盜採砂石，傷害及竊盜之犯行因此中止。而在許多電信詐欺案件，實務常見司法警察扣押被告辦公室或住家的電腦主機後，必然會將電源線及網路線拔除，停止該主機的一切運作功能，包括中斷與外部網際網路的連結，自然也包括停

止解析域名在內。進一步而言，執法機關執行扣押的目的，其一大目的無非在於阻斷系爭犯行再次遂行的可能性，從而，刑事訴訟法第133條所謂之「扣押」，原本即含有「暫時性的處分」的功能，不因最終是否經法院宣告沒收而有異。

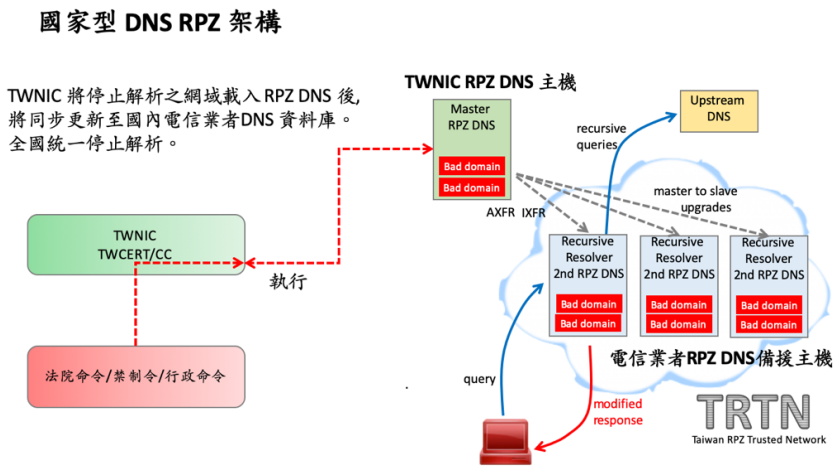
其次，網域名稱扣押我國刑事訴訟法所規定的「扣押」態樣，是否包括網域名稱，以及其所對應之IP位址？對此，我國刑事訴訟法並無明文規定，但參諸刑事訴訟法第133條於2016年6月22日之修法理由載明：「關於不動產、船舶、航空器之保全方法，不限於命其提出或交付」足見扣押之方式，已不限於現實上移轉占有的情形，也包括透過其他方式，限制所有權人所支配權人處分權限的情形。刑事訴訟法第133條第4項、第5項所規定的扣押方式，即屬適例。再觀諸藉由網站和域名涉犯違反著作權法等犯行的情形，對於任何網站而言，網站訊息的進出與傳遞，來自於對其網域名稱的解析，所以透過域名扣押方式，將域名支配權限移轉於公權力之下，由公權力決定該網站營運與否，或者透過前述DNS RPZ的方式為之，將系爭網域名稱列在「黑名單」之中，以停止解析的方式，讓一般大眾無法接取，實際上與扣押的本質並無不同，仍屬刑事訴訟法第133條第1項所稱之扣押。然而值得注意的是，誠如前述，由於審判權的限制，非屬.tw的域名，例如www.amazon.com等網域名稱，由於其域名管理業務並非由TWNIC所管轄，處理頂級域名.com的根伺服器（root

server）亦非位在我國境內，因此，TWNIC並無法在其業務職掌範圍內，命令Verisign等註冊管理機構限制或剝奪域名持用人的權限。所以對於非屬TWNIC管理權限內的域名，僅能透過司法互助的方式，以我國法院所核發的裁定，向該管國家請求協助執行域名扣押。

再者，就DNS RPZ實際執行層面而言，TWNIC同時依據DNS RPZ架構特性，業已規劃符合正當程序之政策模式以及審核要件，以作為RPZ執行依據。而依照TWNIC規劃，限制惡意域名接取依據，包含法院判決或行政機關命令，或有資安疑慮且影響資安重大者。其架構及執行流程如下圖3、4[36]：

圖3

國家型DNS RPZ架構Structure of DNS PRZ (Country Mode)

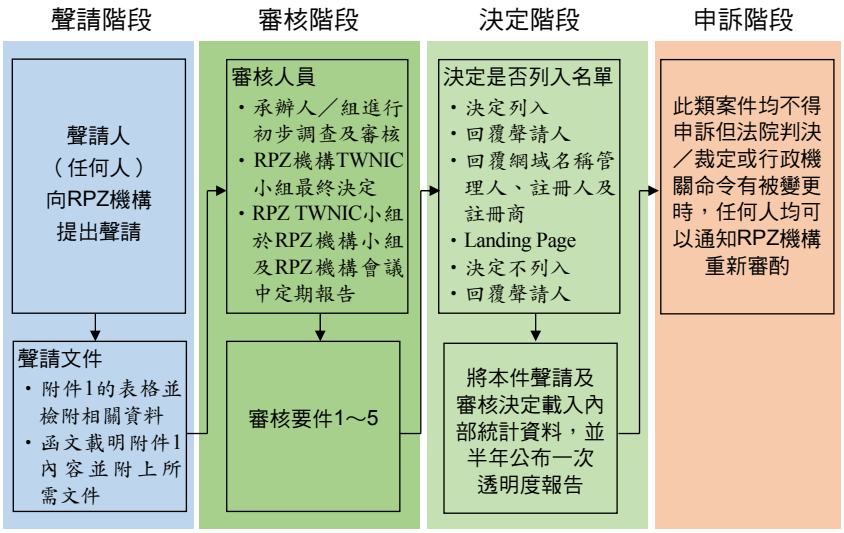


36 同前註。

圖4

聲請DNS RPZ依據及流程圖

情況一：依據法院判決／裁定或行政機關命令



承上所述，目前在DNS RPZ的運作框架下，TWNIC得以根據法院判決、裁定，或者行政機關的命令（實務上或以「行政處分」方式為之），將預計停止解析之網域名稱，載入DNS RPZ資料庫後，同步更新至國內電信業者DNS資料庫，全國統一停止解析。從而，TWNIC對於DNS治理部分，也有更進一步的說明[37]，關於.tw的域名，在技術上，TWNIC可以採取以下作為：第一、針對網域名稱部分：(一)提供關於該網域名稱之相關登記資料；(二)

37 財團法人台灣網路資訊中心110年9月9日第11082000120號函。

更換該網域名稱所有人（registrant）為其他指定之人；(三)更換該網域名稱之受理註冊機構（registrar）為其他指定的受理註冊機構；(四)防止該網域名稱之移轉；(五)防止該網域名稱資訊之更新；(六)防止原網域名稱所有人續約繼續使用該網域名稱；(七)刪除該網域名稱。（然於刪除該網域名稱後，其他人將能另行註冊使用該網域名稱）；(八)停止DNSSEC[38]；(九)就DNSSEC提供新的鑰匙，以取代目前的DNSSEC鑰匙。第二、針對DNS部分：(一)停止解析；(二)將連結至原網域名稱者，轉址至其他指定之網域名稱，通知使用者原網域名稱業經遭扣押或停止解析等（需提供轉址之網址以及需要執行轉址之時間）；(三)更換DNS管理者為其他指定之管理者（須提供該指定之管理者）。

綜上所述，藉由法院核發扣押裁定，對於域名實施DNS RPZ用以阻斷訊號接取的方式，讓侵權內容無法繼續由造訪者透過該網站取得，不僅在法制面及執行面上係屬有據且可行，在我國司法實務上並業已獲得肯認。2021年東京奧運期間，因某知名藝人藉由提供盜版影音內容的電

38 所謂DNSSEC（Domain Name System Security Extension, DNSSEC），即「網域名稱系統安全擴充程式」，網域名稱註冊人得以透過DNSSEC方式，數位簽署持有域名的相關資訊，而來自其他客戶端（如網頁瀏覽者）的查詢在取得回應後，也因回應中含有註冊人的數位簽章，從而確認回應正確無誤。詳請參見David Conrad, DNSSEC: Securing the DNS, ICANN Office of the Chief Technology Officer (OCTO), 2020/7/24, https://www.icann.org/en/system/files/files/octo-006-24ju l20-en.pdf (last visited: Oct. 24, 2021).

視機上盒「安博盒子」，在家中觀賞東奧賽事而喧騰一時，臺灣安博公司負責人及其他共犯因此遭到檢警查緝[39]，並藉由前述法院裁定扣押的方式，向法院聲請扣押涉犯著作權法的網域名稱，並以DNS RPZ的方式執行獲准[40]，而就涉外域名部分，也透過國際司法互助模式，向該管國家司法機關協助執行我國的扣押裁定。而在此之前，我國檢察機關也已意識到資通犯罪具有即時性和跨域性，因此，臺灣高等檢察署於2021年8月，成立「資通犯罪查緝督導中心」，推動「聲請法院扣押域名並執行DNS RPZ（停止解析）」，以違反智慧財產權、兒童及少年性剝削等重大指標性案件為主，統合情資即時阻斷犯行，並同時循線追緝嫌犯[41]。

肆、其他模式：以網站屏蔽命令（Website Block Order）為中心

一、導　論

人類自二十世紀開始保障智慧財產權以來，其相關法制架構是從地域性出發，為內國法的一部分，聚焦在內國

39 參見何毓庭，黑人看盜播奧運掀波　安博老董交保，聯合報，2021年10月9日，https://udn.com/news/story/7321/5804227（最後瀏覽日：2021年11月23日）。

40 參見臺灣新北地方法院110年度聲扣字第19號裁定。

41 王宏舜，資通犯罪猖獗　高檢署點出這6大特性讓查緝變艱鉅，聯合新聞網，2021年12月21日，https://udn.com/news/story/7321/5977416（最後瀏覽日：2021年12月23日）。

公權力的遂行，以及對國民權利的保障。但是，自從網際網路出現以來，已然打破傳統的法治架構。網際網路是跨國境的訊息空間，侵權網站又通常位於外國司法管轄區域，無法單恃內國刑事司法予以規範。而承前所述，利用域名扣押的方式，或可達成禁止使用者繼續造訪系爭侵權網站的效果，然而，一旦行為人迅速更改或申請新域名後，仍可繼續從事侵權行為，未能達到治本目的。況且，透過刑事訴訟，以發動強制處分程序為之，先要有司法警察相當時間的偵查，繼而經檢察官之可核准後，繼而向法院聲請受押裁定，其程序曠日費時，恐怕取得對系爭域名扣押裁定後，已成明日黃花，行為人早已轉移陣地或重起爐灶。

對此，除了刑事程序外，為避免損害繼續擴大，並及時確保權利人權益，自2010年左右開始，越來越多的國家或地區允許權利人在一定條件下，除利用刑事程序外，亦可循民事、行政程序，取得法院或相關主管機關所核發之命令，以類似發禁制令的方式，指示ISP業者即時阻止網路使用者造訪涉及不法內容的網站，進而減少盜版並增加合法內容和服務的消費[42]，此即一般所謂的「網站屏蔽命令」。再者，許多侵犯著作權的不法網站，係以

[42] Nigel Cory, How Website Blocking Is Curbing Digital Piracy Without "Breaking the Internet", Information Technology & Innovation Foundation (ITIF), Aug. 2016, https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online (last visited: Oct. 24, 2021).

BitTorrent[43]（簡稱BT，中文以「位元洪流」稱之，為敘述簡潔，以下以BT稱之）方式傳送影音串流內容，同時間下載越多，傳播就越迅速，若以屏蔽命令限制使用者造訪，在短時間內將減少BT下載點，降低檔案傳播速度，有助於減少法益侵害。簡言之，屏蔽命令可謂是數位時代的特殊法律手段，相當於其宗旨在於阻斷網站與外界的連結與資訊的進出，不讓使用者得以造訪網站上的侵權內容。

---

43 楊又肇，曾被盜版污名化的BitTorrent網路傳輸技術，如今邁入20週年，Mashdigi，2021年7月6日，https://mashdigi.com/bittorrent-turns-into-20-anniversary/（最後瀏覽日：2021年10月24日）。依該文獻說明，由BitTorrent係美國軟體工程師Bram Cohen等人於2001年4月所研發，並且在同年7月2日時首度投入應用的BitTorrent網路傳輸協定，推出至今已經進入20週年。雖然在發展過程中涉及傳播盜版內容等負面形象，但是對於網路傳輸技術應用卻有顯著影響。相比傳統在HTTP/FTP下載時使用的TCP/IP網路傳輸協定，BitTorrent建構在TCP/IP協定基礎之上，並且以P2P檔案傳輸通訊協定運作，更隨著發展擴充傳輸協定。在BitTorrent基本運作模式中，透過.torrent種子檔案定義Tracker資訊與檔案資訊，前者分別對應伺服器位址及設定，後者則闡述下載檔案內容，同時將下載檔案預先規劃相同大小的下載區塊，並且透過.torrent種子檔案比對每個下載區塊索引資訊與hash驗證碼。值得注意的是，由於一般在HTTP/FTP下載時，通常會占據提供下載端的伺服器運算資源與網路頻寬，因此若同時間連入使用人數過多，就會造成伺服器無法負荷，同時也會造成網路頻寬被占滿，可能會造成網路傳輸堵塞或伺服器當機情況，因此BitTorrent技術理念就是將檔案「切割」成多數細小下載區塊，並且透過P2P傳輸方式，讓其他已經下載部分區塊的裝置也能成為分享下載檔案「來源」，藉此分散原本提供下載端伺服器負荷量。換言之，當有更多人下載時，相對會讓整體下載速度變快，同時也會讓檔案可下載性持續延伸。但由於這樣的下載特性，後續也衍生被諸多網路論壇用於提供下載非法盜版內容，例如檔案容量龐大的影片、遊戲或音樂內容，因此也讓BitTorrent技術被烙上盜版工具形象。

而屏蔽命令從技術面而言，大致可分為以下四種方式[44]：

(一)網域名稱屏蔽（DNS Name Blocking）

涉及修改或刪除域名伺服器記錄，致使域名請求無法解析特定IP位址，因而造成域名請求不獲任何回應，或被重新定向到另一個網站，例如以「登錄頁面」（landing page）方式通知用戶造訪已被阻止。此法相當於本文前述之域名扣押。

(二)IP位址屏蔽（IP Address Blocking）

由於IP位址系統是透過ISP業者的路由器（router）運作，故ISP業者可藉由閘道路由器（gateway router）的配置，以便特定IP地址的數據封包被阻擋或重新指向到另一個IP地址。

(三)統一資源定位符（俗稱「網址」，以下仍以URL稱之）（URL Site Blocking）屏蔽

URL是網際網路上特定文件或文檔的位址，包括域名以及文件或文檔的位置。URL屏蔽通常由ISP業者將流量重新導引到具有應被屏蔽之「URL黑名單」的代理伺服器，然後將請求的URL與黑名單進行比較，如果請求的URL與列出的URL匹配，則連接將被拒絕或重新指向到另一個站點，例如警告頁面。

---

44 David Linsay, *Website Blocking Injunctions to Prevent Copyright Infringements: Proportionality and Effectiveness*, 40(4) UNSW LAW JOURNAL 1507, 1507-38 (2017).

(四)混合模式（Hybrid）

上述三種模式的混合使用。混合屏蔽涉及上述技術的組合，並且通常以兩階段方式實施。例如，IP位址屏蔽可用於第一階段，將可能被屏蔽的站點指向到代理伺服器，繼而由代理伺服器以URL屏蔽方式進行，英國即是採行混合模式。

二、各國屏蔽命令實務簡介

目前，世界各先進國家以屏蔽命令打擊網路盜版已趨常態化，茲將近年來各國實務狀況簡介如下[45]：

(一)澳大利亞

2015年2月，澳大利亞聯邦政府針對網路盜版部分，提出「2015著作法修正案」（Copyright Amendment (Online Infringement) Act 2015 (Online Infringement Amendment)）[46]，容許法院核發網站屏蔽命令，法院俟於2016年12月批准了第一份網站屏蔽命令[47]。自2016年12月

---

45 Nigel Cory, The Normalization of Website Blocking around the World in the Fight against Piracy Online, Information Technology & Innovation Foundation (ITIF), June 12, 2018, https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online (last visited: Oct. 24, 2021).

46 Review of the Copyright Online Infringement Amendment, Department of Infrastructure, Transport, Regional Development and Communication, Feb. 13, 2018, https://www.infrastructure.gov.au/have-your-say/review-copyright-online-infringement-amendment (last visited: Sept. 23, 2021).

47 Lianne Tang, Federal Court Orders ISPs to Block Pirate Sites in Australia, LEGALVISION, Oct. 31, 2018, https://legalvision.com.au/sinking-ship-federal-court-orders-isps-to-block-pirate-sites-in-australia/ (last visited: Dec.

在澳大利亞發布第一個網站封鎖令以來，聯邦法院已下令封鎖65個盜版網站，以及超過378個相關域名。自那時以來，澳大利亞排名前50的盜版網站的使用量下降了35%[48]。

除了防制網路盜版之外，線上博奕防治亦得藉由此法取得若干成效。聯邦政府所轄之「澳大利亞通訊暨媒體管理局」（The Australian Communications and Media Authority, ACMA）[49]，相當於我國的國家通訊傳播委員會，根據「1997年電信法」（Telecommunication Act 1997）第313條[50]之規定，向網路服務提供商發出命令，阻

22, 2021).

48 Nick Whigham, 'Shamelessly facilitating crime': Rights holders hit out at Google amid renewed Aussie piracy fight, news.com.au, Feb. 21, 2018, https://www.news.com.au/technology/online/piracy/shamelessly-facilitating-crime-rights-holders-hit-out-at-google-amid-renewed-aussie-piracy-fight/news-story/7cf2b0b441a91c55484bf38c874aa222 (last visited: Dec. 22, 2021).

49 詳請參見該機關網站Who we are, Acma, https://www. acma.gov.au/who-we-are (last visited: Jan. 13, 2022).

50 第313條　接續業者及接續服務提供業者之義務（313 Obligations of carriers and carriage service providers）

(1) A carrier or carriage service provider must, in connection with:
  (a) the operation by the carrier or provider of telecommunications networks or facilities; or
  (b) the supply by the carrier or provider of carriage services; do the carrier's best or the provider's best to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or of the States and Territories.

(1A) For the purposes of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), a carrier or carriage

service provider must, in connection with:

(a) the operation by the carrier or provider of telecommunications networks or facilities; or

(b) the supply by the carrier or provider of carriage services; do the carrier's best or the provider's best to protect telecommunications networks and facilities owned, operated or used by the carrier or provider from unauthorised interference or unauthorised access to ensure:

(c) the confidentiality of communications carried on, and of information contained on, telecommunications networks or facilities; and

(d) the availability and integrity of telecommunications networks and facilities.

Note 1: ***Security***, among other things, covers the protection of, and of the people of, the Commonwealth and the States and Territories from espionage, sabotage, attacks on Australia's defence system and acts of foreign interference.

Note 2: A person who uses a carriage service to supply various kinds of broadcasting services is not a carriage service provider merely because of that use (and therefore not subject to the duty imposed by this subsection): see subsections 87(1) and (2) and 93(1) and (2).

(1B) Without limiting subsection (1A), the duty imposed by that subsection includes the requirement for the carrier or carriage service provider to maintain competent supervision of, and effective control over, telecommunications networks and facilities owned or operated by the carrier or provider.

(2) A carriage service intermediary must do the intermediary's best to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or of the States and Territories.

(2A) For the purposes of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), a carriage service intermediary must do the intermediary's best to protect telecommunications networks and facilities used to supply the carriage service referred to in subsection 87(5) from unauthorised interference or unauthorised access to ensure:

(a) the confidentiality of communications carried on, and of

information contained on, telecommunications networks or facilities; and

(b) the availability and integrity of telecommunications networks and facilities.

Note: ***Security***, among other things, covers the protection of, and of the people of, the Commonwealth and the States and Territories from espionage, sabotage, attacks on Australia's defence system and acts of foreign interference.

(3) A carrier or carriage service provider must, in connection with:

(a) the operation by the carrier or provider of telecommunications networks or facilities; or

(b) the supply by the carrier or provider of carriage services; give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:

(c) enforcing the criminal law and laws imposing pecuniary penalties;

(ca) assisting the enforcement of the criminal laws in force in a foreign country;

(cb) assisting the investigation and prosecution of:

(i) crimes within the jurisdiction of the ICC (within the meaning of the I*nternational Criminal Court Act 2002*); and

(ii) Tribunal offences (within the meaning of the *International War Crimes Tribunals Act 1995*);

(d) protecting the public revenue;

(e) safeguarding national security.

Note: Section 314 deals with the terms and conditions on which such help is to be provided.

(4) A carriage service intermediary who arranges for the supply by a carriage service provider of carriage services must, in connection with:

(a) the operation by the provider of telecommunications networks or facilities; or

(b) the supply by the provider of carriage services; give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:

(c) enforcing the criminal law and laws imposing pecuniary penalties;

(ca) assisting the enforcement of the criminal laws in force in a foreign country;

(cb) assisting the investigation and prosecution of:
(i) crimes within the jurisdiction of the ICC (within the meaning of the *International Criminal Court Act 2002*); and
(ii) Tribunal offences (within the meaning of the *International War Crimes Tribunals Act 1995*);
(d) protecting the public revenue;
(e) safeguarding national security.

Note: Section 314 deals with the terms and conditions on which such help is to be provided.

(5) A carrier or carriage service provider is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith:
(a) in performance of the duty imposed by subsection (1), (1A), (2), (2A), (3) or (4); or
(b) in compliance with a direction that the ACMA gives in good faith in performance of its duties under section 312; or
(c) in compliance with a direction given under subsection 315A(1) or 315B(2).

(6) An officer, employee or agent of a carrier or of a carriage service provider is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the carrier or provider as mentioned in subsection (5).

(7) A reference in this section to giving help includes a reference to giving help by way of:
(a) the provision of interception services, including services in executing an interception warrant under the *Telecommunications (Interception and Access) Act 1979*; or
(b) giving effect to a stored communications warrant under that Act; or
(c) providing relevant information about:
(i) any communication that is lawfully intercepted under such an interception warrant; or
(ii) any communication that is lawfully accessed under such a stored communications warrant; or
(caa) giving effect to authorisations under section 31A of that Act; or
(ca) complying with a domestic preservation notice or a foreign

止網路使用者造訪涉及嚴重刑事或民事犯罪的網站，其中包括違反「2001年互動式賭博法」（Interactive Gambling Act 2001）之網站，諸如：

・向澳大利亞客戶提供被禁止的互動式賭博服務（如：線上賭場、線上老虎機、允許進行線上體育博奕的服務）；

・向澳大利亞客戶提供未經許可監管的互動式賭博服務（如：欠缺澳大利亞有效許可證的線上博奕服務）；

・在澳大利亞發布有關被禁止的互動式賭博服務或未經許可之受監管互動式賭博服務的廣告。

(二)加拿大

2018年，加拿大聯邦法院首次核准盜版網站屏蔽命令，要求主要ISP業者（包括Cogeco、Rogers、Bell、Eastlink和TekSavvy）阻止對盜版IPTV服務業者GoldTV網域和IP位址的造訪[51]。本件命令由承審法官Patrick Gleeson

---

preservation notice that is in force under Part 3-1A of that Act; or

(d) giving effect to authorisations under Division 3 or 4 of Part 4-1 of that Act; or

(e) disclosing information or a document in accordance with section 280 of this Act.

Note: Additional obligations concerning interception capability and delivery capability are, or may be, imposed on a carrier or carriage service provider under Chapter 5 of the *Telecommunications (Interception and Access) Act 1979*. 詳請參見https://www. legislation. gov.au/Details/C2019C00273 (last visited: Oct. 26, 2021).

[51] Ernesto Van der Sar, Federal Court Approves First 'Pirate' Site Blockade in Canada, Torrentfreak, Nov. 18, 2019, https://torrentfreak.com/federal-

所核發，該命令在北美地區堪稱首舉，但相當程度上參照英國有關屏蔽命令的前例。Gleeson法官認為，封鎖措施並非萬無一失，但是他也表示：「從證據中可以清楚地看出，網站屏蔽不會消除用戶對侵權服務的造訪。然而，證據確實顯示，在那些實施了網站屏蔽措施的司法管轄區域，對侵權網站的造訪量顯著減少（It's clear from the evidence that site-blocking will not eliminate user access to infringing services. However, the evidence does establish that in those jurisdictions where site-blocking measures have been implemented there has been a significant reduction in visits to infringing websites）[52]。」

此外，針對屏蔽命令的衡平性，Gleeson法官認為，面對一個具有強而有力表面證據（prima faci）的現時侵權案件，對於非法網站的限制性封鎖並結合處理無意過度封鎖程序的命令，於此網絡中立性和言論自由問題，與所尋求的救濟之間將取得平衡（in the face of a strong prima facie case of ongoing infringement and a draft order that seeks to limit blocking to unlawful sites and incorporates processes to address inadvertent over-blocking, that neither net neutrality nor freedom of expression concerns tip the balance against granting the relief sought）。

---

court-approves-first-pirate-site-blockade-in-canada-191118/ (last visited: Oct. 3, 2021).

52 同前註。

這一案件具有里程碑的意義，也引起了多家第三方機構的關注。著作權人團體固然支持網站封鎖，但加拿大網域註冊局（The Canadian Internet Registration Authority, CIRA）針對上開屏蔽命令持保留見解。而應執行禁制令的ISP業者，除了TekSavvy之外均無異議。雖然，TekSavvy即刻對裁決提出上訴，不過，加拿大聯邦上訴法院以及聯邦最高法院，仍都駁回TekSavvy的上訴，維持第一審的裁決[53]。TekSavvy辯稱，網站屏蔽將違反網絡中立性（net neutrality）。然而，聯邦上訴法院洛克（George R. Locke）法官認為，依照加拿大電信法第36條的文義，並沒有取代聯邦法院核發禁令的衡平權力，包括實施網站封鎖令的權力[54]；而ISP角度而言，TekSavvy遵守屏蔽命令，並不會產生「控制」（controlling）或「影響」（influencing）的效果[55]。此外，在言論自由部分，洛克法官同樣不認為屏蔽命令將會有過度封鎖的效果。最後，聯邦上訴法院不接受著作權人應首先考慮其他非屏蔽選項的建議，例如尋求Cloudflare或金錢支付服務商的幫助[56]。總而言之，洛克法官認為上訴應該被駁回，合議庭其他兩位法官納登（M. Nadon）法官和勒布朗（Rene LeBlanc）

53 Ernesto Van der Sar, Canada's Supreme Court Denies TekSavvy's Site Blocking Appeal, Torrentfreak, Mar 29, 2022, https://torrentfreak.com/canadas-supreme-court-denies-teksavvys-site-blocking-appeal-220329/ (last visited: Apr. 3, 2022).

54 同前註。

55 同前註。

56 同前註。

亦對此表示贊同。

圖5

加拿大聯邦上訴法院駁回TekSavvy上訴判決結論

D. *Conclusion*

[88] Having found no error in the Judge's conclusion that the Federal Court has the power to grant a site-blocking order, and having likewise found no error in his analysis of the applicable legal test, I conclude that this Court should not interfere with the Judge's decision.

[89] I would dismiss this appeal with costs.

"George R. Locke"
J.A.

"I agree
M. Nadon J.A."

"I agree
René LeBlanc J.A."

(三)德　國

相較於歐洲其他地方對於網站屏蔽命令的廣泛使用，遲至2018年2月，德國法院始首次發布暫時禁制命令，要求德國ISP業者（Vodafona Kabel）阻止用戶造訪非法流媒體網站Kinox.to[57]，該網站為德國最受歡迎的非法影音串流

57 Ernesto Van der Sar, Pirate Site Blockades Enter Germany With Kinox.to as First Target, Torrentfreak, Feb. 13, 2018, https://torrentfreak.com/pirate-site-blockades-enter-germany-with-kinox-to-as-first-target-180213/

平臺網站之一，但是位於德國境外。除此之外，針對線上盜版影音侵權，德國也開始融合「自律」與「他律」模式，結合公私部門力量，從組織面上做根本改變。鑑於透過法院命令方式來屏蔽侵權網站，往往無法收到及時的效果，因此，德國於2021年3月，由數家具規模的ISP業者以及著作權人、職業團體項聯合成立「線上著作權爭議處理機構」（Die Clearingstelle Urheberrecht im Internet, CUII），其性質為獨立機關，旨在使用客觀標準檢查阻止對侵權網站的造訪是否合法。審查委員會應權利人的要求進行檢查，如果滿符合條件，則建議對這個侵犯著作權的網站進行DNS封鎖。此外，儘管CUII免除法院訴訟的必要性，但仍藉由「委員會」（其中包括熟悉德國著作權法的退休法官）的方式，審查著作權人提交的每項申訴。CUII的業務監督係由德國電信監管機構「德國聯邦網路局」（BNetzA）[58]負責，受理各項投訴，以確認任何一個網站屏蔽均未違反歐盟的網路中立規則。德國聯邦網路局局長Jochen Homann並表示：「此系統有助於避免漫長而昂貴的法律訴訟（Verfahren hilft, langwierige und kostspielige Gerichtsverfahren zu vermeiden）」[59]。

(last visited: Apr. 3, 2022).

58 參見該機關官方網頁，Bundesnetzagentur (Federal Network Agency), Federal Ministry for Economic Affairs and Climate Action, 2022, https://www.bmwk.de/Redaktion/EN/Artikel/Ministry/bundesnetzagentur-bnetza.html (last visited: Apr. 3, 2022).

59 Clearingstelle Urheberrecht im Internet veranlasst Sperrung einer Streaming-Website, Bundesnetzagentur, Mar. 11, 2021, https://www.

(四)葡萄牙

自2015年開始，葡萄牙當地權利人、ISP業者和政府達成一項備忘錄，根據政府機構IGAC（Inspeção Geral das Atividades Culturais）的命令，ISP業者可以阻止造訪盜版網站。調查結果顯示，自2015年11月至2016年6月實施網站屏蔽命令之後，造訪侵權網站的用戶顯著減少：在葡萄牙排名前250的未經授權的網站中，有65個被阻擋，在此期間葡萄牙境內的使用量減少56.6%，但在全球範圍內增加3.9%；葡萄牙排名前250的未經授權網站的整體境內使用量下降9.3%；然而，全球範圍內全球增加30.8%[60]。

(五)英　國

自2011年以來，英國已屏蔽了數百個網站，在涉嫌智慧財產權侵權網站之網路屏蔽命令範疇，具有引領世界先鋒的地位。民事法院因應串流媒體侵犯智慧財產權的情況，主要依照「著作權、設計和專利法」（Copyright, Designs and Patents Act, CDPA）第97A條的規定，核發此類屏蔽命令。迄今，數百個網站已通過這種方法被屏蔽，通常包括文件共享（P2P/Torrent）、影音串流網站和銷售

---

bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2021/20210311_Clearingstelle.html (last visited: Feb. 3, 2022).

60 A PORTUGUESE GOVERNMENT ANTI-PIRACY PROGRAMME REDUCED TRAFFIC TO LARGE-SCALE PIRACY WEBSITES BY NEARLY 70 PER CENT, ACCORDING TO A NEW INCOPRO REPORT, INCOPRO.

假冒商品的網站等[61]。在2021年10月，英格蘭暨威爾斯商業暨財產法院（HIGH COURT OF JUSTICE BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES INTELLECTUAL PROPERTY LIST (ChD)），對於由哥倫比亞影業、迪士尼、派拉蒙、環球影業、華納和Netflix等聲請人所聯合提出，以BRITISH TELECOMMUNICATIONS PLC等為首的六大ISP業者為相對人，針對極受歡迎的影音串流媒體侵權網站，包括Tinyzonetv、Watchserieshd、Levidia、123movies和Europixhd核發屏蔽命令，由英國上開ISP業者加入過濾名單中予以屏蔽。法院命令認為，根據CDPA第97A的規定，核發禁令已被證明是阻止和勸阻此類侵權活動的最有效手段，特別是一般民眾在造訪對權利人造成重大損害的盜版作品時，並未具有合法利益。任何對其權利和ISP權利的干涉都是出於防止此類侵權的合法目的，換言之，自衡平性而言，該命令保障措施係屬適當[62]。

61 Mark Jackson, Six Big UK ISPs Ordered to Block Five Piracy Streaming Websites, Oct. 25, 2021, https://www.ispreview.co.uk/index.php/2021/10/six-big-uk-isps-ordered-to-block-five-piracy-streaming-websites.html (last visited: Mar. 26, 2022).

62 [2021] EWHC 2799 (Ch), THE HIGH COURT OF JUSTICE BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES INTELLECTUAL PROPERTY LIST (ChD) Case No: IL-2021-000045, Dec. 21, 2021, https://www.bailii.org/ew/cases/EWHC/Ch/2021/2799.pdf (last visited: Mar. 26, 2022).

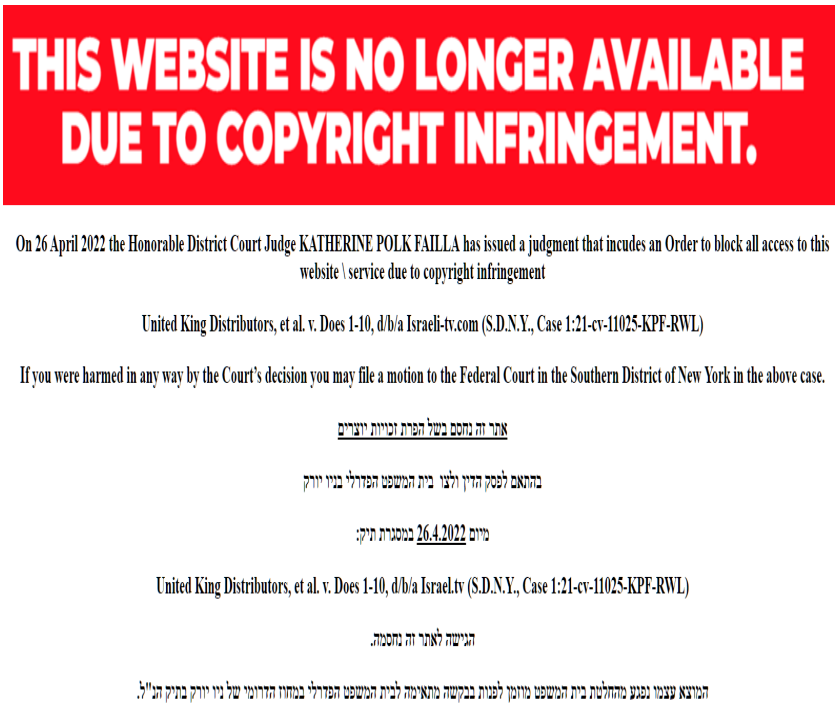
(六)美　國

向來，網站屏蔽在美國而言是一大禁忌，象徵著對言論自由的侵犯，以及對網路自由的不信任，尤其可能斲傷網路中立性。因此，對於網路侵權的遏止，相較於歐洲國家大量採用屏蔽命令，美國仍舊採行最初的域名扣押方式，其中最重要的原因，在於如本文前述：全世界得以順遂執行通用定級域名，如.com、.net等之扣押沒收者，應該只有美國，蓋因其管轄的連結因素最為周全，執行扣押均得在內國範圍完成。然而，近來美國法院已變更見解，表明藉由民事訴訟程序，准許權利人在侵權人未知的情況下，將侵權網站Israel-tv.com、Israel.tv和Sdarot.tv列為被告（本案以下以「以色列盜版串流網站案」簡稱之），針對盜版流媒體服務取得禁制令（injunction），要求每個美國ISP阻止訂閱的消費者造訪該網站。

2021年，包括United King Film Distribution、DBS Satellite Services以及Hot Communication在內的權利人，分別以Israel-tv.com、Israel.tv和Sdarot.tv等盜版串流媒體網站域名（實際犯罪嫌疑人不詳，故另以「DOES」稱之）為民事被告，向美國聯邦紐約南區地方法院（US District Court for the Southern District of New York）提起民事訴訟。最終，於2022年4月26日，原告透過一造缺席判決贏得上開三起訴訟。法院命令Israel-tv.com、Israel.tv和Sdarot.tv的運營商各支付7,650,000美元賠償金予原告。此外，前所未有的是，在所有三項判決中，被告都被禁止

侵犯原告的權利，包括串流傳輸、散佈或以其他方式向公眾提供任何受著作權保護的作品。被告還被禁止從現有網域，或者將來可能使用的任何其他網域操作他們的網站。用戶因此無法連接或使用該網站，並將被ISP的DNS服務器轉移到由原告操作和控制的登錄頁面（詳如下圖6）[63]：

圖6



63 Andy Maxwell, US Court Orders Every ISP in the United States to Block Illegal Streaming Sites, Torrentfreak, May 2, 2022, https://torrentfreak.com/us-court-orders-every-isp-in-the-united-states-to-block-illegal-streaming-sites-220502/ (last visited: May 16, 2022).

簡言之，上開三項判決和永久禁令，命令美國的所有ISP業者對侵犯著作權的行為，實施全面性的屏蔽。不僅如此，還包括「動態命令」（Dynamic Order），旨在防範侵權網站未來可能部署的任何反封鎖對策。再者，這三項禁令都禁止任何第三方公司（包括ISP、網路主機、CDN提供商、DNS提供商、域名公司、廣告服務、金融機構、支付處理商等）與其當前網域的網站，或任何新的網站開展任何業務。所有網域都必須引導到原告操作的登錄頁面，並且必須標示並凍結被告持有帳戶[64]。

總括來說，截至2021年為止，全世界總共至少有48個國家／地區允許以侵犯著作權為由屏蔽網站。其中，33個（不包括歐盟）積極允許權利人使用網站封鎖禁令來阻止著作權侵害。至少另外12個國家／地區（例如：保加利亞、克羅地亞、塞浦路斯、捷克共和國、愛沙尼亞、匈牙利、列支敦士登、盧森堡、馬爾他、波蘭、斯洛伐克和斯洛維尼亞。），法律容許在技術上允許網站屏蔽，但實務上未曾使用[65]。此外，澳大利亞、英國和其他地方的研究證明，如果有足夠多的盜版網站被封鎖，人們就會轉向合法來源，增加此類服務的消費[66]。

---

64 同前註。

65 Nigel Cory, *A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking*, Jan. 2022 ITIF 22, 22-28 (2022).

66 *Id*. at 6-12.

伍、數位時代的網路治理與犯罪防治新思維

誠如前言所述，在數位時代，我們可以預料幾乎日後所有犯罪都會和電腦或網路相關。長久以來，網路空間向來被認為是獨立自主的空間，但網路治理與犯罪偵查是否必須立於對立的狀態？從虛擬空間的思維出發，恐怕許多傳統偵查思維需要改變。向來以「追人」為首要宗旨的查緝思維，未必能夠妥善解決問題。筆者於2011至2012年在哈佛大學Berkman Klein網路暨社會研究中心擔任訪問學者期間，該中心於2011年9月假哈佛大學法學院Austin Hall，舉辦「iLaw 網路法律國際研討會」[67]，探討包括網路智慧財產權在內之最新網路法律議題。筆者應主辦單位邀請，在「全球網際網路」（the Global Internet）此項議程中，就網路治理（Internet Governance）主題發表評論。筆者以「Outcomes of Governance – The Example of Cybersecurity」為題，自犯罪預防及查緝的觀點，評析網路治理之未來走向。在研討會中筆者曾指出，美國貴為網路科技大國，除Google、Facebook等網路服務業巨擘的總部均設於美國外，另有許多如思科（Cisco）等網路設備大廠亦以美國為公司母國；加以美國本土網路使用人口眾

67 會議自2011年9月6日開始迄9月9日結束，研討主題相當廣泛，包括：網際網路的歷史、開放系統、線上自由權及表達自由、探討阿拉伯之春、轉變中的網路——網路安全、智慧財產、使用者創新、隱私權、新科技下的新方法、數位人性等。參與人士來自世界各地，相當踴躍。

多，反恐主義當道，美國政府當局藉由「網際網路」各個面向取得司法管轄權，進而對於存在於網路空間之各種言論資料予以調查甚或扣押取證，堪屬必要手段。換言之，在現今網路世界，透過法律或法律授權行政機關，對於「網路交通」（Internet Traffic）進行即時、廣泛、長期蒐證，不僅為查緝犯罪所必須，也是抑制犯罪損害的必要手段。對此，本文僅提出以下幾點建言，作為各界參考：

一、防治重於查緝

將被告繩之以法，處以適當刑責，固然為傳統刑事司法之基礎原則。但是從本文前開章節說明可知，面對無所不在、無遠弗屆、無時無刻的網路犯罪，任何一國要以其內國刑事司法將行為人定罪，難度益愈升高。在AI技術一日千里，不斷進化的今天，我們恐怕不難想像未來的犯罪行為人，可能僅是一部電腦內的軟體，如好萊塢電影「機械公敵」（I, Robot）中的VIKI，是否能夠以傳統處罰自然人或法人的刑罰繩之，殊有疑問。尤為重要的是，在網路色情領域，如散播私密兒少照片等案件，損害及時防止更為重要。依衛福部統計，2020年違反「兒童及少年性剝削防制條例」的通報案件共1,696件，其中1,333件屬於拍攝兒童或少年性交或猥褻行為與物品，占全數犯罪型態近八成，與2017年581件相比已翻倍成長。其中在社群網站、通訊軟體等平臺查獲者多達1,239件，占犯罪工具的七成，可見數位科技的犯罪比例很高，邇來深偽技術的流

行，專家也憂心將會進一步衝擊青少年[68]。

準此，我們可以逐步仿照「網路內容防護機構iWIN（Institute of Watch Internet Network）」模式[69]，作為下架私密照片、深偽影音甚至防止線上盜版的手段。iWIN是依據兒童及少年權益保障法第46條授權，由「國家通訊傳播委員會」邀請各目的事業主管機關共同籌設，如衛生福利部、教育部、文化部、內政部警政署、經濟部工業局及商業司等共同籌設。依該條條文第1項規定：「為防止兒童及少年接觸有害其身心發展之網際網路內容，由通訊傳播主管機關召集各目的事業主管機關委託民間團體成立內容防護機構，並辦理下列事項：一、兒童及少年使用網際網路行為觀察。二、申訴機制之建立及執行。三、內容分級制度之推動及檢討。四、過濾軟體之建立及推動。五、兒童及少年上網安全教育宣導。六、推動網際網路平臺提供者建立自律機制。七、其他防護機制之建立及推動。」將通訊傳播機關列為召集機關，負主要防治責任，實屬正確。此外，亦賦予網路平臺業者，即提供連線上網後各項網際網路平臺服務，包含在網際網路上提供儲存空間，或利用網際網路建置網站提供資訊、加值服務及網頁連結服務等功能者（同條第4項），如：谷歌、臉書等業者自律

68 郭正芬、蔡容喬，深偽技術犯罪／素人也會換臉軟體變報復神器，聯合新聞網，2021年10月31日，https://udn.com/news/story/7321/5855633（最後瀏覽日：2021年10月31日）。

69 關於iWIN（網路防護內容機構）詳請參見官方網站https://i.win.org.tw/（最後瀏覽日：2021年12月2日）。

責任，該條第2項規定：「網際網路平臺提供者應依前項防護機制，訂定自律規範採取明確可行防護措施；未訂定自律規範者，應依相關公（協）會所定自律規範採取必要措施。」並且負有移除責任，同條第3項規定：「網際網路平臺提供者經目的事業主管機關告知網際網路內容有害兒童及少年身心健康或違反前項規定未採取明確可行防護措施者，應為限制兒童及少年接取、瀏覽之措施，或先行移除。」

此外，兒童及少年性剝削防制條例第8條亦規定：「網際網路平臺提供者、網際網路應用服務提供者及電信事業知悉或透過網路內容防護機構、其他機關、主管機，相關資料至少九十天，提供司法及警察機關調查。」此舉以先下架防堵，後移送偵查之「先行政，後司法」的模式控管，同時兼顧防堵侵害擴大及程序正義。同理，對於線上盜版案件，電信主管機關、電信業者，網際網路平臺提供業者以及權利人等，亦可考慮援用iWIN模式，或者前述德國之CUII模式，以共同治理，自律自清的方式，加強網路盜版之防治與查緝。

二、刑法謙抑性之維持

向來，對於侵害法益的行為是否皆應施以刑罰制裁？一直是個爭論不休的議題。相較於民事賠償、行政罰等，得以處自由刑甚或生命刑為對重要手段的刑事處罰，毋寧是對於人權侵害最大的方式。因此，發動刑罰要件應予嚴格限縮，而非作為第一線的防火牆，此即刑法之「最後手

段性」（ultima ratio）。承上所述，防治重於查緝網路犯罪的重要性日益升高，由犯罪預防及保護法益的角度而言，無論是域名扣押或者是停止解析域名，出發點仍不脫損害的及時防止與減少。誠然，「有權利必有救濟」（Ubi jus, ibi remedium）固然為法治國家建立司法制度的張本，然而，救濟途徑卻未必僅有刑事程序一途，刑罰之謙抑性在法治國原則下仍須兼顧。基於刑事程序的最終目的仍在於課以被告適切刑責，對人權的干預程度較大，發動門檻較民事、行政程序為高，仍應將之視為最後手段，庶幾無違比例原則。再者，刑事資源含括從司法警察機關、檢察機關至法院的各項人力、物力，耗費龐大，往往獲得最終之確定有罪判決曠日費時，對於瞬息萬變的網路犯罪防治，恐難發揮最好的功效。

也因此，為避免司法資源浪費，且為有效統合網路犯罪辦案資源，給予檢察官充分辦案能量支援，調和各處地檢署實務見解的分歧，臺灣高等檢察署遂於2021年12月間，成立「查緝資通犯罪督導中心」，鎖定電信詐欺等資通案件，建構大數據辦案模式，試圖針對域名濫用案件尋求辦案新途徑。該中心轄下並設有「聲請法院扣押域名並執行DNS RPZ（停止解析）」推動計畫，協助各地檢署及執法機關，藉由取得法院令狀的方式，交由TWNIC執行停止解析，停止臺灣使用者連上國外的犯罪網站，達到斷訊的效果。而就在2021年12月24日，針對非法播送串流影音的「安博盒子」機上盒，執法單位對非法影像來源的其中

56個網址，以取得法院扣押裁定，再交由TWNIC及ISP業者進行「停止解析」的方式，讓不法業者形同斷訊，高檢署推動扣押域名並停止解析的計畫收到成效[70]。

三、正視民事、行政手段在防治網路犯罪的重要性

從各國法制面及實務運作觀之，犯罪防治從來不是只有執法機關或司法機關的專屬業務，而是政府部門齊心同力的結果。正如同勞工監理有助於防範逃逸外勞，金融監理有助於防制洗錢，海關監理有助於非法物品入境，環境監理有助於防止污染物擴散，行政機關在犯罪防治上扮演曲突徙薪的預防角色，至關重要。同理，網路世界的監理，各國多半委諸電信通信主管機關，如我國的「國家通訊傳播委員會」（National Communication Committee），從通訊端開始截堵網路濫用情事發生，方為正辦。事實上，檢審機關的起訴、判決主要在於針對被告犯罪行為的評價，對於擴展迅速的網路犯罪，即時防治成效仍屬有限。網路安全的維護以及網路犯罪的防範，必須由多方利害關係人共同參與。因此，TWNIC與參與國內DNS RPZ的ISP業者，採取符合法律及正當程序的措施，共同為網路空間安全與打擊網路犯罪努力，係符合網路中介者的良善治理責任。不惟如此，從本文上開有關網站屏蔽命令章節所示，採行此一機制的國家，幾乎均使用民事或行政手

70 蕭博文，斷開與惡的連結　高檢署推動扣押域名首戰告捷，中央通訊社，2022年2月5日，https://www.cna.com.tw/news/asoc/202202050094.aspx（最後瀏覽日：2022年5月16日）。

段獲取法院命令，強制ISP業者阻斷相關網路域名，以迅速獲得成效，降低損害。預期在不久將來，面對更多的無法找到犯嫌的網路犯罪，以民事或行政手段進行截堵的機率將大為增加。

四、加強國際合作

最近，主管電腦犯罪及網路安全得美國司法部副部長Lisa O. Monaco[71]，於2021年10月20日，在美國華府以「進化中的網路威脅樣貌」（The Evolving Cyber Threat Landscape）[72]為題，發表開場演說闡明，近來網路威脅不僅是國家支持的攻擊者，也與犯罪集團結合在一起，透過勒索軟體攻擊美國相關基礎設施。面對網路威脅，副部長也指出未來三大努力方向：第一、評估如何提高調查、起訴和阻擾嫌犯及其不斷發展技術的能力；第二、在網路安全方面，需要專注於建立一個具有彈性的跨國性全球組織；第三、為追緝此類犯行的下一世代檢察官及調查官做好完善準備。此外，加密貨幣助長洗錢，並且與勒索軟體

71 2021年4月21日就任，由美國總統拜登提名，參議院表決通過，曾於歐巴馬政府時代擔任國土安全暨反恐顧問（Homeland Security and Counterterrorism Advisor 2013-2017），長期耕耘資訊安全及國家安全議題。

72 U.S. Department of Justice, Deputy Attorney General Lisa O. Monaco and Assistant Attorney General Kenneth A. Polite Jr. Deliver Opening Remarks at the Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape', JUSTICE NEWS, Oct. 20, 2021, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr (last visited: Oct. 23, 2021).

連結，將是近年來最具有威脅性的犯罪行為。是以，美國司法部於2020年10月也宣布成立「國家加密貨幣執法小組」（National Cryptocurrency Enforcement Team, NCET）[73]，以應對加密貨幣濫用相關犯罪的調查和起訴。NCET將結合司法部刑事司（Criminal Division）「洗錢暨資產追回科」（Money Laundering and Asset Recovery Section, MLARS）、「電腦犯罪和智慧財產科」（Computer Crime and Intellectual Property Section, CCIPS）。該團隊還將協助追踪及追回因欺詐和勒索而損失的資產，包括向勒索軟體集團所支付之支付加密貨幣。美國司法部指出，加密貨幣被用於各種犯罪活動，包括勒索軟體贖金支付、洗錢，以及非法銷售毒品、武器和惡意軟體。近期多起勒索軟體案件都涉及加密貨幣的付款要求，包括2021年5月針對美國最大燃料管線營運商Colonial Pipeline的攻擊，美國財政部更是在2021年9月首次對加密貨幣交易所發出制裁。

不僅如此，美國白宮在2021年10月13日主辦了一場對抗勒索軟體的線上會議，邀請全球逾30個國家共同參與，包括澳洲、巴西、加拿大、捷克、法國、德國、印度、以色列、義大利、日本、肯亞、墨西哥、紐西蘭、南韓、新

73 U.S. Department of Justice, Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team, JUSTICE NEWS, Oct. 20, 2021, https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team (last visited: Oct. 23, 2021).

加坡及英國等國家，不過，中國與俄羅斯並未參與。根據白宮估計，去年一整年全球所支付的勒索軟體贖金為4億美元，而今年第一季的贖金亦已達到8,100萬美元。於是美國召開了此次會議，打算結盟全球以對抗勒索軟體。美國已列出了4項對抗勒索軟體的作法，包括摧毀勒索軟體基礎架構及駭客、增強對勒索軟體的防禦能力、避免駭客透過加密貨幣來洗錢，以及利用國際合作來打擊勒索軟體的生態體系等[74]。

從以上分析可以得知，在布達佩斯公約架構下，歐洲各國或者其他國家的援引加入，使得網路犯罪查緝的司法互助更形便利。更值得我們注意的是，隨著網路犯罪的激增，電子證據儲存在不同的司法管轄區的情形日益增多。因此，自2017年起經過了近四年的磋商談判，歐洲理事會（Council of Europe, CoE）於2021年11月17日正式通過《布達佩斯網路犯罪公約第二附加議定書（the Second Additional Protocol to the Budapest Convention on Cybercrime），下稱「第二附加議定書」》，於2022年5月12日，在法國斯特拉斯堡的歐洲理事會，由各會員國正式簽署。「第二附加議定書」鑑於網路犯罪持續增加，而足以將這些罪犯定罪所需的證據，可能存在於國外、可移轉或未知地點的伺服器上，所以，「第二附加議定書」專

74 FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware, The White House, Oct. 13, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ (last visited: Oct. 15, 2021).

門設計用於幫助執法當局獲取電子證據，其新作法包括與服務提供商和註冊商直接合作，加快取得與犯罪活動相關的訂戶資訊和流量數據的手段[75]。

然而，以臺灣目前的外交處境，即便參與如國際刑警組職（Interpol）等情資分享機構已戛戛乎其難，若要成為布達佩斯公約或者類似公約的成員國，恐怕更具有難度。本文認為，限於我國目前處境，縱使無法參與國際公約進行司法互助，但仍可漸進以互惠方式，透過個案與請求國、被請求國逐步建立規模化的協議程序（protocol），甚可援引目前已被全球認可的布達佩斯公約模式作為基礎架構，以利與國際接軌。例如，在取證方面，我國業已獲准加入「24/7高科技犯罪網路」（G7 24/7 cybercrime Network）[76]。鑑於各國對保存電磁紀錄之時間均有限制，刑事司法互助又常需透過雙方中央主管機關，甚或外交途徑等正式官方管道傳遞訊息，而有較長程序，為確保我國向外國請求電子證據之刑事司法互助請求，不致因電磁紀錄逾保存期限而無法取得，檢察機關依具體個案情節審酌在向法務部提出刑事司法互助請求「之前」或「同時」，得透過刑事局「24/7高科技犯罪網路」聯繫窗口，請外國

75 Details of Treaty No.224, Council of Europe, 2022, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (last visited: May 15, 2022).

76 由7大工業國倡議組成，全球已有超過70個國家加入該網路，以即時保存各國境內之電磁紀錄不被刪除，我國目前由內政部警政署刑事警察局（下稱「刑事局」）擔任該網路聯絡窗口。

協助保存相關電磁紀錄，俾有效達成刑事司法互助請求之目的[77]。

五、網路治理的未來

行文至此，其實我們可以清楚明瞭，在網路時代，DNS是不可或缺的基礎設施。「掌握資訊，即掌握利益；掌握DNS，即掌握資訊」。自上世紀八十年代中期以來，域名系統一直是網際網路的重要組成部分。不過，美國在DNS領域向來居於主導地位，即便是數位發展極其蓬勃的歐洲，仍然需要透過美國協助，始能完善網路治理。為此，歐盟提出了屬於自己的替代方案，名為「DNS4EU」[78]。歐盟表示，DNS4EU將配備內置過濾功能，能夠阻止惡意網域的DNS名稱解析，例如託管惡意軟體、網路釣魚站點或其他威脅的網路安全的網域[79]。

此外，歐盟官員希望使用DNS4EU的過濾系統，根據法院命令阻止訪問其他類型的禁止內容，而DNS4EU系統還必須遵守所有數據處理相關法律，例如：GDPR，以確

77 參見法務部中華民國108年4月3日法外字第10806510520號函。

78 Equipping backbone networks with high-performance and secure DNS resolution infrastructures – Works, Jan. 12, 2022, European Commission, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works (last visited: Jan. 15, 2022).

79 Catalin Cimpanu, EU wants to build its own DNS infrastructure with built-in filtering capabilities, The Record, Jan. 19, 2022, https://therecord.media/eu-wants-to-build-its-own-dns-infrastructure-with-built-in-filtering-capabilities/ (last visited: May 4, 2022).

保在歐洲處理域名解析所得數據，禁止出售或營利。

陸、結　語

自烏俄戰爭於2022年3月間爆發以來，我們可以很清楚得知，掌握網路，就掌握了勝基。DNS已從全球網路基礎架構的一部分，轉身成為新世代的戰略武器。當烏俄戰爭初起，烏克蘭數位轉型部（Ministry of Digital Transformation）部長Mykhailo FEDOROVE隨即於2022年2月28日，提出正式請求，要求ICANN首席執行官Göran Marby對俄羅斯實施制裁，肇因普丁政權利用網路基礎設施宣傳其戰爭成果以及散播假訊息。具體而言，FEDOROVE部長要求ICANN撤銷俄羅斯所使用的域名“.ru”、“.pф”、“.su”和其他域名，關閉為俄羅斯服務的DNS根伺服器，並協助撤銷相關網域的TLS/SSL證書等舉動[80]，雖在現實上難以達成，但卻也喚起世人有關DNS濫用及網路治理的意識，進而研擬於戰爭時如何在網路世界中制裁侵略國[81]。

向來，域名濫用與不當內容之網路治理等相關內容，較少在法制面上予以著墨。然而，在網路迅速發展與普及

---

80 該聲請書內容詳請參見Mykhailo FEDOROV, Feb. 28, 2022, https://eump.org/media/2022/Goran-Marby.pdf (last visited: May 4, 2022).

81 Thomas Claburn, Ukraine invasion: We should consider internet sanctions, says ICANN ex-CEO, The Register, Mar. 10, 2022, https://www.theregister.com/2022/03/10/internet_russia_sanctions/ (last visited: Apr. 3, 2022).

使用的今日，域名濫用與不法行為息息相關，身處第一線的域名勢必應成為解決問題的出發點。但是，盱衡我國目前現況，如何由法制面授予執行，仍未見完備。觀諸臺灣目前對於網路空間之管理規範，目前僅有兒童及少年福利與權益保障法第46條與動物傳染病防治條例第38條之3，明文規範可對於網路不當內容進行移除或限制接取。然而，除此之外，目前並無通盤性的立法，得以處理域名濫用的問題。

對此，本文建議，從宏觀層面而言，首先應從「優化電信監理」著手，不應僅將網路犯罪視為刑事範疇，而應善用行政、民事手段。因此，在2022年6月29日，NCC通過「數位中介服務法」草案，希望透過多方協力參與網路治理，保障數位基本人權、促進資訊自由流通，建立自由、安全及可信賴的數位環境，將原「數位通訊傳播服務法」草案名稱修正為「數位中介服務法」，以突顯該草案係以提供數位中介服務者為規範對象，並參考歐盟數位服務法（DSA）草案等國際相關法制規範，衡諸我國國情而訂定，以數位中介服務提供者為規範對象，包括連線服務、快速存取服務及資訊儲存服務（包含線上平臺及指定線上平臺），並依其服務型態、規模等課予不同義務，以促進服務提供者之問責及資訊透明，並介接政府各部會之實體作用法，強化違法內容之處理[82]，此一立法方向堪屬

[82] NCC公布「數位中介服務法」草案，以網路治理精神共同建構自由、安全、可信賴之網路環境，國家通訊傳播委員會，2022年6月29

正確。其次，從個別爭議領域，如：智慧財產權侵害，得以援用德國CUII模式，權利人、ISP業者及政府監理機關共同治理的模式，無需藉由法院令狀及得以屏蔽侵權網站，不但得以迅速減少損害擴大，亦可妥善維護網路中立性，達到有效衡平的網路治理。

日，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=47684（最後瀏覽日：2022年8月9日）。

參考文獻

一、中文部分

- TWNIC（2021）。成立宗旨。https://twnic.tw/about.php
- 王宏舜（2021）。資通犯罪猖獗　高檢署點出這6大特性讓查緝變艱鉅。聯合新聞網。https://udn.com/news/story/7321/5977416
- 行政院資通安全處（2021）。109年國家資通安全情勢報告。https://nicst.ey.gov.tw/Page/7AB45EB4470FE0B9/7234b46b-fe52-4295-8bae-41d9ea36d447
- 何毓庭（2021）。黑人看盜播奧運掀波　安博老董交保。聯合報。https://udn.com/news/story/7321/5804227
- 周子馨（2021）。南韓N號房主嫌終審定讞！至少關34年、公開個資10年。TVBS新聞網。https://tw.news.yahoo.com/%E5%8D%97%E9%9F%93n%E8%99%9F%E6%88%BF%E4%B8%BB%E5%AB%8C%E7%B5%82%E5%AF%A9%E5%AE%9A%E8%AE%9E-%E8%87%B3%E5%B0%91%E9%97%9C34%E5%B9%B4-%E5%85%AC%E9%96%8B%E5%80%8B%E8%B3%8710%E5%B9%B4-055734593.html
- 林郁萍（2021）。號稱亞洲最大成人平台SWAG被抄　負責人夫妻檔等5人遭送辦。中時新聞網。https://www.chinatimes.com/realtimenews/20210402004244-260402?chdtv
- 國家通訊傳播委員會（2022）。NCC公布「數位中介服務法」草案，以網路治理精神共同建構自由、安全、可信賴之網路環境。國家通訊傳播委員會。https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=47684
- 許伯崧、董容慈（2021）。網紅小玉DeepFake換臉謎片YouTube官方宣布：無限期停止營利資格。公視新聞網。

https://news.pts.org.tw/article/552248
- 郭正芬、蔡容喬（2021）。深偽技術犯罪／素人也會換臉軟體變報復神器，聯合新聞網。https://udn.com/news/story/7321/5855633
- 陳昱奉（2014）。數位時代之犯罪偵查與網路自由及隱私權之保障——從網域名稱（Domain Name）之扣押、沒收談起。臺灣嘉義地方檢察署研究報告。https://www.cyc.moj.gov.tw/media/136016/551410383574.pdf
- 陳昱奉（2019）。跨境電腦犯罪偵辦之未來走向——從「電腦犯罪公約（Convention on Cybercrime）」暨「In Our Sites行動」出發。*台灣國際法學刊，15*（2），95-105。
- 黃勝雄（2020）。DNS RPZ摘要說明。TWNIC。https://blog.twnic.tw/2020/09/23/15311/
- 愛范兒（2016）。全球網路的新「波瀾」：美國正式交出域名管理權。數位時代。https://www.bnext.com.tw/article/41205/icann-domain
- 楊又肇（2021）。曾被盜版污名化的BitTorrent網路傳輸技術，如今邁入20週年。Mashdigi。https://mashdigi.com/bittorrent-turns-into-20-anniversary/
- 蕭博文（2022）。斷開與惡的連結　高檢署推動扣押域名首戰告捷。中央通訊社。https://www.cna.com.tw/news/asoc/202202050094.aspx
- 蘇文彬（2020）。刑事局破獲盜版影音網站楓林網，每月獲利估至少400萬元。iThome。https://www.ithome.com.tw/news/136848

二、英文部分

- 2020 Internet Crime Report (2020). https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- About PIR (2021). the new. https://thenew.org/org-people/about-pir/

➢Beginner's Guide to INTERNET PROTOCOL (IP) ADDRESSES. ICANN (2011). https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf
➢Building the Information Society: a global challenge in the new Millennium, Declaration of Principles (2003). World Summit of the Information Society 2003. https://www.itu.int/net/wsis/docs/geneva/official/dop.html
➢Bundesnetzagentur (Federal Network Agency) (2022). Federal Ministry for Economic Affairs and Climate Action, https://www.bmwk.de/Redaktion/EN/Artikel/Ministry/bundesnetzagentur-bnetza.html
➢Catalin Cimpanu (2022). EU wants to build its own DNS infrastructure with built-in filtering capabilities. The Record. https://therecord.media/eu-wants-to-build-its-own-dns-infrastructure-with-built-in-filtering-capabilities/
➢CERN (2019). A Short History of the Web. https://home.cern/science/computing/birth-web/short-history-web
➢Claburn, Thomas (2022). Ukraine invasion: We should consider internet sanctions, says ICANN ex-CEO, The Register. https://www.theregister.com/2022/03/10/internet_russia_sanctions/
➢Clearingstelle Urheberrecht im Internet veranlasst Sperrung einer Streaming-Website (2021). Bundesnetzagentur. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2021/20210311_Clearingstelle.html
➢Conrad, David (2020). DNSSEC: Securing the DNS. ICANN Office of the Chief Technology Officer (OCTO). https://www.icann.org/en/system/files/files/octo-006-24jul20-en.pdf
➢Convention on Cybercrime (2001). Budapest. https://rm.coe.int/

1680081561

- Cory, Nigel (2016). How Website Blocking Is Curbing Digital Piracy Without "Breaking the Internet". Information Technology & Innovation Foundation (ITIF). https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy- online
- Cory, Nigel (2018). The Normalization of Website Blocking around the World in the Fight against Piracy Online. Information Technology & Innovation Foundation (ITIF). https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online
- Cory, Nigel (2022). A Decade After SOPA/PIPA, It's Time to Revisit Website Blocking. *Itif, Jan. 2022*, 22-28.
- Details of Treaty No.224 (2022). Council of Europe. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224
- Equipping backbone networks with high-performance and secure DNS resolution infrastructures – Works (2022). European Commission. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works
- FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware (2021). The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/
- FEDERAL BUREAU OF INVESTIGATION, Internet Crime Complaint Center IC3 (2021). IC3 Mission Statement, https://www.ic3.gov/Home/About
- FEDOROV, Mykhailo (2022). https://eump.org/media/2022/Goran-Marby.pdf

➢History & Milestones (2019). GoDaddy. https://aboutus.godaddy.net/newsroom/history-and-milestones/default.aspx
➢How the Domain Name System (DNS) Works (2021). VERISIGN. https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml
➢Jackson, Mark (2021). Six Big UK ISPs Ordered to Block Five Piracy Streaming Websites. https://www.ispreview.co.uk/index.php/2021/10/six-big-uk-isps-ordered-to-block-five-piracy-streaming-websites.html
➢Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices (2018). DEPARTMENT OF JUSTICE. https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected
➢Linsay, David (2017). Website Blocking Injunctions to Prevent Copyright Infringements: Proportionality and Effectiveness. *UNSW Law Journal, 40*(4), 1507-1538.
➢Maxwell, Andy (2022). US Court Orders Every ISP in the United States to Block Illegal Streaming Sites. Torrentfreak. https://torrentfreak.com/us-court-orders-every-isp-in-the-united-states-to-block-illegal-streaming-sites-220502/
➢Morgan, Steve (2020). The 2020 Data Attack Surface Report. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/ArcserveDataReport2020.pdf
➢Piscitallo, Dave (2012). Thought Paper on Domain Name Takedowns. ICANN Blog. https://www.icann.org/en/blogs/details/thought-paper-on-domain-seizures-and-takedowns-8-3-2012-en
➢Piscitallo, Dave (2012). Guidance for Preparing Domain Name

Orders, Seizures and Takedowns. ICANN Security Team. https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf

- Review of the Copyright Online Infringement Amendment (2018). Department of Infrastructure, Transport, Regional Development and Communication. https://www.infrastructure.gov.au/have-your-say/review-copyright-online-infringement-amendment
- Styler, Joe (2022). The top 25 most expensive domain names GoDaddy. https://www.godaddy.com/garage/the-top-20-most-expensive-domain-names/
- Tang, Lianne (2018). Federal Court Orders ISPs to Block Pirate Sites in Australia. LEGALVISION. https://legalvision.com.au/sinking-ship-federal-court-orders-isps-to-block-pirate-sites-in-australia/ (last visited: Dec. 22, 2021).
- THE UNITED STATES DEPARTMENT of JUSTICE (2021). Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside, Department of Justice. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside
- U.S. Department of Justice (2021). Deputy Attorney General Lisa O. Monaco and Assistant Attorney General Kenneth A. Polite Jr. Deliver Opening Remarks at the Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape'. JUSTICE NEWS. https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr
- U.S. Department of Justice (2021). Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team. JUSTICE NEWS. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-

team
- Van der Sar, Ernesto (2018). Pirate Site Blockades Enter Germany With Kinox.to as First Target. Torrentfreak. https://torrentfreak.com/pirate-site-blockades-enter-germany-with-kinox-to-as-first-target-180213/
- Van der Sar, Ernesto (2019). Federal Court Approves First 'Pirate' Site Blockade in Canada. Torrentfreak. https://torrentfreak.com/federal-court-approves-first-pirate-site-blockade-in-canada-191118/
- Van der Sar, Ernesto (2022). Canada's Supreme Court Denies TekSavvy's Site Blocking Appeal. Torrentfreak. https://torrentfreak.com/canadas-supreme-court-denies-teksavvys-site-blocking-appeal-220329/
- Welcome to ICANN! (2012). https://www.icann.org/resources/pages/welcome-2012-02-25-en
- WeLeakInfo.com Domain Name Seized (2020). Department of Justice. https://www.justice.gov/usao-dc/pr/weleakinfocom-domain-name-seized
- What Does Verisign Do? (n.d.). VERISIGN. https://www.verisign.com/en_US/company-information/index.xhtml
- Whigham, Nick (2018). 'Shamelessly facilitating crime': Rights holders hit out at Google amid renewed Aussie piracy fight. news.com.au. https://www.news.com.au/technology/online/piracy/shamelessly-facilitating-crime-rights-holders-hit-out-at-google-amid-renewed-aussie-piracy-fight/news-story/7cf2b0b441a91c55484bf38c874aa222
- Who we are (n.d.). Acma. https://www.acma.gov.au/who-we-are
- William Largent (2018). New VPNFilter malware targets at least 500K networking devices worldwide. TALOS CISCO. https://blog.talosintelligence.com/2018/05/VPNFilter.html