網路治理的機會與挑戰

財團法人台灣網路資訊中心　著

目 次

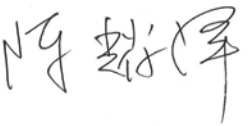
推薦序一

資訊科技日新月異的新世代，推動數位發展是國家的重要戰略議題。行政院於 2020 年從資料治理、智慧加值、萬物互聯、資安防護與數位匯流等五大面向加速推動數位發展，期許臺灣能從數位追隨者成為先行者。

因此，臺灣通往數位轉型的路上，網際網路治理（Internet governance）的議題更顯重要。《網路治理的機會與挑戰》一書，提供我們前瞻性的視野，從最原始的網路本質的認識出發，探討網路管理、治理概念，更延伸至資訊安全與政策發展、網路資源的充分利用、網路安全與管理基礎設施等具體議題。本書要旨與精神，充分與臺灣積極推動的數位轉型，以及臺灣科技發展整體性規劃密切相關，展現出網路治理多元的可能性。

近期，區塊鏈、元宇宙等網路應用的盛行與實現，為人們描繪甚至建構出一種前所未有的社會形態。但看似前程似錦的未來，背後可能是更複雜的挑戰。數位科技的進步，使我們生活更快速便捷，可是連帶衍生的問題，同樣也是我們必須面對的風險。在新的時代，有新的數位議題，以及新的挑戰，期待透過《網路治理的機會與挑戰》的出版，開啟多方協力合作，公民參與，甚至國際合作交流的契機，讓我們一同「創造機會，迎接挑戰」。

國家通訊傳播委員會

主任委員 

推薦序二

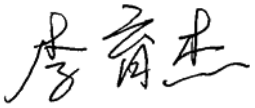
伴隨著快速的 5G 佈建與更先進的資訊技術的推進，全球已跨入網路世界的下個維度，尤其在域名系統、網路位址政策及網路安全等關鍵議題有了更廣泛、更深入的討論。

臺灣一直以來都是亞太地區技術與產業的關鍵要角，整體網際網路的發展走向，不但牽涉安全穩定的網路使用環境建構，也顯現與全球網路議題相互接軌、展現相當重要的網際網路治理精神。

財團法人台灣網路資訊中心出版《網路治理的機會與挑戰》，正是在「資訊安全」、「網路政策」、「網路技術」等領域，提供最新的發展趨勢介紹及議題探研，也兼及了重要的網路趨勢議題。

維護網路言論自由、促進資訊自由流通不僅是網際網路治理的原則，也是關鍵使命。隨著人工智慧（AI）、大數據分析、雲端運算、物聯網（IoT）、5G 行動通訊等數位科技的發展，產業格局、社會運作都有了創新開展的面貌，對於政府而言，數位治理的擘析與規劃，不僅象徵國家運作效能的優化，也能創造公共價值的應用實踐；如何建立在自由與可信賴間取得平衡的網路環境，在便利地使用之餘，也能達致公平性、透明性、可課責性與包容性，都將是未來的機會，也是挑戰，需要大家的集思廣益與團結合作，也期待本書能夠帶來更多經驗交流與互動，共同建構臺灣韌性安全的數位環境。

財團法人台灣網路資訊中心

董事長 

推薦序三

全球網際網路的使用量遽增，如何建構更安全穩定的網路使用環境，成為資訊及數位科技領域不容忽視的重要課題。

財團法人台灣網路資訊中心（TWNIC）長年來積極促進、協調並推動臺灣與國際網際網路組織之間交流與合作，推展網際網路應用之普及及協調資訊服務之整合、交換，除了相關議題的研討會議活動外，2020、2021 年分別出版《網路治理與資訊安全》、《新世代的網路治理》電子書，彙整當前關於「資訊安全」、「網路政策」、「網路技術」與「趨勢議題」的討論成果；2022 年延續討論的主題與成果，出版《網路治理的機會與挑戰》，除了以饗讀者，也是網路技術研究、產業發展等相關領域相互交流分享、提供管理機制建議的平臺。

近年來 DNS 濫用嚴重，本書內容從網路本質與基本架構，到 DN、IP 以及網路安全的應用等三大面向，探討現今網際網路治理議題中，包含 DNS（Domain Name System）、RPKI（Resource Public Key Infrastructure）、以及未來即將開放的 New gTLD（新通用頂級域名）等重要關鍵，都有所涉及。另一方面，論全球域名系統、網路位址政策及網路安全的深度討論，以及結合重要時事的分析與探討，也是《網路治理的機會與挑戰》的一大特點，更好、更安全的臺灣網路發展，有賴多方的協作、全民參與和政府的擘劃與支持。

TWNIC 是臺灣網路關鍵基礎設施的營運者，推動數位轉型與持續提供對網路環境有益的服務是恆久不變的承諾，也期待您的加入，讓這個生態系的討論能夠更加成長、茁壯！

財團法人台灣網路資訊中心

董事暨執行長 黃勝雄

資訊安全

公共網際網路 vs.非公共網際網路

APNIC 文摘

https://blog.twnic.tw/2021/02/09/16821/

本 APNIC 文摘原標題為 Public Internet vs Non-public Internet，由 Azhar Khuwaja 撰文。

以雲端為主的基幹網路數量持續增加，技術亦不停發展，更能配合各種不同的服務應用。雖然此應用因觀點不同難以具體評估數量，但無論從地區覆蓋率、網路連接點（point of presence，POP）數量、部署光纖長度，到頻寬可承載的位元數，都可看出以雲端作為網路基幹越來越普遍。

在作者去年〈是否應改變在雲端時代推廣 IPv6 的手法了？〉（Opinion: Do we need to change the way we promote IPv6 in the cloud era?）的文章中，他曾指出雲端的普及已經徹底改變企業自架網路基礎建設的需求，也因此，即使地區網路註冊管理機構（Regional Internet Registries，RIR）向這些企業組織強烈推銷 IPv6，他們也難以感受到 IPv6 的必要。

眼看雲端為主的骨幹網路越來越普及、雲端為本的基礎建設和虛擬資源都以驚人速度成長，更不用說許多企業直接利用雲端作為資料中心，作者希望進一步探討雲端興起對網際網路管理的影響，同時他也質疑，RIR 對網際網路基礎建設的如此改變是否做好準備，他們又如何看待自身責任逐漸限縮的未來？

作者表示，他一直相信網際網路只有一個。但他認為，雲端時代出現了二種不同的網際網路：公共網際網路（public Internet）和非公共的網際網路（non-public Internet）。作者解釋，非公共不一定

代表「私人」；一般而言，大眾還是能透過網際網路使用大部分雲端資源。他指出，「非公共」的用語是用來區別雲端業者自認「更安全、效能更好」的全球網路，以及大家熟悉的網際網路。

作者本身即為雲端工程師，比一般人更了解雲端業者如何費盡心力讓提供的網路服務更快、更有效，也更安全。畢竟雲端服務不像僅此一家的公共網際網路，必須無時無刻面對眾多競爭者。

但是，無論是哪家雲端業者，都只想把客戶的 IP 訊務留在自己經營的全球網路（也就是自家雲端）。雲端網路賦予企業使用者更多控制權、也可自由利用更客製化的量測標的，確認網路的效能和安全。以這個面向而言，作者承認雲端網路的確優於公共網路。他比喻，雲端網路的設計像是業者依自身需求，將最有利於自家網路的協定和擴充程式組裝而成，換句話說，就是網際網路的「科學怪人」（a Frankenstein of protocols and extensions）。

作者認為，我們正迎來「專屬軟體網際網路」的時代，各家雲端業者將持續各自經營、管理自家的全球網路。隨著非公共網路成為主流，所謂的「公共網際網路」很可能因此退至邊緣（如「最後一哩」或「最初一哩」），用途僅剩下連接使用者和雲端業者提供的網路。

那麼，RIR 對這個發展又有什麼因應計畫？作者認為，諸如發配 IP 位址、推動 IPv6、指派自治系統號碼、推廣路由最佳化及最佳安全作法，以及各種培力宣導計畫等，都是 RIR 過去做得很好、未來也應持續努力的項目。

然而，由於雲端業者不一定會公開自家骨幹網路分配、使用 IP 位址的規畫，RIR 最重大的責任之一，即時更新 WHOIS 資訊，很可能因而難以達成。屆時，RIR 的重要性或將持續削弱，作者也鼓勵讀者一同持續關注二種網路未來的勢力消長。

從 BGP 觀察網際網路連線發展：2020 年回顧

APNIC 文摘

https://blog.twnic.tw/2021/02/01/16744/

APNIC 首席科學家 Geoff Huston 每年年底都會回顧當年度邊界閘道器協定（Border Gateway Protocol，BGP）量測結果，透過這些數據，一窺網際網路連線的行為和結構變化。Geoff 今年亦依慣例撰文，回顧 2020 年的 BGP 量測資料，並分享他的觀察結果。

BGP 是利用 Bellman-Ford 單起點最短路徑演算法建立的協定。透過這個演算法，網路中的裝置（BGP Speaker）得以透過互連裝置了解所在網路的拓樸結構。簡單來說，任何裝置若得到關於當地網路的新資訊，都會立即告知鄰居裝置。就像八卦一樣，透過口耳相傳，一瞬間「祕密」就變成「新聞」。

BGP 基本上就依此原理運作：任一裝置只要從鄰居裝置得知新的 IP 位址前綴連線資訊，就會跟自身擁有的資訊比較；若發現新資訊提供的路徑比較好，就會在更改路徑的同時，一併通知所有鄰居裝置新路徑的資訊。相反的，若發現某條路徑已無法使用，也會通知所有鄰居將「撤銷」該路徑。

在 BGP 量測中，最重要的量測目標是每個路由的路由空間大小及更新層級，也可稱為變異量（churn）。而要量測這個變異量，最理想的方式是保有一個非常穩定的本地資料儲存環境。必須確保此環境不受當地網路影響，蒐集到的資料才能忠實反映外部大環境的變化。

本文使用的量測標的，是設定於自治系統 AS131072 中的 BGP

裝置。這個自治系統不會生成訊務，也不會從 BGP 產生路由。這個裝置接受的 eBGP 饋送包括來自位於 ANPIC 澳洲網路的 AS4608，以及 APNIC 日本網路的 AS4777。

以下分別簡述 2020 年 IPv4 及 IPv6 的 BGP 觀測重點。

觀測發現，IPv4 的 BGP 網路在 2020 年的成長穩定趨緩。Geoff 分析，呈現此趨勢的原因有四：

一是許多網際網路市場已趨近飽和，「開墾」等級的擴張自然比 10 年前更少見。

再者，網路相關服務市場也非常密集，無論是終端使用者或發布端，需要利用位址的內容和服務都越來越多。然而服務和顧客數量持續成長，並不代表需要用到的位址或路由表項目會更多。

第三，網路服務市場的密集與網路連線市場整併相輔相成，尤其以行動網路市場最明顯：競爭者數量日益減少，單一業者的規模則日益擴大。因為市場主要參與者數量減少，共享位址等解決方案的應用也更容易。

最後無法忽視的，是 IPv6 部署率持續成長。IPv4 位址持有數前 10 名的經濟體中，就有 6 個經濟體也在 IPv6 位址持有數中排前 10 名，分別是美國、中國、日本、德國、巴西和英國，這些國家總計持有 62%（已通告）IPv6 位址，以及 69%（已通告）IPv4 位址，可期待這 6 個經濟體持續帶動 IPv6 部署成長。

在 IPv6 方面，觀測結果發現 IPv6 的位址分配長度和公告位址的前綴長度缺乏明顯關聯性，而且很多持有人不會在單次路由通告中就附上完整的 IPv6 位址前綴。不只如此，通告中的 IPv6 位址前綴長度非常不統一，從/48、/32、/44、/40 到/29 的長度都算常見。

一般認為這種情形導因於使用者透過指定路由來操縱、分配訊務，但 Geoff 認為以目前 IPv6 訊務量仍遠低於 IPv4 訊務的情況，難以將此視為唯一理由。他推測，使用特定前綴以迴避、反制路由

劫持也可能是另一個原因。

Geoff 也在文中預測未來 BGP 發展。首先，雖然依過去資料或可預期 IPv4 訊務將持續成長，但 IPv4 位址自 10 年前就已逐漸枯竭，未來究竟還有多少成長空間？答案恐怕難以樂觀。

Geoff 也提醒，目前網際網路上雖然慣用雙協定技術以兼容 IPv4 和 IPv6，但雙協定只是手段，終極目標仍是轉換成完全只使用 IPv6 的網際網路。雙協定的設定，是合理情境下一定優先使用 IPv6；如此一來，未來一旦迎來 IPv6 數量正式超過 IPv4 的臨界點，整個網際網路就會在短時間內汰換轉成全面使用 IPv6。20 年前，大家以為這個未來會在 5 年內出現，而 20 年後的現在，人們依舊期待 5 年內會看到轉變。

這也顯示，網際網路的發展實在難以預測。即使 IPv4 耗盡的現實已長達 10 年，人們仍無法捨棄 IPv4，甚至發展各種手段技術繼續使用 IPv4。即使 IPv6 在過去幾年內有顯著成長，至 2020 年結束為止，我們使用的仍是以 IPv4 為主的網際網路。

BGP 攻擊將構成企業嚴重的營運風險

國際瞭望 撰輯

https://blog.twnic.tw/2021/02/08/16983/

網路安全團隊往往將目光放在關注新興網路安全風險而忽略既有風險，例如本文的主題：邊界閘道協定（Border Gateway Protocol ，BGP）。

BGP 是當代網路的支柱，將全球數百萬個網路（亦稱為自治系統或 AS）連成網際網路。若 BGP 受攻擊或停止運作時，可能招致嚴重後果，網路會陷入中斷或癱瘓，並因此使大型網路服務供應商（Internet Service Provider，ISP）乃至於國家無法使用網路，影響數百萬家企業及用戶。

相關案例是網路服務供應商 Verizon 在 2019 年 6 月時，因路由器系統資訊外洩，導致大量流量被導向某位客戶。因為 BGP 的設計是偏好「最佳路徑」的路由，一旦某個端點告知其上游將利用另一條路徑到達目的地，而這資訊剛好出錯時，原本的訊務可能就會被轉向。Cloudflare 的 Tom Strickx 將這個情況比喻為：導航系統突然將整個高速公路的流量引導到一條安靜的住宅街道上。

BGP 也很容易受到操弄與攻擊，當代亦有許多國家利用 BGP「封網」的案例。有心人士還可使用 BGP 劫持網路訊務，例如 2017 年多個大型網站如 Google、Apple、Facebook 及直播平臺 Twitch 的訊務突然被轉至俄國網路，以及 2018 年數百萬個 Google IP 位址訊務被轉到中國電信。

企業的數位化轉型，使其更加依賴服務供應商的雲端系統及軟體，也因此，一旦遇到這種針對網路基礎建設的攻擊，將更難以防

備。本文建議企業應評估其網路服務供應商、雲端託管及內容傳遞網路（Content Delivery Network，CDN）都有遵守 BGP 管理最佳做法，其中一個確保 BGP 安全的最佳做法就是網路營運商之路由安全相互協議規範（Mutually Agreed Norms for Routing Security，MANRS），並要求 ISP 過濾 BGP。

此外，網站 isbgpsafeyet.com 及資源公鑰基礎建設（Resource Public Key Infrastructure，RPKI）等服務，亦可幫助企業評估 BGP 安全性。

參考資料：

https://www.forbes.com/sites/forbestechcouncil/2021/01/11/bgp-attacks-pose-a-substantial-operation-riskare-enterprises-paying-attention/?sh=1ba3332d45ba

零信任的起源及重要性

APNIC 文摘

https://blog.twnic.tw/2021/05/17/18519/

本 APNIC 文摘原標題為 Where does zero trust begin and why is it important?，由 Kathleen Moriarty 撰文。

零信任（zero trust）是資訊安全架構的重要轉變：我們從過去由外而內的縱深防禦（defence-in-depth）模型，逐漸轉向以資料為中心的分層控管模式。

零信任的概念，由研究機構 Forrester Research 前副總裁 John Kindervag 提出，重點是將應用分層獨立，防止被攻擊者逐步擊破。隨著時間演進，此概念的內涵益發詳盡複雜，應用也更廣泛。

本文作者為網際網路安全中心（Center for Internet Security）技術長，過去亦曾擔任網際網路工程任務組（Internet Engineering Task Force，IETF）安全領域主席。眼見零信任已成為網路安全的未來趨勢，特撰此文介紹零信任的基本概念及應用實例，為對零信任尚一知半解的網路安全從業人員們指點迷津。

作者首先介紹零信任的基本架構。此架構的重點在於疊列中的每一層都不信任其他層（無論是軟體或硬體）的元件，換句話說，每個元件都預設其他相連或需要的元件可能有危險。因此，每一層的所有元件都必須通過驗證，也必須有能力偵測到攻擊，無論此攻擊的成敗。

這也是為什麼此概念稱為「零信任」模型。因為元件之間毫無信任，所有動作都必須在驗證對方的安全性質及身分後才能執行。這個架構的原則是「絕不信任，永遠驗證」。

零信任的核心宗旨包括：身分、驗證、授權、存取管控及加密。在零信任架構中，上述要素必須經過反覆確認，整個過程保持刻意及高機動性。雖然目前大部分相關討論仍聚焦於網路架構中的零信任，但過去幾年來，無論在關鍵基礎建設、裝置韌體、軟體或資料領域，零信任概念的應用也越來越常見。

零信任應用逐漸普遍的實例之一，是由美國航太公司洛克希德．馬丁（Lockheed Martin）提出的網路擊殺鏈（Cyber Kill Chain）。這個和零信任約莫同期提出的概念，重點在於將攻擊分成不同階段，並根據每個階段制定相應的偵測及防治策略。

網路擊殺鏈的發想背景，是為了應付越來越成熟、甚至演變至包含供應鏈攻擊的進階持續性滲透攻擊（advanced persistent threat attack，APT）。透過在每個攻擊階段實施防衛及管控措施，加上動態的身分認證機制，可以更有效地偵測並防範來自敵人的側面或權限提升攻擊。

在應用程式及功能中的每個層級都設置偵測及防範技能，同時啟動動態存取權限控管機制，要求任何可疑元件經過驗證，其實便是零信任核心宗旨的實踐，也是擊殺鏈有效的原因。

從僅限於網路架構、形容應用分層的定義開始，零信任的概念如今已被廣泛運用於各層面。此概念的核心宗旨，以動態驗證機制確認每個元件的安全性，不僅能及早偵測異常事件，更能有效防止單一漏洞引發連鎖性的擴大傷害。另一方面，零信任架構和擊殺鏈的異曲同工之妙，也再度證實此模型的價值。如前所述，零信任的概念不僅可應用於網路基礎架構，在接觸使用者的終端服務也有其功效。作者更期許零信任架構未來逐步發揚光大，打造以資料為基礎的網路安全架構。

DNSSEC 簽署金鑰更新儀式

APNIC 文摘

https://blog.twnic.tw/2021/11/16/20734/

本 APNIC 文摘原標題為 DNSSEC KSK Ceremony 43，由 Cameron Steel 撰文。

2021 年即將邁入尾聲，這也代表又到了 DNS 界鮮為人知但舉足輕重的季度盛事——域名系統安全擴充（Domain Name System Security Extentions，DNSSEC）簽署金鑰（Key Signing Key，KSK）汰換儀式的舉辦時間。這是第 43 次 KSK 儀式，已於今（2021）年 10 月 14 日（美國時間）於美國維吉尼亞順利落幕。

作者自承是此儀式的熱心粉絲，每次儀式都會全程觀看直播，過去也寫過長文介紹何謂 DNSSEC 簽署金鑰汰換儀式，以下是簡短版本的介紹：

大眾熟知的域名（如 google.com、twitter.com 等）都是透過域名系統（DNS）發配並保存紀錄。DNS 的架構由樹狀階層的伺服器所組成，每個伺服器都有自己負責的區（zone）。簡單來說，一個區就是特定前綴（suffix）下的所有域名清單。以 google.com.au 為例，這個域名中就是在.au 區下的 com.au 區下的 google.com.au 區。

在各種區中，最重要的就是根區（root zone）。根區在 DNS 階層的最頂端，含有所有頂級域名（top-level domain，TLD）的資訊。網際網路發明初期，由於使用人數不多、技術等級不足等種種原因，並未特別重視 DNS 訊務的隱私和安全。所有 DNS 查詢都是公開的，這也代表任何人都可以輕而易舉地竊聽或從中攔截、調包 DNS 查詢內容。實例而言，使用者欲前往 Google 而送出 DNS 查詢

後，有心人士可從中攔截、並調包傳回使用者電腦的回應封包，藉此將使用者帶到完全不同的網站。

隨著時間演進，也出現許多新的加密協定用來保護 DNS 訊務安全，如傳輸層安全協定（Transport Layer Security，TLS）。但如果希望從根本確保 DNS 資料正確，就需要 DNSSEC。DNSSEC 建立從域名到根區的驗證鏈，透過每層驗證確保 DNS 資料的正確性。任何驗證鏈都需要一個最終定錨，而在 DNSSEC 中，這個定錨就是根區的簽署金鑰（Root Key Signing Key，Root KSK）。

根區 KSK 作為 DNSSEC 驗證的定錨，自當加倍安全及透明的對待，才能確保網際網路社群的信任。每季舉辦的儀式就是此透明度的重要一環，唯有在此儀式中，受指派的特別代表才有權存取根區 KSK，並重新生成未來 3 個月 DNSSEC 使用的數位簽章。

第 40 屆 KSK 金鑰汰換儀式於 2020 年 2 月舉行，也是 COVID-19 全球疫情爆發前的最後一場實體儀式。儀式當天發生了眾人皆未料想到的意外——在儀式前的例行檢查中，相關人員發現「保險庫的保全機制運作不良」，導致他們「無法接觸存有重要儀式元件的保險箱」。白話來說，就是他們被鎖在自己管的保險庫外面了。

這個保險庫的保全機制顯然真正固若金湯，因為儀式整整延遲了三天才再度舉行，也因為嚴重延期，原訂的硬體安全模組（Hardware Security Module，HSM）HSM3 銷毀作業都延至第 42 屆儀式舉行。

依慣例，每次 KSK 金鑰汰換儀式需邀請指定社群代表到場見證。然而，COVID-19 疫情下，無法再請這些來自全球各地的社群代表都飛到美國，並擠進一個小房間見證儀式。也因此，第 41 及 42 屆儀式都大幅調整形式，盡力確保所有參與人員的健康安全。

最主要的形式調整包括：除必要人員外，其他人員都以遠端形式參與；過去儀式皆於加州、維吉尼亞州輪流舉行，但自 40 屆開

始儀式都僅於加州舉辦；第 41 屆儀式更一次生成了可以用 9 個月的數位簽章，以降低儀式舉行的頻率。

那個因為保險庫打不開而來不及銷毀的 HSM3，現在也還留在加州場館中等待銷毀。但第 43 屆儀式仍不會展開銷毀作業——因隨著疫情趨緩，這次儀式即將回歸至維吉尼亞州舉行。

這次是 2019 年 11 月後，KSK 金鑰汰換儀式總算再次於維吉尼亞州的場館舉行。為避免再次發生保險庫打不開的意外插曲，維吉尼亞場館今年 6 月就已經先打開保險庫改過密碼，所幸正式儀式當天，也沒有任何意外發生。

第 43 屆儀式比起前二屆，也更類似過去的形式。本屆儀式僅生成 3 個月份量的數位簽章，也會有三位加密負責人（Crypto Officer）在場執行儀式。其他見證人，包括 Verisign 代表、外部稽核代表，以及第四位作為備案人選的加密負責人，都仍以遠端方式出席。第四位備案加密負責人持有的保險箱鑰匙，也在儀式前以防竄改封裝包裹寄到現場。

除了例行的簽章生成作業外，第 43 屆儀式還啟用了新的 HSM（HSM6E）。除了參考 IANA 對儀式說明的網站外，作者身為此儀式的資深粉絲，這次也透過推特實況轉播。若有興趣，亦可觀賞 YouTube 直播影片紀錄。

俄羅斯通過新法，可能封鎖國外社群媒體網站

國際瞭望 撰輯

https://blog.twnic.tw/2021/01/22/16676/

2020 年 11 月，俄國國會通過三項新法案，該法將更嚴厲的管控線上平臺內容，打壓異議，包括封鎖 Twitter 及 YouTube 等網站。第一項法案授權封鎖「歧視」俄羅斯媒體的外國網站，第二項法案的規範內容是，若科技公司不按照俄國政府的要求刪除「不當內容」，該公司將被處以巨額罰款。第三項法案將授權政府監禁在網路上發布「中傷言論」的使用者。

若法案順利通過，YouTube、Facebook 及 Twitter 可能遭政府下架，因為上述網站會如實標註影片內容來自俄國官媒。根據新法，俄國當局能封鎖或放慢這些網站的網速。

根據路透社報導，自 2020 年 8 月以來，Twitter 一直將俄羅斯媒體的帳戶標記為「國家附屬」（state-affiliated），此舉激怒了俄國總統普丁，其呼籲俄國建立自己的社交媒體平臺，以獲取更大的網路控制權。

一直以來，俄國反對派領導人 Alexei Navalny 及異議人士利用 Facebook 及 Twitter 繞過國家的審查制度，和數百萬俄國人交流。目前，俄國當局已採取多種方法來限制網路內容，例如 2019 年通過的《網路主權法案》允許政府追蹤、過濾及控制網路流量。

參考資料：
https://www.npr.org/2020/12/23/949608378/russian-lawmakers-pass-bills-that-could-block-social-media-sites-and-stifle-diss

RIPE NCC 回應歐盟的數位時代網路安全戰略

國際瞭望 撰輯

https://blog.twnic.tw/2021/01/21/16678/

歐盟於 2020 年 12 月 16 日發布《數位時代網路安全戰略》（Cybersecurity Strategy for the Digital Decade）。戰略包含強化 DNS 根伺服器的安全性，並由歐盟委員會、歐洲網路與資訊安全機構（Eropean Union Agency for Cybersecurity，ENISA）、歐盟成員國、歐盟的二個根伺服器維運方（RIPE NCC 及 Netnod）以及多方利害關係團體共同制定「應對可能影響根伺服器系統性及可用性之極端情況的緊急計畫」。

RIPE NCC 並未直接參與戰略制定，也很驚訝戰略中包含「評估營運方維護網際網路在任何情境下皆保持全球通用的角色」。然而，RIPE NCC 仍歡迎歐盟委員會與多方利害關係團體合作以因應歐盟的顧慮。未來，RIPE NCC 將持續積極與包括歐盟機構的利害關係方交流，並分享自身的技術專長和經驗。

目前全球共有 13 臺根伺服器，分別由 12 個不同的單位負責維運。根伺服器以 a 到 m 的英文字母作為編號（a.root-servers.net.到 m.root-servers.net.），每個英文字母代表號背後也都有多個「mirror instances」配合 anycast 技術提供解析服務，也因此具有一定程度的防禦阻斷式攻擊能力。RIPE NCC 如同其他 11 個根伺服器維運方，有自信能為歐盟境內網路使用者提供穩定且安全的服務。

DNS 基礎建設的本質是去集中化的系統，因此，戰略中提到「歐盟 DNS 根伺服器營運方」的概念有誤導之嫌。目前全球各地

都設有根伺服器，RIPE NCC 提供的服務也遍及歐盟與歐洲之外，這種去集中化、重複及獨立操作的模式是 DNS 與網際網路安全、穩定及靈活性之基礎，確保全球使用者可穩定的使用網際網路。

RIPE NCC 及 RIPE 社群將共同致力於與所有利害關係團體（包括 ENISA、會員國，以及多方利害關係社群）合作，以支持歐盟委員會制定技術上合理的政策，確保所有使用者皆可使用全球互通的網路。

參考資料：

1.https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-the-eu2019s-cybersecurity-strategy-for-the-digital-decade
2. https://blog.twnic.tw/2019/02/22/2673/

已故員工也可能存在資訊安全風險

國際瞭望 撰輯

https://blog.twnic.tw/2021/03/09/17114/

近期的勒索軟體攻擊事件突顯出網路上存在多餘帳號的危險，特別是前雇員的帳號。在企業當中，一旦發生員工離職，依照標準的資訊安全作業流程，應當刪除該名員工的使用者帳號，若有員工過世，理當採取相同的做法。

今（2021）年 1 月，英國的資安公司 Sophos 便曾在其部落格撰文介紹相關案例，利用勒索軟體 Nefilim 進行攻擊的駭客，透過 Citrix 軟體的漏洞劫持某企業中已故員工的帳號，進而取得權限更高的管理者帳號，並掌握極具價值的資料，使得企業高達 100 多個系統均受到影響。

這起事件為企業（包括：資訊部門、資安團隊，以及人事部門）帶來教訓，有效的帳號不應該閒置在網路上，或是處於不受監控的狀態，因為一旦發生異常登入或有網路犯罪的活動跡象，便沒有相關的負責人可以採取補救措施。

Sophos 在文章中提出一項折衷方案：如果企業在員工離職後確實有保留其帳號之需求，應當導入一組服務帳號（service account），且拒絕互動式登入，以防止任何非必要的存取活動。當帳號不需使用時便將其停權，並定期審核活動目錄（Active Directory）。

另一項重點是，應避免建立不必要的管理者帳號，因為這些帳號如果受到攻擊，等於是對攻擊者大開門戶。此外，千萬不要因為某人是主管或負責管理網路，就認為其需要擁有管理者帳號，應依據使用者實際所需的權限，提供其對應的存取範圍即可，必要時再

提升權限，並且僅可存取特定服務。

Fortinet 的 Derek Manky 表示，人事部門與資訊安全部門之間絕對需要積極協作，才能改善員工的網路衛生習慣，包括審查及執行新進員工的存取申請，以及離職時的帳號刪除流程；另外，除了利用多重身分驗證機制之外，也應要求員工定期變更密碼，並定期提供教育訓練，以提高員工的資訊安全意識。

參考資料：

https://www.scmagazine.com/home/security-news/ransomware/even-dead-employees-pose-a-security-risk-when-their-accounts-are-still-active/

2020 年：MANRS 創紀錄的一年

國際瞭望 撰輯

https://blog.twnic.tw/2021/04/07/17346/

MANRS（Mutually Agreed Norms for Routing Security）是由網路營運商、網路交換中心（Internet exchange points，IXPs）、內容傳遞網路（Content Delivery Network，CDN）、雲端供應者及合作夥伴共同組織而成的自治社群，旨在推動全球採用 MANRS 行動及改進路由安全。

2020 年全球受到 COVID-19 疫情的影響，也突顯出安全、可靠的網路對於人們有多麼重要。對 MANRS 而言，這為社群之間的合作帶來更大的動力，以確保資料可以經由安全路徑抵達正確的地方。

去年加入 MANRS 的參與者數量創下新紀錄，從年初的 317 名到年底增加為 588 名，幾乎增加一倍，目前 MANRS 的參與者，所管理分布在全球 60 多個國家的自治系統（Autonomous System，AS），共計 651 個。

MANRS 促使路由事件的通報量，從 2017 年的 5,000 筆下降到 2020 年的 4,000 筆以下，提高了網路整體的安全性，雖然無法斷言皆為 MANRS 的功勞，但或許可將路由事件的減少，歸因於實施路由最佳作法的網路營運商日益增加。

在《2020 年 MANRS 社群報告》中彙整了一些去年的成功案例，同時詳細說明 MANRS 在人員培訓及合作關係的領導倡議方面所帶來的具體影響。報告中也概述了 2021 年及往後的目標與規畫，包括大使與獎學金計畫，以及對於設備供應商的新方案。

MANRS 團隊去年尚處於陡峭的學習曲線，但深受鼓舞於網路運營商之間日益增強的共同責任感，事實證明，只要社群之間齊心協力創建出路由安全的基準線，便能保護網路的核心。

參考資料：

https://www.internetsociety.org/blog/2021/02/2020-a-record-year-for-manrs/

一隻海狸造成加拿大英屬哥倫比亞 900 位網路使用者的服務中斷

國際瞭望 撰輯

https://blog.twnic.tw/2021/05/11/18583/

英國廣播公司（British Broadcasting Corporation，BBC）在 2017 年曾報導過，根據科學家 Cris Thomas 所發表的研究報告，全球關鍵基礎設施的主要敵人並非敵對國家或激進團體，而是毛茸茸的可愛松鼠。日前，在加拿大英屬哥倫比亞的 Tumbler Ridge，則發生了一起因海狸而引起的斷網事故。

Tumbler Ridge 是位於洛磯山脈山腳下的一個地區城市，人口數大約只有 2,000 人。2021 年 4 月 24 日，當地因為一條重要的光纖電纜遭到海狸啃咬，導致 900 位左右的網路使用者服務中斷，影響人數幾乎達到當地人口的一半，可說是相當嚴重。

電信公司 Telus 的發言人 Liz Sauvé 表示，光纖電纜共有多處遭到海狸啃咬，導致網路連線在當地時間 4 月 24 日的凌晨 4 點完全中斷。工作人員在附近找到海狸築起的水壩，牠們似乎是在那裡的小溪旁挖地洞，進而挖堀到埋藏在地底下約 3 英尺（0.91 公尺）深、並以 4.5 英吋（11.43 公分）厚的套管所保護的光纖電纜。

Sauvé 提到，從現場所拍攝的照片來看，海狸可能使用了 Telus 的材料來建造巢穴，因為原本應當埋在地底下的光纖標記膠帶竟出現在水壩上方。

由於當地氣候寒冷，導致電纜上方的部分地面結冰，也增加了這項搶修作業的困難度，所幸在隔天下午 3:30 便完成修復，並恢復正常服務。

參考資料：

https://www.cbc.ca/news/canada/british-columbia/beaver-internet-down-tumbler-ridge-1.6001594

家貓帶給我們的網路安全啓示

國際瞭望 撰輯

https://blog.twnic.tw/2021/12/06/21110/

史丹佛大學的資深研究學者 Herbert Lin，是網路政策與安全領域的專家，在洛杉磯時報（Los Angeles Times）的一篇社論文章中，透過自身與家貓相處之案例，以淺顯易懂的方式說明為何保護電腦設備安全會如此困難。

Lin 本身對貓毛過敏，偏偏他女兒帶了一隻貓（名為 Pounce）回家長住，這迫使 Lin 必須設法將 Pounce 限制在特定區域內活動，一開始這方法看似奏效，但 Pounce 很快便能突破屏障。

從這個經驗當中，我們可以看到幾項與網路安全有關的實例：

- 若要成功對抗堅定的攻擊者（Pounce），必須儘早使出全力，如果只部署最低限度的安全措施，肯定會失敗。
- Pounce 具備反覆嘗試的時間優勢，只要成功一次就能脫身，因此每項禁閉措施都必須達到有效性。
- 擁有更多資源與更高度的智慧，並不保證勝利，Pounce 依然可以無限次去嘗試繞過障礙。
- Pounce 背後有一個強大的保護者——Lin 的女兒，為維護良好的關係，Lin 不希望激怒女兒。同樣的，在境外活動的駭客即使名義上是自由行動者，往往也會得到政府的支援，因此很難說服這些保護者採取行動。
- 在 Pounce 逃出禁閉區之前，Lin 會認為自己的措施是有效的，這種情況會反覆發生，因此容易讓人陷入虛假的安全感。
- 試著以 Pounce 的高度去觀察環境並不容易，因此 Pounce 可

以找出規避或破壞禁閉措施的方法。

- 操控人員可能勝過任何技術防禦，這在網路安全領域稱為「社交工程」(social engineering)。當 Pounce 哀怨地喵喵叫並望向主人時，主人便會心軟打開禁閉區的門讓牠出去。以網路術語來說，Lin 的女兒就是一位「受信任的內部使用者」，但她叛變了。

直到女兒帶著 Pounce 搬出家中，Lin 才算真正贏得這場戰役。Lin 表示，這個事件帶給我們的教訓是：沒有電腦設備的地方，便不存在網路安全威脅。牙刷與冰箱即使不具高科技的通訊功能，依然可以正常使用，別為自己招來更多無謂的網路安全風險。

參考資料：
HERBERT LIN (2021.11.7). Op-Ed: What a house cat can teach us about cybersecurity. Los Angeles Times. 檢自：https://www.latimes.com/opinion/story/2021-11-07/op-ed-what-a-house-cat-can-teach-us-about-cybersecurity (Nov. 18 , 2021)

淺談網路攻擊與主動防禦

國際瞭望 撰輯

https://blog.twnic.tw/2021/04/15/17745/

網路攻擊情勢嚴峻

今（2021）年 1 月，在世界經濟論壇發布的《2021 年全球風險報告》第四章[1]提及，網路攻擊呈現日益複雜的趨勢，國家與非國家行為者都可能參與規模更大更危險的網路攻擊，透過無人機或其他技術的針對性攻擊將變得更加普遍。根據報告統計[2]，在 2020 年，遭受最多次網路攻擊的國家是美國，共有 156 起；英國經歷 47 起網路攻擊，排名第 2；中國則遭遇 15 起，位列第 8。報告指出，中等國力的國家是更易受到網路攻擊的目標，這類國家缺乏強權的網路防禦資源，且因技術與軍事能力落後，預期她們會投入大量預算在國防及建立同盟上，以進行網路防禦。

網路攻擊行為者之目的多元，有些純粹為了金錢或尋找樂趣，但更多國際級駭客透過網路攻擊，以引發目標國的動盪不安。各國也透過強化相關法規及擴大對網路安全領域的投資來應對，例如：法國總統馬克宏（Emmanuel Macron）將網路防禦稱為優先事項[3]，並表示法國政府自 2017 年以來便開始應對相關威脅，包括加強警察與司法單位合作、撥款 5 億歐元協助企業與公部門強化網路防禦，以及贊助相關研究。

---

1 World Economic Forum. The Global Risks Report 2021 16th Edition

2 World Economic Forum. The Global Risks Report 2021 16th Edition

3 Ania Nussbaum. Macron Rushes to Shore Up French Cyber Defenses After Attacks. Bloomberg 2021/02/18

然而，上述模式仍處於被動，近來，許多國家透過結盟或提倡主動防禦來防堵駭客威脅。去年以色列與阿拉伯聯合大公國，就因網路安全議題結盟，二國不計歷史深仇並共同應對來自伊朗的網路攻擊[4]，以色列甚至分享其相關駭客技術研究給阿拉伯聯合大公國，以使盟友在應對伊朗威脅時能先發制人。美國也因屢屢受到來自各方的網路攻擊而發展出主動防禦措施（Active Cyber Defense，ACD）[5]，來支持聯邦及地方政府的網路安全。

面對日益嚴峻的網路攻擊情勢，究竟主動防禦的概念為何？以及該如何進行才能有效抑制網路攻擊？而該措施與威懾或主動針對敵國發動網路攻擊有何差異，為本文探討重點。

主動防禦之概念與相關措施

主動防禦的概念精髓在於，防禦方必須持續觀察對手的惡意網路行為並分析其發動攻擊之目的，在對方發布網路行動前對該行為進行破壞，洞燭機先瓦解對方的行動。根據美國網路空間日晷委員會（Cyberspace Solarium Commission，CSC）第二工作組研究分析主任 Robert Morgus，其對於美國 SolarWinds 遭駭事件的分析[6]，主動防禦策略若要發揮作用，相關單位必須掌握完善情報。然而，情報的蒐集必定有限，因此，國家必須透過整合網路安全策略，釐清情報蒐集的優先順序，並縮小不同政府部門之間的情報落差。此外，政府並須整合不同部門，將責任分擔給受網路攻擊影響的利害關係人所組成的系統，包括透過法規規範私人企業必須強化內部網路安

4 Sean Lyngass. Israel, UAE say they’re allies in cyberspace. They have plenty of tech power to draw upon. Cyberscoop 2020/09/25

5 NSA. Active Cyber Defense (ACD) 2015/08/4

6 Robert Morgus. The SolarWinds Breach Is a Failure of U.S. Cyber Strategy. Lawfare 2020/02/18

全工作。

其他相關措施還包括設置獨立單位處理網路攻擊與事件，例如美國總統拜登考慮將目前由國土安全部管轄的網路與基礎設施安全局（Cybersecurity and Infrastructure Security Agency，CISA）設置為獨立機構，並增加預算及人力資源[7]，同時對關鍵基礎設施進行投資；亦可運用經濟、科技、法律與外交等多重手段，增加敵國惡意網路行為的成本，進而阻止其攻擊行為。例如在歐巴馬時代，美國對中國實施一系列制裁及貿易訴訟，並運用相關外交政策壓制中國，最後在 2015 年與中國達成協議，此舉明顯平息了中國的敵對行動[8]。

Wyatt Hoffman 與 Ariel Levite 在 2017 年曾撰文[9]，針對主動防禦的優缺點進行比較分析，其論述摘要如下表：

優點	缺點
• 可更了解潛在威脅、攻擊者的能力與意圖。 • 有更多與駭客攻守方面的選擇。 • 增加破壞或終止攻擊方計畫中或進行中攻擊行動的能力。 • 增加攻擊難度、攻擊成本、與攻擊風險，達到嚇阻作用。	• 由於人為錯誤或攻擊者操弄，反而事與願違。 • 可能破壞無辜的第三方電腦或網路，或因錯誤的攻擊策略導致附帶損害。 • 可能演變為互相攻擊，導致衝突加劇及升級。 • 影響性難以評估，可能導致他國潛在的政治與法律制裁。

[7] PALMISANO, S. J., & KIERSTEN E. TODT, K. E. (2020.12.9). A cybersecurity agenda for the Biden administration. FORTUNE 2020/12/09

[8] Ciaran Martin. (2021.1.15). Cyber 'Deterrence': A Brexit Analogy. LAWFARE.

[9] Hoffman, W.,& Levite, A. (2020.12.9). Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?. CARNEGIE CYBER POLICY INITIATIVE (June 14, 2017)

主動防禦在於協調各個政府部門及私人企業，共享情報並深化網路防禦措施與意識，若將主動防禦的概念誤植為主動對敵國進行網路攻擊，並預期達到威懾效果，則恐會波及無辜，並演變成更大規模的衝突與外交危機。

主動防禦不等於擴張網路權力

主動防禦的目標是確保網路安全，而非擴張網路權力（cyber power）[10]。網路安全，意指確保國土安全、國家網路設備及數位服務功能的完善，囊括了消費者、企業、個資以及國家機密的所有線上保護措施。但網路權力指涉的則是運用網路能力保護國家安全不受任何威脅影響，在此概念下，國家可將自身網路能力投射至任何相關政策目標上，包含攻擊敵國。

擁有網路權力的國家固然可對敵國的基礎設施進行攻擊，打擊網路犯罪、戰爭與不實訊息，但卻無法阻擋敵國持續採取駭侵行動。例如，美國曾對俄國的網路研究機構進行網路攻擊，目的是迫使俄國無法再傳遞與選舉相關不實訊息[11]，雖然美國的鷹派網路攻擊策略值得被部署，但通常像俄國這類具有主動進攻能力的國家，亦擁有良好且不易被破壞的網路基礎架構。因此，若美國貿然發動攻擊，容易使俄國進一步採取「以其人之道還治其人之身」的報復行動，並無助於減少網路攻擊。

---

[10] Hoffman, W.,& Levite, A. (2020.12.9). Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?. CARNEGIE CYBER POLICY INITIATIVE (June 14, 2017)

[11] Hoffman, W.,& Levite, A. (2020.12.9). Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?. CARNEGIE CYBER POLICY INITIATIVE (June 14, 2017)

結語

主動防禦已經成為網路防禦的重大政策，其概念並非主動攻擊敵國，而是偕同各政府部門進行情報共享，並持續強化既有網路防禦措施。目前，主動對敵國進行網路攻擊並不能被視為「防禦手段」，各國也無相關法規授權部門或企業進行主動防禦。透過妥善的情報蒐集與共享，和他國結盟共同應對威脅國，以及訴諸外交或其他制裁手段增加他國攻擊成本，迫使其面對艱難選擇的後果，才能有效遏制網路攻擊。

國家、網路衝突與暗網

國際瞭望 撰輯

https://blog.twnic.tw/2021/05/23/18252/

根據一份於 2021 年 4 月 8 日發布的最新研究，國家間的網路攻擊已愈加頻繁、多元且公開，自網際網路問世以來，我們現在離「進階網路衝突」的距離是最近的。

這項研究由英國薩里大學（University of Surrey）的犯罪學資深講師 Mike McGuire 博士主持，並由惠普公司贊助。根據研究結果，在 2017 年至 2020 年之間，由國家政府發起的重大網路事件成長率達 100%，研究中分析了自 2009 年以來，有國家政府涉入的 200 多起網路安全事件，企業是最常見的網路攻擊目標（35%），其次是網路防禦（25%），媒體及通訊系統占 14%，政府單位及監管機構占 12%，關鍵基礎設施則占 10%。研究的資料來源包括暗網線民取得的第一手資料，以及相關領域（如：網路安全、資訊、政府、學術界及執法單位）專家小組的諮詢訪談。

該研究的主要發現如下：

- 64%的專家小組成員認為：2020 年網路衝突升級的情況「令人擔憂」或「非常令人擔憂」；75%的專家小組成員認為：COVID-19 疫情為國家提供了網路攻擊的契機。
- 供應鏈攻擊在 2019 年增加了 78%；在 2017 年至 2020 年之間，超過 27 次可能是由國家政府發動的供應鏈攻擊。
- 超過 40%的網路攻擊事件屬於混合式攻擊（Hybridization），其特色是同時進行實體與數位攻擊，例如：攻擊能源廠。
- 國家用來獲取 COVID-19 相關 IP 個資的手法很明顯學自網

路罪犯，這個特徵也顯示國家政府與網路犯罪的地下經濟來往密切，不僅是受益者也是貢獻者。

- 證據顯示，許多國家廣泛蒐集「零時差漏洞」，且暗網交易中 1 到 1.5 成的買主是國家政府（或其代理人）。

參考資料：

https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/

NCSC 改版「網路安全 10 步驟」指南

國際瞭望 撰輯

https://blog.twnic.tw/2021/06/23/18934/

英國網路安全中心（National Cyber Security Centre，NCSC）已發布「網路安全 10 步驟」指南的最新版本，該指南首次發布於 2012 年，由 NCSC 的前身——英國政府通信總部的資訊安全部門所撰述。

過去 10 年來，不僅網路環境經歷重大演變，例如雲端服務的成長及居家工作情形日增，網路威脅的樣態也大有不同；此外，勒索軟體等新興威脅也與日俱增。時空環境大有不同，指南也須與時俱進，並讓適用於擁有專職網路安全人員的大型組織，最新版本的網路安全 10 步驟如下所述：

1. **風險管理**：透過風險管理措施保障企業資料及系統安全。
2. **參與及培訓**：為職員進行網路安全培訓。
3. **資產管理**：掌握企業擁有的資料與系統類型，並了解他們的業務歸屬。
4. **架構及配置**：設計、建構、維持及管理系統安全。
5. **弱點管理**：確保企業系統在其生命週期中獲得良好保護。
6. **存取權限控管**：掌握並了解誰能取得系統及資料權限。
7. **資料安全**：確保資料在傳送、儲存及銷毀時皆得到適切保護。
8. **記錄及監控**：確保組織系統能偵測與調查網路安全事件。
9. **網路安全事件管理**：事先部署網路安全事件的因應對策。
10. **供應鏈安全**：與合作夥伴及供應商齊心協力防堵網路攻擊。

該指南係為網路安全專業及相關技術人員量身訂做，指南也可

搭配 NCSC 推出的董事會網路安全工具包（Cyber Security Toolkit for Boards）一起使用，該工具包為董事會與網路安全人員提供優質的議題討論框架，企業網路安全人員能因此為董事會提供進一步的資源。

採取上述 10 步驟，可降低組織遭受網路攻擊的可能性，即使不幸遭遇網路攻擊，也可將傷害最小化。NCSC 官網亦提供詳細介紹經常發動網路攻擊惡意行為者的相關影片，若欲即時了解影響英國的網路安全問題，可參閱 NCSC 最新推出的報告與諮詢建議。

參考資料：

1. https://www.ncsc.gov.uk/blog-post/10-years-of-10-steps-to-cyber-security
2. https://www.ncsc.gov.uk/collection/10-steps

COVID-19 疫情期間釣魚、勒索軟體及網頁程式攻擊激增

國際瞭望 撰輯

https://blog.twnic.tw/2021/07/01/18964/

科技電信業者 Verizon Business 發布《2021 年度 Verizon 資料外洩報告》（Verizon's data breach report for 2021），根據報告內容，在 2020 年所有資料外洩案件中，有 39%來自於網頁程式，且網路釣魚及勒索軟體攻擊也較 2019 年大幅增加，而人為疏失仍是網路安全漏洞產生的主要因素。

Verizon Business 執行長 Tami Erwin 表示，因 COVID-19 疫情肆虐，許多企業將關鍵業務轉移至雲端系統，人為疏失造成的漏洞與對數位設施的日益依賴，皆雙雙為惡意行為者帶來可趁之機。

報告針對 2020 年發生的 29,207 起網路安全事件進行調查，確認有超過 5,200 起資料外洩事件。分散式阻斷服務攻擊（Distributed Denial of Service，DDoS）是最常見的網路攻擊類型，但造成資料外洩案件的主因是社交工程（social engineering）與網頁程式攻擊，在這些資料外洩事件中，85%是來自人為因素，其中 61%則涉及使用未經授權的憑證，更有超過 10%的資料外洩事件與勒索軟體有關，是 2019 年的二倍之多。

此外，涉及網路釣魚的資料外洩案件數，也從 2019 年的 25%上升至 36%，在所有駭侵案件中，網頁程式攻擊案件數達 80%。網路釣魚及勒索軟體因疫情而大幅增加並不意外，但報告也發現 2020 年終端用戶的硬體設備遭駭的比例下降——駭客也與時俱進，將攻擊目標轉向雲端及電郵系統。

資料外洩也使企業付出更高代價，造成的損失中位數為 21,659 美元，但對大多數組織而言，損失成本估計高達 650,000 美元。社交工程攻擊案件數量自 2017 年穩定上升，其中「公務信箱駭侵」的案件數尤其大幅飆升。報告中提到的其他研究結果包括：即使是較粗糙簡易的網頁程式攻擊，近年來手法也越來越高明；勒索軟體集團逐漸將目標轉向有能力與意願支付高額贖金的對象；不同產業正面臨著不同型態的網路攻擊；駭客關注的資料類型也因產業而異。

參考資料：

Ikeda, S. (2021.5.19) Verizon Data Breach Report 2021: Pandemic Has Caused Major Surge in Phishing, Ransomware and Web App Attacks. CPO Magazine. Retrieved from: https://www.cpomagazine.com/cyber-security/verizon-data-breach-report-2021-pandemic-has-caused-major-surge-in-phishing-ransomware-and-web-app-attacks/ (May 19, 2021)

網路釣魚仍為勒索軟體最便利的途徑之一

國際瞭望 撰輯

https://blog.twnic.tw/2021/08/18/19510/

根據網路平臺業者 Cloudian 所發布的一項調查，網路釣魚仍是勒索軟體集團所使用的主要駭侵途徑之一。該調查針對過去二年曾遭遇勒索軟體攻擊的 200 名 IT 決策者進行訪談，其中超過一半受訪者所處的單位，在遇襲前曾經舉行過網路釣魚相關的內部訓練，49%的受訪者則是在具備基礎防禦措施的情況下仍然遇襲。

將近 25%受訪者所遭遇的勒索軟體攻擊始於網路釣魚，而這些受害者中，65%曾接受過反網路釣魚培訓課程。在所有受害者當中，大約有三分之一表示公共雲端系統是勒索軟體集團的駭侵入口。

報告指出，上述現象反映出網路釣魚手法越來越成熟，駭客還會透過假冒信任的聯絡人（例如高階主管）的電子郵件發動攻擊，這些電子郵件有時包含了個資（通常來自社群媒體），致使謹慎的人亦遭受害。

勒索軟體集團的駭侵速度也令人吃驚，56%受訪者表示，駭客有辦法於 12 小時內挾持資料並發送贖金要求。在遭受網路釣魚攻擊的企業中，76%受訪者指出駭客於 12 小時內便能管控系統。

報告補充，44%受訪者的所有資料都遭勒索軟體集團挾持，包括財務、營運、客戶及員工資料。一旦遭駭，企業平均必須停業 3 日。在遭駭成本方面，受害企業平均財務損失額度近 50 萬美元，55%受訪者最終選擇支付贖金，平均額度為 22.3 萬美元，但實際上有將近 15%受訪者支付了 50 萬美元或更高額，且即使支付贖金，

也僅有 57%受訪者能取回所有資料。

所謂「道高一尺，魔高一丈」，即使企業已做好準備，駭侵攻擊仍難以預防。勒索軟體可迅速滲透組織，並對組織造成重大影響，即使透過支付贖金挽回，因應勒索軟體攻擊的其他損失，加總之平均額度高達 18.3 萬美元。

平均而言，雖然受害者能透過保險給付成本總額的 60%，但將近 90%受害者表示，保險費率亦會在遇襲後提高，平均增幅為 25%。

參考資料：

Jonathan Greig (2021). Phishing continues to be one of the easiest paths for ransomware. 檢自：
https://www.zdnet.com/article/phishing-continues-to-be-one-of-the-easiest-paths-for-ransomware-report/ (Jul. 23, 2021)

為何 NCSC 推薦使用三個隨機單詞組成的密碼

國際瞭望 撰輯

https://blog.twnic.tw/2021/09/08/19673/

常見的密碼設定原則多會強調「複雜性」（complexity），但由於人類大腦很難記住隨機字串，因此常會使用可預測的模式（例如用數字 0 來取代英文字母 O），以符合密碼所需的複雜性，相對的，攻擊者也會熟悉這些策略，並據此優化攻擊手法。

英國網路安全中心（National Cyber Security Centre，NCSC）近期在一篇部落格文章中，向民眾介紹他們推薦使用三個隨機單詞組合成密碼的邏輯。傳統的複雜密碼雖難以記住，但有可能讓犯罪分子猜中；相反的，由隨機單詞組成的密碼不僅容易記憶，更具備足夠強度的保護力，其他原因還包括：

- **長度（Length）：**由多個單詞組成的密碼，理論上字元數會比獨立的單詞更長。「長度」是密碼的常見要求，透過使用組合單詞所創造出的「密碼單詞」（passphrase），便是實現這項要求的方法之一。
- **影響（Impact）：**為了提高宣導的成效，NCSC 必須採用快速且易於理解的方式，透過不同的媒體向民眾進行推廣。「三個隨機單詞」這句話淺顯易懂，即使民眾並非電腦專家，也很容易理解其推廣內涵。
- **新奇（Novelty）：**傳統的密碼多為獨立單詞，較容易被犯罪分子猜中，透過「三個隨機單詞」的密碼設定邏輯，可以鼓勵民眾思考過去不曾使用過的密碼組合。

- **可用性（Usability）：**一般若要符合密碼複雜性，最大的問題是使用者必須花費較多心力去設定、記憶及輸入複雜的密碼，容易造成使用者重複使用密碼；相較之下，要求使用者輸入 3 個隨機單詞組成的密碼，則相對容易許多。

為了提高密碼被破解的難度，NCSC 認為使用者必須增加密碼的多樣性（diversity），以降低可被廉價且高效的搜尋演算法破解的密碼數量，而「三個隨機單詞」的密碼設定策略，將可有效鼓勵使用者設計出未曾使用過的密碼。

參考資料：
Kate R (2021). The logic behind three random words. NCSC.
檢自：https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words (Aug. 13, 2021)

網路政策

歐盟的平臺管制野心：數位服務法及數位市場法

國際瞭望 撰輯

https://blog.twnic.tw/2021/01/29/16751/
https://blog.twnic.tw/2021/02/19/17034

2019 年 7 月烏蘇拉· 范德賴恩（Ursula von der Leyen）就職歐盟執委會主席時，就曾宣告歐盟管制線上環境的決心。歐盟緊接著於 2020 年提出「打造歐洲數位未來」的數位戰略計畫並開放徵詢公眾意見，《數位服務法》（Digital Service Act，DSA）作為計畫中的草案之一，始終備受關注。2020 年 12 月 15 日，歐盟執委會公告以《數位服務法》為主的一系列草案，這是歐盟在 21 世紀首度徹底翻修網際網路相關規範，迎來歐盟準備實質管制境內外網路的歷史轉捩點。

《數位服務法》其實就是 20 年前歐盟《電子商務指令》（E-Commerce Directive）的大改版。為了因應數位時代，歐盟新修並擴大《電子商務指令》的管轄範圍，且重新命名為《數位服務法》，以期加強管制新興數位服務、資訊社會服務供應業者，包括主機代管、雲端服務等所謂的「線上中介」（online intermediary）產業。在這之前，德國及法國都已各自推出移除非法或有害線上內容的管制法規，《數位服務法》的出現將統整並更新各國現有的不同法規，確立一套歐盟境內通用的管制規範。

經過長達半年的公眾諮詢期，歐盟執委會終於在 2020 年 12 月公告《數位服務法》草案，更加碼發布《數位市場法》（Digital Markets Act，DMA）草案，主要目標對準了全球化科技巨頭，希望在確保

公平競爭、維護創新環境的同時，保障個人使用者的隱私、安全，以及使用網際網路的權利。

雖然法案細節幾經諮詢調整，但其中始終不變的骨幹是瞄準線上世界的「守門員」（gatekeeper），也就是那些履遭指控壟斷市場、破壞競爭的世界級科技企業及線上平臺。換言之，歐盟希望推出一套「預防性」規範，確保那些科技巨頭未來公平對待其他企業客戶，進一步保護、促進市場競爭。另一方面，歐盟也認知到此議題包含一般消費使用者及企業的二個面向，因此，除了以保護個人使用者為主軸的《數位服務法》之外，另外推出了保護中小企業的《數位市場法》。

數位服務法（DSA）

根據歐盟《數位服務法》專屬網頁中的介紹，法案中針對網際網路生態系統中不同的線上中介服務業者，根據其角色、規模及影響力，訂定不同的管制規則。《數位服務法》中列出的規管對象（參閱下圖）包括：

- 提供網路基礎建設的中介服務業者（Intermediary services），例如：網際網路服務供應業者、域名受理註冊機構，涵蓋下項業者。
- 雲端及網站主機代管等服務供應業者（Hosting services），涵蓋下項業者。
- 銷售方及消費者都使用的線上平臺（Online platforms），例如：網路商家、應用程式商店、共享經濟平臺，以及社群媒體平臺。
- 具散布非法內容，並造成社會傷害之高度風險的極大型線上平臺（Very large platforms）。

圖片來源：歐盟《數位服務法》專屬網頁

於歐盟經濟體內提供服務的所有線上中介服務業者，無論母公司是否位於歐盟境內，都必須遵守《數位服務法》。小型企業及微型企業也將依比例原則承擔法律義務及責任。

《數位服務法》的另一個特點是，將使用者超過 4 千 5 百萬人（約歐盟人口數 1 成）的「極大型平臺」特別劃分出來，自成一類，並針對這些極大型平臺的內容管理、廣告及演算法，設定更嚴格的透明化及當責要求，例如：極大型平臺必須建檔並公開包含廣告內容、目標觀眾、觸及對象總數等資料的歷史紀錄，在非法內容控管上，通報當局時也必須提供更多細節說明。

如同 GDPR，數位服務法亦祭出高額罰金，若極大型平臺違反法規，將面臨高達年度營業額 6%的罰鍰。此外，若在歐盟調查下發現企業提供「不正確、不完整或誤導性的資訊」，罰鍰最高可能達到企業年度營業額 1%。換句話說，若科技巨頭拒絕遵守《數位服務法》規範，等著他們的會是數百億的罰金。

數位市場法（DMA）

數位市場法的主要規管對象是「守門員」（gatekeeper）平臺，例如：搜尋引擎、社群媒體、某些即時通訊軟體、執行系統與拍賣網站等，這些「守門員」作為企業與消費者之間的關鍵交流管道，手中掌握莫大權力。必須注意的是，「守門員」平臺與《數位服務法》中僅以使用者人數定義的「極大型」平臺不同。「守門員」平臺必須滿足三個要件：對歐洲內部市場具重大影響力；其中介性質重度影響買賣雙方，以及業界地位；無論是現在或可預見的未來，都長久穩固。舉例而言，Amazon 和 Android、iOS 的應用程式商店都是所謂的「守門員」平臺：無論賣家或消費者都仰賴此平臺進行交易，且其規模嚴重影響商品成敗——出版商若不在 Amazon 上架，書籍將乏人問津；App 若不在 Android 及 iOS 的應用程式商店上架，就完全沒有人會使用。

《數位市場法》中將守門員平臺的營業內容分成二種類型：核心服務及附屬服務。前者如作為 Amazon 及應用程式商店等銷售平臺，後者則是這些平臺另外的收益管道，如收費作業、廣告等。整體而言，《數位市場法》主要針對的是附屬服務，如禁止平臺限制顧客僅能使用平臺本身付費服務等法條，預計將重創平臺的附屬服務財源。

除此之外，若平臺未能遵守規範，將面臨最高可達全球營業額10%的罰金。不僅如此，若屢犯不改，罰則甚至可能從企業結構下手，強迫受罰對象進行結構重組、拆分脫手部分業務。

目前二則法案都只是在草案階段，意味這些法條規範在進入歐盟國會投票前，仍將經歷多次辯論、修正及調整。不可否認，以歐盟的政治地位及經濟實力推出此等法案，若確定成立必將重現 GDPR 當年之風聲鶴唳，事實上，光是現在的草案，就已引發各界

熱烈討論。接下來將彙整各家分析看法，一窺眾人對歐洲欲打造的數位未來，有何批評指教。

在介紹《數位服務法》（Digital Service Act，DSA）及《數位市場法》（Digital Market Act，DMA）的由來，並簡介二則法案的規管對象及罰則後。顯示出歐盟早在 2019 年就宣示推動數位立法、管制線上行為的決心，事實上，去年歐盟《數位服務法》概念文件開放意見徵詢時，就將法案分成二大支柱：一是強化數位服務的法律責任義務，進而確保線上環境的安全及信用；二是建立事前規範原則，管制「守門員」（gatekeeper）平臺的行為。

根據歐盟去年 12 月公告的法案草案，第一個支柱就是《數位服務法》，第二支柱則獨立出來，成為《數位市場法》。本篇將進一步介紹二項法案中特別值得注意的規範，並陳列多種對於法案內容的見解分析，以助於讀者了解各家觀點。

《數位服務法》的主要規範

以下是《數位服務法》的主要規範：

- **定期報告**：中介業者應定期發布年度報告，詳列當年度（1）來自當局的下架要求、（2）業者發給使用者的下架通知，以及（3）業者自行實施內容審查的紀錄。
- **規範範圍僅限於「非法」內容**，不處理「有害」（harmful）內容。
- **通知後下架**（notice and takedown）。
- **使用者有權對平臺處置提出異議**。
- **廣告透明度規範**。平臺刊登廣告時應揭露：（1）該內容為廣告、（2）廣告刊登代表身分，以及（3）廣告投放對象的判斷依據。極大型平臺另必須遵守更嚴格的透明度規範，如須

維護公開線上資料庫，提供過去一年平臺刊登過的廣告資訊等。

- **極大型平臺須進行風險評鑑**，特別應評估：（1）非法內容散布、（2）對基本人權的不良影響，以及（3）平臺服務遭蓄意操縱以傷害公共利益及公共安全等系統性風險，並審視平臺本身的內容審查、推薦內容及廣告投放機制如何影響上述風險。

其中如「僅處理非法內容」、「通知後下架」、「使用者有權提出異議」等規定，都符合人權團體的期待。數位人權倡議團體 Access Now 於 2020 年 10 月提出的分析文件中，就強調平臺內容管制義務應僅限於「非法」內容，因為「有害」難以定義，不僅人與人之間的詮釋不一，歐盟各國的法律定義也依國情不同有所差異。另一方面，由使用者負責舉報違法內容的「通知後下架」機制，以及保障使用者內容遭下架後提出異議的權利等，都在賦予平臺使用者更多力量的同時，避免平臺內容審查責任過重，導致過度「自我審查」而衍生侵害言論自由及使用者基本人權的疑慮。

除此之外，如廣告透明度、極大型平臺須進行風險評鑑等要求也頗獲好評，認為當局終於正視大型平臺可能對社會造成的實質傷害，並肯定法案保護消費者的立意。然而，評論也指出法案內容不夠明確，如廣告透明度要求缺乏明確的格式規定，恐讓有心人士在揭露資訊的形式上取巧，反而造成資訊混亂、引發爭端。極大型平臺的風險評鑑應由誰負責執行，又如何評估（質化分析？量化標準？）法案中列出的系統風險等問題，若不小心規範，都可能留有操作空間。

《數位市場法》的主要規範

事實上，比起《數位服務法》，大眾注意力更集中於管制巨頭企業，也就是所謂「守門員平臺」的《數位市場法》。

以下是《數位市場法》的主要規範：

- **禁止守門員平臺結合使用資料**，如比較分析第三方商家蒐集的使用者消費資料和平臺自身蒐集的使用者資料，達成更精準的使用者側寫剖析。
- **守門員平臺必須允許賣家自由標價**，如在自家網站和平臺上使用不同的商品定價。
- 守門員平臺不得要求使用者必須透過平臺內建的交易流程或應用程式進行交易，亦不得要求使用者必須登入平臺以進行交易。
- 禁止守門員平臺在搜尋結果中優先呈現自家產品或服務。
- **應遵守「可交互運作性」**（interoperability）**及「資料可攜性」**（data portability）**原則**。前者如使用者應可直接於守門員平臺上使用第三方的交易程式付款，後者則可視為 GDPR 的延伸，即使用者有權檢視、編輯並移轉儲存在平臺上的資料。
- 守門員平臺如欲併購或收購其他企業，必須先行取得歐盟執委會同意。

目前大部分對《數位市場法》的評析多呈現大方向、整體性的評論，較少如《數位服務法》逐條探討的意見分析。主要原因可能是《數位市場法》的「事前」（ex ante）特性，與依判例檢討既有體制並訂定新法的「回溯」（ex post）型法案不同，「事前」性質的法案是「以政策領導法規」，立法者設想希望達成的結果，並訂定法規以確保結果實現。

專家分析及見解

德國聯邦經濟暨能源部（Federal Ministry for Economic Affairs and Energy）競爭及消費者政策部門主管 Thorsten Käseberg 分析，《數位市場法》傾向列出具體規則（rule）而非開放式標準（standards），這麼做的好處是縮減詮釋空間、增加執法效率，壞處是法案也因此缺乏彈性，難以依案件調整執法方式。他也提醒，《數位市場法》標榜的是反壟斷、促進競爭，法案目的不應是「破壞特定企業的主導地位」，而應著眼於確保競爭過程公平公正。

美國智庫 CSIS 資深顧問，於歐巴馬執政時期任美國國際貿易委員會主席的 Meredith Broadbent 亦持同樣看法，她認為少數的大型領導性平臺實質上減少中小企業擴張規模的成本，而依企業規模而異的法案內容，更可能導致中小企業寧願限縮企業規模以迴避規範。她質疑，《數位市場法》以企業規模為規管標準的做法違反傳統反壟斷法「保護市場結構、加強市場效率」的立法精神，加上缺乏「拉下大企業對中小企業有利」的實際歷史證據，恐難發揮預期的功效。

然而，管束科技巨頭乃民心所向、時勢所趨。高偉紳律師事務所（Clifford Chance）合夥人、同時具代表網路巨頭及中小企業經驗的 Thomas Vinje 預測，各國法令將逐漸向歐盟的《數位市場法》靠攏。雖然有意見認為《數位市場法》擺明針對美國企業，未來的拜登政府或許會有反制行動，但 Vinje 不認同此意見，並指出「約束科技巨頭」如今在美國已是少數獲二黨共識支持的議題。

前歐盟議會議員、現任史丹佛大學網路政策中心政策主任的 Marietje Schaake 雖樂見歐洲數位法案的野心，但也認為還需要更統合性的做法。歐盟去年不僅推出數位戰略計畫，亦發布《民主行動計畫》，目標是打擊不實訊息、保護媒體自由及捍衛選舉安全。今

年歐盟亦計畫推出人工智慧相關法案，而這些法案彼此關聯，必將互相影響。歐盟必須準備好完整、融會貫通的一系列配套做法，才能持續保護歐盟的經濟及公共利益。

Eurid 宣布.eu 域名撤回期限延長三個月

國際瞭望 撰輯

https://blog.twnic.tw/2021/03/17/17247/

自今（2021）年一月以來，英國仍有成千上萬的.eu 網站及電子郵件信箱因脫歐過渡期間終止，而處於停權狀態。.eu 註冊管理機構 Eurid 日前宣布將延長域名撤銷期限，域名所有人還有 3 個月的機會以符合.eu 監管框架。

英國於 2020 年 12 月 31 日正式脫歐，這代表英國公民失去註冊.eu 域名的權利。歐盟法規規定.eu 不能分配給居住在非歐盟成員國中的非歐盟公民，因此，自今年 1 月 1 日起，Eurid 被迫停權來自英國 5 萬名用戶手中的 81,000 個.eu 域名。

域名停權，代表該域名的網站及電子郵件服務暫時失效，但並非完全撤銷。用戶仍可更新註冊資料以符合歐盟標準，確認後功能即可恢復。Eurid 一開始給用戶的期限是到 2021 年 3 月 31 日為止，現在將延長至 6 月 30 日。

Eurid 警告，若未能在 6 月 30 日前更新資料，自今年 7 月 1 日開始，域名將被撤銷，直到 2022 年 1 月方可重新註冊。

2018 年歐盟提出在英國脫歐後立即全面撤銷在英國營運的.eu 域名，此一聲明激怒了約莫 30 萬位域名持有人。批評者認為這違反業界讓域名自然到期的最佳做法，並侵犯財產權，最終，Eurid 宣布與歐盟執委會（European Commission，EC）達成協議，英國的.eu 域名持有人會有更多時間調整註冊資料。

目前，更改資料的時限延長，預期將有更多.eu 域名能在英國脫歐的情境下倖存，然而，過去幾個月監管的不確定性導致英國.eu

域名減少：2017 年時，共有超過 30 萬個域名在英國註冊，但在 2020 年最後一個季度僅有 12 萬個.eu 域名被註冊。

參考資料：

https://www.zdnet.com/article/uk-owners-of-eu-websites-just-got-an-extra-three-months-before-their-domains-get-withdrawn/

2021 網路治理展望

國際瞭望 撰輯

https://blog.twnic.tw/2021/02/23/17080/
https://blog.twnic.tw/2021/03/15/17253/

網路治理學者 Wolfgang Kleinwächter 每年初都會撰文回顧去年全球網路治理發展，並提出新年預測及展望。Wolfgang 自 80 年代便積極投入網路治理，從 ICANN 創立，到聯合國成立網路治理專家小組等重大歷史，他都參與其中。他也是歐洲網路治理論壇（European Dialogue on Internet Governance，EuroDIG）、全球網路治理學術網路（Global Internet Governance Academic Network，GigaNet）及網路治理暑期學校（Summer School on Internet Governance，SSIG）的共同創辦人。

Wolfgang 今（2021）年 1 月也不例外地發表長文，首先回顧 2020 年，細數重要國家及地區強權去年的網路政策方向，進一步分析這些國家區域戰略未來衝突或互補的可能。接下來分別就網路安全、數位經濟、人權、科技四大面向，預測 2021 年網路治理發展，亦檢視多方利害關係與多邊／雙邊談判協議的網路治理路線之爭，隨著網路治理議題逐年演化改變，多方利害關係參與是否將持續主導未來的網路治理發展？

2020 年最重大的改變，就是 COVID-19 疫情在一年之間大幅加速全球數位轉型。從工作、學習到民生需求，幾乎所有人都仰賴網路維繫得來不易的日常生活。然而，若有人以為這個席捲全球、改變民生樣貌的疫情，將促使人們打破疆界、團結一心，共同面對威脅，那可就大錯特錯。相反的，我們在 2020 年看到的是「我國優

先」成為常態。各國的保護主義心態不僅反映在實體國界的嚴格管制上，網路也成為各國聲張主權的場域，更不時被當作強權互相攻防的利器。

歐盟

如前所述，2020 年各地政府或多或少傾向保護主義，這也不免讓人憂慮，各國政府是否將趁勢把現實世界中涇渭分明的國界推入網際網路，進一步促使網路邁向分裂。歐盟始終堅決擁護「不分裂的網路」，但前有發明網路的美國，後有近年急起直追的中國，夾在二大網路強國之間，歐盟不免感到難以施展。歐盟執委會主席范德賴恩（Ursula von der Leyen）去年 9 月發表聯盟咨文時，就宣告將展開歐盟的「數位十年」，強調歐盟應在保護隱私及網路使用權、言論自由、資料自由流通，以及網路安全的原則上，推動歐盟從連線、技術到公共服務的數位進展。

范德賴恩及她的數位內閣都對歐盟的「新綠色數位計畫」深具信心。憑借 2018 年通用資料保護規則（GDPR）的成功經驗，歐盟於 2020 年底推出「打造歐洲數位未來」的數位戰略計畫，計畫中除了備受矚目的《數位服務法》（Digital Service Act，DSA）及《數位市場法》（Digital Markets Act，DMA）草案，還包括《數位世代網路安全戰略》，以及二本分別針對人工智慧及資料管理的白皮書。這個內容豐富的「計畫包」是來自歐盟的清楚訊息：歐盟在下個世代將領銜「建立規則」，而非等著「遵守規則」。

美國

拜登於 2021 年入主白宮，歐盟期待拜登領導的華府修正川普過去 4 年的路線，重返國際組織及條約，訂定更穩健、友善的外交

政策。另一方面，川普掀起的中美貿易戰仍餘波盪漾，吸引數十個國家簽署的「乾淨網路」計畫是否就此喊停？美國在新政府下的網路政策動向備受全球關注。

當然，國際關係不只是中美角力。包括世界貿易組織（World Trade Organization，WTO）的數位貿易協商、經濟合作暨發展組織（Organization for Economic Cooperation and Development，OECD）的全球數位稅制協商、聯合國的網路安全公約討論，以及聯合國秘書長 Antonio Guterres 領銜推動的「數位合作地圖」，華府的政策決策在諸多網路外交議題都仍具備強大影響力。拜登政府打算加入主導，還是繼續自外於國際協商，另行尋找志同道合的盟國多邊談判？期待華府選擇前者的國家有之，樂見其持續採後者路線的國家也不少。唯一可以確定的，是世界皆靜待美國作為。

中國

美國及歐盟若想重建跨大西洋的數位夥伴關係，就不能不處理中國議題。為了反制美國去年 8 月提出的「乾淨網路」計畫，中國緊接著於 9 月推出《全球數據安全倡議》，倡議中大量挪用歐盟類似議題文件的用語，根據中國外交部長王毅，中國將「致力於為加強全球數位治理貢獻中國智慧」。然而，無論是《全球數據安全倡議》的八個項目，或是同年 11 月烏鎮世界互聯網大會中所發表的四項原則、五點主張，對歐美最重視的原則議題如人權、言論自由，或多方利害關係治理模式等，皆隻字未提。

很明顯的，中國對何謂「網路空間命運共同體」有自己的想像，而這個共同體並不在乎網路治理「由下而上、透明化的多方利害參與」的核心原則。去年烏鎮峰會以「數字賦能、共創未來——攜手構建網路空間命運共同體」為題；Wolfgang 質疑，若中國及歐美如

此缺乏共享價值，雙方該如何「共創未來」？而完全無視政府之外的多方利害關係團體，又怎麼可能「構建網路空間命運共同體」？

俄羅斯

在網路安全議題上，俄羅斯大多時候與中國同一陣線，前者也樂於歡迎阿里巴巴、華為等中國科技巨頭於境內投資。然而，二國的網路安全理念仍具顯著差異。在對網路空間的想像上，俄羅斯視美歐為死敵、勢不兩立，中國則仍想強調國際對話、協作的重要。這也導致二國網路戰略的不同：簡略而言，俄國戰略以破壞、造成傷害為主，中國則希望保持現有局面並趁機上位。

可惜的是，俄羅斯在 2020 年沒什麼大展身手的機會。雖然分別擔任金磚五國（巴西、俄羅斯、印度、中國及南非，又稱 BRICS）及上海合作組織的主席，但二個組織皆未能在 2020 年產出任何實質成果。在聯合國中為了反制《布達佩斯公約》成立的跨政府專家委員會，也沒有任何進展。國內的數位轉型亦不如預期，俄國政府將斯科爾科沃打造為「俄羅斯矽谷」的野望，在十年後的今天仍未實現。

印度

印度深知自己在數位時代的優勢——坐擁大批優秀數位技術人才，加上龐大的國內市場，並不難理解印度傾向數位主權，推動資料在地化、加強發展網路攻擊技術，以及嚴格限制外國企業以保護本土 IT 產業等做法。去年，印度在外交部下成立「新興及戰略科技」（New Emerging and Strategic Technologies，NEST）新部門，負責支援協調印度參與聯合國數位貿易、人權及致命自動武器系統法律專家小組等網路外交事務。

印度有懷抱數位野心的本錢，但著眼永續數位發展，印度似乎尚未在「封閉式全球化」、「新數位社會契約」或「自由家長主義」（Libertarian Paternalism）等不同路線中做出選擇。有些人還記得1955 年印度發起的「不結盟運動」——不在冷戰的美蘇之間選邊站，並與理念相同的國家結成鬆散同盟，反對任何形式的殖民主義、帝國主義及新殖民主義。印度可能再次發起「數位不結盟運動」嗎？若成真，位於拉丁美洲、東南亞、非洲的搖擺國們，以及新興科技勢力如沙烏地阿拉伯、以色列、臺灣及新加坡，又是否願意加入？

非洲聯盟

非洲聯盟去（2020）年 5 月啟動「非洲數位轉型戰略（2020-2030）」，目標是在未來 10 年建立非洲單一數位市場，保障人口、服務及資本的自由流動，促使個人及企業都無縫接軌線上活動。不只如此，還要制定非洲境內統一的政策及法律規範，以強化洲內各國貿易互通、資本流動及社經整合為原則，建立並改善數位網路，在網路經濟中與其他洲平起平坐。

非洲的優勢包括 15 億人口組成的消費市場，以及大量的「數位原生」年輕人口。范德賴恩上任後，首次出訪非洲的目的地便是非洲聯盟總部所在地——衣索比亞首都阿迪斯阿貝巴。二聯盟的夥伴關係中，數位發展是不可或缺的關鍵一環。非盟暨歐盟數位發展中心（AU-EU-Digital4Development (D4D) Hub）於去年 12 月正式成立，預計將成為推動二洲多方利害關係對話、合夥關係及非洲數位經濟投資的重要動力。

然而，想及早和「數位非洲」打好關係的不只有歐洲，中美二國長年來也都在非洲投注不少資金，美其名為「攜手打造非洲數位

轉型」，事實無非意圖搶占市場先機。非洲的網路空間是否將再次淪為強權角力的戰場？值得大家繼續關注。

前面總覽網路強權 2020 年的網路戰略發展，接下來則進一步放大格局，從網路安全、數位經濟、人權、科技四大面向，提點讀者今年值得關注的重要全球趨勢。

作者首先斷言，2021 年間，全球不會達成太多共識。各國政府將首重國內需求，以國家政策為優先。但值得慶幸的，各國似乎都認同保護全球網際網路的公共核心，也就是協調管理根伺服器、域名及 IP 位址之全球機制的重要。借用 ICANN 執行長 Göran Marby 的用語，所謂的「技術」網路治理（Technical Internet Governance，TIG），意即網際網路的「技術開發」面向，已不再是各國爭取話語權的主戰場，也逐漸擺脫過去眾人擔心的「分裂」危機。然而，更上一層，網際網路的「使用」層、含括更多議題的「網路治理」（Internet Governance，IG）場域，卻正邁向不同次元的「分裂」。

當然，TIG 及 IG 之間的界線並非涇渭分明；技術議題無法擺脫政治意涵，政治議題也始終帶有技術成分。不可否認，此類議題近幾年來益發政治化、更難以自外於各方意識形態干涉，然而即使進展緩慢，仍有值得期待的發展，聯合國秘書長 António Guterres 提出的數位合作地圖便是一例。

那麼，2021 年的數位網路討論將聚焦於哪些議題？作者從四大領域切入，總覽今年網路治理的關注重點。

網路安全

聯合國當中有二個專門探討網路安全議題的團體，分別是 2004 年成立、2018 年第 6 度重啟的「政府專家小組」（Group of Governmental Experts，GGE），以及 2018 年成立的「開放式工作小

組」（Open-Ended Working Group，OEWG）。

值得注意的是，過去始終由俄羅斯主導的 GGE，2018 年卻是在歐美「西方國家」支持下重啟；而 OEWG 則是由俄羅斯發起、在中國支持下成立。然而，如同專家指出，「開放式工作小組」的名稱大有誤導之嫌，因為該工作小組雖號稱「開放」，但實際上仍僅容許聯合國成員國加入，而且必須依聯合國大會規章行事。另一方面，聯合國同時決議通過這二項處理相同議題、理念卻互不相容的工作流程，亦被學者稱為「國際共識的最終斷裂」。

依照章程，GGE 及 OEWG 本應於 2020 年提出成果報告，然而受疫情影響，OEWG 將延至今年夏季、GGE 則將於今年秋季發布成果報告。

數位經濟

此領域有三個重要議題，分別是數位貿易、數位稅及永續發展。

世界貿易組織（World Trade Organization，WTO）1998 年通過《電子商務暫緩課稅》案，此案容許資料跨國自由流通，促進活躍的跨國數位貿易，也是近年來全球經濟成長的一大主因。然而，究竟是否應落實此案入國際法，WTO 過去 20 多年來始終無法達成共識。2019 年日本擔任 G20 主席，提出「信任的資料自由流通」（Data Free Flow with Trust）倡議，本來應於 2020 年夏天的 WTO 部長會議討論，也因疫情延至今年夏天。

數位稅其實與電子商務一體兩面。為了拓展財源，近年許多國家開始立法徵收數位稅，也因此導致大大小小的數位稅戰爭。經濟合作暨發展組織（Organization for Economic Cooperation and Development，OECD）下的工作小組最近終於達成結論，提出所謂的「雙支柱方案」：一方面建立「應於何處繳稅」的規範，確保跨

國科技巨頭（如 Amazon、Facebook、阿里巴巴、騰訊）在賺進大筆鈔票的地方繳納相應稅額；另一方面則推出「基本稅」，防止企業為了避稅躲到稅法寬鬆的國家。

美國於 2020 年 6 月退出此協議，但今年新上任、更重視國際合作的拜登政府是否將重返協議，各界不無期待。歐盟也已下達最後通牒，表示若「雙支柱方案」至 2021 年中仍未敲定，他們將推出自己的歐盟數位稅法。

數位經濟的發展不應將低度開發及未開發國家排除在外。減緩數位落差、鼓勵全球南方（global South）的數位發展，進一步達成數位經濟全球雨露均霑的永續發展目標，將是未來十年的重要功課。

人權

隨著日常民生數位化的程度逐步加深，數位化帶來的人權挑戰也越來越多。從因應不實訊息及仇恨言論、避免人臉辨識以防制犯罪之名遭濫用，到確保創新數位服務演算法的安全，都是數位時代面臨的人權挑戰。遺憾的是，雖然「保護人權」的聲音從未消失，但大部分國家政府始終缺乏配合行動的意願，公民社會的意見也仍被漠視。

科技／技術

許多人主張技術本身完全中立，但事實並非如此。技術、程式由人類編寫而成，亦無可避免地繼承人類的主觀意識、立場及偏見。人工智慧及演算法都是最佳實例，而隨著我們的居家環境、公共運輸甚至城市越來越「智慧」，人工智慧自然成為跨國協商的重要議題。

聯合國教科文組織（United Nations Educational, Scientific and Cultural Organization，UNESCO）預計於今年 11 月第 41 屆 UNESCO 大會採納 AI 倫理規範。不僅是 UNESCO，許多其他國際組織也都視 AI 為關鍵議題：世界財產權組織（World Intellectual Property Organization，WIPO）探討 AI 及智慧財產權的關係、歐洲安全暨合作組織（Organization for Security and Cooperation in Europe，OSCE）檢視 AI 對言論自由的影響、國際勞工組織（International Labour Organization，ILO）聚焦於 AI 如何改變未來工作樣貌、國際電信聯盟（International Telecommunication Union，ITU）則討論 AI 如何適用所有人。歐盟議會也於去年招標研究案，探討立法規範 AI 的可能性。這些討論值得持續關注。

另一方面，新技術需要新的標準，也因此，在多項新技術終將成熟並主導數位發展的 2021 年，許多專家也預言將展開「標準化戰爭」，科技強權們將為爭奪訂定標準的權利展開激烈競爭。國際電信聯盟（ITU）自然首當其衝，原訂去年 11 月舉行的世界電信標準化全會（World Telecommunication Standardization Assembly，WTSA）因疫情延至今年春天，預計會議中也會討論多項標準提案。

治理模式之爭：多邊 vs.多方

如前所述，網路治理議題近年政治化程度加重，政府自然而然掌握更多領導權，這是否代表由國家政府主導的多邊主義（Multilateralism）終將取代網路治理標榜的多方利害關係（Multistakeholder）參與模式？作者認為並不盡然。他指出，自 2005 年聯合國世界資訊社會高峰會（World Summit on the Information Society，WSIS）提出多方利害關係參與的治理模式後，廣納業界、公民社會、學界及技術社群的多方模式，無論在過去或未來，都將

是全球數位網路治理的唯一前進道路。

正如作者所言，多方模式過去近 20 年來始終是網路治理不可動搖的中心原則，但其曠日廢時、成效不彰的缺點也不乏批評聲音。作者期待聯合國秘書長去年推出的數位合作地圖帶來改變，希望未來的多方模式也能因此產出具體成果。

回顧作者於 2020 年初發布的文章，可以發現 2020 年的網路治理就像去年世界上其他大部分全球政策，囿於 COVID-19 疫情，幾乎沒有任何進展。在此同時，疫情也大幅縮短全球數位化進程，從健保資料的數位化及利用，科技巨頭的網路中介平臺如何改造現代社會的資訊內容及散布方式，到政府防疫措施演變為數位監控現實的潛在危機，都將更新、更急迫的網路治理議題推上檯面。隨著各國疫苗施打率逐漸上升，2021 年全球是否終能走出 COVID-19 陰影，數位網路的討論又能否端出具體成果，不妨拭目以待。

緬甸網路安全法草案受到廣泛譴責

國際瞭望 撰輯

https://blog.twnic.tw/2021/03/30/17332/

緬甸軍政府起草了新的網路安全法案，該案若通過，政府將可取得用戶個資，甚至阻止用戶連線特定網站。因該法不符合國際法，一旦通過，將破壞國際企業在緬甸設立在地資料中心的可能。根據目前草案，在緬甸營運的線上平臺必須保留所有用戶資料（包括 IP 地址，住家地址及身分證字號）三年，並保存在政府指定的系統中。

緬甸軍政府已將自己任命為國家行政委員會，並表示該法案是打擊網路犯罪及有害線上活動的必要手段。然而，該法因其壓迫性、含糊其辭的條款，以及賦予政府無窮權利禁止網路內容並起訴文章作者而受到各方譴責。緬甸 MCRB（Myanmar Centre for Responsible Business）在聲明中警告，該法要求資料在地化的做法不僅影響公民社會，還會阻礙國際投資及當地產業的成長，尤其對於 ICT 產業影響重大。相關資料必須被儲存於政府指定的網頁中，這將使當地產業易受到網路攻擊，對於使用大量資料的銀行及電商而言尤其如此，金融機構無法降低網路安全風險，將使外國投資者望之卻步並損害在地產業。

挪威電信集團 Telenor 在一份聲明中表示，法案應送至議會並經過辯論，同時與多方利害關係人進行磋商，以確保該立法合乎目的並符合憲法。Telenor 認為該法應採取透明性及明確性原則，並排除政府可透過行政命令直接存取使用者帳戶的規定，同時，個資保護、電子交易及網路安全法律應分開管理。

無國界記者組織亞太區負責人 Daniel Bastard 在一份聲明中表示，該法威脅緬甸公民獲得可靠資訊的權利，以及記者或部落客個資的機密性，其力促在緬甸開展數位業務的廠商拒絕遵守該法。

全球工會聯盟（UNI Global Union）則呼籲日本電信業者 KDDI、卡達的 Ooredoo 及挪威的 Telenor 大力反對該法，聯盟秘書長 Christy Hoffman 表示，該法使政府牢牢掌握權力，是政府壓制工會、學生、教師及工人的有力武器。

人權觀察組織亦力勸政府撤回法律，指出該法將強化政府監控並阻礙公民獲得基礎服務。倡議自由網路的社運組織 Access Now 表示，緬甸軍政府的斷網行動意圖使異議者保持緘默，已公然違反人權法。

參考資料：

https://www.zdnet.com/article/myanmars-proposed-cybersecurity-bill-draws-wide-condemnation/

歐盟將允許英國及歐盟間保持資料流通自由

國際瞭望 撰輯

https://blog.twnic.tw/2021/04/01/17328/

金融時報報導，歐盟執委會預計通過一項決議草案，一旦確認英國的個資法規符合歐盟規格，將允許英國及歐盟之間的資料保持自由流通。

決議若通過，與保健、保險及科技等，這些常需要跨境傳輸顧客個人資料的產業將大幅受益。根據決議草案，嚴重犯罪情事的搜索令及監聽內容等警察辦案資料也可自由流通，有利於歐盟及英國未來的執法合作。

此決議將同時造福歐盟及英國，雙方皆樂觀其成。歐盟資料保護委員會（European Data Protection Board，EDPB）雖將嚴格檢視決議內容，但 EDPB 並無權杯葛此決議。歐盟議會每四年會定期審查英國的資料保護法規是否符合歐盟規範，一般民眾若認為有不符規範之情形，亦可隨時訴請歐盟最高法院裁決。

歐盟執委會副主席 Vera Jourova 表示，相較於其他資料保護規範與歐盟相去甚遠的國家，英國在符合歐盟法規上的確占有優勢，也因此能確保雙方之間資料持續自由流通。「在此同時，我們也必須超前部署決議內容。我們要保持警醒，防止協議傷害歐盟公民權利的可能。」

英國法律本來就容許本國資料傳輸至歐盟境內，脫歐過渡期將於 2021 年 6 月 30 日截止，歐盟這項決議草案必須在此期限前通過，雙方之間的資料流通才能維持不中斷。

參考資料：

https://www.ft.com/content/43ed5e0a-7b0a-40db-800f-6f3b9c58b9a8

ICANN 針對 NIS2 提出回應聲明

國際瞭望 撰輯

https://blog.twnic.tw/2021/04/23/17999/

歐盟執委會去（2020）年底提出《網路與資訊系統安全指令》修正提案（Revised Directive on Security of Network and Information Systems, NIS 2 Directive），目的是增修 2016 年發行的 NIS 指令（NIS Directive），以符合當代數位版圖。顧名思義，本指令目的是提供歐盟所有會員國網路安全的最高指導原則。

去年底公布的修正提案（NIS 2 Directive）中，亦有專章列出網域名稱系統（Domain Name System，DNS）相關規定，而根據提案內容，歐盟境內所有 DNS 相關服務，包括遞迴解析器、根區權威解析器營運、頂級域名及其他所有域名服務的供應業者，都必須遵守此原則。提案中將 DNS 服務視為必要服務，並規定所有在歐盟境內提供 DNS 服務的業者採行網路安全措施，若任何事件嚴重影響服務，也必須立刻通報相關單位。

另一方面，通用資料保護規則（General Data Protection Regulation，GDPR）及數位服務法（Digital Service Act，DSA）都有的「小型／微型企業免責」條款，在 NIS 2 中將不適用頂級域名註冊管理機構及 DNS 服務供應業者。

NIS2 指令草案循慣例開放徵詢公眾意見，期間為 2020 年 12 月 16 日至 2021 年 3 月 21 日。ICANN ORG 於 2021 年 3 月 18 日提出回饋意見，聚焦於二大重點：

- 希望釐清 NIS2 中視為「必要服務」的 DNS 服務供應業者身分；

- NIS2 第 23 章中域名註冊資料揭露的相關規定。

不只 ICANN ORG，ICANN 社群中也有許多利害關係團體分別提出反饋意見。目前公眾意見徵詢已截止，所有歐盟收到的回應聲明皆公告於此頁面。

參考資料：

1.https://www.icann.org/en/announcements/details/icann-org-provides-feedback-on-the-proposed-nis2-directive-19-3-2021-en

2.https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/

ICANN70 精華回顧

國際瞭望 撰輯

https://blog.twnic.tw/2021/04/27/18024/

持續進化的 ICANN 線上會議

2021 年第一場 ICANN 會議，原訂於墨西哥坎昆舉行的 ICANN70，囿於疫情，在今年 3 月 22 至 25 日，依墨西哥坎昆時區以線上形式舉行。這也是自 COVID-19 全球疫情爆發後，ICANN 第四次舉行的線上會議。

累積去年的經驗，本次 ICANN70 線上會議亦再次圖新，除了持續改善線上會議功能，也新增其他會議工具。自去年起，社群便不斷反映虛擬形式大幅阻礙會議期間的社交及私下互動機會，為回應社群需求，ICANN ORG 會議規劃團隊積極開發新工具，本次 ICANN70 會議期間，與會者可以利用會議網站，在議程之外，自行安排和其他與會者的會議，從一對一到多人會議都沒有問題。

以往的 ICANN 實體會議皆會提供聯合國六個官方語言的即時口譯，去年 ICANN 會議皆轉為線上形式，雖自 ICANN68 起提供即時口譯服務，但與會者須另外下載軟體才能使用服務。本次會議開始，與會者無須另外下載軟體，直接使用 Zoom 內建的翻譯功能就能享受即時口譯服務。雖然僅限定議程有即時口譯及專業逐字稿服務，但 ICANN70 期間所有議程都開啟 Zoom 即時逐字稿功能。雖可能未盡準確，但亦不無小補。

另一方面，所有高關注議題及大會議程也都會同時於 YouTube 轉播，如此一來，受限網路頻寬難以使用 Zoom 的與會者，仍可即

時參與相關議程。

多國代表分享境內資料保護法規

ICANN70 期間原預定舉辦二場大會議程，分別是「政府規範提案討論」及「註冊管理機構自願承諾」。「政府規範提案討論」場次本預計由歐盟及美國代表分享境內規劃中的網路規範法案，可惜最終因與談人時間難以配合而取消。

不過，DNS Women 在 ICANN70 期間舉行了類似的議程，邀請多國代表分享境內的資料保護法規。議程中分別請到來自澳洲、美國、阿根廷、墨西哥、巴西的代表，在顧及 ICANN70 做為拉丁美洲地區會議初衷的同時，亦充分展現 ICANN 社群的多元性。

議程首先由來自澳洲的 Holly Raiche，分享澳洲的網路平臺競爭規範經驗。澳洲競爭及消費者保護委員會（Australian Competition and Consumer Commission，ACCC）於 2019 年發布《數位平臺調查》結案報告，其中針對隱私保護提出的建議包括：強化澳洲隱私法中的個資保障、大幅改革現有的澳洲隱私法、制定數位平臺隱私法規，以及對嚴重的侵犯隱私行為訂定罰則。

來自阿根廷的 Romina Cabrera 則分享阿根廷的隱私法制現況。他表示疫情導致電子貿易蓬勃發展，亦間接帶動人們對個資保護、隱私法規的重視。他強調，數位發展會帶動人們對資料、隱私、線上交易的理解持續進化，這也表示隱私法規應與時俱進，在制定法規的同時，應保障人權、加強意識教育，並確保過程的開放透明。

Karla Valente 則介紹美國現況。美國並沒有聯邦規格的統一資料保護法，資料保護的相關法條散見於消費保護、兒童保護、公平交易，或各州內部的資料保護法規。但美國政府已意識到聯邦層級資料保護規範的重要，可以期待 2021 年出現相關法規。

他也分享資料保護法規的全球趨勢，包括資料保護官的設置、針對違法行為的罰則加重、企業組織開始重視隱私保護、「知情同意」的概念成為原則，以及越來越多針對資安事件因應對策最佳做法的討論等。

墨西哥代表 Fatima Cambronero 分享該國的資料保護法規現況。在 2010 年前，墨西哥的資料保護法規情境與當今美國相同，缺乏由中央政府統一頒布的資料保護規範，僅有各州自行設立的法規。2017 年墨西哥頒布全國通用的《個人資料保護法》。

此法將個人資料分成三種類型，包括基本個資、特殊個資，以及敏感個資。法中對資料控管者的規範雷同 GDPR，雖然墨西哥法律沒有 GDPR 著名的「被遺忘權」，但有類似的「被刪除權」：資料主體可主張自己權益因資料控管者疏失受損，資料控管者將因此挨罰。另一方面，該法也禁止 WHOIS 揭露註冊人的個人資料。

來自巴西的 Vanda Scartezini 分享巴西情形。巴西的《資料保護法》（Lei Geral de Proteção de Dados，LGPD）自 2020 年 9 月開始實施，罰則將於今年 8 月生效。LGPD 的原則大致與 GDPR 相同，但仍有幾處重要差異。首先，由於巴西憲法禁止「匿名」，LGPD 沒有 GDPR 的「被遺忘權」。除此之外，LGPD 中也缺乏如「資料主體有權限制資料控管者的資料處理範圍」及「資料主體有權拒絕資料自動處理」等規範。

另一方面，在法律適用範圍（全球適用）、要求企業組織設置資料保護負責人，以及高額罰金（2%年度收入，最高可罰至 5 千萬里約）等規範，則與 GDPR 非常類似。

大會議程：註冊管理機構自願承諾

由於另一場大會議程因故取消，ICANN70 僅剩一場大會議

程，討論主題是 new gTLD 申請流程中的「註冊管理機構自願承諾」（Registry Voluntary Commitments，RVC）。

有別於 2013 年更新的基本註冊管理機構協議（Base Registry Agreement）中，規定所有 new gTLD 註冊管理機構在發放特別管制 TLD 前，須查核申請人身分的「強制公共利益承諾」（Public Interest Commitment，PIC）條款；2012 年申請流程中的「自願性公共利益承諾」（Voluntary PIC），供註冊管理機構任意列出「自願遵守」的承諾。

這種自願性的 PIC 非出自於 ICANN 社群正規的政策制定流程，ICANN ORG 在新增此條款前，也從未徵詢社群意見。也因此，自願 PIC 缺乏相關規範及稽核程序，常被註冊管理機構用來不合理的擴權，藉此傷害註冊人權益，甚至當成賺錢的工具。

負責檢視 2012 年 New gTLD 申請指南、檢討申請流程的 New gTLD 申請政策制定流程（New Generic Top-Level Domain（gTLD）Subsequent Procedures Policy Development Process，SubPro PDP）工作小組今年初終於提交結案報告，報告中建議將「自願性 PIC」改為「註冊管理機構自願承諾」RVC，並新增相關規範條件，避免重蹈 2012 年覆轍。

然而，仍有意見質疑自願性 PIC 的價值，事實上，ICANN 董事會去年也曾提醒 SubPro 工作小組，ICANN 在強制註冊管理機構履行合約時不能超過 ICANN 使命範圍。舉例而言，若註冊管理機構在 RVC 中提出關於網站內容的承諾，則由於 ICANN 無權干涉內容，可能導致履約執行上的困難。

即使 SubPro 結案報告已通過 GNSO 理事會並抵達董事會，社群對 RVC 仍有強烈的不同意見。最主要的爭議在於：註冊管理機構雖有權提出 RVC，若 ICANN ORG 作為簽訂合約的甲方無法執行 RVC 條款，則 RVC 將僅是紙上談兵。究竟應如何確保 RVC 確實執

行？有意見認為 ICANN 不應該執行超出 ICANN 使命的 RVC。如何在確保 RVC 符合公共利益、滿足反對者顧慮的前提下，仍能充分執行？議程請到董事會、註冊管理機構、一般使用者、非企業團體、ICANN 履約部門及智慧財產權團體代表，分別就各自立場發言。由於議程安排方式，發言者皆僅重申立場，可惜未能激發不同立場之前的互動對話。

董事會公開會議重要決議

如同每次 ICANN 會議，ICANN70 亦以公共論壇（Public Forum）後緊接著公開董事會議作結。公共論壇中的發言大致集中於幾個議題，政策議題如剛結束的 SubPro、註冊資料服務、熱門議題 DNS 濫用，其他社群關心的則是何時重啟實體會議，如何避免社群倦怠疲乏，以及在缺乏實體會面機會下，怎麼持續吸引新血加入 ICANN 等議題。

ICANN70 的 ICANN 董事會公開會議中，通過以下三項重要決議：

- 接受安全及穩定諮詢委員會（Security and Stability Advisory Committee，SSAC）第二次組織審核執行結案報告。
- 接受域名衝突分析專案（Name Collision Analysis Project，NCAP）研究一（Study 1）報告，繼續進行研究二（Study 2）
- 啟動「非公開註冊資料標準化存取／揭露系統」（System for Standardized Access/Disclosure to Non-Public Registration Data，SSAD）執行設計流程（Operational Design Phase，ODP）

詳細決議內容及緣由說明可參考董事會決議網頁。

ICANN71 精華回顧

國際瞭望 撰輯

https://blog.twnic.tw/2021/07/07/19198/

ICANN71 線上會議已於今（2021）年 6 月 17 日圓滿落幕。本會議原訂於荷蘭海牙舉行，這已經是第 5 場因 COVID-19 疫情而改成全程遠端的 ICANN 會議。ICANN71 屬於政策論壇（Policy Forum），會議主要目的為供社群成員討論並推進政策工作，故議程安排亦以政策發展流程（Policy Development Process，PDP）相關議程為主，另有 3 場大會議程，討論社群共同選出的高關注議題。會議期間也宣布本年度的 ICANN 社群傑出獎（ICANN Community Excellence Award）得主。

政策發展流程（PDP）相關議程

- **通用頂級域名註冊資料臨時條款加速版政策制定流程第二階段** A（Expedited Policy Development Process on Temporary Specification for gTLD Registration Data Phase 2A，**簡稱** EPDP P2A）

為徹底研議 EPDP 第二階段未及探討的議題，若干 EPDP 工作小組成員要求通用域名支援組織（GNSO）理事會延伸第二階段，啟動第二階段 A（EPDP P2A）流程。EPDP P2A 將針對：（1）是否應區分註冊人資料屬於法人或自然人，並揭露法人資料；（2）同一註冊人的多筆註冊資料採用同一筆匿名電子郵件信箱的可能性，提出政策建議。

EPDP P2A 工作小組已於今年 6 月 3 日發布初步報告，並開放

徵求公眾意見。報告中提出 5 項初步建議，但這些建議皆尚未通過小組共識決議。在每項建議下，小組也提出衍生問題徵求社群反饋，希望來自社群的建議，可以協助小組在未來撰寫結案報告時，找到更明確的方向。

- 議程連結：
  https://71.schedule.icann.org/meetings/oz6vrh2dXs9GkymW

- **國際化域名加速政策發展流程（**Expedited Policy Development Process for Internationalized Domain Names，IDN EPDP**）**

GNSO 理事會今年 5 月底決議成立國際化域名加速版政策發展流程（IDN EPDP）。本工作小組的任務是針對（1）所有通用頂級域名（gTLD）的定義及異體字（variant）的管理方式，以及（2）如何更新合約方須履約遵守的 IDN 實施指南 4.0 版提案，向 GNSO 理事會提出政策建議。

在 ICANN71 的推廣議程中，ICANN 職員 Pitinan Kooarmornpatana 介紹 ICANN 中的 IDN 發展，長期參與 ICANN 內 IDN 相關工作流程的社群成員 Akshat Joshi 及 Edmon Chung，也分別說明何謂「根區標籤生成規則」（Root Zone Label Generation Rules，RZ-LGR），以及 IDN 異體字的議題。目前此 EPDP 正在招募參與者及觀察員，詳情可參考此文章。

- 議程連結：
  https://71.schedule.icann.org/meetings/TZvWRhnydWDPSE64v

- **轉移政策審核（**Transfer Policy Review**）**

GNSO 今年 2 月，啟動審核域名轉移政策的二階段政策發展流程（PDP）。本 PDP 的主要任務，是檢視、評估是否需修正既有的域名轉移政策，讓受理註冊機構或註冊人間的域名轉移流程更方便、安全、有效率。

工作小組於 ICANN71 期間舉行工作會議，會議討論聚焦於本 PDP 的主要目標，包括原本的四大目標：

- 容許註冊域名持有人將域名轉移至其他服務供應業者，增加消費者選擇及競爭。
- 確保受理註冊機構間域名轉移政策（Inter-registrar transfer policy，IRTP）的保護措施，足以防止域名轉移詐騙或域名劫持（domain hijacking）。
- 釐清 IRTP 文字，確保 ICANN 驗證受理註冊機構對政策的理解及實踐一致。
- 釐清域名轉移爭議解決政策文字，確保仲裁方及審查委員對政策的理解及實踐一致。

以及小組開始工作後，新增的二個目標：

- 網域名稱系統安全擴充（Domain Name System Security Extension，DNSSEC）具減緩域名劫持的效果。工作小組應釐清 DNSSEC 在域名轉移中扮演的角色，並制定相關守則。
- 對註冊人而言更好用、有效的域名轉移方式。

o 議程連結：
https://71.schedule.icann.org/meetings/MRRdeaFX8gLWGzZan

大會議程

- 法律規範對 ICANN 政策議題的影響

本議程請到政府機關代表，介紹涉及網際網路運作的法規草案。首先由歐盟執委會代表 Olivier Bringer 簡介歐盟內涉及 DNS 的二則法規草案：《網路與資訊系統安全指令》修正提案（Revised Directive on Security of Network and Information Systems, NIS 2 Directive）及數位服務法（Digital Services Act，DSA）。

接著，歐盟議會代表 Alexander Sege 則是介紹將增修於《布達佩斯網路犯罪公約》（Budapest Convention）中，聚焦加強跨部門協作及電子證據揭露的協定草案，草案中第六章〈要求域名註冊資訊〉很可能與 ICANN 有關。

除了法案介紹，來自根伺服器安全諮詢委員會（RSSAC）、GNSO、一般使用者諮詢委員會（ALAC）及國碼域名支援組織（ccNSO）的代表，也探討 ICANN 的多方利害關係治理模式與國家或地區法規對 ICANN 政策的影響拉鋸，同時回顧 GDPR 與 WHOIS 的衝突，分享應如何汲取教訓、為未來做好準備。

- 議程連結：

  https://71.schedule.icann.org/meetings/gcLZWTBtkzuM3cXug

- ICANN **多方利害關係模式**及**網路治理生態系統**

本議程分為二部分，首先由 ICANN 社群內部各團體推派代表參與座談，說明各自團體的功能及參與 ICANN 的目標，也分享在疫情肆虐下缺乏實體會議的過去 18 個月，眾人參與 ICANN、從事政策制定工作受到哪些影響。與談人亦暢談 ICANN 多方利害關係治理模式的優缺點，各自提出理想做法、改善建議，以及對 ICANN 社群的期許。

第二部分則請到對 ICANN 具備深厚了解，但參與重心並非 ICANN 的外部人員，分別是前 ICANN 董事、目前任職網際網路協會（Internet Society，ISOC）戰略規劃公關資深總監的 Rinalia Abdul Rahim，以及外交基金會（DiploFoundation）創辦人 Jovan Kurbalija，分享他們對 ICANN 的觀察，也針對 ICANN 的組織及運作方式提出客觀的建議。

- 議程連結：

  https://71.schedule.icann.org/meetings/Ws3N7bsspep4Nk4Nw

- **了解封鎖名單資料庫**

最後一場大會議程以「封鎖名單資料庫」（Reputation Block List，RBL）為主軸，與談人包括 RBL 營運人員、ICANN 技術長辦公室（OCTO）安全、穩定及靈活性（SSR）部門研究人員，以及 ICANN 社群代表（註冊管理機構、受理註冊機構、一般使用者）。

RBL 營運業者分享他們如何蒐集資料、維護資料庫，也解釋各種資料性質及處理脈絡的不同。他們強調 RBL 只是資料庫，使用者如何擷取、解讀並呈現資料，才是決定資料代表意涵的關鍵。ICANN OCTO 代表，同時也是域名濫用報告系統（Domain Abuse Activity Reporting，DAAR）專案負責研究人員，Samaneh Tajalizadehkhoob 博士則解釋 DAAR 如何選擇及使用 RBL，她也同意上述觀點，指出資料的意涵取決於解讀的角度。

註冊管理機構及受理註冊機構身為域名營運管理方，與 RBL 營運方有微妙的關係：他們可能因 RBL 而發現轄下域名的異狀，有時則必須要求 RBL 撤除被列入封鎖名單的轄下域名。域名管理方最重視的，是 RBL 的資料來源、處理方式是否透明負責。一般使用者也將大幅受益於來源流程透明公開的 RBL，這不僅增加 RBL 本身的可信度，也能進一步協助使用者正確理解、判讀 RBL 資料代表的實際意義。

- 議程連結：
  https://71.schedule.icann.org/meetings/WGNGP5GJupYJrCnXo

2021 年 ICANN 社群傑出獎（ICANN Community Excellence Award）

本年度 ICANN 社群傑出獎共有二位得主，分別是 Marilyn Cade 及 Rafik Dammak。

Marilyn Cade 是 ICANN 元老成員之一，自草創時期便積極參與

ICANN。她曾擔任 GNSO 理事、企業利害關係團體執行委員、提名委員會（NomCom）委員，以及多個跨社群工作小組成員。她對於為 ICANN 社群招攬新血充滿熱情，也對 ICANN 的英才計畫（Fellowship program）及線上學習課程（ICANN Academy）貢獻良多。Marilyn Cade 已於去年 11 月與世長辭，她溫暖、活躍、總是面帶笑容的身影，將永存我們心中。

Rafik Dammak 在過去十多年來，始終勤勉參與 GNSO 及各種跨社群工作小組。他曾擔任 GNSO 理事會副主席、非營利利害關係團體執行委員、EPDP 工作小組副主席，也參與 NomCom。由於定居於亞太地區，Rafik 常需在非工作時段參與各種會議，而他為 ICANN 工作付出的時間及精力，社群有目共睹。他在主持各方意見強烈對立的工作小組時，仍能保持中立、不帶入個人或自身團體立場的專業態度，也是獲選的一大原因。

ICANN72 精華回顧

國際瞭望 撰輯

https://blog.twnic.tw/2021/11/29/21017/

ICANN72已於2021(今)年10月28日落幕,這也是自COVID-19疫情以來，第 6 次全面線上舉行的 ICANN 會議，共有來自 156 個不同國家、1,305 名與會者遠端參與。根據 ICANN ORG 分享的統計資料，13.8%與會者來自非洲地區、22.1%來自亞太地區、7.63%來自拉丁美洲加勒比海地區、20.8%來自歐洲地區；來自北美地區的參與人數比例最高，共占全體與會人數的 35.6%。

綜觀 ICANN72 會議中討論，有三大議題特別受到社群重視，以下分別就此三大議題，簡記 ICANN72 的社群討論重點。

國際化域名（IDN）及全球通用（UA）

第一個議題，是國際化域名（Internationalized Domain Name，IDN）及全球通用（Universal Acceptance，UA）。

目前，ICANN 社群中負責制定政策的二大支援組織，國碼域名支援組織（country code Names Supporting Organization，ccNSO）及通用域名支援組織（Generic Names Supporting Organization，GNSO），都有進行中的 IDN 政策制定流程。

ICANN 董事會在 2019 年決議通過 IDN 異體字頂級域名（top-level domain，TLD）標籤發配規則時，也要求 GNSO 及 ccNSO 未來在制定 IDN 相關政策時，除參考上述規則，也應定期互通有無，確保通用頂級域名（generic top-level domain，gTLD）與國碼頂級域名（country code top-level domain，ccTLD）的 IDN 政策中，關

於異體字的處理方式保持一致。

目前 ccNSO 的政策發展流程（Policy Development Process，PDP）ccPDP4，就是在處理 IDN 議題。ccPDP4 有二大主要任務，分別是制定 ccTLD 的異體字管理規則，以及 IDN ccTLD 的淘汰流程。

GNSO 內的 IDN 政策流程，則為省略議題報告的加速版政策發展流程（Expedited PDP，EPDP），首要任務也是制定 IDN gTLD 的異體字管理規則，另外也將檢視 IDN 實施指南 4.0 版提案，並提出修訂建議。

過去二十幾年來，域名系統（Domain Name System，DNS）因 new gTLD 及 IDN 的推出而持續擴張。目前市面上有超過 1,200 筆 new gTLD，其中也有使用不同文字、字符，長度不一的各種字串（如：.дети、.london、.engineering），除此之外，更有超過 60 筆 ccTLD 都有自己語言的 IDN。

然而，目前仍有許多應用程式、裝置或系統不支援使用 IDN 的域名或電子郵件信箱。全球通用（UA）的終極目標，就是希望使用不同語言文字的域名及電子郵件，都能獲得一樣的待遇，使用者得以自由選擇域名或信箱的語言。

全球通用推廣小組（Universal Acceptance Steering Group，UASG）由相信 UA 重要性的社群自發組成，除定期發表研究報告，也積極招募 UA 大使，希望觸及更廣大的網路社群，提高 UA 的公共認知。UASG 自 2017 年起開始系統性蒐集、彙整 UA 相關統計數據及量測資料，希望更精確掌握全球 UA 現況。

目前 unicode@ASCII.ASCII 的全球接受比例僅約 14 至 15%左右。許多評論認為 IDN 將主導下一回合 new gTLD 申請，然而這樣的 UA 表現，實在難說服申請人勇於大量申請 IDN 域名。有鑑於此，UASG 近期也積極改變推廣策略，希望招募更多對 UA 議題有基本了解，具備人脈網路、地區影響力的人士，不僅將 UA 的重要性帶

出 ICANN，更動用力量，讓科技產業了解 UA 的重要性。

- ICANN72 相關議程：

  GNSO EPDP on Internationalized Domain Names

  DNS Women: Universal Acceptance – Where Are We Today

DNS 濫用

自 2019 年底的 ICANN66 蒙特婁會議開始，DNS 濫用已成為 ICANN 會議的常駐議題。本次會議中，許多不同利害關係團體也針對 DNS 濫用展開諸多討論。

合約方（Contracted Party House，CPH）[1]就利用本次會議，與社群分享他們近期為防治 DNS 濫用的自發性工作，包括新發布的報告及白皮書等。

在諸多建議報告中，最受社群關注的是合約方今年 10 月甫發布的「信任通報人框架」（Trusted Notifier Framework）。

其實不少註冊管理機構及受理註冊機構都早有仰賴信任通報人，以處理 DNS 濫用或內容濫用的做法。本框架只是合約方提出的自發性指導原則，供希望開始招募信任通報人的合約方參考。框架中列出信任通報人須符合的條件，建議與信任通報人之間的關係應留有紙本協議證明，並訂出通報流程。

在政府諮詢委員會（Governmental Advisory Committee，GAC）的 DNS 濫用議程中，任職於日本總務省的 Masamichi Takeda 分享域名濫用方常用的「受理註冊機構跳轉」（registrar hopping）手法。簡單來說，域名註冊人會在註冊域名遭通報濫用後，迅速跳轉到另一個受理註冊機構，並以此類推。日本執法機關認為，這種情況下不

[1] 由 gTLD 註冊管理機構及受理註冊機構組成，因與 ICANN 有合約關係，統稱為合約方。

僅註冊人能輕易逃逸，受理註冊機構也因此樂於撇除查證濫用註冊人的身分，嚴重妨礙域名安全執法工作。

ccNSO 在 ICANN72 也特別安排了二場議程討論 DNS 濫用議題，重點放在 ccNSO 是否應更積極參與 ICANN 的 DNS 濫用社群討論及作為。

其實，ccNSO 始終密切關注安全議題，內部也有許多 DNS 濫用相關作為及討論，部分 ccNSO 成員也簽署了合約方提出的 DNS 濫用框架。在討論中，不少成員鼓勵同儕加入 ICANN 的域名濫用活動報告（Domain Abuse Activity Report，DAAR）系統，不僅因為越多資料越有助於濫用分析及防治，ccTLD 營運方也將因此更全面掌握旗下域名的濫用情形。

然而，ccNSO 成員也強調，ccTLD 及 gTLD 的屬性截然不同，不同 ccTLD 的規模相差極大，且大部分與 ICANN 之間並未簽署託管（delegation）合約，也不一定與當地政府有正式關係，但身為 ccTLD 營運方，與國內 CERT 打好關係至關緊要。

- ICANN72 相關議程：

  GNSO: CPH DNS Abuse Work Group Community Update

  GAC Discussions: DNS Abuse Mitigation

  ccNSO: DNS Abuse – What's the role of the ccNSO? (1 of 2)

  ccNSO: DNS Abuse – What's the role of the ccNSO? (2 of 2)

更包容、平等參與的混合模式 ICANN 會議

ICANN72 唯一的一場大會議程，聚焦於社群最殷切期待的議題：何時 ICANN 才能重返實體會議？雖然名為「混合模式」會議，但與會者最在乎的無非是「混合」中的「實體」元素。本議程請到許多今年已嘗試「混合模式」的網路治理相關組織，針對如何儘量

縮小現場及遠端的與會體驗差異，以及了解影響與會者選擇實體或線上參與的主要因素，並就此調整議程安排等，分享自身經驗同時提出建議。

議程中，ICANN ORG 代表 Ashwin Rangan 也分享，ICANN 如何確保來自全球各地的所有人，無論使用何種裝置、網路連線品質如何，都能平等參與會議。目前 ICANN 在考慮的未來改善方向還包括啟用更多新的互動工具，如線上白板 Jamboard，也在思考整合會議網站及 ICANN 專屬社群媒體平臺的可能。

未來若以混合模式舉行 ICANN 會議，他們也規劃在實體會議場地設立多角度攝影機，如此一來，線上參加的與會者也更能身歷其境。強制要求現場參與者都登入數位參與平臺，也是確保所有與會者之間交流互動最大化的關鍵。

最後開放的社群討論時間中，ICANN 董事長 Maarten Botterman 表示，非常理解大家都迫不及待重啟實體會議的心情，但 ICANN 會議規劃仍須以所有人的健康安全為第一優先。他強調，即使明年真的舉辦實體會議，會議場館也將採取嚴格防疫措施，包括強制配戴口罩、需出示疫苗證明，進出場館需量測體溫等。

- ICANN72 議程：

  Plenary Session: Designing Hybrid ICANN Public Meetings to Equalize In-Person & Remote Participation

加密技術正身陷危機

國際瞭望 撰輯

https://blog.twnic.tw/2021/05/21/18330/

現在，全球大部分的訊息都是以端對端（end-to-end）加密的方式傳送。然而，世界上越來越多國政府的立法行動，正為這個保護使用者隱私的技術帶來巨大危機。

許多歐盟國家政府希望科技公司「開後門」，破解自身加密技術並提供資訊給執法機關。在印度，政府要求 WhatsApp 提供另一種技術來追蹤使用者在應用程式中傳送的訊息。巴西的最高法院很快會對 Facebook 提出的上訴做出判決，判決結果無疑將決定該國政府對加密技術的施政方針。這些案例都很可能改變網際網路發展的方向。

本文作者為 WhatsApp 執行長，他指出，為使用者提供的端對端加密服務，理應連企業自身都無法破解。唯有如此，使用者的私人對話才能受到真正的保護。雖然有些政府單位是真心想打擊犯罪，而對方因此認為端對端加密妨礙他們的辦案效率，希望破解或繞道取得資料也情有可原。但作者強調，無論是過去或現在，人與人之間的私下談話本來就應受隱私保障。難道只因為對話從實體空間移至線上傳輸，政府就有權力竊聽、取得這些隱私內容嗎？只因為某些行為拜科技之賜成為可能，不代表我們就應該從事這些行為。

另外一個不該為政府破例的理由很簡單：凡在系統中開了一扇後門，系統就因此多了一個可利用弱點。已有無數的慘痛經驗可以證明，沒有任何後門是安全的。瞻博網路公司（Juniper Networks）

就是最好的範例：該公司路由軟體中為了美國政府方便刻意設置的弱點，日後被揭露成為外國駭客入侵的關鍵。

作者重申，無論原始意圖再正直、再無害，任何企圖「繞道」隱私的手段都只會導致更糟的結果。我們已經見識過現代科技如何在賦予人民發聲管道的同時，反被許多國家政府利用以監控、鎮壓不同意見。堅持守護隱私為基本人權，是我們持續保護自己免於淪為新興科技受害者的重要防線。

參考資料：

https://www.wired.com/story/opinion-encryption-has-never-been-more-essential-or-threatened/

全球數位稅的展望及挑戰

國際瞭望 撰輯

https://blog.twnic.tw/2021/05/17/18256/

數位稅基本概念及目前推動情形

近來數位稅（Digital tax）的議題在國際政壇上風起雲湧，起因是COVID-19疫情使數位經濟發展更趨蓬勃，連帶使Apple、Facebook及 Amazon 等科技企業大量獲益，歐美各國也開始討論，該如何針對這些科技巨頭進行課稅。由於各國法規訂定難以追上數位服務的日新月異，導致政府損失重大財政收入來源[1]，各國因數位商業模式的變革決定研擬課徵數位稅，經濟合作暨發展組織（Organization for Economic Cooperation and Development，OECD）自 2012 年起也開始針對數位稅研擬相關立法，同時欲建構一個全球適用的數位稅徵收標準，法國亦在 2019 年通過了徵收數位稅的法案。

OECD 於去（2020）年 12 月警告[2]，目前全球數位稅爭議已進入白熱化階段，若徵收全球數位稅，可能使全球 GDP（國內生產總值）每年削減超過 1%。目前全球數位稅的推動仍缺乏共識，若各國在數位稅的政策層次上各自為政，可能會進一步導致貿易衝突。數位稅推動的困難之處在於世界各國的接納程度、數位利潤分配模式、數位企業種類識別、數位稅之課徵是否影響他國投資意願，以及美國課徵意願等議題[3]。此外，企業可能會以被課數位稅

1 林琮紘。〈淺談各國與我國數位稅課徵模式〉。科技政策研究觀點。2020/02/05

2 Silvia Amaro. Digital tax conflicts could wipe more than 1% off global GDP every year, OECD warns. CNBC. 2020/10/12

3 林琮紘。〈淺談各國與我國數位稅課徵模式〉。科技政策研究觀點。2020/02/05

為由提高服務價位，目前部分基本人權也透過數位方式實施，例如提供教育服務的線上平臺，若要針對這類服務課稅，可能涉及社會正義的議題。

目前許多國家都已實施數位稅方案，但其制度設計及徵收門檻各有不同[4]。例如，奧地利僅針對數位廣告課徵稅收，而波蘭僅對媒體服務課稅，土耳其課稅項目較廣泛，包括廣告、中介活動及銷售用戶個資。印度將針對收入超過 26 萬美元的外國企業課稅，但肯亞卻沒有任何門檻。同時，多國也針對支付服務、數位內容以及企業內部服務等項目採取數位稅豁免措施。

OECD 的目標是凝聚各國對於推動數位稅的共識，因疫情之故，各國僅能進行遠端會議，美國也於去年 6 月退出談判。原本 OECD 的目標是於 2021 年中之前達成協議[5]，但目前看來卻是困難重重。根據美國稅政智庫 Tax Foundation 發布的報告[6]，數位稅的課徵應以消費稅為基礎，課徵對象是數位經濟活動，在數位稅的議題上，各國應追求共同的稅率基礎及針對遠端數位交易的通用標準，避免因歧異產生齟齬。鑒於數位活動的跨國性，弭平各國課稅歧見是全球數位稅能否順利徵收的關鍵，在共識未成的情況下，國際爭議及企業反彈可能層出不窮。

跨境課稅爭議：美法衝突及跨國科技企業看法

目前，法國的數位稅法案適用於任何透過「數位活動」獲取營收高於 7.5 億歐元的全球性科技巨頭，以及營收高於 2,500 萬歐元

[4] Amie Ahanchian, Donald Hok, Philippe Stephanny, Elizabeth S. Shingler. Digital Services Tax: Why the World is Watching. Bloomberg Tax. 2021/01/06

[5] Silvia Amaro. Digital tax conflicts could wipe more than 1% off global GDP every year, OECD warns. CNBC. 2020/10/12

[6] Daniel Bunn, Elke Asen, Cristina Enache. Digital Taxation Around the World. Tax Foundation.

的法國本土數位科技公司[7]。法國數位稅特別針對二種企業，其一是扮演中間人的數位商場，它負責連結顧客及企業，例如：Amazon；其二是投放網路廣告的企業，特別是使用個資以投客戶所好發送廣告的平臺，例如：Google 及 Facebook。目前，英國、義大利及西班牙也正規劃該國版本的數位稅。

在 2020 年底，法國根據其數位稅法案，要求美國科技公司 Facebook 及 Amazon 繳交數位稅，此舉激怒[8]了美國，美國認為法國違反公平貿易原則，且 Facebook 及 Amazon 的企業總部都設在美國。美國前總統川普認為只有美國能對美國企業課稅，因此，美國也打算對法國產品課以全額關稅作為報復手段。今年一月，二國元首已進行談話並促成二國暫停爭議，美國也暫緩對法國課徵報復性關稅[9]，然而，只要雙方一天未達成協議，相關爭議仍有可能持續發生。

數位稅代表的是將當代網路經濟價值及成果重新分配的一種手段[10]，其中涉及複雜的政治經濟學及正義課題，作為被課稅的一方，大型跨國科技企業也有可能對此反彈。

在法國政府準備針對美國科技業課稅之際，美國全國商會（U.S. Chamber of Commerce）表示，法國的數位稅制度每年將創造約 5 億歐元的稅收，但大部分都由美國企業支付。當時諸多大型科技企業的主管警告[11]，徵收數位稅會導致成本提高，且數位稅還包括溯及

---

7 Kay Ko. 開第一槍！法國今年向 Google 等科技巨頭開徵數位服務稅。INSIDE. 2020/11/27

8 France demands digital tax payments from US tech groups. Financial Times.

9 顏嘉南。法緩徵數位稅 歐美貿易戰暫休兵。工商時報。2020/01/22

10 Jim Tankersley. How Tech Taxes Became the World's Hottest Economic Debate. The New York Times. 2020/10/12

11 中央社（2019 年 8 月 20 日）。〈法國推數位稅，美科技業批破壞稅制不公平〉。科技新報。

既往的原則，也不符合法學原理，且數位稅的課稅對象及標準目前仍多所爭議。有鑑於此，美國資訊技術產業委員會（Information Technology Industry Council，ITIC）的副總裁 Jennifer McCloskey 也贊成數位稅應在多邊架構下達成協議，以杜絕爭議。

數位稅發展前景

綜上所述，因跨境課稅爭議及科技企業的疑慮，未來數位稅的推動及實施仍在未定之天。在 2020 年 TWIGF 年會[12]上，目前任教於國立臺灣大學政治學系的蘇翊豪助理教授指出，數位稅課徵目標是數位經濟活動，而許多數位經濟活動無實體工廠，因此與過去的課稅方式必然有所差異，國家主權已無法管理跨國企業並確保公平租稅，全球數位稅的倡議也由此產生。

歐盟主席范德賴恩（Ursula von der Leyen）在去年 9 月發表談話[13]，若全球數位稅的徵收仍缺乏共識，那歐盟將在今年初提出自己的版本，針對在歐盟經營數位經濟的企業課稅，此舉已受到國際關注。

數位稅也可能被用於國際戰略，現在是數位經濟當道的年代，在各國各自課徵數位稅的脈絡下，數位稅可能被策略性的用於貿易衝突甚至貿易戰，前段所提及之美法跨境課稅爭議便是一例。國際數位稅是否能順利推動，有賴未來國際組織及各國及科技企業的協調，才能減少課稅爭議乃至貿易報復之情形。

---

[12] 年會影片連結可至 TWIGF 2020 臺灣網路治理論壇觀賞。

[13] Natasha Lomas. Europe will go it alone on digital tax reform in 2021 if it must, says EU president, as bloc directs €150BN in COVID-19 relief toward cloud, AI and broadband. TE. 2020/09/16

網路犯罪審判權（國際管轄權）之衝突及調和

文／NII 產業發展協進會法務副理 鍾欣紘律師

https://blog.twnic.tw/2021/06/23/18952/

審判權是什麼？

當刑事案件歷經檢察機關偵查、起訴，並將案件移交到法院審理後，法院並不會直接進入到被告所為行為之犯罪構成要件檢驗（實體事項），而是會優先就承審法院是否具有該案件審判權、管轄權等程序事項進行審查，也就是法院受理案件後，關於審查之順序，應遵循「先程序、後實體」原則，如果法院跳過了程序事項審查的步驟，而直接進行案件的實質審理，到最後發現法院明明沒有審判權而無受理之權限，卻一時不察而直接下了判決，依照刑事訴訟法第 379 條第 1 項第 5 款規定，該判決當然違背法令，而得作為上訴第三審[1]之法定事由。

但並不是每個案件都需要聚焦在判斷審判權的有無，若案件之行為人、被害人、行為地或結果地等，未與外國產生聯繫（數個司法管轄權），此時就不須於此程序事項上耗費太多時間。舉例來說，某甲在臺北車站持槍朝某乙射擊，導致某乙身受重傷，送往醫院急救後仍不治身亡，此時某甲涉及的《刑法》第 271 條第 1 項殺人罪，

[1] 依據《刑事訴訟法》第 252 條第七款規定：「案件有左列情形之一者，應為不起訴之處分：……七、法院對於被告無審判權者。」；同法第 303 條第六款：「案件有下列情形之一者，應諭知不受理之判決：……六、對於被告無審判權者。」所以案件會經過檢察官、原審法官，其實要因為無審判權而上訴到三審並沒有那麼容易。

由於此案件發生於我國境內，且行為人及被害人皆為我國籍，所以承審法院就毋庸在「是否有刑事審判權」進行過多的著墨。

該如何判斷國家是否有審判權？

審判權屬於國家主權一部中的司法權之行使，性質上屬於國家的高權（或主權）行為，乃在彰顯國家主權之行使及維持，故欲判斷法院是否具有審判權，亦即國家是否可以對特定案件進行審判，需先考量的是國家是否有處罰犯罪行為人的權力，若特定犯罪行為會受到我國《刑法》的效力範圍所涵蓋，我國有執行刑罰之權力，我國法院亦取得該刑事案件之司法管轄權。

在國際法上，決定國家管轄權的基本原則包含「領域管轄原則」（territorial principle）、「被告國籍原則」（Active Nationality Principle）、「被害人國籍原則」（Passive Nationality Principle）、「保護原則」（Protective Principle），以及「世界法原則」（Universality Principle），此五項原則又稱國際管轄權五原則[2]。其中領土[3]作為國家之客觀構成要件之一，國家原則上可以在領土內行使絕對獨立性及排他性的權力，對其領域內之人、事、物享有並得行使管轄權，此稱為「領土主權」（territorial sovereignty），故除具有外交豁免權[4]外，犯罪之行為或結果，有一在我國領域內者，我國法院對該犯罪當然具有刑事審判權。國際管轄權五原則亦體現於我國《刑法》中，我國刑法

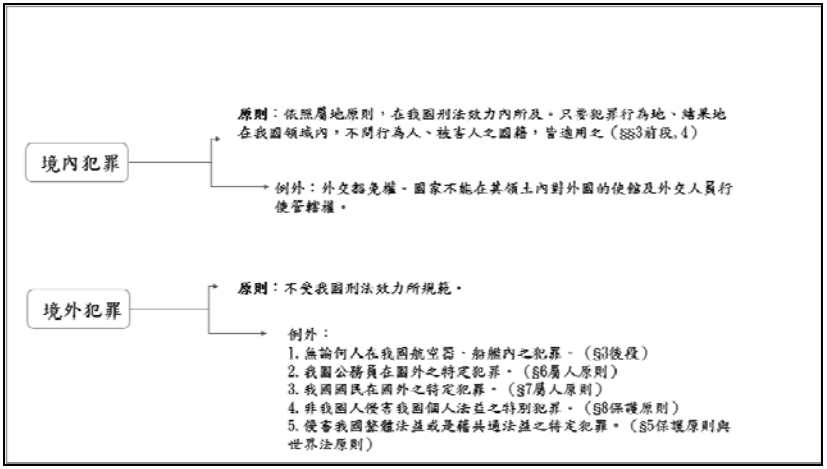
---

2 Khalifa, Abdelmonem Mohamed Magdy. (2020). *Overcoming the conflict of jurisdiction in cybercrime.* Unpublished masters dissertation. American University in Cairo. Dept. of Law, Cairo. Retrieved from https://fount.aucegypt.edu/cgi/viewcontent.cgi?article=1845&context=etds

3 範圍包含領陸（land territory）、領空（territorial sky）、領海（territorial sea）。

4 並不代表具有外交豁免權之人其犯罪行為即不會受到處罰。外交人員如觸犯他國法律，雖駐在國對其並無司法管轄權，但回國後通常仍要接受本國司法機關的調查及相關處置。

適用範圍之相關規定請參見下圖：



網路犯罪之特殊性

隨著網際網路的興起，一方面縮短相隔異地之人的聯絡距離，另一方面又擴大人類生活領域，也改變了犯罪模式。傳統的犯罪行為轉由透過網路進行，例如：網路詐欺、網路賭博[5]、妨害名譽[6]、散播猥褻物品、濫用個人資料、侵害著作權[7]等犯罪，藉由網路具有大量傳播、即時性、匿名性、跨國境、缺乏有效監管等特性，降

[5] 臺灣臺中地方法院（2018 年 6 月 6 日）。臺灣臺中地方法院 104 年度重易字第 1030 號刑事裁定。司法院法學資料檢索系統。檢自 https://law.judicial.gov.tw/FJUD/default.aspx (May 21, 2021)。

[6] 臺灣士林地方法院（2021 年 4 月 8 日）。臺灣士林地方法院 110 年度易字第 187 號刑事判決。檢自 https://law.judicial.gov.tw/FJUD/default.aspx (May 21, 2021)。

[7] 經濟部智慧財產局著作權主題網（2018 年 8 月 14 日）。電子郵件 1070814。檢自 https://topic.tipo.gov.tw/copyright-tw/cp-407-855168-c4cd5-301.html (May 21, 2021)。

低犯罪成本並擴大其犯罪規模，除此之外，也衍生出新興的犯罪問題，例如：阻斷式攻擊、惡意程式等，這些犯罪不會受到行為人或被害人所在位置之限制，與傳統犯罪通常都侷限於一定地域範圍內之特性有所不同。

基於網路犯罪可以不受物理空間限制之特性，網路犯罪時常牽涉數個國家，亦即有複數國家皆得依照前述的國際管轄權五原則，主張對特定犯罪具有管轄權，此時，就會發生積極的管轄權衝突。

舉例而言，阿拉伯聯合大公國的國民甲，在網路上散布電腦病毒，而使包含埃及、奈及利亞的國民造成巨大的經濟損失；新加坡、韓國、菲律賓等國家則因為政府機關大量感染該病毒，衍生成國安危機。若以國際管轄權五原則進行檢驗，阿拉伯聯合大公國基於「領域管轄原則」得行使管轄權；埃及與奈及利亞則基於「被害人國籍原則」亦得行使管轄權；另外，根據「保護原則」，新加坡、韓國、菲律賓等國亦得主張管轄權，然而一個犯罪行為人不可能同時接受五個國家進行審判，基於一事不再理原則[8]，若每個國家都對某甲進行審判、處罰，也會有犯罪遭重複評價之弊，故某甲僅須受一個國家審判。綜上，此時該如何決斷由哪個國家審判，除涉及國家主權之行使、蒐集證據之完整性及便利性外，亦涉及被告人權之保障。

我國實務上，過去曾有法院因為網頁伺服器架設在美國而裁定移轉管轄之前例，若對於跨境網路犯罪管轄之認定，直接適用司法管轄權仍傾向於以領土邊界（territorial borders）作為劃分基礎之傳統管轄概念，似乎又不太合適，如自民國 23 年開始即沿用至今的《刑法》第 3、4 條之規定。故為了避免犯罪者藉由網路無空間限制、可匿名之特性，於我國境外實施犯罪而規避查緝，進而保障人

[8] 全國法規資料庫（1966 年 12 月 16 日）。《公民與政治權利國際公約》。檢自 https://law.moj.gov.tw/LawClass/LawSingle.aspx?PCODE=Y0000039&FLNO=1(May 22, 2021)

民基本權利及解決日益漸增且變化多端的犯罪手段，學理上曾發展出對於網路犯罪之管轄權認定的相關學說，有採「廣義說」：縱使只是單純在網路上設置網頁，提供資訊或廣告，只要某地藉由網路連結至該網頁，該法院即取得管轄權，缺點是幾乎在世界各地均有可能成為犯罪地，涉及各國司法審判權之問題，且對當事人及法院均有不便；有採「狹義說」：強調行為人之住居所、或網頁主機設置之位置，若位於我國則取得管轄權，缺點是過於僵化；亦有倡議應專設「網路管轄法院」，然似乎只聞樓梯響，迄今仍尚未設立。

上開學說固有見地，然多數法院[9]採取「折衷說」立場綜合判斷：應綜合考量管轄法定原則之目的，在於防止利用自由選擇法院而達到間接操控法院判決之結果，藉此保障被告接受公平審判之權利，以及配合網路犯罪之複雜性。亦即，網路犯罪之管轄法院不應過度侷限，且不應過度廣泛認定，尚應斟酌其他具體事件，如設置網頁、電子郵件主機所在地、傳輸資料主機放置地及其他有無實際交易地等相關情狀認定之，由法院進行裁量。

管轄權衝突之解決機制

從另一個角度來看，當有複數國家發生積極管轄權衝突時，評價未必是負面的。試想，若有犯罪發生，卻沒有一個國家去「爭取」對該案件之管轄權，反而會因此造成明明有犯罪發生卻無法被訴追的窘境，此漏洞儼然成為犯罪的溫床、罪犯的避風港，故管轄權之衝突及競合毋寧為跨境犯罪的必然。

---

9 臺灣士林地方法院（2021）。臺灣士林地方法院 110 年度易字第 187 號刑事判決。臺灣彰化地方法院（2021）。臺灣彰化地方法院 110 年度訴字第 226 號刑事判決。臺灣桃園地方法院。臺灣桃園地方法院 109 年度易字第 480 號刑事判決。檢自 https://law.judicial.gov.tw/FJUD/default.aspx (May 22, 2021)。

由於司法管轄權係各國國家主權的高度體現，對於跨國司法管轄權競合衝突問題，原則上仍須考量國家主權平等、共同目標追求、共同管轄及人權保護之目的下，與其他國家進行個案協商。

為了提供處於多重管轄（multiple jurisdiction）之國家間有適當指引，多數國際公約都有處理各國間管轄權衝突之問題規定，例如2001 年 11 月簽署通過《網路犯罪公約》[10]（Cyber-crime Convention）第 22 條第 5 款規定，當締約國發生管轄權積極衝突時，當事國應透過協商、談判尋求解決，但並沒有規定哪個國家的管轄權應該優先，而且，為了避免因消極的管轄權衝突所生之弊病，亦未於條文中規範具體解決方案供依循。

犯罪偵查之困境

除了前述有關審判權之爭議外，跨境犯罪之查緝亦往往使偵查機關傷透腦筋，由於跨境犯罪所涉之行為人、證據通常散落於世界各處，縱使《刑法》對於領域外之特定犯罪或有適用可能，但一國刑事訴追機關之權限有其空間限制，刑事訴追機關之作為涉及國家主權，因此其執行之範圍僅限於該國境內。

為了消弭跨境犯罪對偵查主體所帶來的執法困境，各國間多透過條約建構跨境執法合作網絡，例如我國立法院於民國 110 年 5 月 4 日通過之《中華民國（臺灣）政府與貝里斯政府刑事司法互助條約》[11]，即透過雙邊條約之方式，就有關刑事調查、追溯、法院程

[10] Council of Europe. (2001). Convention on Cybercrime. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (May 22, 2021)

[11] 行政院（2020 年 11 月 5 日）。〈行政院會通過「中華民國（臺灣）政府與貝里斯政府刑事司法互助條約」〉。檢自 https://www.ey.gov.tw/Page/9277F759E41CCD91/483b7fec-cb16-4862-bd3a-3dd011b13ef7 (May 21, 2021)。

序、犯罪防制及相關刑事司法程序相互協助，其中包含取得證據或證詞、提供得做為證據之文書、紀錄或物品、確定案件關係人位置或確認其身分、文書之送達、執行搜索及扣押，以及其他不違反受請求方法律之任何刑事協助等事項進行互助，將可大幅降低跨國刑事調查所面臨之困境。

參考資料：

1. 立法院議案整合暨綜合查詢系統（2021）。檢自：https://misq.ly.gov.tw/MISQ/IQuery/misq5000Action.action （2021/05/21）
2. 全國法規資料庫（2021）。檢自：https://law.moj.gov.tw/ (2021/05/22)
3. 林鈺雄（2019）。《新刑法總則》。元照。
4. 陳靜慧（2018）。《跨境電腦犯罪之司法管轄與發展趨勢～以網路詐欺犯罪為中心》（進修出國報告）。嘉義市：臺灣嘉義地方法院檢察署。

網路空間規範與美俄角力

國際瞭望 撰輯

https://blog.twnic.tw/2021/07/26/19221/

日益熾烈的美俄網路空間衝突

美俄網路空間衝突早已非新鮮事，早在 2016 年，俄國便已試圖介入美國大選[1]，近年來美俄網路空間衝突更為劇烈，情節重大者包括駭人聽聞的 SolarWinds 及 Colonial Pipeline 駭侵案。SolarWinds 駭侵案於去（2020）年底被揭發，是有史以來美國所遭受最重大的網路攻擊事件，駭客目的是竊取美國機密情報，透過這些情報，甚至可左右美國對俄外交決策。

駭客的目標是由 SolarWinds 企業推出，名為 Orion 的 IT 管理軟體，該軟體為 SolarWinds 的主要軟體產品，其客戶多達 33,000 多間企業及美國重要政府機構，因此，該案影響遍及包括美國財政部（Department of the Treasury）、國土安全部（Department of Homeland Security，DHS）、商務部（Department of Commerce）及國防部（Department of Defense，DOD）等重要部門及多達 18,000 間企業[2]。

今年 5 月 7 日發生的 Colonial Pipeline 駭侵案則與 SolarWinds

---

1 John Walcott (2018). Russia intervened to help Trump win election: intelligence officials. 檢自：https://www.reuters.com/article/us-usa-election-cyber-russia-idUSKBN13Z05B (Jun. 16, 2021)

2 Shruti Dhapola (2020). Explained: A massive cyberattack in the US, using a novel set of tools. 檢自：https://indianexpress.com/article/explained/us-solarwinds-hack-cybersecurity-fireeye-russia-7110550/ (Jun. 15, 2021)

性質迥異，駭侵對象是美國燃油管線業者 Colonial 企業，目標是破壞美國關鍵資訊基礎設施並使燃油供應中斷。其幕後主使為 DarkSide 勒索軟體集團，該集團竊取近 100GB 資料並提出勒索，因擔心駭侵範圍變大，Colonial Pipeline 關閉整個系統，導致由德州延伸至紐澤西州長達 8,850 公里的重要燃油管線暫停運作，拜登政府於二日後宣布進入緊急狀態[3]。雖然目前並無證據認定 DarkSide 勒索軟體集團為俄國政府支持的駭客團體，但其使用俄語且可能來自俄國，因此不排除此案與俄國相關。

由於這些事件已對美國構成嚴重威脅，美國政府也開始轉守為攻，除要求國內企業增強網路安全機制及強化國家網路安全戰略外，亦透過外交手段威懾及制衡俄國，並提出增加俄國網路攻擊成本之法案。

美國對俄制裁及外交談判

今年 4 月，拜登總統正式下令，針對 SolarWinds 駭侵案對俄進行經濟制裁[4]，拜登表示其目的並非要加劇二國衝突，而是威懾俄國不輕易遂行網路攻擊，並使二國衝突不致擴大。制裁內容包括：1.針對涉入干擾 2018 年大選的 30 間俄國企業及個人究責；2.驅逐 10 名俄國外交團的官員；3.制裁 6 間為俄國情治單位提供情報的俄國企業；4.自今年 6 月 14 日起，禁止美國金融機構參與由俄國政

[3] Bing, C., & Kelly, S. (2021.5.8). Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed. 檢自：https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/ (Jun. 18, 2021)

[4] Lucian Kim (2021.4.15). U.S. Slaps New Sanctions On Russia Over Cyberattack, Election Meddling. 檢自：https://www.npr.org/2021/04/15/987585796/u-s-slaps-new-sanctions-on-russia-over-cyber-attack-election-meddling (Jun. 18, 2021)

府使用的債券交易。若俄國持續其行徑，美國不排除在未來對俄國進行更嚴厲的制裁措施。

在制裁過後，北大西洋公約組織（North Atlantic Treaty Organization，NATO，簡稱：北約）發布聲明[5]，表示支持並聲援美國對俄制裁。由此可見，對拜登政府而言，對俄施壓不僅能提高俄國遂行網路攻擊之成本，亦能拉近與歐洲盟友的關係。美國主動對俄國制裁的措施，也象徵美國認定 SolarWinds 駭侵案明顯超出傳統網路諜報行動之範疇[6]，並對網路攻擊畫出新紅線：網路行動應適可而止，不應涉及大量公私部門。

拜登於今年 6 月 16 日在瑞士日內瓦與普丁進行的磋商中，美國政府也明列 16 項包括能源部門及水利系統的關鍵資訊基礎設施[7]，明確告知俄國不得對其遂行駭侵。此外，美國參議院也已推出《國際網路犯罪預防法案》（International Cybercrime Prevention Act）[8]，參議員 Lindsey Graham 為該法案起草者之一，他表示法案精神在於增加網路罪犯的犯罪成本，並認為該法案將有助於追捕執行 Colonial Pipeline 及 JBS 駭侵案而被俄國藏匿的網路罪犯。此外，

---

5 NATO (2021.4.23). North Atlantic Council Statement following the announcement by the United States of actions with regard to Russia. 檢自：https://www.nato.int/cps/en/natohq/official_texts_183168.htm (Jun. 21, 2021)

6 Morrison Forester (2021). U.S. Government Responds to SolarWinds Hack, Seeks to Establish New Norms for Cyber Espionage. 檢自：https://www.mofo.com/resources/insights/210419-us-government-responds-solarwinds-hack.html (Jun. 18, 2021)

7 Phil Muncaster (2021). US Warns Russia of Cyber-Attack No-Go List. 檢自：https://www.infosecurity-magazine.com/news/us-warns-russia-of-cyberattack/ (Jun. 21, 2021)

8 Maggie Miller (2021.6.17). Senators unveil legislation to crack down on cyber criminals. 檢自：https://thehill.com/policy/cybersecurity/558982-senators-unveil-legislation-to-crack-down-on-cyber-criminals?rl=1 (Jun. 18, 2021)

即使拜登目前已就網路安全議題與普丁磋商，但 Graham 認為要制止俄國的不當行徑，唯一方法是增加其駭侵或窩藏網路罪犯之成本。

顯而易見，美國已為俄國訂定網路行動之紅線，但制裁及威懾並非遏止網路攻擊的最佳解方。長期以來，美俄雙方之所以於網路空間敵對，除歷史宿怨外，二者對於網路空間規範的迥異想像亦是重大原因。因此，若要簽訂雙邊協議，雙方須建構互信基礎，並就該議題達成共識。

網路空間價值觀：基本差異

過去認為美俄之間無法達成網路協議的原因，在於美國無法採取更具體的威懾政策，逼迫俄國與其達成談判，且俄國絲毫不理會美國的警告，也未承認或證實美國對其發出的指控，展現出一種漠不關心的態度。然而，美國的威嚇僅能短期改變俄國行為，並非長治久安之道，若美俄不就相互觀點差異進行磋商，未來俄國仍不會放棄任何可能的駭侵機會。

哈佛大學貝爾佛中心（Belfer Center）便就此發表論文，論文中分別納入美俄雙方網路空間觀點差異[9]。貝爾佛中心網路安全專案主任 Lauren Zabierek 認為，雙方無法達成協議的原因包括**資訊不對等**與**網路觀念的根本差異**。首先，美國對自己的網路軍事實力開誠布公，但俄國卻從未如此，資訊不對等造成雙方無法溝通。此外，俄國認為國家政府有權控制網路，對俄國而言，在網路上散布反政

[9] Joe Uchill (2021.6.11). How far apart are the US and Russia from agreeing to cyber rules?. SC Media. 檢自：https://www.scmagazine.com/home/security-news/apts-cyberespionage/how-far-apart-are-the-us-and-russia-from-agreeing-to-cyber-rules/ (Jun. 17, 2021)

府言論的異議分子視同罪犯，甚至要求網路平臺移除相關言論[10]。但美國看待網路的基本價值觀是自由主義及人權觀念，二者對於網路犯罪之觀點因此產生極大差異，若欲達成協議，雙方須彌平此認知鴻溝並找出共同利害核心。

近年來，美國已將推廣網路空間中的適切國家行為及民主價值納入國家戰略中，並頻頻指控俄國違反民主侵害人權的種種行徑，而俄國則展現出依然故我不予理睬之態度，因此未來雙方要磨合彼此觀點並達成妥協實屬不易，Zabierek 認為雙方的共同憂懼是針對國內關鍵基礎設施的攻擊，隨著網路攻擊影響力與日俱增，這或許是展開協商的契機。

結語

目前美國及俄國顯然尚未針對網路空間達成任何共識或協議，雙方觀念鴻溝也非一時半刻可解，但隨著網路和平日漸重要，身為世界首強的美國將更加無法容忍俄國的駭侵行動。預計美國將持續透過外交手段及增設法規對俄國施壓，但美國也開始與俄國就網路安全議題進行磋商，未來可持續觀察二國是否能保持溝通，進而產出具國際規範效力的協議。

[10] BBC News (2021.5.25). Russia threatens to slow down Google over 'banned content'. 檢自：https://www.bbc.com/news/technology-57241779 (Jun. 21, 2021)

北約成員國同意新的網路防禦政策

國際瞭望 撰輯

https://blog.twnic.tw/2021/07/20/19186/

北大西洋公約組織（North Atlantic Treaty Organisation，NATO）於 2021 年 6 月 14 日剛結束在比利時布魯塞爾舉行的高峰會，會後發布公報宣示「（會員國）再次確認北約防禦指令，同盟國將根據國際法，動員所有力量以積極遏止、防禦並反擊所有類型的網路威脅，包括混合型攻擊中的網路威脅」。

高峰會中，會員國亦通過新的網路防禦政策，政策將容許會員國視情況啟動北約公約第 5 條《集體防禦條款》；根據此條款，任一北約會員國受到的攻擊都將被視為針對北約全體的攻擊，其餘會員國並將因此考慮採取行動回應。

公報中亦指出，具重大惡意的網路行動可能被視為武裝攻擊。此外，成員國同意視北約為一個資訊共享及探討國際網路安全議題的平臺，並持續改善北約的網路防禦。

美國總統拜登表示，這是北約七年來首次更新網路防禦政策，認為它將改善北約盟國的集體防禦能力，進一步抵禦針對國家網路及關鍵基礎設施的惡意攻擊。拜登的國安顧問 Jake Sullivan 指出，新政策將從國防、政治到情報等各層面，提升北約成員的整體網路安全。

參考資料：

1. Maggie Miller (2021.6.14). NATO members agree to new cyber defense policy. The Hill News. 檢自：
https://thehill.com/policy/cybersecurity/558383-nato-member-states-agree-to-ne

w-cyber-defense-policy-following(Jun. 25, 2021)
2. NATO (2021.6.14). Brussels Summit Communiqué. 檢自：
https://www.nato.int/cps/en/natohq/news_185000.htm(Jun. 25, 2021)

美國政府提出打擊及防制勒索軟體手段倡議

國際瞭望 撰輯

https://blog.twnic.tw/2021/07/09/19007/

《打擊勒索軟體報告》

有鑑於 2020（去）年針對醫院或學校等組織的勒索軟體激增，美國安全技術研究院（Institute for Security and Technology）轄下的勒索軟體工作小組發布了《打擊勒索軟體報告》[1]，撰寫者包括企業界及政府代表，報告中廣納公私部門觀點，藉以協助美國政府及產業應對相關威脅。

報告指出，勒索軟體攻擊已構成「緊急國安風險」，並提出 48 項公私部門可採取的建議措施[2]，儘管這些措施五花八門，但報告第 6 頁提出五大優先建議，作為未來各部門及機構應對勒索軟體之方向，包括：

1. 美國須與各國政府及執法機構合作，共同協調一個整體策略，以應對日益猖獗的勒索軟體攻擊，國家須依據該策略主動打擊勒索軟體罪犯。
2. 白宮應帶頭領導美國政府進行「反勒索軟體行動」，其中包括：由國安會及國家網路總監領導創建協調工作小組；設立

[1] 報告連結。

[2] Maggie Miller. Coalition unveils plan to help government, industry confront ransomware attacks. The Hill News Retrieved from: https://thehill.com/policy/cybersecurity/550876-coalition-unveils-plan-to-help-government-industry-confront-ransomware?rl=1 (Apr. 29, 2021)

勒索軟體工作小組；設置由私部門主導的惡意軟體威脅中心。

3. 各國政府須成立基金，支持各個組織應對勒索軟體及其他網路安全活動，若組織遭勒索，在支付贖金前應考量其他選擇並進行通報。
4. 進行國際協調，發展一項協助各個組織應對勒索軟體攻擊的總體框架，並透過財政激勵或法規，協助一些資源匱乏的重要部門。
5. 對加密貨幣產業執行更嚴格的監管措施，將其納入反洗錢（Anti-Money Laundering，AML）及反恐募資（Combatting Financing of Terrorism，CFT）之法規中。

勒索軟體工作小組於今年 4 月成立，並於成立後不久即發布報告，代表勒索軟體氾濫已是不可不防的重大議題，究竟勒索軟體攻擊如何衝擊美國社會及關鍵基礎設施安全，本文將於以下段落進行概述及評論。

勒索軟體攻擊已構成嚴重傷害

根據報告，去年將近 2,400 個美國組織受到勒索軟體攻擊，其中包括近 1,700 所學校，以及 560 個醫療機構。針對醫療機構的攻擊使得相關醫療設施停擺，並因而延遲患者治療時程，美國安全技術研究院的執行長 Philip Reiner 更進一步指出，針對醫院的攻擊已深切危及美國公民生命安全。此外，勒索軟體受害者在去年支付了價值近 3.5 億美元的加密貨幣贖金，金額較 2019 年成長了 3 倍以上。

除上述統計資料外，今年 5 月 7 日發生的 Colonial Pipeline 燃油管道系統駭侵案亦是勒索軟體集團所為[3]。Colonial Pipeline 負責美國

[3] 陳曉莉（2021 年 5 月 10 日）。美國最大燃油管道系統 Colonial Pipeline 遭

東岸 45%燃油供應，為美國最大的精煉油管道系統，每天運量多達 1 億加侖。此次駭侵案已侵犯美國關鍵基礎設施，並造成所有管道作業暫停的嚴重後果，美國總統拜登也於 5 月 9 日宣布美國進入緊急狀態。

根據 BBC 報導[4]，遂行此次攻擊的組織為去年 8 月問世的 DarkSide 勒索軟體集團，它們滲透 Colonial Pipeline 網路並加密系統檔案，下載了近 100GB 的大量資料進行勒索。DarkSide 的攻擊手法精緻複雜，在攻擊前就會針對受害者的財務進行分析並判斷可勒贖金額，同時建置外洩資料系統以向受害者展示目前竊取之資料。不僅如此，DarkSide 還設有媒體中心發布攻擊訊息，並與其他專門解密的業者進行合作。如此全面縝密的手法，代表勒索軟體已從過去的零散勒贖升級為精密的產業鏈，透過產業鏈中各個角色分工合作，勒索軟體集團構成的威脅日益增大，甚至可能被敵對國家重金雇用進行更大型的網路攻擊。

根據一項由英國薩里大學（University of Surrey）犯罪學資深講師 Mike McGuire 博士主持的研究[5]，國家間的網路攻擊已變得更加頻繁、多元且公開，研究結果亦指出，國家已開始與駭客團體合作，國家行為者會自行或透過代理人於暗網購買駭侵工具。在研究訪談的網路專家小組中，有 65%認為國家從網路犯罪中獲利，而 58%的專家表示，招募網路罪犯進行攻擊的情況逐日普遍，未來若勒索軟體集團與敵對國家合作，可能會造成更大的網路安全破口，甚至發展成網路戰爭。有鑑於此，美國政府也於此駭侵案後提出幾項應對

勒索軟體攻擊，美國宣布進入緊急狀態。iThome。檢自：https://www.ithome.com.tw/news/144276 (May 10, 2021)

4 Mary-Ann Russon (2021.5.10). US fuel pipeline hackers ‘didn’t mean to create problems’. BBC News. Retrieved from: https://www.bbc.com/news/business-57050690 (May 10, 2021)

5 研究報告下載點。

勒索軟體之政策倡議。

美國政府的勒索軟體政策倡議

由於 Colonial Pipeline 駭侵案情節重大，美國政府已宣布將進行國際合作打擊勒索軟體。在緊急應對措施方面，美國網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency，CISA）正為關鍵基礎設施營運商準備一份諮詢建議報告，提供他們進一步應對惡意軟體的方針；聯邦調查局（Federal Bureau of Investigation，FBI）則是發布「病毒緩解措施指標」進行協助；美國能源部也與石油、天然氣及電力公司共享資訊及建議[6]。

然而，上述措施僅是亡羊補牢，美國網路安全專家仍憂心於美國既有網路防禦措施[7]，並提出三點缺失。首先，由於美國公共設施民營化的傳統，85%的美國關鍵基礎設施由私人企業擁有，少有法規具體規範企業應如何保護其網路。第二，絕大多數勒索軟體攻擊來自國外，其中以俄國為大宗，當組織偵測到勒索軟體並向主管機關 FBI 進行通報時，由於 FBI 僅有國內調查權，因此無法對外國駭客進行執法。換言之，目前沒有任何一個聯邦機構直接負責捍衛美國公民免於勒索軟體攻擊。第三，在 Colonial Pipeline 事件發生的五天後，該企業還未與 CISA 共享駭客資訊，足見資訊通報機制不足。

---

6 The Cyberwire. US Government responds to the Colonial Pipeline ransomware attack. Aveddon ransomware warning. Retrieved from: https://thecyberwire.com/newsletters/policy-briefing/3/90(2021/05/12)

7 Dilanian, K., & Ainsley, J.(2021.5.12). Who's in charge here? Colonial Pipeline hack exposes huge holes in U.S. cyber defenses, say experts. NBC News. Retrieved from: https://www.nbcnews.com/news/us-news/who-s-charge-here-colonial-pipeline-hack-exposes-huge-holes-n1267057 (May 12, 2021)

針對上述情況，美國政府已發布行政命令[8]試圖進行改善，該命令明確要求建構更即時完善的資訊通報機制，未來美國國會須立法強制受攻擊之美國關鍵基礎設施營運商通報政府，以及為美國所有軟體建立網路安全標準，同時部署加密及多重身分驗證（Multi-factor authentication，MFA）。其中還提到要建構「零信任環境」[9]，在外部軟體及設備證明自身清白前，組織須假定其具有惡意並審慎應對。網路安全公司 Tempered Networks 市場總監 Gary Kinghorn 對此提出評論，他認為零信任環境可提升企業檢測惡意軟體的能力，在零信任環境中，未經明確授權的存取及通訊將被阻止，並因此使惡意軟體的傳播面臨阻礙。

最後，非營利網路安全組織 Silverado Policy Accelerator 執行主席 Dmitri Alperovitch 建議，美國應向駭客團體所屬國籍之國家要求起訴或引渡駭客，若該國拒絕，則應主動發動制裁。

結語

勒索軟體為美國帶來嚴峻挑戰，同時也暴露出美國網路安全政策的結構性問題，在經歷 Colonial Pipeline 駭侵案後，可觀察美國國會是否將展開相關立法，落實及深化拜登總統的行政命令。

---

8 Maggie Miller (2021.5.12). Biden signs executive order to improve federal cybersecurity. The Hill News. Retrieved from: https://thehill.com/policy/cybersecurity/553243-biden-signs-executive-order-to-improve-federal-cybersecurity-following (May 12, 2021)

9 Breuninger, K. & Macias, A. (2021.5.12). Biden signs executive order to strengthen U.S. cybersecurity defenses after Colonial Pipeline hack. CNBC News. Retrieved from: https://www.cnbc.com/2021/05/12/biden-signs-executive-order-to-strengthen-cybersecurity-after-colonial-pipeline-hack.html (May 12, 2021)

數位電商模式及法令管制的新思維及調適——以外送平臺為例

文／國立臺北商業大學財政稅務系副教授 黃士洲

https://blog.twnic.tw/2021/08/15/19559/

數位電商與第一代電商差在哪裡？

十多年前開始流行「電子商務」（Electronic Commerce），到現在可以說已經變成包山包海的概念及口號。不過，近幾年電商的營運加入了社群媒體及雲端大數據，從一部分的電商進化到「數位電商」模式。

一般電商（或稱之為「第一代電商」）模式，例如：網路平臺上開店、作網拍，或透過網路平臺張貼型錄、聯絡及付款方式，相對於最為傳統的實體商業通路，差別在於接單、付款及客服等商業流程，透過線上化及電子化而獲得優化。至於數位電商則在一般電商的基礎上，進一步結合社群媒體及雲端大數據，由演算法記錄、追蹤、分析消費者參與互動的資訊及行為，之後再以社群、分享來進行準確、分眾的行銷。

數位電商的營運大多架構在特定的國際平臺，例如：Facebook、Google Play、YouTube、Amazon，或如蝦皮、阿里巴巴等跨國網拍平臺，也被經濟合作暨發展組織（Organization for Economic Cooperation and Development，OECD）描述為「高度數位化營運模式」（highly digitalized business models），其特徵為在消費者所在國並不需要相當規模的實體營運處所，且仰賴智慧財產權（如：演算法、

雲端技術）以及使用者參與貢獻資訊[1]。數位電商的特徵雖然開啟了不少新商機，讓零散的商家、個體戶可以快速、低廉地觸及並滿足消費者需求，隨之孕育各式各樣的「零工經濟」（Gig Economy，如：餐飲外送與勞務外包），以及「分享經濟」（Sharing Economy，如：分享機車與錯時停車）。

相形於第一代電商只是把原來的營業流程予以線上、電子化，數位電商則以大數據及社群媒體來善用消費者資訊，已經不是單純的「量」的「改變」（Change），毋寧宜視之為「質」之「革新」（Transformation），較為恰當。正當數位電商蓬勃發展之際，其營運模式也隨之衍生新的風險及問題。以全球視野來說，最常被提起的是跨境電商之課稅漏洞及個資保護。

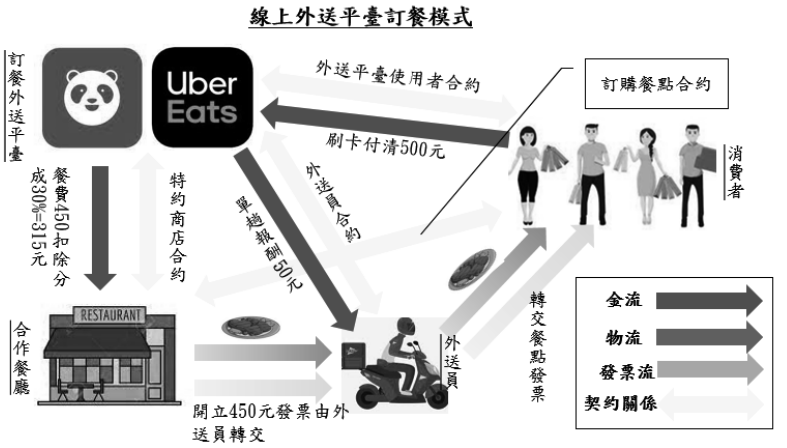
電商營運模式及稅務管制間的彼此調適：外送平臺與發票

有些消費者利用 Foodpanda（以下簡稱富胖達）App 平臺訂餐，餐點送到後，對發票內容會有點疑慮——我明明線上刷了 500 元，怎麼富胖達的發票只打服務費 50 元，剩下餐費怎沒打上呢？再摸摸餐點袋裡，或許會找到餐廳開的餐費發票，或許啥都沒有，這樣對嗎？到底有沒有逃漏稅啊？

- **外送平臺營運模式解說**

若要釐清這個問題，得先從外送平臺的營運模式說起：

[1] 關於高度數位化營運模式的三項特徵，可參閱 OECD, Tax Challenges Arising from Digitalisation-Interim Report 2018, 第 24 頁，第 32-35 段。



資料來源：本文作者整理。

消費者小華在透過 APP 平臺向「彭湃牛排館」下單訂購 450 元的菲力牛排外送特餐，加上 50 元外送費，用綁定的信用卡一共刷了 500 元；約莫半小時後，外送員小明提著牛排餐盒，在樓下按門鈴請小華取餐，餐盒旁貼了一張 450 元的牛排館發票，50 元外送費則由平臺商開立雲端發票直接歸戶給小華。

外送員小明這一單賺到 50 元外送報酬，彭湃牛排館則是在按照 7：3 的分成比例，跟平臺結算 315 元的餐點費。但在隔天，小華急性腸胃炎住院，醫生懷疑牛排配菜可能感染大腸桿菌，小華致電平臺客服後，客服建議小華直接聯繫牛排館求償。

- **外送平臺的契約關係**

上面外送平臺的契約關係有二個主軸，一是訂餐平臺派遣外送員取送餐，其二是合作餐廳販售餐點給消費者，二組契約關係在法律上彼此獨立，外送平臺只對餐點送達負責，餐點的品質問題則由合作餐廳負責；所以，外送平臺也只對外送／平臺服務部分的收款來開立發票，餐點的銷售額則由合作餐廳開立。如果合作餐廳是不

使用統一發票的小規模營業人（每月營收 20 萬元以下），消費者也就拿不到發票（可能有手開收據）。

這樣的契約關係，也可參考富胖達的網站說明[2]如下：

- **請問我消費的發票是如何開立呢？**

foodpanda 係專業的餐點網路平臺服務業者，因此您將會收到由 foodpanda 開立的平臺服務費電子發票。

您所訂購的餐點係由各個餐廳店家精心製作準備，並且從餐廳店家直接外送至消費者手中，所以您收到餐點的同時，也會一併收到由餐廳店家開立的餐點金額發票／收據。

- **請問我訂購的餐點有瑕疵我該向誰求償呢？**

您所訂購的餐點係由各個餐廳店家精心製作準備，並且從餐廳店家直接外送至消費者手中，所以餐點製作瑕疵（例如食品安全）將由餐廳店家直接負責。

若餐點在運送途中因為碰撞、翻覆導致包裝破損、污損等，屬於外送服務直接致使餐點品質有瑕疵時，則由 foodpanda 負責。

富胖達的發票流程對應了雙主軸（餐點與遞送）的契約關係，消費者只拿到一張富胖達的外送服務發票；但也有電商平臺直接按照消費全部總額開立發票，這是怎麼回事？

- UberEats **落地臺灣經營基於刷卡及稅務成本考量**

不同於富胖達是境內公司，早先 Uber Eats（以下簡稱「吳柏毅」）是以跨境電商（荷蘭登記公司）的身分提供外送服務，為了簡化境內及境外帳務，將餐點費及外送費直接合開一張發票（與富胖達的比較如下表[3]）。在 2021 年 2 月吳柏毅改以境內子公司營運，換言

[2] Foodpanda.com (2021). 常見問題。檢自：https://www.foodpanda.com.tw/contents/contact.htm (Jul. 26, 2021)

[3] 林昱鈞（2020 年 2 月 5 日）。〈熊貓、UberEats 開發票方式大不同〉。工商時報。檢自：https://ctee.com.tw/news/tax-law/215244.html (Jul. 26, 2021)。

之，落地成為本地電商[4]，比照富胖達營運模式。境外改境內的可能是為了省下 1.5%的國外刷卡手續費，以及從消費總額開發票，改為只針對外送費開發票，也可節省相當的營業稅成本。

外送平台開立發票一覽

項目＼平台	Foodpanda、Quickpick	Uber Eats
公司屬性	境內電商平台	境外電商平台
開立發票	1. 一張總款項實體發票（Foodomo、Cutaway等適用） 2. 有餐點費、外送費各一張實體發票（Lalamove、Deliveroo、街口外送、有無外送等適用）	餐點費、外送費合開一張雲端發票
營所稅	B2C外送費收入減除成本後計稅	
營業稅	每兩個月報繳一次	

資料來源：財政部　　製表：林昱均

圖片來源：工商時報

以消費總額開一張發票，或將餐點費、外送費分由店家及外送平臺各開一張發票，營業稅務成本差別頗大。若由外送平臺按消費總額（如前例的 500 元），之後外送平臺還得向店家取得餐點費（450 元）發票，才能扣抵進項稅額，如果合作店家是不使用統一發票的麵店、早餐店或路邊餐廳等小規模營業人，無法提供可以扣抵的統一發票，這時候餐點費理當內含的營業稅額就得由外送平臺自行吸收，或者向合作店家及消費者提高餐點分潤與外送費。不論何種做法，在外送平臺競爭白熱化、利潤錙銖必較之時，在在都削弱了競爭力。再者，除了無法取得部分店家發票扣抵的問題之外，若以境

[4] 林昱鈞（2020 年 2 月 5 日）。〈熊貓、UberEats 開發票方式大不同〉。工商時報。檢自：https://ctee.com.tw/news/tax-law/215244.html (Jul. 26, 2021)。

外電商身分營運，申報營業稅進銷項扣抵時，往往還須核對跨境金流，付出額外帳務處理成本。

優化外送平臺的稅務管制流程建議

自 2020 年起，外送平臺已經成為我們應對疫情衝擊與疫後新常態，不可或缺的重要物流通道，尤其是在 2021 年 5 月中實施三級警戒，餐飲業全面禁止內用之後，大小店家都更加仰賴外送平臺服務。但是占掉外送服務一大部分的店家，根本開不出發票來，連收據也可能不會主動開立，而企業帳務管理又受到我國特有統一發票制度的制約——「有紙本發票才能報帳、抵稅，儘量不要拿一般收據」[5]，相當不利小店家在外送平臺經濟之中的公平競爭。

若以繼續維持統一發票作為唯一稅務憑證的現行制度為前提，小店家的稅務困境，還是可以透過政策鬆綁及平臺的協力，獲得相當的改善，特別是當外送或其他平臺掌握了特約店家所有銷售資料及金流，定期自動彙報稽徵機關，相當程度減少小店家隱匿銷售額逃漏稅的動機：

1. 現行普通收據扣抵企業費用有千分之三十的上限限制，可以針對利用平臺銷售的店家，予以適度放寬，或乾脆排除適用。
2. 依照平臺銷售資料，「小店家」已經達到使用統一發票的標準時，小店家若選擇導入雲端電子發票系統，可申請配套的鼓勵、補助措施。
3. 允許平臺可以用旗下特約店家的名義，以雲端方式，向消費者代開統一發票或收據，當消費者有扣抵營業稅或列報企業費用的需求時，可以自行列印，視同特約店家所開立。

---

[5] 《營業稅法》第 33 條規定，除非財政部例外准許，否則只有依規定取得的統一發票才可以作扣抵稅額的進項憑證；營利事業所得稅查核準則第 67 條第 2 項規定，以普通收據列報費用不可以超過營業費用總額的百分之三。

美國拜登總統發布行政命令，尋求恢復網路中立

國際瞭望 撰輯

https://blog.twnic.tw/2021/08/09/19319/

美國總統拜登簽署任內第 52 號行政命令，要求針對國內若干產業的主要企業強化監管及問責機制，以期促進市場競爭。

網路寬頻管制為拜登的內政重點，也在命令中占有相當篇幅，其中亦呼籲聯邦通訊委員會（Federal Communications Commission，FCC）訂定管制辦法，改善寬頻產業競爭及透明度。以下是命令中列出的辦法，以及對消費者的可能影響：

防止 ISP 與用戶達成協議：

根據 FCC 資料，約莫 2 億美國公民僅能從 1 至 2 個寬頻網路選項中做選擇。網路服務供應商（Internet Service Provider，ISP）與房東私下簽約合夥的情形常見於低收入社區，不僅剝奪租戶的寬頻選項，也妨礙其他寬頻業者進入當地市場，若 FCC 確實採取拜登行政命令中的措施，上述情況可望大幅改善。

恢復「寬頻服務內容標示」

所謂的「寬頻服務內容標示」（Broadband Nutrition Label），是在歐巴馬總統任內提出，但之後由川普總統廢除的法案，其要求網路服務業者依標準格式揭露包括價格、加值費用、網速等資訊。若 FCC 重啟此規定，ISP 就必須向 FCC 如實報告價格、客戶簽約率、網速及可用性資料，供 FCC 製作標示表。

ISP 不得訂定過高的解約金

美國 ISP 時常要求消費者繳納高額解約金，行政命令中鼓勵 FCC 限制解約金的額度，但並未明確訂出金額上限。無論如何，一旦解約金額有所限制，消費者也將擁有更換 ISP 的更大彈性。

恢復「網路中立」規範

川普 2017 年廢除歐巴馬總統任內設立的「網路中立」（net neutrality）原則，ISP 業者因此可坐地起價，隨意調整頻寬。川普政府後期，共和黨甚至希望進一步擴大此自由。然而，隨著拜登上任，FCC 可望重啟網路中立規範，行政命令特別鼓勵 FCC 重拾網路中立原則，再次禁止 ISP 恣意封鎖用戶網路或降低網速。

行政命令敦促 FCC 採取行動

行政命令雖不具約束力，但的確是對 FCC 施壓，敦促對方改善 ISP 產業的透明度及當責。無論未來 FCC 是否將採用相關措施，該命令都已為消費者帶來曙光，未來是否會有相應的監管措施仍尚待觀察。

參考資料：

1.David Anders (2021.7.9). Biden seeks return of net neutrality, greater competition among ISPs in executive order. CNET. 檢自：https://www.cnet.com/home/internet/biden-seeks-return-of-net-neutrality-greater-competition-among-isps-in-executive-order/ (Jul. 16, 2021)

2.New America (2021.3.5). OTI Applauds Bill to Create a 'Broadband Nutrition Label'. 檢自：https://www.newamerica.org/oti/press-releases/oti-applauds-bill-to-create-a-broadband-nutrition-label/(Jul. 16, 2021)

中國將實施《個人信息保護法》

國際瞭望 撰輯

https://blog.twnic.tw/2021/09/23/19946/

中國第十三屆「全國人民代表大會常務委員會」第三十次會議於今（2021）年 8 月 20 日閉幕，會中表決通過《個人信息保護法》，該法旨在保護網路用戶資料隱私，將於今年 11 月 1 日實施。

《個人信息保護法》將與《數據安全法》共同成為中國網路監管二大支柱，往後中國企業恐面臨更多法遵要求。《數據安全法》於今年 9 月 1 日實施，為企業制定一個劃分營利資料及涉及國安資料的框架；《個人信息保護法》則是參考歐洲《通用資料保護規則》（General Data Protection Regulation，GDPR），為用戶隱私設定保護框架。專家指出，這二項法規皆要求中國企業檢視其儲存及處理資料之措施，以確保合規。

根據《個人信息保護法》，企業處理個資須出於明確且合理之目的，並應在能達成目標之最小範圍內取得資料。此外，該法還明訂，企業蒐集個資前須取得用戶知情同意，並為跨境資料傳輸訂定明確規則。最後，該法還要求個資處理者指定個資保護負責人，並定期執行稽核。

在上述二法推出之際，中國監管機構頻頻對中國網路產業出手，造成眾多企業惶惶不安，相關案例包括：今年 7 月，國家互聯網信息辦公室（Cyberspace Administration of China，CAC）宣布將對滴滴出行涉嫌侵犯用戶隱私展開調查；今年 8 月 17 日，中國市場監管總局（State Administration for Market Regulation，SAMR）發布《禁止網路不正當競爭行為規定（公開徵求意見稿）》，規範內容包括促

進公平競爭及禁止虛假評論；今年 1 月，由政府支持的中國消費者協會（China Consumers Association）發布聲明，批評科技公司濫用個資促銷旗下產品，此後，監管機構時常譴責企業及 App 侵犯用戶隱私。工業和信息化部也指控 43 款 App 非法傳輸用戶資料，並要求這些 App 於今年 8 月 24 日前修正做法。

參考資料：

Josh Horwitz (2021.8.20). China passes new personal data privacy law, to take effect Nov. 1. Reuters. 檢自：
https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/ (Aug. 27, 2021)

他山之石：德國線上著作權聲明系統（CUII）

國際瞭望 撰輯

https://blog.twnic.tw/2021/12/08/21104/

德國自 2021 年 2 月開始啟用以 DNS 封鎖為手段處理網路非法內容的自律機制，該機制稱為線上著作權聲明系統（Online Copyright Clearance System，CUII）。

CUII 受德國聯邦網路局（Bundesnetzagentur）及負責保護市場競爭的聯邦卡特爾局（Bundeskartellamt）二個官方機構的支持，該倡議由著作權團體所提出，主要目的是透過更有效、快速的方式實施 DNS 封鎖，以處理網路上的著作權及智慧財產權侵權行為，參加者包括音樂、電影、遊戲及科學期刊等產業的協會，以及主要的 ISP 業者。機制運作的基礎源自德國的法律：權利人可在某些狀況下要求 ISP 業者阻撓網路使用者造訪非法展示著作權作品的網站。

運作上，封鎖 DNS 的申請案會由 3 人組成的委員會依相關法律進行審查，受理申請的前提是，針對非法內容提供者提出訴訟顯然沒有勝算。當委員會全數通過實施 DNS 封鎖，該封鎖建議會轉給德國聯邦網路局，由其判斷是否符合網路中立準則，倘該機關沒有表示意見，則 ISP 業者便可執行封鎖。

此項機制引發了侵害人權及自由市場之擔憂，倘若封鎖 DNS 在像是德國這樣的民主國家變得正常化，恐怕會成為極權國家進行實質網路言論審查的藉口。此外，CUII 機制運作是建立在 ISP 及內容業者間的協議，也導致該機制會被認為是執法機構的私人化，造成內容業者與經常被用於分享侵權內容的串流平臺之間的不公

平競爭。CUII 機制自運作以來，已裁定 6 個串流平臺應當封鎖，數量雖然看似不多，但是該機制利用法律為基礎，且政府在過程中採非正式介入的做法，先例一開恐後患無窮。

參考資料：

Nathalia Sautchuk-Patrício (2021.11.8). Content Blocking at the DNS Level in Germany. CircleID. 檢自：https://circleid.com/posts/20211108-content-blocking-at-the-dns-level-in-germany (Nov. 18 , 2021)

網路技術

改善 DoH 隱私保護及 ODoH

APNIC 文摘

https://blog.twnic.tw/2021/01/07/16551/

本 APNIC 文摘原標題為 Improving the privacy of DNS and DoH with oblivion，由 Geoff Huston 撰文。

過去很長一段時間，我們明知 DNS 不夠安全、不夠可靠，但畢竟算是堪用，所以即使 DNS 完全無法保障隱私，越來越多的中間人攻擊（man-in-the-middle attack）問題出現，我們仍然盲目地相信 DNS，對問題視而未見，沒有改善 DNS 的念頭。史諾登事件是最後的當頭棒喝，迫使我們正視 DNS 的種種問題。

從那開始，IETF 針對網際網路維運的隱私保護展開一系列密集動作，DNS 自然是其中一環。DoT（DNS over TLS）和 DoH（DNS over HTTPS）都是這個情境下的產物。

但是，DoT 及 DoH 提供的隱私保護都還是不夠。準確來說，這二個方式都是逼使用者從兩難中抉擇：是要揭露個資給 ISP，還是讓應用程式業者（如 Google、Cloudflare）看到我的隱私資訊？

最簡單的答案，應該是二個都不要。ODNS 及 ODoH 就是為此誕生的二種解法。

ODNS 透過在不同節點加密不同資訊的方式，確保 DNS 查詢保密。遞迴解析器只會知道使用者端解析器的身分，不會知道查詢資料。另一方面，權威解析器收到查詢後雖然可以得知查詢資料，卻不知道查詢來源的使用者端解析器身分。最後，權威解析器回傳查詢結果時，雖然其他節點可能從而得知部分查詢內容，但無法得知權威解析器、第一個遞迴解析器和使用者端解析器的身分。

然而，因為 ODNS 是使用既有的 DNS 解析器基礎架構，所以在加密原始查詢資料上不免仍有限制。ODoH 採取的是另一種方式：將使用者端到遞迴解析器的 DoH 通信期拆解成 2 個通信期：使用者端到代理人（proxy），代理人到遞迴解析器。

ODoH 在 DoH 的架構上加上「代理加密」的元素，由代理人避免目標或來源得知對方身分，且由於 DoH 本身就有的加密方式，代理人也無法得知 DNS 查詢內容。

ODoH 的優點在於不需要將加密資訊硬塞進傳統的 DNS 查詢封包，缺點則是 ODoH 架構下 2 個主要加密節點（代理人和遞迴解析器）必須由不同角色營運，否則就有被破解的風險。另一方面，ODNS 因為沒有代理人的設定，不須擔心上述 ODoH 的缺點。但 ODNS 的問題是雖然查詢全程加密，但任何旁人都能一眼看出這是一個 ODNS 查詢。

現代人益發重視隱私保護，是否意味著這 2 種新的 DNS 加密方式也會因此流行？作者認為大部分使用者不會特別去設定自己的 DNS 查詢方式，但很多網路上的應用程式很可能樂於利用這些新的加密技術，進一步促進應用程式及網際網路基礎建設的斷層，最終導致 DNS 分裂。

網際網路永續將是下一個重要環保議題

國際瞭望 撰輯

https://blog.twnic.tw/2021/01/06/16563/

因燃燒煤炭或石油所造成的環境汙染是顯而易見的，但多數人並未意識到我們正在燃燒天然氣或煤炭以為網際網路提供動力。此外，人們往往認為這是網路服務供應商（ISP）或資訊中心應負的責任，但事實上我們無時無刻都因網路服務而耗費電力。

網路的基礎是 IPv4 位址，透過 IPv4，伺服器及各種設備（電話、平板電腦、電腦等）之間能夠進行資訊交換及連結。當設備退役或移轉到 IPv6 時，IPv4 位址將處於休眠狀態（dormant，亦稱為 sleeping addresses）。然而，即使是處於休眠狀態，這些位址仍需要電力，因此，會浪費許多能源。

許多產業，特別是電信、金融服務、醫療保健及網路領域，都擁有數以萬計的休眠 IPv4 位址，這對網路領域從業者而言是難題，也是機會。

然而，政府對 ISP 的監管並不會影響數以百萬計的休眠 IPv4 位址，此外，關注資訊中心的消費者團體同樣忽略休眠位址造成的資源浪費。因此，我們需要一種激勵業者處理 IPv4 休眠位址的新手段，就像 GoDaddy 在 2000-2010 年間將閒置域名重新引入市場，我們也可以建立一個平臺，鼓勵業者在上面出租閒置的 IPv4 位址。另一方面，針對那些囤積大量 IPv4 位址的個人，業者也應採取適當的對應手段。

鼓勵你的雇主或公司，告訴他們租賃 IPv4 位址是筆值錢生意，若改變成真，我們可以在避免浪費 IPv6 位址的同時，大量減少閒

置的 IPv4 位址，更進一步打造永續的網際網路。

參考資料：

http://www.circleid.com/posts/20201217-the-next-green-initiative-is-internet-sustainability/

太有禮貌的無線網路

APNIC 文摘

https://blog.twnic.tw/2021/02/24/17038/

本 APNIC 文摘原標題為 Is WiFi too polite?，由 Ali Abedi 撰文。

在無線網路（WiFi）中，某個裝置發送資料封包後，收到封包的裝置會計算封包的循環冗餘（cyclic redundancy check）以檢測可能錯誤，若計算結果沒問題，就會回傳確認訊息（acknowledgement，ACK）給發送裝置。這個機制能有效降低無線網路的錯誤率，也可以處理實體及媒體存取控制（Media Access Control，MAC）層的再傳輸問題。

大部分的網路都會使用如無線網路保護存取（WiFi Protected Access 2，WPA2）等安全協定，防止未授權的裝置加入網路。也因此，大家都以為唯有收到來自已知存取點或相同網路中其他裝置的封包時，無線連網裝置才會回傳確認訊息。

但事實並非如此。作者研究團隊發現，只要封包目的地位址跟自身 MAC 位址相同，任何無線連網裝置都會確認所有收到的封包。更明確的說，在實體層上無論什麼封包，甚至封包本身缺乏有效負載，都仍然可以成功傳送並收到確認訊息。當然，這些無效的封包極可能無法通過再上一層的檢測，就此被擋下。

這種即使不認識對方也無條件回傳確認訊息的行為，被作者團隊稱為「有禮貌的無線網路」。團隊用實驗室裡的無線連網裝置進行測試，發現這些裝置全部都「很有禮貌」。

為了擴大測試範圍，團隊在車頂上裝了一個無線網路轉換器，在實驗室所在的加拿大滑鐵盧市裡開車亂晃一個小時，總共測試到

分屬 186 家不同廠商的 5,328 個無線網路節點，這些節點來自 147 家廠商的 1,523 的無線網路用戶裝置，以及 94 家廠商的 3,805 無線網路存取點。

WiFi Client Device		WiFi Access Point	
Vendor	# devices	Vendor	# devices
Apple,	143	Hitron	723
Google	102	Sagemcom	601
Intel	66	Technicolor	410
Hitron	65	eero	195
HP	63	Extreme N.	188
Samsung	56	Cisco	156
Espressif	47	HP	104
Hon Hai	46	TP-LINK	101
Amazon	41	Google	80
Sagemcom	38	D-Link	75
Liteon	33	NETGEAR	69
AzureWave	30	ASUSTek	51
Sonos	30	Aruba	46
Nest Labs	27	SmartRG,	44
Murata	24	Ubiquiti N.	35
Belkin	20	Zebra	35
TP-LINK	20	Pegatron	28
Cisco	16	Belkin	25
ecobee	13	Mitsumi	25
Microsoft	13	Apple	19
Others	630	Others	789
Total	1523	Total	3805

測試結果發現，團隊感測到的總共 5,328 個 Wifi 存取點和裝置，收到團隊為測試所送出的假封包後，無一例外都會回傳確認訊息。換句話說，幾乎所有現代使用的無線連網裝置都非常「有禮貌」。

有禮貌的無線網路會帶來很多安全威脅。舉例而言，攻擊者可

以傳送一個本地迴路（back-to-back）的假封包給目標裝置，然後分析目標裝置回傳的確認訊息，藉此挖掘裝置使用者的個人資料。

最近的研究已發現，光是透過監測無線網路信號，就可以推測出包括地點、手勢、呼吸頻率和按鍵動作等環境資訊。也就是說，攻擊者可以利用太有禮貌的無線裝置所回傳的確認訊息進行推測，進而掌握裝置使用者無意洩漏的資訊。

作者團隊也做了實驗，確認這種攻擊是否真的可能成功。他們將作為測試攻擊目標的平板電腦放在隔壁房間，然後利用上述手法傳送假封包給平板電腦，取得確認回應。測試結果發現，攻擊者的確可以透過傳送多個假封包，分析收到所有確認回應中的不同信號，以推測裝置所在環境的某些資訊。

這些只是初步發現。進一步而言，攻擊者能否利用此類攻擊偵測到網路占用率？有可能利用此攻擊隔牆偵測到另一端的人在做什麼嗎？更甚者，光是透過分析收到的回應訊號，我們是否能預測牆壁另一邊人的心率、呼吸頻率等重要生命跡象資訊？這些都是團隊認為值得未來進一步研究的議題。

DoH 是對的嗎？

APNIC 文摘

https://blog.twnic.tw/2021/03/11/17124/

本 APNIC 文摘原標題為 DoH the right thing，由 APNIC 資深研發科學家 George Michaelson 撰文。

DoH 的強力支持者兼主要推手 Mozilla 基金會，今年 1 月 4 日剛結束 FireFox 瀏覽器使用 DoH 的公眾意見徵詢。1 月 14 日，美國國家安全局（National Security Agency，NSA）也針對 DNS over HTTPS（DoH）發布建議報告，DoH 因此再度被推上風口浪尖，成為網路社群討論焦點。本文簡介 NSA 建議內容，也說明建議報告引發的社群反應。文章目的並非判定 DoH 的好壞，而是從眾人反應理解 DoH 對不同使用者的意義。

NSA 文件中對 DoH 提出的建議，最簡化而言，是建議企業使用者僅於公司網路內部啟用 DoH。作者認為，文件並未斷言 DoH 為「惡」，而是提醒讀者 DoH 可能過度預設 DoH 查詢的目標對象，所以使用者在啟用 DoH 前應考慮周全，最好只在值得信任的本地網路中使用 DoH。

有些人可能認為，DoH 就是要保護網際網路上，也就是不同網路之間的傳輸隱私，在本地網路使用有何意義？但作者提醒，「本地網路一定安全」的假設其實大有風險，惡意人士潛伏於本地網路、偷窺內部訊務的案例也越來越多。也因此，作者認為 NSA「於本地網路使用 DoH」的建議並非沒有可取之處。

既然如此，為何網路社群對 NSA 文件的反應正反不一？作者舉出二個主要原因：一是 NSA 的身分導致有些人對建議內容存疑，

另一個原因，則是此建議可能波及那些原始目的就是躲避本地網路限制的 DoH 使用者。

作者解釋，許多質疑聲音並非反對建議本身，而是不信任提出建議的 NSA。幾年前，NSA 被發現故意在某個美國國家標準暨技術研究院（National Institute of Standards and Technology，NIST）核定、市面上也廣泛使用的加密運算法中植入弱點，藉此竊聽和蒐集情報。此事揭露後，NIST 的公信力一落千丈，對所有不是美國人的人而言，NSA 既然可為了貫徹美國利益無所不用其極，這個單位發布的所有建議都不得不引人三思：這是否又是 NSA 為了自家利益設計的圈套？

或許不能怪這些人過於小心謹慎，但作者認為 NSA 這次提出的建議不宜以人廢言。「在內部網路使用 DoH」的確能防範近來益發常見的內部網路駭侵事件，而「外部網路的 DoH 供應商可能並非想像中值得信任，授權他人代理改動 DNS 查詢也不一定對你有利」的建議也很正確。但對某些人而言，他們需要的正是 DoH 這種特性。

究竟是誰需要 DoH？他們為什麼使用 DoH？DoH 可以將使用者的 DNS 訊務轉至 HTTPS 上傳送，藉此避開二種情況：針對特定查詢的封鎖機制，以及中間人攻擊。所以有些人使用 DoH 可能只是為了保護隱私，但對另一些人而言，他們使用 DoH 是為了躲過針對性的封鎖機制。

在機場或旅館裡，常會遇到需要先從登錄頁面輸入資訊或付錢，才能繼續使用的網路。這就是一種利用 DNS 的封鎖機制。這種時候你或許會想要使用 DoH，避免旅館收費後還持續監視你的 DNS 訊務。中國的網路長城是另一種大家都熟知的封鎖情境，而在「牆內」的人如欲取得被封鎖的服務，很可能就需要 DoH 的協助。

至於開頭為什麼要提到 Mozilla 的公眾意見徵詢？作者在結尾再次說明， Mozilla 作為 DoH 中介者，可以決定 Mozilla 的產品（如 FireFox 和 Thunderbird）使用者怎麼用 DoH。他們希望使用者能參與討論，共同決定 DoH 的預設方式、使用者可以調整哪些設定等。很顯然，Mozilla 提供的服務和 NSA 的建議扞格不入，而由瀏覽器提供 DoH 服務，也一直被網路維運社群視為一大風險。

無論對 DoH 的意見為何，唯一可以肯定的，是在「保護隱私」和「打倒巨頭」二大口號領軍的當代網路治理討論中，DoH 將持續成為各方激辯的重要議題。

Geofeed 及牧羊人：如何定位網路？

APNIC 文摘

https://blog.twnic.tw/2021/03/22/17386/

本 APNIC 文摘原標題為 Geofeeds and shepherding: Where is that network?，由 APNIC 資深研發科學家 George Michaelson 撰文。

網路維運人員常會需要知道某個網路區塊在哪裡使用。這問題可以分成二個部分：

1. 在邊界閘道協定（Border Gateway Portocol，BGP）中，誰是這個網路區段的授權來源？
2. 這個網路區段在現實世界中的哪裡使用？

前者是路由問題，後者則涉及現實世界中的地理位置。由於路由問題已有資源公鑰基礎建設（Resource Public Key Infrastructure，RPKI）解決，本篇僅探討第二個問題，也就是如何得知網路區段在現實世界中的地理位置。

如前所述，有些時候我們會需要知道某個網路的位置。可能是為了追究智財問題或執法需求，也可能是需要在急難狀況下尋人，或業者希望提供更精準的客製化服務。RIPE NCC 這篇文章統整各種可以定位地理位置的資料來源，除此之外，RIPE NCC 自己也維護名為 RIPE IPmap 的地圖，提供相同功能。

然而，由於這些來源使用的是區域網際網路註冊管理機構（Regional Internet Registry，RIR）在分配位址時，也就是使用者註冊時填寫的資料，有時候並不一定等於實際使用時的地理位置。

APNIC 作為 RIR，在分派位址資源時，也會記錄資源分派到的地理位置。這地理位置可能代表分派對象的法人所在地或法人登記

地址，若分派對象為個人，也可能是該個人的位置。這些位置資訊並非由註冊人自己維護，而是由 APNIC 以註冊管理機構的身分，當成公開註冊資料維護。若註冊人希望使用更特定的位置資訊，他們必須以註冊人才有的「維護者」（maintainer）權限取得或更改此資訊。

資源分配資料中的地理位置資訊，代表註冊單位在註冊時所填寫的位置。這個位置資訊會以 ISO3166 國碼清單中列出的 2 字元國碼顯示，但也有些資料中的地理位置顯示 ZZ，這可能代表資源尚未發配、沒在使用，或保留中。

目前為止所說的地理位置資訊，都有「註冊資訊」和「實際使用資訊」不符合的可能，換句話說，雖然我們以「註冊資料」推斷網路使用的地理位置，但這推測並不一定準確。

於是，有些人想出新的方法，就是在 RPSL（Routing Policy Specification Language，呈現網際網路路由資訊的標準格式）加入一個名為「geofeed」的欄位。

「geofeed」的概念非常簡單。它起源於 Google 提出，在 IETF 以 RFC 8805 發布的機制，這機制訂定使用者用來自行發布地理位置資訊的 IP 前綴格式，只要利用 CSV 檔，使用者甚至可以提供精確的街道、郵遞區號等位置資訊。含有地理位置資訊的 CSV 檔會以 URL 方式產出，為了讓人們方便找到 URL，就必須在註冊資料檔案中新增一個「geofeed」欄位。

那麼，這一切又跟「牧羊」有什麼關係？「牧羊」其實是 IETF 中的行話，用來形容推動一份文件從工作小組共識決議、草稿、審核到最終以 RFC 發布的過程。而本文作者 George Michaelson 在 APNIC 負責的業務包含 WHOIS 和 RDAP 的註冊管理機構功能，geofeed 若能解決地理位置資料的問題，對他大有好處。也因此，他被託付了把「geofeed」這頭羊趕進羊圈的「牧羊」大任。

但 geofeed 欄位提供的資訊，真的會比現在能取得的地理位置資訊更好嗎？作者解釋，geofeed 欄位的資訊是網路區段的實際營運者提供，而且他們還可以利用 RPKI 簽章進一步驗證提供的資訊。作者認為，若能通過這樣的高標準，足以證明 geofeed 欄位的資訊可靠。

當然，市面上也有其他定位方式，例如內容傳遞網路業者就常仰賴其全球 BGP 分布率，利用三角定位鎖定某個 IP 區段的地理位置。這也表示，若 geofeed 成功變成公開註冊資料的欄位之一，大型業者將失去靠規模掌握網路位置的優勢，反之，規模較小的中小型業者至少在鎖定網路地理位置上，可以和大企業站上相同的起跑點。

改善大城市以外的網路連線：日本案例分享

APNIC 文摘

https://blog.twnic.tw/2021/09/29/20014/

本 APNIC 文摘原標題為 How do we improve Internet connectivity outside major cities? A Japanese approach，由 Satoru Tsurumaki 撰文。

將高速寬頻網路從大城市延伸至地方，對很多國家都是個挑戰，日本也不例外。雖然日本的國土幅員比澳洲或美國小，因此無須架設長達百萬公里的電纜，但在日本，地方人口享有的網路頻寬仍較大都市低，地方網路服務供應業者（Internet Service Provider，ISP）的投資報酬率也低於大都市的同業。

為了改善這些問題，日本總務省於 2019 年指示啟動研究計畫，檢視在日本網際網路二大中心東京、大阪的周邊區域建立訊務聚合中心，是否能有效降低開銷並提高訊務傳播效率。作者所屬的 BBIX 公司是本研究計畫的參與成員之一，他們的任務是在東北地區的仙台及九州地區的福岡，分別設立網際網路交換中心（Internet Exchange Point，IXP）。結果顯示，這二個區域的網路訊務往返時間（round-trip time，RTT）大幅改善，縮短將近 15 毫秒。

以下作者將進一步說明日本網際網路建設的背景，以及本研究計畫的實際執行方式和結果。

日本的網際網路有二個主要匯集點：首都東京及西日本的中心，大阪。幾乎所有主要的 IXP 和轉接服務業者，都從這二個大都市提供服務。

有了 IXP，ISP 及其他 ISP 無須經由海外，就可以在當地交換

路由資訊和訊務，因此擴大網路服務範圍。IXP 在轉接當地訊務上扮演的角色越來越吃重，研究顯示，IXP 可以有效縮短自治系統（Autonomous System，AS）層級的平均路徑。

在日本，位於東京和大阪以外地區的 ISP，主要利用以下方式確保上游網際網路連線：

1. 向位於東京或大阪的轉接服務業者購買當地轉接服務。

2. 租借一條線路，連接到東京或大阪的轉接服務業者或 IXP。

二種作法都有 RTT 延長和所費不貲的問題。在某些只有一家服務業者的地區，甚至無法透過重複備援確保容錯。另一方面，日本一般民眾的寬頻消費者數量已幾近飽和。這表示 ISP 無法期待使用者人口突然激增，因此帶動銷量成長。種種難題下，地方的 ISP 處境並不容易。

在此研究計畫下，BBIX 與 J-Stream、QTnet 及 TOHKnet 合作，分別於仙台及福岡建立 IXP。

仙台的 IXP 有和東京一樣的網路段（segment），福岡的網路段則和大阪一樣。乍看之下或許有點奇怪；研究目的改善當地的網際網路連線，使用一樣的網路段似乎無法滿足這個目標。然而，IXP 的成長仰賴網路使用者及內容提供者，二者之間是雞生蛋、蛋生雞的循環關係。主要的內容傳遞網路（Content Delivery Network，CDN）業者都已經連接到東京和大阪的 IXP，因此，藉由分別於仙台和福岡設定和東京、大阪一樣的網路段，研究可以充分觀察一個已與所有主要 CDN 業者連接，而無須另行逐一與業者簽約的 IXP，實際上能享受到的充分效益。

作者團隊量測 RTT 和下載影片的畫質，探究地方 IXP 能否實際改善當地的網路連線。量測結果發現，仙台和福岡的伺服器與市中心內容伺服器之間的 RTT 大幅改善，速度增加達到 87%，實際傳輸時間約減少 15 毫秒。內容下載方面，量測結果顯示下載速度

增加約 37%。

這顯示從離使用者較近的地點傳遞內容，可以有效提升大型線上遊戲改版更新時需要大量訊務的使用者體驗——而這在過去一直是很多玩家的痛點。

根據這些量測結果，我們對在地方設立 IXP 的可能效益，包括增加地方網路頻寬、透過縮短內容傳遞距離協助提高地方 ISP 投資報酬率等，也取得基本但重要的概念。未來，類似的 IXP 設置可以進一步支援如 5G 或多階取邊緣運算等，需要低延遲率、高頻寬的新興技術。

個人意見：內容傳遞網路和網路集中化

APNIC 文摘

https://blog.twnic.tw/2021/09/17/20058/

本 APNIC 文摘原標題為 Opinion: CDNs and centrality，由 Geoff Huston 撰文。

今年 6 月 17 日又有一波大規模網路斷線事件，受害者包括數家澳洲和紐西蘭大型銀行、澳洲郵政、香港股市和全球多家航空。根據事後統計，約 500 家企業的網站都遭波及，網站因此斷線長達 4 小時。

這 500 家企業有什麼共通點，導致他們成為此意外的共同受災戶？答案是：他們都是 Akamai 的客戶。更精確的說，他們都使用 Akamai 的 Prolexic 分散式阻斷服務攻擊（Distributed Denial of Service，DDoS）防護系統。

Akamai 的事後聲明解釋，此防護系統非預期停擺的原因，是系統使用的某個路由表數值意外超標。

研發人員在網路路由裝置設計上的永恆課題，就是如何在產品 CP 值和產品壽命之間取得最佳平衡，而網際網路的成長速度也是重點考量之一。網路持續擴張，維運人員為了跟上變化，也必須定期更新升級裝置。在這永不間斷的競逐長征中，人類總是難免失足。Akamai 的事件即為一例。

當然，這問題並非 Akamai 所獨有。所有網路服務供應業者都希望提供最佳服務品質、最好的價格，同時又永遠超前網路的擴張速度。但就如前所述，馬有失蹄，人有失足，系統總是會出錯或過載，服務斷線也因此在所難免。

今年光是 6 月就發生二起大事件，6 月初的 Fastly 事件導致知名網站如美國社群網站 Reddit、Amazon、直播平臺 Twitch、音樂串流平臺 Spotify 和影音內容串流服務 Hulu 斷線。

如同 Akamai，6 月初的事件並不是駭客攻擊。這比較像內容傳遞網路（content delivery network，CDN）中潛伏的不定時炸彈，總有一天，會因為某個環節的設置出錯，引爆炸彈，導致大批網站斷線。

Fastly 的客群廣大，而那麼多人之所以選擇 Fastly，大概也是看中它的廣大客群。換句話說，在 CDN 的世界中，Fastly 之所以顯得突出，單純是因為它的規模；而這規模又吸引更多人使用 Fastly，進一步擴大其規模。因大而大，這是大的生長循環。

結束背景說明，作者也分享他心目中 CDN 集中市場的問題。

首先，對企業來說，比起為了分散風險而同時使用多家供應商，只選擇一個 CDN 供應商並用它提供所有內容和其他服務簡單多了。換句話說，企業的課題不是選擇多家或一家，而是如何選到最好的一家。選定之後，企業和他們的 CDN 供應商就是命運共同體了。

再者，可以選擇的 CDN 也沒幾家。如果你的標準是全球規模、足以應付大部分和最激烈的 DDoS 攻擊，供應商本身會靈活安排以達到內容傳遞最佳化的同時，又可以讓顧客自行控管安全功能（如私有金鑰），那選擇清單大概也寥寥無幾。

Fastly 和 Akamai 都名列使用度最高的 CDN 供應商，其他就是 Amazon CloudFront、Google Cloud、Microsoft 的 Azure、Cloudfare 和 Limelight。這樣總共是 7 家。當然市面上還有其他供應商，有些可能僅服務特定區域，有些則有特殊技術專項。但是，今日的 CDN 世界，大致就是由上述 7 家供應商所構成。

作者認為，這才是真正的問題。在網際網路的內容層，幾乎所

有人都在使用某種形式的 CDN，但可以選擇的 CDN 供應商屈指可數。在過度集中的 CDN 市場裡，大型供應商所能提供的服務等級和價格，絕非小型供應商能望其項背。大型業者賺得越多，規模就越大，與其他小型競爭者之間的差距也就越拉越遠。

換句話說，許多小型 CDN 業者形成的「光環」包圍一小撮 CDN 巨頭組成的「核心」，就是當代 CDN 市場的樣貌。小型業者必須提供大型業者缺乏的專門或客製化服務，才有辦法存活。但這個小型業者的營利空間，其實也掌握在大型業者手中；後者選擇提供的服務內容，將直接影響前者的利基大小。這也代表整個 CDN 市場是大者越大，小者越小。而無可避免的結果，就是業者一旦出包，受到牽連而斷線的網路服務只會越來越多。

一般而言，這種大型事件會導致人們對服務供應商失去信任，甚至開始尋找替代方案。這種時候，股東都會擔心公司股價是否因此下跌。然而，無論是 Fastly 或 Akamai 的股價，事件後反而都水漲船高。

在金融市場裡，股市泡沫是指某一特定行業的股票價格自行持續上升或急速發展。投資人認定某公司或產業前景會一路大好，選擇忽視理性的市場評論及收益分析；這樣的投資人一多，就會形成股市泡泡。作者指出，過度集中化的市場尤其容易產生股市泡泡。對投資人來說，投資一家主導市場的公司，等於可以回收整個市場成長的利潤，要是這家公司最後得以獨占市場，那利潤更能翻上不知幾倍！然而，為了這個預期利潤，市場也可以忽視泡泡背後科技本身不夠穩定，類似事件未來只會繼續發生的事實。

我們正在目睹網際網路的許多層面從多元、活躍、高度競爭，逐漸變得高度集中，甚至邁向寡占或獨占的局面。高度集中化衍生高度的互相依賴，後果是任一環節出錯，都不再只是為一小撮人帶來些微不便，而將引發殃及多人的大型事故。

最後作者重申，大規模和集中化不一定代表高服務品質。6 月的二起事件就告訴我們，大規模和集中化，其實也讓所有人承受更高的風險。

個人意見：Akamai 的回應聲明非比尋常

APNIC 文摘

https://blog.twnic.tw/2021/09/03/19606/

本 APNIC 文摘原標題為 Opinion: Why is this unusual?，由 Geoff Huston 撰文。

今年 6 月連續發生二起大規模網路斷線事件，內容傳遞網路（content delivery network，CDN）服務供應業者 Fastly 和 Akamai 分別因為系統設定上的失誤，導致全球許多重要企業和組織網站斷線。受害者從 Amazon、直播平臺 Twitch、音樂串流平臺 Spotify，到澳洲和紐西蘭大型銀行、香港股市和全球多家航空，幅員遍布全球。

本文作者為 APNIC 首席科學家，他在 7 月曾發布部落格文章，分析 CDN 集中市場的問題。他在文中指出，我們正在目睹網際網路的許多層面從多元、活躍、高度競爭，逐漸變得高度集中，甚至邁向寡占或獨占的局面。

然而，這篇文章並非為了再開 CDN 集中市場的討論。此文目的是帶讀者了解 Akamai 在大規模斷網事件後發表的解釋聲明，在作者眼裡如何非比尋常。Akamai 的回應可參考部落格原文，作者有全文附錄。

Akamai 的回應聲明富含大量資訊，詳細解釋事件發生的根本原因。聲明中不僅陳述他們在問題出現當下的即時補救措施，也說明為了預防事件再次發生採取的行動，以及未來將如何改善監控通報流程的長程計畫。

過去類似事件發生時，當事者回應往往僅模糊表示有些「運作

失常」導致「服務中斷」，並指出「目前團隊正在緊急處理中」。這種僅用無意義字眼堆砌而成，彷彿提及任何細節都會導致業者身敗名裂的曖昧聲明，似乎已成為常態。

這也是為何 Akamai 這篇詳盡誠實的事件報告，如此令人耳目一新。

作者指出，許多其他產業的事後聲明都已不再有這種避重就輕、防衛性質濃厚的問題。航空產業就是個很好的例子，誠實的事件報告並不是為了找戰犯或咎責，而是找出事件發生的原因，了解如何改正現有的安全疏失，避免同樣的事件再次發生。

諸如汽車、核能和化學產業，都是在經歷慘痛教訓後大幅改善服務和產品的安全性，而公開、冷靜且誠實的事件調查是強化安全的唯一途徑。我們應視事件為學習機會，從而了解系統可能如何失靈。也因此，坦誠且完整的事後分析，是避免日後事件重演的關鍵。唯有如此，服務和產品才會越來越安全。

但作者批評，即使其他產業都已經了解這點，資訊科技產業還是認為自己與眾不同。過去十幾年來，軟體銷售業者已經習慣不負責任地販售不安全的問題產品，對業者而言，加強產品的安全韌性只是不必要的開銷。作者認為，這種態度至今仍是業界常態，從近日越來越頻繁的大規模網路斷線事件可見一斑。

「迅捷行動，勇於破壞」（move fast and break things）已成為網路產業的中心思想。這個說法來自 Facebook 創辦人 Mark Zuckerberg，他不僅將此當成企業內部的研發原則，甚至加碼指出「若沒有任何東西被破壞，就表示你動作還不夠快」。

作者也揶揄，我們或許已經該知足，對 Facebook 不是製造飛機、核電廠或汽車的公司心懷感恩。但如前所述，這種除了速度一概不顧的研發態度已擴散至整個產業，不只 Facebook，其他像是 Amazon、Apple 和 Google 也都或多或少習慣這種方式，在追求快速

創新的路上破壞了不少東西。

從另一個角度而言，資訊科技產業之所以還能逃避冷靜詳盡的事後調查流程，可能是基於「網路斷線事件不會立刻直接危及公共安全」的錯誤假設。事實上，網域名稱系統（Domain Name System，DNS）平臺無法解析域名，乍聽之下可能無足輕重，但若許多其他系統的基礎運作仰賴 DNS，那 DNS 的失靈將導致一連串系統接連失效，骨牌效應的後果不容小覷。

越來越多關鍵公共基礎建設，諸如汽油管線、交通運輸、自來水系統等的中控系統都逐漸數位化，這也代表數位服務基礎建設的安全和韌性，已經是民生基礎穩定的關鍵後盾。我們需要防範的不只是來自外部的惡意網路攻擊；在這些極度複雜且環環相扣的系統中，看似微小的環節失誤也可能造成大規模的系統癱瘓。

其實，Akamai 這份事件報告越顯得平凡無奇，對整個產業才是好的發展。這表示所有業者都樂於在事件發生後，投入時間精力探討問題來源。作者再次強調，事後調查和報告不是為了抓戰犯，而是正確了解這些數位建設作為現代社會基礎的重要性，鼓勵公開病灶和規律改善，持續鞏固數位服務的韌性及安全。

作者期許類似詳盡的報告能成為業界常態，也期許業者和大眾終能認知到數位服務已和公共安全密不可分，我們也應用對待公共安全的標準對待數位基礎建設。

衛星通訊及政府管制

APNIC 文摘

https://blog.twnic.tw/2021/09/01/19680/

本 APNIC 文摘原標題為 Satellite communication and regulation，由 Ulrich Speidel 撰文。

低軌道（Low Earth Orbit，LEO）衛星網路服務如 Starlink 和 OneWeb 的興起，加上即將推出的 Project Kuipe，重新燃起大眾對衛星網際網路通訊的興趣。這些興趣不僅限於低軌衛星能為網路服務未及地區帶來的好處，更多是位於網路發達地區，但對目前使用的網路服務不滿意的人，期待低軌衛星能實現他們對網路的期待。

直至目前為止，衛星網路的主要服務對象，是所在地區沒有光纖、數位用戶線路（digital subscriber line，DSL），或是便宜無線和行動通訊網路的人。現在，許多人開始吹捧衛星網路，聲稱它的傳輸速率會比地面網路更快。作者已經在 APNIC 部落格發表過一系列文章，詳盡介紹衛星網路的優缺點，本篇聚焦的重點議題，將決定你究竟可不可以使用衛星網路服務，以及你用的衛星網路服務，能不能做到目前地面網路做不到的事。

這二件事背後的決定因素，就是國家法規。

衛星通訊利用的是無線電波，這表示在一顆衛星接收訊號的通訊頻道中，必須只存在它要接收的那個訊號，否則輕則通訊干擾，重則衛星可能因此失常。

也因此，同一個地區不能有太多相鄰的衛星，或地面上同時有太多人在同一個頻道上通訊，否則彼此都會被嚴重干擾。這表示，衛星通訊不是隨便把一顆衛星丟到空中，然後任意選一個頻率開始

到處互傳訊號。你必須申請頻譜，這代表跟衛星地面站所在國家的監管機構交涉，通常還需要國際之間的協調，協調結果還必須獲得國際通訊聯盟（International Telecommunications Union，ITU）的認可。國際之間的通訊頻道協商是複雜的談判過程，每個國家都希望儘量取得越多頻譜越好，但又不能多到惹火其他國家，讓對方開始故意干擾你的訊號，或甚至因此開戰。

高度最高的同步衛星，無論傳輸或接收訊號的範圍都可涵蓋半個地球，這也表示他們的頻譜無論如何一定會與多個國家衝突。其他軌道上的衛星則依軌道傾斜度和高度不同，通常四散在二個緯度之間，隨著他們經過的國家領土變換通訊頻譜。這的確是更彈性的作法，但也讓運作變得更複雜。然而，無論是同步衛星，或是較低的中軌道衛星和低軌衛星，都受法規限制而無法達到最高傳輸速率。

國際之間的頻譜協調，更容易遇到當地的各種規範阻礙。對國家政府而言，只因為你的衛星會飛過我的國土上方，有辦法跟我國領土內的地面站通訊，並不代表我就希望你的衛星為我國民眾服務。

國家拒絕的原因百百種，有些地方可能網路服務由中央政府壟斷，額外的衛星網路服務等於破壞生意。有些地方可能害怕人民可以透過衛星網路服務，取得政府不想要他們接收的資訊。有些政府則可能提出條件，要求衛星服務供應方封鎖特定網站或服務，才讓對方提供衛星網路服務。在後者情境下，對政府而言最理想的處理方式，是衛星服務業者把控管通訊閘道的地面站設在國內，繳錢連結政府設立的防火牆，由政府一手把關人民可以取得和傳送的資訊。

當然，這種政府行為不僅限於低軌衛星。無線電波無視國界的特性，從過去就常是專制政府的眼中釘。作者來自德國，他至今仍

記得所謂的「西方電視」在推倒柏林圍牆中扮演的角色有多關鍵。更不用說二次世界大戰期間，許多德國人在希特勒統治下，仍冒著生命危險聽 BBC 廣播。也因為這種情形，伊朗政府在 1984 年立法禁止人民持有或使用無線電視，但大部分民眾仍持續觀看無線電視。

然而，衛星網路和衛星電視不同，知法犯法的難度變得很高。這是因為網路需要雙向通訊，不像電視只由衛星發送訊號給使用者。而一旦使用者必須傳送訊號，就很容易被政府發現，並循線找到訊號來源。

作者指出，有時候即使不在這種嚴格管制衛星通訊的國土境內，使用者仍會受到影響。中國就曾經禁止所有飛過該國領空的外國航空公司利用衛星提供機內無線網路，作者自己也有多次搭乘漢莎航空和全日空往返歐洲及日本時，在中國領空出現網路問題的經驗。同樣的道理，任何在中國登記營業的航空公司，旗下飛機的機內無線網路都位於「防火長城之內」。

Starlink 的接受器「Dishy」天線中內建有 GPS 接收器，是公開的事實。作者認為這個接受器的真實功能是問題關鍵；究竟是為了協助接收器定位衛星，還是確認使用者的「Dishy」接收器沒有被移出基地臺？後者技術上而言並無不合理之處，因為 Starlink 可以透過這種方式，確認特定地區中正在使用服務的訂戶人數。

但換個角度而言，在管制人民網路自由的國家中，這個 GPS 也很可能被用來封鎖使用者希望取得的網路服務或內容。最糟的情況下，國家當局甚至可能會利用這個 GPS 資料找到你的位置，登門請你去「喝茶」。

個人意見：從 Facebook 的錯誤中學習

APNIC 文摘

https://blog.twnic.tw/2021/11/05/20411/

本 APNIC 文摘原標題為 Opinion: Learning from Facebook's mistakes，由 Geoff Huston 撰文。

今年 6 月內容傳遞網路（content delivery network，CDN）服務供應業者 Akamai 因為系統設定上的失誤，引發大規模斷網事件，受害者包括數家澳洲和紐西蘭大型銀行、澳洲郵政、香港股市和全球多家航空。根據事後統計，約 500 家企業的網站都遭波及，網站因此斷線長達 4 小時。

本文作者，APNIC 首席科學家 Geoff Huston，在事件後特地發表部落格文章，稱讚 Akamia 事後發表的聲明不同於過去網路斷線事件的企業聲明，清楚且詳盡，並期許未來類似事件發生時，能看到更多和 Akamai 相似的聲明。

今年 10 月 4 日，Facebook 也發生了斷網事件。考慮到全球的 Facebook 使用者人口，這很可能被視為網路史上影響範圍最大的斷網事件。

那麼，關於這次斷線事件我們知道什麼呢？根因是什麼？Facebook 做了什麼緊急補救措施？為什麼修復時間竟長達 6 小時之久？Facebook 是否有採取任何後續措施，以防未來發生類似事件？簡而言之，從全世界最受歡迎、影響力無遠弗屆的平臺，竟然把自己下架 6 小時的事件中，業界可以學到什麼教訓？

然而，Facebook 在事件後第一時間發表的聲明中，除了道歉並確認事件並非外部攻擊所導致外，沒有就上述問題提供任何解答。

作者認為，這份聲明可謂完美示範了怎麼寫出整整四段文字但什麼都沒說。

另一方面，非當事人的 Cloudflare，光從外部角度，就能把事件的來龍去脈說明得更清楚。根據 Cloudflare 的部落格文章，事件的根因是 Facebook 從權威域名伺服器中移除了 facebook.com 的邊界閘道協定（Border Gateway Protocol，BGP）路由。

其實，在 DNS 中，移除 BGP 路由的時間若不是太長，通常不會造成什麼問題。這是因為 DNS 的運作重度仰賴遞迴解析器中儲存的 DNS 快取資訊，只要快取的存活時間（time to live，TTL）夠長（超過一天），那即使路由被移除，大部分的遞迴解析器仍能仰賴快取資訊順利運作。也就是說，如果使用者的網路有設置多個不同遞迴解析器，那使用者可能完全不會發現任何異樣。更何況，以 Facebook 的熱門程度而言，大部分的解析器中，應該都留有該網站的域名快取資訊。

然而，Facebook 設定的 TTL 時間非常短。也因此，一旦 BGP 路由被移除，快取隨之過期，解析器就再也無法透過域名找到權威伺服器了。作者解釋，這種「找不到」是 DNS 最討厭的「找不到」；因為這種情況下，用戶端送出的查詢雖然找不到權威主機，但並不會得到「NXDOMAIN」（此域名不存在於 DNS）的回應，只會等到超時還是沒有回應。

等不到回應的遞迴解析器，會就伺服器儲存的所有 IP 位址，再次一筆一筆送出查詢，同時回傳「SERVFAIL」代碼給用戶端。這個代碼的意思是「雖然我無法解析這筆域名，但很可能是我的問題，不妨試試其他解析器」。如此一來，用戶端的解析器又會向網路中其他遞迴解析器再次送出查詢，重複上述徒勞無功的工程。Cloudflare 的部落格文章解釋，全世界想連到 Facebook 的人實在太多了，於是全球的 DNS 解析器突然必須同時處理比平常多 30 幾倍

的查詢，其他平臺網站的連線也可能因此受到影響。

雪上加霜的是，就在 Facebook 域名從網路上全面消失的時候，公司內部的指令控制工具似乎也不見了。連 Facebook 設於全球各地的資料中心都無法交換訊務，整個情況因此變得更嚴重。

作者總結，我們可以從這次事件學到的教訓包括：

- 每次需要改變網路設定時都務必先行演練，並規劃好備用方案。
- TTL 在 DNS 中很重要。如果要使用時限短的 TTL，所有相關設定都必須加倍謹慎，因為一旦問題發生，將無法仰賴快取應急。
- 不要把所有雞蛋放在同一個籃子裡。以 DNS 設定而言，就是不要把所有權威 DNS 域名伺服器都放在同一個自治系統（Autonomous System，AS）的同一個 BGP 裡。
- 最好分開管理公司內部的指令控制工具操作系統和產品開發服務；二者的基礎建設、路由和 DNS 域名都要分開設定。如此一來，即使指令操作出了問題，至少還能照常提供服務。
- 「行動迅捷，勇於破壞」（move fast, break things）的行事作風，結果只會讓東西壞掉而已。每一次壞掉都只會讓使用者越來越不耐煩，最終選擇放棄使用你的服務。
- 「速度」和「韌性」之間只能擇一時，企業必須審慎思考願意承擔的風險，以及服務失效的後果。對某些公司而言，樂於擁抱高風險可能是經營理念，但公司的顧客、廣告商和股東是否抱持相同理念？

本文發表日期後，Facebook 於自家網站發布更詳細的事件報告。作者也將此報告的連結補充在部落格文章留言處。新的事件報告中，Facebook 表示每次事件後，他們都會展開詳盡的事後調查，進一步加強系統的韌性。Geoff 進一步指出，這個「加強系統韌性」

的使命應擴及整個網際網路，向航空和核能取經，了解如何以產業為單位從事件學習教訓，每一次的改善都應是整個產業的共同進步。

DNS 是否開放？

APNIC 文摘

https://blog.twnic.tw/2021/11/24/20940/

https://blog.twnic.tw/2021/11/18/20956/

本 APNIC 文摘原標題為 DNS openness，由 Geoff Huston 撰文。

本文作者，APNIC 首席科學家 Geoff Huston 今年 9 月底受歐洲電子通傳監管機構（Body of European Regulators for Electronic Communications，BEREC）之邀出席工作坊，針對「DNS 開放程度」（DNS Openness）發表見解。本文即為作者在工作坊的分享內容。

首先，作者解釋 BEREC 的「DNS 開放程度」意指為何。他解釋，BEREC 考量的 DNS 開放程度，並不僅限於「開放競爭」的特定意涵，而包括資訊內容的取得和傳播、應用程式及服務的使用和提供，以及使用 DNS 服務時，使用者在連網裝置的選擇上是否不限使用者所在地區，或欲取得之資訊、內容、應用程式或服務地區的限制？

也就是說，這裡的「開放」，其實是想知道 DNS 是否統合一致。

其實，若所謂「DNS 開放程度」只是在問大家是否都能使用 DNS、所有 DNS 伺服器的回應是否一致，那答案是肯定的，因為這就是 DNS 的設計初衷。DNS 的設計原理，就是以回應查詢的一致性為本，容許遞迴及本地解析器仰賴快取加速資訊的傳遞。DNS 的回應也不會因對象而異；無論送出查詢的是誰、位置在哪、使用哪個平臺，伺服器都只會回傳一樣的回應。

當然，以上是設計原理最理想的實踐狀態，實際狀況更複雜多變。事實上，並非每個使用者看到的 DNS 都一樣，對於「我們身

處同一個網際網路中嗎」的問題，作者的回答是「我無法肯定，但的確希望如此！」

不同國家對國內網路服務供應業者有不同的法規限制，這直接影響業者針對某些域名提供「正確」DNS 解析回應的能力。一般人第一個聯想到的例子，可能是中國和網路長城。事實上，諸如英國、美國、澳洲、印度、俄羅斯、伊朗、越南、法國及土耳其等，很多族繁不及備載的國家，都有國內專屬的 DNS 限制規範。有些國家的作法是直接禁止解析特定域名，有些則會以「無此域名」（NXDOMAIN）回應，也有些是直接將使用者引導至別的域名。

作者以自己國家為例，澳洲 1997 年頒布的《電子通訊法》中第 313 節規定，通訊業者依法必須「盡全力防止電訊網路被用於違法用途」。實作上，這代表澳洲的網路服務供應業者（Internet Service Provider，ISP）必須自主設置過濾機制，阻擋內容涉及暴力、恐怖主義及犯罪行為的域名解析。

在 DNS 中，「清白饋送」（clean feeds）也獲得某種程度的歡迎；有些解析器會提供「不解析與惡意軟體、濫用或犯罪內容、竊聽軟體，以及類似濫用行為或安全威脅之域名」的功能，市面上如 Quad9 或 Cloudflare 的 1.1.1.2 惡意軟體封鎖解析服務都屬此類。若使用者選擇開啟此功能，實質上等於利用 DNS 過濾內容。

除此之外，也有更改 DNS 回應以營利的作法。其中代換 NXDOMAIN 回應的手法最為常見：在此情境下，當使用者鍵入尚未被註冊的域名，並不會收到「此域名不存在」的回應，而將被引導至預先設定的搜尋引擎或類似網頁。.com 和.net 的註冊管理機構 Verisign 可謂此手法的先驅，他們在 2003 年用此方式，把所有輸入未註冊.com 和.net 域名的使用者導向 Verisign 的宣傳網頁。

Verisign 的作法是在域名區域檔案中插入萬用字元（wildcard）登錄資料，以達到以上效果。嚴格來說，這並沒有「破壞」DNS

的一致性，只是巧妙利用了 DNS。但在這之後，越來越多模仿作法變本加厲，許多最終跨越了那條線，DNS 的一致性也因此受到影響。

作者認為，DNS 是否統合一致的討論核心，其實是在探究網際網路基礎建設是否誠實無欺。域名和路由是網際網路基礎建設的二大弱點，即使終端一切運作如常，若路由的真實性不保，則使用者就算被誤導至錯誤目的地，也將一無所知。

在惡意軟體猖獗的今日，許多人可能同意，甚至強力支持業者無論是依法或為防範安全威脅而過濾訊務，雖然這也代表 DNS 不再完全一致。或許也可以說，在安全與統合一致的 DNS 之間，大多數人為了保全前者，願意在後者上作出妥協。

除了統合一致外，還可以用更多不同角度解讀「開放」。

DNS 的解析協定是由網際網路工程任務組（Interenet Engineering Task Force，IETF）發布的公開標準，沒有任何使用對象的限制。在此之中，幾乎所有協定都不受智慧財產權限制，而更改協定的 IETF 流程也開放所有人參與。若以常見的「開放」標準而言，作者肯定 DNS 是一個開放系統，也可視為開源系統。

再者，若開放服務代表所有人都可以使用 DNS 系統提供的域名解析服務，則 DNS 也算是一種開放服務。當然，這是以公共 DNS 而言，企業內部自架或刻意設計的封閉系統在此不納入考量。

DNS 的內容呢？DNS 系統裡承載的資訊是否公開開放？若要精細區分區域檔案和檔案中的每筆紀錄，前者可能不是，但後者完全公開。除此之外，DNS 查詢和回應預設並未加密，所以也算是公開資料。

然而，最後一項特徵，如今成了 DNS 的最大問題。這表示只要有心，任何人都可以輕易透過蒐集、彙整 DNS 訊務資料，大致摸透目標對象的網路行為。

作者指出，在此情境下，所謂的「開放」不再是強項，而變成了弱點。這不一定是 DNS 本身的弱點，而是我們這些網際網路使用者的弱點。DNS 是所有網路行為的基礎，而其身為開放協定的特性，表示我們這些使用者的資訊和行為，都因此公開給任何想偷窺的第三方蒐集利用。

難道不得不像魚缸裡的金魚一樣公開任人觀賞，就是我們使用網際網路必須付出的代價？難道公開開放、信任，以及隱私保護之間，一定必須犧牲後者以保全前二項價值？若不是，我們應該如何在這之中取得平衡？

由於 DNS 是網際網路的核心，作者認為，DNS 是用來觀察網際網路中諸如隱私管理、信任、統合及分裂、濫用及破壞等議題的有效濾鏡。在眾多議題中，他選擇深入探討信任、域名解析及分裂化 3 個議題；這三者將是取決 DNS 能否持續作為中心膠著劑，支撐整個網際網路的關鍵。

DNS 與信任

作者認為，「過度信任的協定」最能精準形容 DNS 解析；這個協定彷彿來自另一個只存在互信互愛的世界。在 DNS 解析協定中，向伺服器送出查詢後，解析器無論收到什麼回應都會百分之百相信。然而，現實是 DNS 系統非常容易駭侵，有心人士可以輕鬆從中攔截、代換或假造回應，但送出查詢的那端卻完全無法確認。換句話說，信任在 DNS 中反而帶來傷害。

為了減緩傷害，後代開發出驗證 DNS 回應的方法，透過在根區簽署 DNS 紀錄，並在解析過程中驗證數位簽章，確保傳給終端的回應完整正確。這個技術叫做 DNS 安全擴充（DNS Security Extensions，DNSSEC）。

然而，自 2004 年出現至今，DNSSEC 的全球部署率仍僅有 3 成左右。而這異常平緩的成長幅度，可能來自幾個原因。

首先，解析器若要進行 DNSSEC 驗證，需要耗費更多效能和時間。當然，在快取正常發揮作用的前提下，這些必須多花的效能和時間幾乎微不足道。但不可否認，DNS 回應附帶數位簽章後尺寸增加，也會造成其他效能問題，而這就不是快取能輕易解決的了。簡而言之，在極度重視速度和效率的 DNS 中，DNSSEC 耗能和耗時的問題實難以忽略。

另一個問題在於付出和回報的不平等。DNSSEC 部署的最終受益人是終端使用者，但大部分使用者連網際網路仰賴 DNS 運作都一無所知，遑論要求驗證自己的 DNS 查詢和回應。DNS 解析只是 ISP 供應的基本服務之一，而對根本不知 DNS 是什麼的使用者而言，DNS 的品質絕非選擇 ISP 的參考標準。

另一方面，對通常負責提供遞迴解析器服務的 ISP 而言，部署 DNSSEC 不僅花錢、花時間，增加 DNS 服務出錯的風險，使用者也無感，毫無經濟效益。在權威伺服器方面，他們雖然有動機取得數位簽章，證實自己轄下域名真實無誤，但若中轉的遞迴解析器和使用者端的解析器都不驗證 DNSSEC，那即使花錢安裝了 DNSSEC，也無法發揮效用。

DNSSEC 重要性和部署率的顯著反比，是市場失敗的典型案例。但這個失敗案例隱含更嚴重的後果；若整個 DNS 生態系統無法同心協力加固、改善 DNS 信任，那重視此價值的人只好另循管道，如把一部分 DNS 分割出來，並透過其他手段確保此特定部分的安全及信任。

DNS 解析

解析器是 DNS 系統的「中間人」，負責連結終端使用者和權威伺服器。然而，這個「中間」的角色，也意味著他們的資源最青黃不接。使用者不會為每筆解析器處理的查詢回應付費，伺服器也不會依解析器每筆回傳的查詢或快取資料付費。換句話說，解析器無論從上游或下游，都拿不到與勞力付出相應的報酬。

ISP 對此的因應作法，是把解析服務的開銷納入向顧客收取的網路使用費率。然而誠如上述，一般使用者對 DNS 解析的品質毫無要求，也不會以此作為選擇 ISP 的依據；對 ISP 而言，提供 DNS 服務只賠不賺，絕對不能在上面多花資源。這惡性循環的結果，是 ISP 提供的解析服務往往軟體版本過時，服務品質也不怎麼樣。

一般使用者可能難以察覺差異，但對速度就是生命、極度重視 DNS 解析效率的開發人員而言，ISP 提供的解析服務難以滿足需求。來自第三方的公共解析服務因應而生；使用者可以選擇不用自己 ISP 提供的解析服務，改使用第三方的公共解析服務。

根據 APNIC 量測數據顯示，約 65%的網路使用者會用 ISP 提供的遞迴解析服務，35%則選擇繞道使用第三方提供的公共解析服務。

作者提醒，不能將此數據解讀成「35%個人使用者自行選擇改用開放解析服務」。構成這 35%的有很多是 ISP 業者；換言之，他們連自架解析服務系統都不做，直接使用公共解析器為客戶提供服務。作者推測，這種做法最大的動機是省錢。不只如此，許多企業基於服務韌性和持續性的考量，比起 ISP，也更偏好使用公共解析服務。

既然全球有 35%在使用公共解析服務，是否代表公共解析服務的市場競爭一定百家爭鳴、十分激烈？很可惜並非如此。事實是，

Google 的公共解析服務 8.8.8.8 就占了這 35%的 30%。

在此就不贅述公共解析服務過度集中於 Google 的正反效應，但必須謹記的是，DNS 作為網際網路的核心基礎建設，保持高度獨立和中立非常重要。而 DNS 中有如此顯著的一部分僅仰賴單一供應方，無論對方是否立意良善，對 DNS 的長遠健全都是一大隱憂。

DNS 分裂

在 DNS 信任的段落最後，作者提到若整個 DNS 無法系統性地改善信任問題，特別重視此議題的人將另循管道，如把一部分 DNS 分割出來，透過其他手段確保此特定部分的安全及信任。若你這聽起來很像 DNS 被分裂了，那你想的沒錯。

DNSSEC 能保障使用者收到的 DNS 回應正確完整，但無法保護 DNS 的訊務隱私。為了達到保護隱私的目的，許多新技術如 DNS over TLS（DoT）、DNS over HTTPS（DoH）因應而生，但類似技術的發展演進，讓許多人擔憂這會把 DNS 解析功能越來越推到終端應用層次。

擔憂的人有擔憂的理由，支持此發展的人也有其根據。對後者而言，這樣的演變可以提升應用程式的敏捷度、彈性和反應速度。對追求日新月異的網路內容及服務產業而言，與其坐等因缺乏資源而進化遲緩的 DNS 基礎架構演變成符合需求的樣貌，不如把事情集中於終端自行解決。

然而，這也代表 DNS 分裂不再是危言聳聽，而是很可能實現的未來。

最後作者指出，真正的開放技術並非不容變更、只供鑑賞的博物館展示品，應是擁抱創新、接受使用者和開發人員的改變。雖然

有些網路治理組織或單位，希望透過所謂的多方利害關係治理模式，廣納不同利害關係人的觀點，最終在不同目標中取得妥協，但這種緩慢的進程，可能趕不上直接粗暴的市場力量。

某種程度而言，DNS 的發展反映了網際網路大環境的演變：在缺乏法規管制，僅仰賴市場力量和使用者偏好作為發展驅動力的環境中，結果往往是沒有迴旋餘地的勝負，而且贏者全拿。

DNS 可以在此多方壓力中保持原樣，仍以單一、統合且一致的域名空間為網路使用者服務嗎？作者沒有答案，但他的結論仍是樂觀的。他認為，本文列出的種種都顯示 DNS 在改變，而這也代表 DNS 仍保持開放，願意接受變革，甚至轉型。這是好的象徵。

DANE 的過去、現在與未來

文／中華電信工程師 林方傑

https://blog.twnic.tw/2021/04/15/17961/

DANE 是為了緩解什麼問題？

關於 DANE（DNS-based Authentication of Named Entities）問世的理由，筆者認為必須從「在網路上安全傳輸」的需求講起。資訊安全至少有 CIA 三個面向[1]，我們先關注其中的「Confidentiality」。如何避免所傳送的資料遭竊取？「加密傳輸」是理所當然的對策。而加密傳輸最直覺的做法，是由連線二端約定好加解密的關鍵（如對稱式加密金鑰），只要協議夠複雜且未被外界得知，則資料的隱密性在傳輸過程中應可得到一定程度的保障。

但有個衍生（類似雞生蛋、蛋生雞）的問題是，在尚未完成加密傳輸協議的情況下，**連線二端如何確保加解密關鍵不被第三方得知呢？**這時「非對稱加密演算法」的「以公鑰加密只有對應之私鑰可解密」之特性便能派上用場。由於私鑰只應由金鑰製造者持有，選用對應公鑰來加密訊息便確保了只有私鑰製造／持有者可解密[2]。

然而，這又會衍生另一個問題，若誤將駭客的公鑰當作原連線對象所提供，或者連線對象根本是冒名頂替的，則資料仍可能被揭露給非預期的對象。那麼**如何確保公鑰及對象正確呢？**找第三方掛保證是有幫助的選項。現行「公開金鑰基礎建設」（Public Key

[1] 關於 CIA 可參閱：https://www.forcepoint.com/zh-hant/cyber-edu/cia-triad

[2] 關於 HTTPS 原理、對稱式加密、非對稱式加密可參閱：https://medium.com/@RiverChan/基礎密碼學-對稱式與非對稱式加密技術-de25fd5fa537、https://www.youtube.com/watch?v=w0QbnxKRD0w 等解說。

Infrastructure，簡稱 PKI）[3]機制中，有「憑證頒發機構」（Certificate Authority，CA）當掛保證的第三方，負責將公鑰及公鑰來源方的識別等資訊製成「數位憑證」（digital certificates）供查驗。由於數位憑證是基於「數位簽章」（digital signature）[4]技術，可保障資料的「完整性」（Integrity）及「不可否認性」（Non-Reputation）。在網路世界中，被連線的伺服器便可靠這樣的憑證（實務所需的格式及內容如 RFC 5280「X.509」所定義），對外做出「自己是域名的合法代表、是正確公鑰的提供者」等有力聲明[5]。

但，CA 總是可信嗎？撇開惡意 CA 或作業疏失導致錯發（mis-issue）憑證，現行「PKIX」（Public-Key Infrastructure for X.509 certificates）機制中，任何 CA 可為任何域名簽發憑證[6]。這種自由度的風險在於，若一家規模較小的 CA 遭駭並胡亂為知名公司或服務的域名簽發了憑證，這將給予駭客絕佳的攻擊機會。舉個例子[7]，假設 Jason 架了個網站，並以域名 a-example-domain.com 搭配 CA1 簽發的憑證對外提供服務。而駭客可從比較沒那麼有名、審查不是那麼嚴格的 CA2，也為 a-example-domain.com 取得另一張憑證，置於假造的站臺主機。如果再搭配快取污染（cache poisoning）等手段誤導終端客戶連上駭客的假站臺，由於 CA2 的憑證也有效，瀏覽

---

3 關於 PKI 可參閱：https://zh.wikipedia.org/wiki/公開金鑰基礎建設等說明。

4 關於數位簽章可參閱：https://medium.com/@yellowgirl3614/密碼學-三-數位簽章-f8c6a78da46b 等專文。

5 關於數位憑證筆者參閱了：https://medium.com/schaoss-blog/前端三十-28-web-http-和-https-的差別是什麼-21ccafb6f36f、https://www.ssl.com/faqs/what-is-an-x-509-certificate/等介紹。

6 Richard Barnes (2011.10.6). DANE: Taking TLS Authentication to the Next Level Using DNSSEC. IETF Journal. https://www.ietfjournal.org/dane-taking-tls-authentication-to-the-next-level-using-dnssec/

7 引用自：https://docs.microsoft.com/zh-tw/windows-server/networking/dns/what-s-new-in-dns-server。

器網址欄同樣有個精美的鎖頭，一般用戶不容易察覺有異。實際案例可參閱 2011 年 DigiNotar 遭駭等事件報導[8]。

有哪些對策、如何緩解？

因應上述的問題，「憑證透明」（Certificate Transparency，CT）、「HTTP 公鑰固定」（HTTP Public Key Pinning，HPKP）等安全機制被提出。前者（CT）要求 CA 將所簽發憑證都登錄到可供查驗的日誌，但一般認為資訊透明主要補強憑證誤發後偵測及追查，事前的防範則幫助有限[9]；後者（HPKP）原理是在 HTTP header 中指定 CA、讓使用者第一次連線取得並記下供後續驗證，但這方法因缺乏彈性已式微[10]。

DANE 也能用來保護域名免受錯發或濫發憑證的糾纏。考量網路連線乃至憑證的簽發本來都與域名息息相關，加上有 DNSSEC（Domain Name System Security Extension）這個安全協定可確保 DNS 所傳遞資料的完整性（data integrity）、來源可驗證性（origin authentication of DNS data），以及可驗證之不存在性（authenticated denial of existence）[11]，DNS 應該是個不錯的傳遞憑證相關資訊之管道。而 DNS 紀錄的公開性（任何人都可透過 DNS 查詢取得）[12]更

---

[8] 關於 CA 遭駭可參閱：John Leyden (2011.9.6). Inside 'Operation Black Tulip': DigiNotar hack analysed. The Register. https://www.theregister.com/2011/09/06/diginotar_audit_damning_fail/、Comodo SSL Affiliate | The Recent RA Compromise. https://zephyrnet.com/comodo-ssl-affiliate-the-recent-ra-compromise/

[9] 關於 CT 的討論筆者參閱：https://blog.apnic.net/2019/07/05/whither-dane/、https://certificate.transparency.dev/

[10] 關於 HPKP 的議題筆者參閱：https://zh.wikipedia.org/wiki/HTTP 公鑰固定、https://blog.gslin.org/archives/2016/09/14/6842/hpkp-遇到的阻礙/

[11] DNSSEC 的優點引用自〈DNSSEC 安全技術簡介〉，http://www.cc.ntu.edu.tw/chinese/epaper/0022/20120920_2206.html

[12] 關於 DNS 紀錄為公開資料可參閱筆者文章〈重新認識 DoT/DoH、DNSSEC

可讓客戶端直接自域名維運者（DNS operator）取得第一手且可信的「憑證聲明」[13]，做為後續查驗憑證的指引或依據。

那麼，DANE **的憑證聲明可以如何派上用場呢？**承前例，如果 Jason 為 a-example-domain.com 設定 A 或 AAAA 紀錄、定義站臺伺服器 IP 位址的同時，也透過 DNS 紀錄對外聲明：「我這域名只該搭配 CA1 所簽發的憑證」，則當終端客戶被誤導向 CA2 的假站臺時，就可索取並對照上述 Jason 關於憑證的聲明，從而獲得發現異常的機會。反過來說，對於 CA1（或任何被青睞且被聲明的 CA）來說，也可在將 a-example-domain.com 的憑證簽發給聲稱是 Jason 的人之前，先透過 DNS 查詢、參考 DNS 紀錄所承載的聲明，來確認 Jason 是否真的要索取一份本 CA 的憑證[14]。

而除了如上述規範可簽發憑證的 CA，限制可用的憑證是哪幾張，甚至直接指定「信任錨點」（trust anchor）[15]都屬於 DANE 的使用案例（use case）。依照 RFC 6394，憑證聲明可分為「CA Constraints」、「Service Certificate Constraints」、「Trust Anchor Assertion and Domain-Issued Certificates」如表 1 所列：

的定位與原理〉，https://blog.twnic.tw/2020/02/27/6205/

13 Richard Barnes (2011.10.6). DANE: Taking TLS Authentication to the Next Level Using DNSSEC. IETF Journal. https://www.ietfjournal.org/dane-taking-tls-authentication-to-the-next-level-using-dnssec/。其中「DNS/domain operator」雖然不見得等同於「domain holder」或 service owner，但前者一定經後者授權才能扮演此角色。

14 Richard Barnes (2015.10.14). Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE). https://datatracker.ietf.org/doc/rfc6394/、Eric Osterweil (2015.8.6). A New Internet Architecture for Secure Key Learning: DANE. https://cs.gmu.edu/~eoster/doc/2015-08-US-Telecom-DANE.pdf

15 關於 trust anchor、chain of trust 的觀念筆者參閱：https://medium.com/@clu1022/那些關於 ssl-tls 的二三事-十二-chain-of-trust-f00da1f2cc15、https://csrc.nist.gov/glossary/term/trust_anchor

CA Constraints	客戶端只應該接受指定 CA 所簽發的憑證
Service Certificate Constraints	客戶端只應該接受特定的憑證
Trust Anchor Assertion and Domain-Issued Certificates	客戶端只應該接受「域名提供」之信任錨點及憑證

表 1　DANE 的憑證聲明

資料來源：筆者翻譯自 Richard Barnes (2011; 2015)

其中，「CA Constraints」及「Service Certificate Constraints」由於規範的是憑證或信任錨點，使 DANE 可做為現行 PKIX 的輔助，而不只是替代方案。相對的，「Trust Anchor Assertion and Domain-Issued Certificates」則補強了自簽或系出「無」名門憑證的缺陷，如終端客戶、瀏覽器、乃至 OS 通常不會有這些憑證的信任錨點（以判斷憑證簽發單位的真偽）。在現行 PKIX 機制下，面對瀏覽器「此網站的安全性憑證有問題」的提醒，終端客戶也只能接受憑證並承擔風險；但在 DANE 的運作下，終端客戶可基於 DNS（SEC）提供的可靠聲明資訊（做為對照組），對所得之憑證有更大的信心。

實作面上，一種新的 DNS 紀錄類型「傳輸層安全性驗證（Transport Layer Security Authentication，TLSA）」被提出，每一筆 TLSA 紀錄都有「Usage」、「Selector/Matching」、「Certificate for Association」之欄位，如表 2 所列：

Usage	選用哪一種憑證聲明（選項如上表所列三項）
Selector/Matching	TLS 憑證應該如何比對，例如：完整比對，或者只比對雜湊值（hash digest）
Certificate for Association	實際要被比對的資料

表 2　TLSA 紀錄的欄位

資料來源：筆者翻譯自 Richard Barnes (2011);.RFC 6698 (2012)[16.]

[16] RFC 6698《The DNS-Based Authentication of Named Entities (DANE) Transport

關於各欄位的值域可參閱 RFC 6698，這裡先不詳述，而再承前例情境示範 TLSA 紀錄設定的方向：為了聲明終端客戶（針對此服務）只該接受 CA1 所簽發的憑證，Jason 可為 a-example-domain.com 的 https 服務提供一筆「_443._tcp.a-example-domain.com」的 TLSA 紀錄定義如表 3：

Usage	選擇代表「CA constraint」的值
Selector/Matching	提示待比對資料是如何取得（即如何被驗算），如 SHA-1 digest
Certificate for Association	CA1 本身憑證的雜湊值

表 3　TLSA 紀錄的應用

資料來源：筆者翻譯自 Richard Barnes (2011).

綜觀來說，DNS 解析及 DNSSEC 是 DANE 運作的基石。DNS 解析的公開性（指任何人都可查詢）可提高資訊透明度並有助於檢核[17]。DNSSEC 應用的數位簽章技術，可為 DANE 基於 DNS 解析傳遞憑證聲明等資訊的管道增加可信度。而基於域名階層所建構的 DNSSEC「信任鏈」（Chain of Trust）也使信任錨點數大為收斂（僅剩 DNS root 根域名）。相對的，web PKI 中每家 CA 都對應一個信任錨點、且有「任何一家 CA 可簽發任何域名的憑證」及「不同 CA 可為同一個域名簽發各自版本的憑證」等備受爭議的自由度[18]，使得資安防護在 web PKI 機制中因可攻擊的點多（每個信任錨點都可能是破口）而更具挑戰性。

Layer Security (TLS) Protocol: TLSA》https://www.ietf.org/rfc/rfc6698.txt

[17]https://www.farsightsecurity.com/blog/txt-record/caa-records-farsight-20170825/

[18] RFC 6698《The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA》https://www.ietf.org/rfc/rfc6698.txt

DANE 的現況及前景

前面都在說 DANE 的好話，接下來討論些待克服的挑戰及潛在問題。

首先是 DNS 相關議題：除了（伺服端）為域名進行 DNSSEC 簽署的比率待提升，DNS 解析的耗時（且 DNSSEC 牽涉額外、專用 DNS 紀錄的查詢）[19]、「DNS 維運者」隨 DANE 的發展而在網路資訊安全領域中的戲分越發吃重、會否增加單點失效的風險都需要各界集思廣益。而最關鍵的，客戶端的應用程式會否支援新 DNS 紀錄的查詢及結果的判讀，目前看來在 web 領域（即瀏覽器）的接受度及配合度不太樂觀（據說這與「CAA 紀錄」被發展相關，但是另一段故事了）[20]。

有趣的是，相對於在 web 領域的窒礙難行，mail 領域對 DANE 的態度就顯得親切得多。比如微軟就宣布其 Windows Server、Office 365 等產品或服務支援 DANE[21]，關於 DANE 如何為 SMTP 帶來幫助，則可參閱相關討論[22]。

---

[19] 引用自：https://blog.apnic.net/2019/05/27/dns-oarc-30-bad-news-for-dane/ 的 “extended time taken to perform DNSSEC validation…”

[20] 關於 DNS、DNSSEC 應用在 DANE 的意義，DANE 所遭遇的反對引用自：https://blog.apnic.net/2019/07/05/whither-dane/。

[21] https://techcommunity.microsoft.com/t5/exchange-team-blog/support-of-dane-and-dnssec-in-office-365-exchange-online/ba-p/1275494、https://www.theregister.com/2020/04/07/microsoft_dane_office/

[22] https://blog.apnic.net/2019/11/20/better-mail-security-with-dane-for-smtp/

NCSC 發布分散式帳本技術白皮書

國際瞭望 撰輯

https://blog.twnic.tw/2021/06/03/18657/

由於比特幣這類以區塊鏈技術為基礎的加密貨幣日漸流行，分散式帳本技術（Distributed Ledger Technology，DLT）的知名度大大提升。因此，英國國家網路安全中心（National Cyber Security Centre，NCSC）特別發布分散式帳本技術白皮書，協助相關人員權衡使用 DLT 技術的風險效益及優缺點，以判斷是否要採用。

本文撰述了部分白皮書內容，並釐清對於 DLT 技術的誤解如下述：

- 區塊鏈並非「資料庫，而是一種儲存資料的方式。換句話說，區塊鏈是一種 DLT 技術：使用者僅能增加資料，不得篡改既有資料。許多組織已建構自己的區塊鏈系統，但目前沒有建置系統的通用做法，系統間通常互不相通。
- DLT 技術有諸多不同類型，且集中化及透明化的程度各不相同，相異的 DLT 技術具有截然不同的基礎資料結構，保持正副本同步的相關機制也各自歧異。舉例而言，比特幣的區塊鏈系統與用於虛擬公證服務的 DLT 技術幾乎無共通之處。
- DLT 技術並非總是儲存資料的最佳選擇。儘管 DLT 技術在某些去中心化的情境下有用，但它們也有許多缺點，包括：高成本、規模限制、不利隱私，以及缺乏變更設計的靈活性。當資料持有人依法須刪除特定資料時，DLT 技術僅能追加而無法刪除資料的特性也將帶來困擾。此外，若公鑰被當成身分識別工具，一旦使用者遺失私鑰或資料外洩，將無法存取

資料或證明資產所有權。

- 目前 DLT 技術尚處於開發階段，其安全性研究並不充分，DLT 技術系統架構通常相對複雜，且許多相關技術仍未經測試。此外，部分 DLT 技術靠著涉及大筆金錢的特性（如：虛擬貨幣）確保資料完整性，這也使安全性評估更加複雜。
- DLT 技術在某些情況下（如去中心化環境中）的確有其效用，加密貨幣、數位資產交易平臺及虛擬公證服務皆為相關案例。

參考資料：

1. https://www.ncsc.gov.uk/blog-post/is-blockchain-the-right-tool-for-you
2. https://www.ncsc.gov.uk/whitepaper/distributed-ledger-technology

DNS 安全協調技術研究小組（DSFI-TSG）期中更新

國際瞭望 撰輯

https://blog.twnic.tw/2021/06/21/18926/

根據 ICANN 財政年度 2021-2025 戰略計畫，ICANN ORG 應與社群協作，針對安全及穩定議題，建立一個有效加強協作溝通的機制。有鑑於此，ICANN 於 2020 年 5 月成立「DNS 安全協調技術研究小組」（Domain Name System Security Facilitation Initiative Technical Study Group，DSFI-TSG）。

小組召集人，同時也是 ICANN 安全與穩定諮詢委員會（Security and Stability Advisory Committee，SSAC）駐董事會聯絡人的 Merike Käo 近日發表部落格文章，表示小組在一年工作後取得長足進展，已著手準備撰寫建議報告。

TSG 充分探討在強化 DNS 生態系統中多方利害關係人協作互動、進而加強 DNS 安全上，ICANN 的能力及義務。小組列出各種惡意攻擊事件使用的攻擊向量（attack vector）並以重要程度排序，也找出各攻擊向量的對應緩解方案。除此之外，既有緩解措施中技術、執行及程序上的落差，以及尚未出現緩解對策的空缺處，小組都逐項記錄。

研究小組過去一年來定期舉行為時 3 小時的雙週會議，小組成員背景各異（事件回報、技術標準、ICANN 政策及既有程序、執行現況），也確保研究小組在剖析此複雜重大的議題時，保有靈活且多元的觀點，進而作出全面且充分評估的決定。

如前所述，研究小組已準備開始撰寫建議。在提出建議時，小

組主要考量的重點包括：

- 可以幫到誰？
- 誰將負責執行？
- 執行時可能遇到哪些挑戰？
- 誰有責任、辦法協助面對這些挑戰？
- ICANN 在這之中扮演的角色？

ICANN DNS 論壇（ICANN DNS Symposium）於今年 5 月 25 至 27 日舉行，研究小組亦於論壇首日簡報，分享工作進度。論壇期間的議程簡報及錄影皆會公布於論壇網頁，供感興趣的人們前往查看。

參考資料：

https://www.icann.org/en/blogs/details/dns-security-facilitation-initiative-technical-study-group-interim-update-20-5-2021-en

2021 年 IPv6 部署概況

APNIC 文摘

https://blog.twnic.tw/2021/07/16/19213/

本 APNIC 文摘原標題為 IPv6 adoption in 2021，由 RIPE NCC 資深研究員 Stephen Strowes 撰文。

2011 年的「世界 IPv6 日」（World IPv6 Day）是第一次大規模測試 IPv6，進而促成 2012 年 6 月正式啟動 IPv6。今年是 2021 年，也是「世界 IPv6 日」十週年，IPv6 的全球部署率至今仍不盡一致。IPv6 在某些地區可能已是主要的網路協定，在某些地方則可能仍在未定的未來部署計畫中，大部分地區則散落在這二個極端之間。

這篇文章會回答二個問題：現在 IPv6 的全球部署情況為何，去年來又有什麼值得注意的變化？

首先回答第二個問題。COVID-19 疫情導致全球許多變化，網路訊務模式也是其中之一，如週間的網路訊務就大幅從企業網路轉向家用網路。從下面的 APNIC 互動地圖截圖，我們可以看到過去一年來，IPv6 部署程度差異最大的前 20 名。

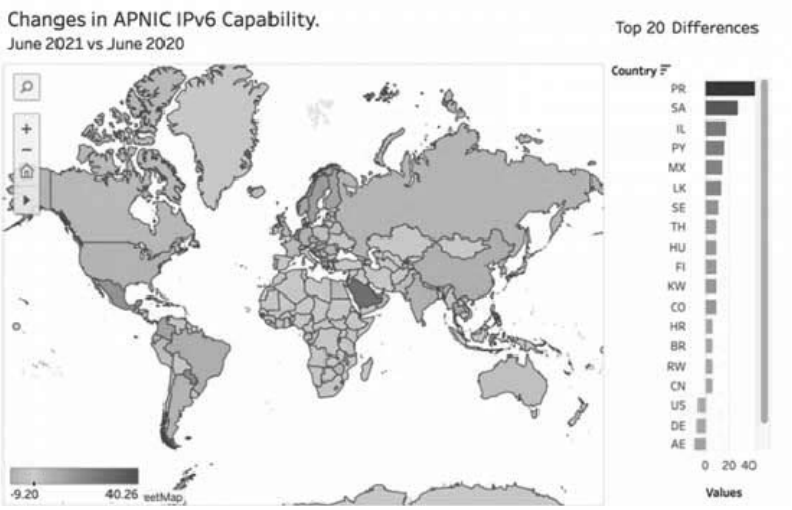


圖 1　IPv6 部署程度差異（2021 年 6 月 vs 2020 年 6 月）

顯示灰色的部分表示沒有改變，藍色表示 IPv6 部署率，橘色則表示 IPv6 部署率降低。

從圖中可看出，波多黎各很明顯是去年 IPv6 部署率成長的最大贏家，當然，我們也必須記得波多黎各的人口數相對偏低，而且鑑於該地的特殊屬性，有時可能難以判定資料確切的地理位置來源。大型美國網路業者也都在波多黎各提供服務，所以波多黎各行動通訊網路的高 IPv6 啟用率，很可能是因為納入美國行動通訊業者的資料。此外，資料擷取和分類的精細程度，也會大幅影響訊務測量判定的結果。

改變幅度第二大的是沙烏地阿拉伯，這個人口超過 3 千 4 百萬的國家，IPv6 部署率在過去幾個月內已成長至 4 成以上。第三名的以色列也在過去一年內成長至約 25%，第四名的巴拉圭直至 2019 年底都沒有任何 IPv6 啟用跡象，但從 2020 年底持續成長，到今年 6 月已達到 20%部署率。墨西哥則在過去幾年來穩定成長，至今也

達到約 4 成的 IPv6 部署率。

另一方面，也有些令人驚訝的變化，像是顯示橘色的美國。美國一直都是 IPv6 部署率的模範生之一，也很難想像美國會像其他部署率仍偏低的國家，未來還有短期內 IPv6 部署率激增的狀況。為什麼美國去年的 IPv6 部署率不增反降？作者研判，很可能是因為美國境內大部分地區已解封。企業網路的 IPv6 啟用程度一向低於家用和行動網路，換句話說，許多美國人已經從居家辦公改回通勤上班，大筆網路訊務再度轉回企業網路，也因此導致 IPv6 部署率微幅降低。德國很可能也是類似的情形。

作者指出，沒有證據顯示任何網路調降 IPv6 啟用程度，所以這些國家的微幅降低並不代表 IPv6 部署率下降，只是網路訊務的流向改變。

當然，仍有好些經濟體的 IPv6 啟用程度趨近於零，而且並不在少數。但作者也樂觀表示，這個數字只會越來越少。事實上，圖 1 就是最好的例子。2020 年 IPv6 部署率仍掛鴨蛋的巴基斯坦，到 2021 年 6 月已爬升至 2.3%。巴基斯坦人口超過 2 億，所以 2.3%實際代表的訊務改變不容小覷。其他如關島、盧安達、克羅埃西亞也都有成長。

作者鼓勵大家前往 APNIC 製作的互動地圖，自行點選查看不同經濟體去年和今年的 IPv6 部署差異。由於經濟體的網路使用者人口數和訊務量息息相關，人口數越高的經濟體，其 IPv6 部署率自然也更容易影響全球使用 IPv6 的訊務量。依人口數排名的經濟體及 IPv6 部署率如下列表：

經濟體	2021年IPv6部署率	2020年增量	網路使用者人數（約略數、引用維基百科）
中國	21.30%	5.40%	989M
印度	73.40%	4.60%	756M
美國	45.50%	-6.10%	312M
印尼	<1%		212M
巴西	38.20%	6.00%	160M
奈及利亞	<1%		136M
俄羅斯	10.40%	3.40%	119M
孟加拉	<1%		117M
日本	41.60%	1%	116M
巴基斯坦	2.30%	2.30%	101M

表中經濟體人口都具相當規模，因此 IPv6 部署率的變化，即使比例看似不高，都將顯著影響使用 IPv6 的訊務量。觀察過去一年趨勢，可以看出 IPv6 啟用率有所成長。當然，如前所述，這很可能是許多人轉向居家工作的結果，而隨著疫情趨緩，人們回復通勤上班，數字也可能如美國一樣再度下降。

眾所皆知，IPv6 部署推廣乃未竟之業。通向 IPv6 全面部署的未來還有漫漫長路，但就像過去幾年來的趨勢一般，雖然進度緩慢，這個未來總有一天會來臨。但作者也提醒，全球 IPv6 部署率仍分配相當不均，雖然大型內容供應業者都已經啟用 IPv6 很多年，網路服務供應商的程度仍參差不齊，企業網路更是遠遠落後。

無論如何，光是去年一年內，我們就看到許多大小經濟體的 IPv6 部署率成長。這仍是值得樂觀的大好消息！

中國計畫於 2030 年達到全國網路僅使用 IPv6

國際瞭望 撰輯

https://blog.twnic.tw/2021/08/30/19598/

中國國家互聯網信息辦公室（Central Cyberspace Affairs Commission and Cyberspace Administration，CAC）於 2021 年 7 月 23 日發布《關於加快推進互聯網協議第六版（IPv6）規模部署和應用工作的通知》（以下簡稱《通知》），其中提到中國將於 2030 年達成全國僅使用 IPv6 的願景，各級產業及政府已被告知採取相關行動，鼓勵消費者購買新的 Wi-Fi 路由器。

為完成該願景，中國設下預計於 2023 及 2025 年達成的階段性目標。到 2023 年，中國 IPv6 活躍用戶將達到 7 億人；使用 IPv6 的物聯網設備將達到 2 億臺；新上市的家庭無線路由器將啟用並完全支援 IPv6；30%的官方路由器及其他消費者裝置亦被要求使用 IPv6；半數的行動裝置訊務及 15%固網訊務將通過 IPv6。到 2023 年底，中國將禁止新建網路使用 IPv4 協定。

到 2025 年，IPv6 用戶將達到 8 億人；將有 4 億臺物聯網設備使用 IPv6；70%行動裝置訊務將通過 IPv6；政府網站及 20%固網訊務將被要求使用 IPv6；50%的家庭路由器將使用 IPv6。屆時，95%的大型商業網站及 App 必須支援使用 IPv6。根據《通知》，全面部署 IPv6 尚須 5 年時間。

此外，《通知》還提到將要求私營企業（特別是雲端服務供應商及內容傳遞網路＜Content Delivery Network，CDN＞供應商）確保其產品能通過 IPv6 順利運作，目前中國已擁有可進行相關測試

的基礎設施。

中國早有部署 IPv6 之決心，並於 2017 年發布《推進互聯網協議第六版（IPv6）規模部署行動計畫》，《通知》可被視為該計畫之延續，其中除強調 IPv6 部署成果外，「全國僅使用 IPv6」的網路願景更是新訂目標。然而，根據 CDN 供應商 Akamai 發布的網路現狀（State of the Internet）報告，目前中國 IPv6 部署率為 23.5%，世界排名第 32，要在 2030 年完成全面部署 IPv6 的願景並不容易，且除了中國之外，目前沒有任何國家提倡部署單一 IPv6 網路。

參考資料：

Simon Sharwood (2021.7.26). China sets goal of running single-stack IPv6 network by 2030, orders upgrade blitz. The Register.
檢自：https://www.theregister.com/2021/07/26/china_single_stack_ipv6_notice/ (Aug. 6, 2021)

DANE 在 web 以外領域之應用

文／中華電信工程師 林方傑

https://blog.twnic.tw/2021/10/28/20324/

DANE 全名為 DNS-based Authentication of Named Entities，可譯為「基於 DNS 的域名實體認證」。在〈DANE 的過去、現在與未來〉一文曾提及，雖然在 web 領域中，DANE 因為各方支援度或接受度有限而顯得有些窒礙難行，但這並不代表這項技術沒有其他可用武之地。本文將摘要 DANE 在 web 以外領域的應用，包括（1）SMTP、（2）VoIP、（3）Jabber/XMPP。對於各項主題，我會先花點篇幅簡介其用途、碰到的問題，接著說明 DANE 在其中發揮的效益。

SMTP

SMTP 全名是 Simple Mail Transfer Protocol，可譯為「簡單郵件傳輸協定」。「協定」（protocol）一詞代表著 SMTP 也是一種共同語言[1]，具備事先協議好的格式及規則，使不同機器得以成功交流且忽略彼此軟硬體的差異；「郵件傳輸」指明了協定被應用的情境；至於剩下的「簡單」，將透過下述的回顧協助大家體會。

在早年沒有 Outlook、Thunderbird 等郵件軟體可用的時代，人們會使用連線程式（如 telnet）登入郵件主機、再下 SMTP 的指令執行郵件傳送[2]。筆者認為，SMTP 的「簡單」除了可見於基於文字指令的操作及運作，更在於這些文字是以「明文」傳輸的預設狀態。

---

1 關於「Protocol」的概念與類比，可參：https://www.ithome.com.tw/node/6349

2 關於 SMTP 指令與 telnet 的相關操作可參閱：http://www.tsnien.idv.tw/Internet_WebBook/chap14/14-4%20SMTP%20%E5%8D%94%E5%AE%9A.html、https://ithelp.ithome.com.tw/articles/10189886 等文章。

以明文傳輸，代表任何人截獲傳輸中的訊務都可一窺其內容。針對這種資訊外洩的風險（即資安 CIA 中的 confidentiality 議題），直覺的對策是採用加密傳輸，而 SMTP 也確實有「StartTLS」這種「明文通訊協定的擴充功能[3]」，用於以明文通訊的雙方協議建立加密連線，運作程序大致為：（1）發信方透過 DNS 查詢找出收信方郵件主機及其 IP；（2）收發信雙方都使用 SMTP StartTSL extension（定義於 RFC 2487）進行加密連線的通知及協商；（3）在交握完成後，收發信雙方便可進行加密連線的建立[4]，如圖 1。

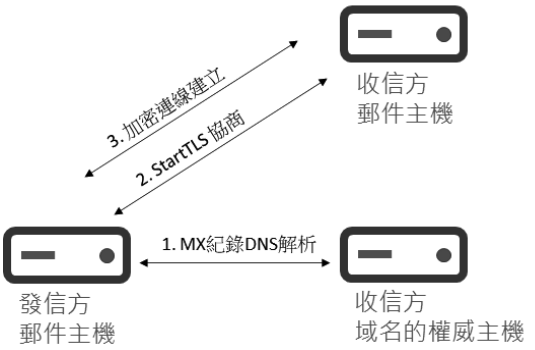


圖 1　收發郵件雙方應用 SMTP StartTLS extension

（筆者繪製，詳可參閱〈Better mail security with DANE for SMTP〉[5]）

---

[3] 維基百科（2020）。STARTTLS. 檢自：https://zh.wikipedia.org/zh-tw/STARTTLS (Aug. 25, 2021)

[4] 關於收發郵件雙方使用 StartTLS extension，筆者參閱：https://help.hcltechsw.com/domino/11.0.0/conf_securingsmtpsessionsusingthestarttlsextension_c.html；關於 email client 與 email server 及協商的細節步驟則參考：https://sendgrid.com/blog/what-is-starttls/ 與 https://blog.yowko.com/telnet-check-smtp/、http://en.redinskala.com/what-is-the-difference-between-the-heloehlo-commands/等。

[5] 關於 SMTP StartTLS 的安全弱點，https://blog.apnic.net/2019/11/20/better-mail-security-with-dane-for-smtp/ Figure 2、3。

既然有了加密連線，似乎可高枕無憂？很遺憾的，問題還沒結束。大家可以留意到，前述加密連線的協商是在初始未受保護的連線下進行，也未進行身分驗證。這使得「中間人攻擊」（MITM attack，即 man-in-the-middle attacks）仍然有機可乘。如果有駭客在加密連線協商的過程中攔截並竄改傳輸訊息，比如將一方回覆的「能」支援加密連線改為「不能」，或替換進偽造的憑證，前者會造成連線只得續用明文傳輸（downgrade）[6]，後者則讓駭客能將信件轉寄到其指定的郵件主機（divert）[7]。簡言之，以 StartTLS 協商建立加密連線是可以抵抗被動的流量竊聽，但對於主動發起的 MITM attack 卻束手無策，如圖 2。

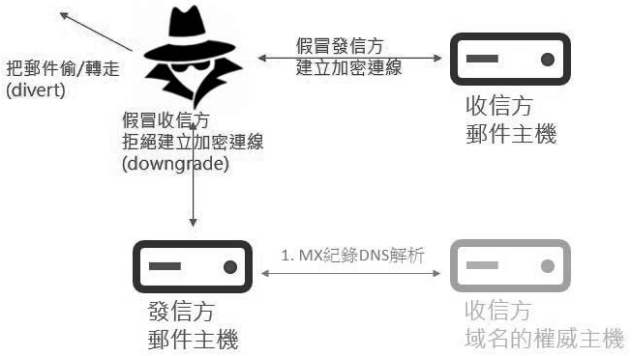


圖 2　SMTP 遭受 MITM attack

（筆者繪製，詳可參閱〈Better mail security with DANE for SMTP〉[8]）

6　關於 StartTLS 的 fallback 行為，
https://gcn.com/articles/2015/10/05/starttls-email-encryption.aspx

7　關於 SMTP StartTLS 的安全弱點，可參閱：
https://blog.apnic.net/2019/11/20/better-mail-security-with-dane-for-smtp/
Figure 2~3。

8　關於 SMTP StartTLS 的安全弱點，可參閱：
https://blog.apnic.net/2019/11/20/better-mail-security-with-dane-for-smtp/
Figure 2~3。

那麼我們今天的主角 DANE 如何拔刀相助呢？關鍵在於以 DNS 解析緩解前述「沒有身分驗證」及「加密連線的協商易被介入」二個問題。首先，如果溝通對象的數位憑證[9]能有來自第三方的對照，則對於提高憑證的可信度應該有所幫助。而事實上，DNS 伺服器就是個收發郵件二端以外的第三方、可將驗證憑證所需的「fingerprint」資訊存於「TLSA 紀錄」（TLS Authentication record）並透過解析提供。而 DANE 的基礎 DNSSEC 在確保 DNS 資料完整性（Integrity）的同時也保障了前述 fingerprint 的正確性，因此改善了沒有身分驗證的問題。

至於另一個問題，透過「域名有 TLS 紀錄即代表該域名對應設備具有使用 TLS 的能力」這樣的約定，前述可能被惡搞的收發郵件雙方協商過程便可被 DNS 解析取代（如圖 3），且 DNS 所傳遞的資料之完整性也同樣受到 DNSSEC 的保護。

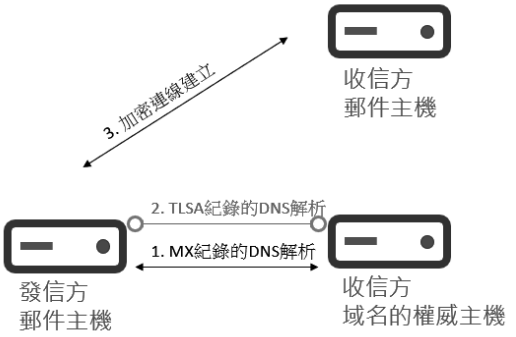


圖 3　SMTP 及 DANE

（筆者繪製，詳可參閱〈Better mail security with DANE for SMTP〉[10]）

9　關於數位憑證，可參閱：
https://docs.oracle.com/cd/E19900-01/820-0848/ablok/index.html

10　關於 SMTP StartTLS 的安全弱點，可參閱：
https://blog.apnic.net/2019/11/20/better-mail-security-with-dane-for-smtp/
Figure 2~3。

VoIP

VoIP 全名為 Voice Over Internet Protocol，即一般所稱的網路電話。儘管傳統電話技術穩定且成熟，VoIP 因其廣泛的用途（除語音外也可傳輸視訊）及高性價比（跨境通話尤其划算，有研究估計成本可降 40%以上）仍備受青睞[11]、甚至有喧賓奪主的趨勢。相較於傳統電話技術是以「線路交換」（circuit switching）為基礎，需要為傳輸雙方建立固定路徑並保留頻寬，也因此成本較高[12]，VoIP 則是基於「封包交換」（packet switching），將資料切割為封包在網路上（盡力）傳送。

VoIP 是如何運作的呢？以 Alice 要用網路電話跟 Bob 通話為例，SIP（Session Initiation Protocol）[13]連線至少包含通話雙方的話機[14]，以及各自對應的 SIP 代理伺服器，如圖 4。

圖 4　網路電話 SIP 連線示意圖

（筆者引用並精簡自〈The Threat Model (VoIP)〉[15]）

---

[11] 關於 VoIP 的好處，可參閱：https://www.idtexpress.com/zh-TW/blog/voip-cheap-compared-traditional-calls/

[12] 邵喻美。VoIP 網路電話技術發展與應用。國立台灣大學計算機及資訊網路中心電子報。檢自：https://www.cc.ntu.edu.tw/chinese/epaper/0002/20070920_2006.htm (Aug. 25, 2021)

[13] 可譯為會談啟始協議，是實務中 VoIP 的技術。關於 SIP，可參閱：https://www.dialogic.com/glossary/sip-client、https://kknews.cc/zh-tw/tech/8v8k2yq.html

[14] VoIP 話機常稱 SIP UA，UA 則是 User Agent 的簡稱。關於 UA，可參閱：https://www.ithome.com.tw/node/38869

[15] 關於 SIP 連線，可參閱：http://what-when-how.com/voip/the-threat-model-voip/

圖中編號（1）的角色之所以能找到（2），（2）又能找到（3），是透過 DNS 解析「SRV 紀錄」（Service Record，可譯為服務定位紀錄）[16]，取得網路電話服務相關的主機名稱及 port 資訊。此外我們仍然需要 DNS 為我們解析出主機名稱對應的 IP。

那麼 VoIP 潛藏著什麼問題呢？首先，如果 SRV 紀錄遭竄改，則話機終端或者 SIP 代理伺服器就可能與錯誤的對象連線。另外，憑證是否可信也會是個議題，除了因為在 VoIP 的情境中，憑證可見於 PBX（Private Branch eXchange，IP-PBX 網路電話交換機）系統中或交換機上[17]，任何 CA 可為任何域名簽發憑證[18]，因此使得駭客有機會以你我域名的名義取得憑證安裝於其假造的線上服務伺服器之情況，以及實務系統架構中有「middle-boxes」存在的空間，如防火牆設備（或駭客）可居中插手憑證的安排，如圖 5。

[16] 關於 SRV 紀錄，可參閱：
https://www.cloudflare.com/learning/dns/dns-records/dns-srv-record

[17] 關於數位憑證與 VoIP，可參閱：
https://okay.network/blog-news/free-wildcard-certificates-with-the-white-label-voip-servers.html

[18] Richard Barnes. (2011.10.6). DANE: Taking TLS Authentication to the Next Level Using DNSSECIETF Journal.
https://www.ietfjournal.org/dane-taking-tls-authentication-to-the-next-level-using-dnssec/

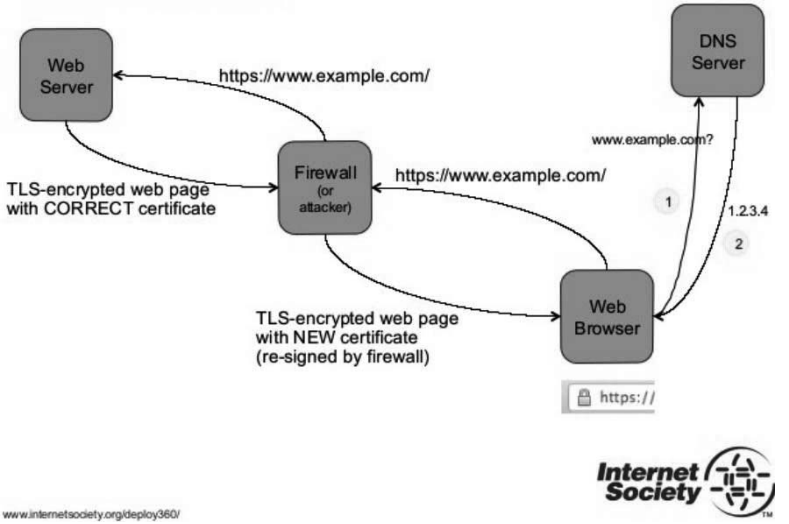


圖 5　憑證可信度議題之一示意圖（可留意左上及中間節點使用的不是相同的憑證）

（引用自〈DNSSEC and VoIP: Who are you really calling?〉P.36[19]）

相對於直接公布解答，有輸入也有輸出更可深化理解，因此想邀請讀者朋友，想想看並試著回答以下二個問題：

1. 上一段提到的二個問題可以怎麼緩解？
2. 在 SMTP 篇章討論的問題及解法是否有可以借鏡之處？

解答將於下個篇章揭曉，請先帶著您的答案一起看下去。

Jabber/XMPP

根據維基百科的描述，XMPP 全名為 Extensible Messaging and Presence Protocol，是一種以 XML 為基礎的開放式即時通訊（instant

[19] 關於 DNSSEC 及 VoIP，請參閱：
https://www.slideshare.net/Deploy360/dnssec-and-voip-who-are-you-really-calling

messaging，簡稱 IM）協定[20]，Jabber 則是其前稱[21]。XMPP 被標榜具有開放、標準、分散式等特性[22]，該協定因為被 Google Talk 採用而聲名大噪。

從技術的觀點，XMPP 的運作模式、網路結構與 email 服務相近，任何人都可以在自己的網域上架設並運行 XMPP 伺服器，並搭配 DNS SRV 紀錄對外發布它的存在（如同郵件主機與 MX 紀錄的設置）。XMPP 以 JabberID（JID）識別用戶，這不只用途與 email address 相似，長相也是由使用者名稱、@符號加上網域名稱構成[23]。看到這兒，推測 XMPP 與 DNS、DNSSEC、DANE 有關應當很合理！

事實上，因為 XMPP 服務的運作也需要網域名稱與 DNS 紀錄來發布提供服務的伺服器是誰與所在，並在建立加密連線的過程中用上數位憑證，這也就衍生出二個問題如下[24]：

1. 「secure delegation」問題：我連的是正確的伺服器嗎？伺服器名稱與位置（IP）沒遭竄改過嗎？
2. 「identity verification」問題：跟我連線的伺服器，真的是它所宣稱的那臺嗎？它所出示的憑證不是假造的嗎？

而這二項除了與 VoIP 所面臨的問題（之二）類似，也可以用 DNSSEC 與 DANE 緩解：DNSSEC 應用的數位簽章技術可確保 DNS 紀錄不在傳輸過程中被竄改，也因此提高了透過 DNS 紀錄取得之伺服器資訊的可信度；另外服務提供者（同時也是域名持有者）應

---

[20] WIKIPEDIA (2021). XMPP. WIKIPEDIA. 檢自：https://en.wikipedia.org/wiki/XMPP (Aug. 25, 2021)

[21] 關於 Jabber，可參閱：https://www.itread01.com/content/1545528426.html

[22] 關於 XMPP 的特色，可參閱：https://xmpp.org/about/technology-overview.html

[23] 關於 JabberID 等，可參閱：https://slidetodoc.com/xmpp-protocol-and-application-development-using-open-source/

[24] 關於 DANE+XMPP，可參閱：https://www.ietf.org/proceedings/84/slides/slides-84-dane-3.pdf

用 DANE 的 TLS 紀錄（承載 certificate fingerprint[25]）、DNS 解析機制（讓使用者取得 TLSA 紀錄內容）、DNSSEC 的保護效果（防止 DNS 資料在傳輸過程中被竄改），便可讓服務使用者取得足以驗證憑證的可信資訊，從而確認連線對象身分的真實性。而這也是作者對於 VoIP 段落提問的解答了。附帶一提，關於如何提升 XMPP 的安全性，具體的設定步驟可參閱〈.IM TLD DNSSEC DLV DANE XMPP TLSA RR〉一文[26]。

小結

雖然本文以 DANE 在 web 以外領域之應用為標題，但討論 DANE 實在少不了做為基礎的 DNSSEC。不（只）是為了充篇幅，而是從 SMTP、VoIP、XMPP 的相關資料中，體會到三者所面對的問題是有交集的。如果用 secure delegation 與 identity verificaton 來代表，則二者分別可藉 DNSSEC 與 DANE 來緩解。以上是作者個人的理解，盼能給大家帶來幫助，如果有疏漏或偏誤也再請不吝指導了！

[25] 關於 certificate fingerprint（A certificate's fingerprint is the unique identifier of the certificate），請參閱：https://knowledge.digicert.com/solution/SO9840.html

[26] 關於 XMPP 的安全設定，請參閱：https://op-co.de/blog/posts/yax_im_dnssec/

趨勢議題

IPv4 位址已成為新型態的金融資產

國際瞭望 撰輯

https://blog.twnic.tw/2021/01/28/16740/

IPv4 位址已成為新興金融資產，根據網路專家 Andree Toonk 的估算，Amazon 目前大約擁有 1 億個 IPv4 位址，若依市價計算，價值高達 25 億美金。儘管 Amazon 實際上僅用到手上 IPv4 位址數量的一半左右，但 Amazon 不但沒有出售的打算，甚至最近還花下一億巨資，從非營利公司 ARDC 再度購入 4 百萬筆 IPv4 位址。

2019 年底，RIPE NCC 宣布所有 IPv4 位址已分配完畢，在缺乏新的 IPv4 位址及可供重新分配的既有 IPv4 位址之情況下，企業若需要新的 IPv4 位址或想擴展既有網路，唯一的選擇就是向他人購買。近年來，IPv4 位址的交易相當活絡，根據 IPv4 位址區塊大小的不同，目前行情為每個位址 23-30 元美金，且多年來價格持續穩定成長。

IPv4 位址價格不斷上升，不僅既有供應商難以推出新的大規模服務，新的供應商也難以搶下一席之地。報導中引述網路服務供應業者 Freedom Internet 執行長，表示 IPv4 位址的價位高昂，但公司資本有限，因此只能用租賃，而非購買的方式持有 IPv4 位址。這也表示公司租賃的成本必須包含在提供的服務價格中，導致他們的價格始終難以和其他大型業者競爭。

理論上，未使用的 IPv4 位址就可脫手售出，然而位址價值不斐，因此持有企業大多不願意這麼做。託管服務供應商 Heficed 的 CEO Vincentas Grinius 認為，IPv4 位址的價格將在未來五年翻倍，不僅成為交易商品，更將衍生多種新型態的租賃結構。然而，隨著

近年 IPv6 佈建率持續成長，Grinius 也預估 IPv4 的價值可能在十年內達到高峰後開始下降。

參考資料：

https://www.sidn.nl/en/news-and-blogs/ipv4-addresses-the-new-gold

IPv4 上新聞了

APNIC 文摘

https://blog.twnic.tw/2021/05/27/18669/

本 APNIC 文摘原標題為 IPv4 in the headlines，由 APNIC 首席科學家 Geoff Huston 撰文。

IPv4 通常不是主流媒體會關心的議題。即使網際網路社群為了 IPv4 位址耗竭鬧得沸沸揚揚，這件事也從未因此登上新聞版面。也因此，當華盛頓郵報刊登了「大批五角大廈持有的休眠 IP 位址在川普離開辦公室的前一刻瞬間復活」為題的報導，網路社群不免因此吃驚。

美國國防部持有來自 ARIN 大約 221,828,864 筆位址，包括約 1,207 筆的個別位置前綴，其中 11 筆含有/8 前綴。這些位址很多都是當年網際網路還是國防部先進研究計畫署（Defense Advanced Research Projects Agency，DARPA）轄下研究計畫時，由網際網路號碼分配機構（Internet Assigned Numbers Authority，IANA）直接發配的。

華盛頓郵報的「瞬間復活」標題，不了解網路位址作用的一般大眾可能難以正確理解。其實這只是代表某個單位「宣告」（accounce）了這批平常沒在用的位址。APNIC 首席科學家 Geoff Huston 也為此撰文，說明為何這次「宣告」引起注意，並提出他認為可能的背後原因。

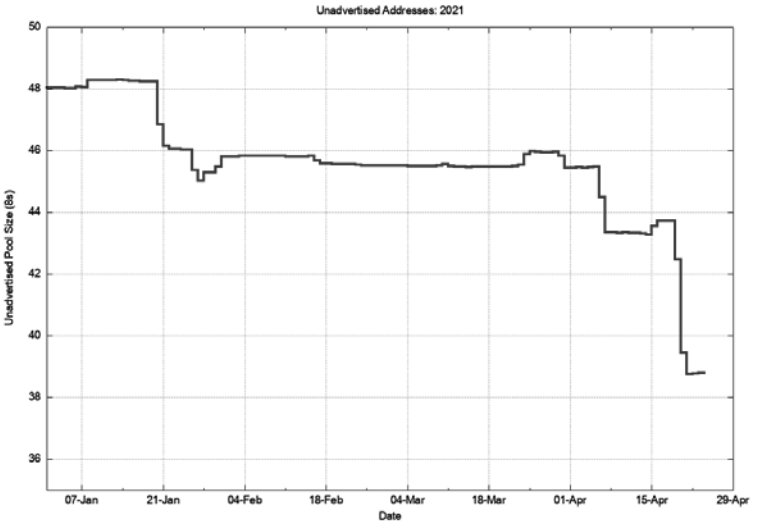
過去幾年來，Geoff 每年初都會發布長文，回顧過去一年的 IP 位址全球動態。從觀測數據中，我們可以推測出許多結論：諸如地區網際網路技術發展及國家數位化政策對當地 IP 位址成長率的影

響，或是網路市場中如何在少數業者把持中逐漸僵化、不利競爭，以及 IPv6 的發展趨勢等。

在進入正題前，Geoff 先解釋 IP 位址發配的雙層架構。IANA 掌握所有 IPv4 和 IPv6 的位址資訊，並將這些位址以區塊分給負責區域位址發配的區域網際網路註冊機構（Regional Internet Registry，RIR）。也可以把 IANA 想像成批發商，負責將 IP 位址「批貨」給 RIR。換句話說，每當 RIR 的位址庫存量不足，就會向 IANA 申請發貨。雖然每個 RIR 發配 IP 位址的方式細節上可能不同，但「要取得更多 IP 位址，必須證明有相當需求」的基本原則一致。RIR 也都保有轄下位址發布情形的紀錄，而觀察這些紀錄變化，我們也能看出每個地區的 IP 位址發展趨勢。

一旦取得 IP 位址，要如何使用端看持有者的決定。通常，分派出去的 IP 位址會被用來支援網際網路提供的公共服務。為了達成此功能，必須向邊界閘道協定（Border Gateway Protocol，BGP）宣告這些發派後的位址。也有些位址並不會在公共網路上宣告，或只是放著不用。RIR 手中不會有這些未宣告或使用的位址資訊，僅能透過觀測數據將位址分成「已宣告」和「未宣告」。

從觀測數據中，也可發現登上報紙版面的美國國防部突然宣告位址事件。觀察以下圖表，可看出國防部分別在 1 月 20-21 日、4 月 6-7 日及 19-20 日宣告了手中持有的位址。



讀者可能會問，為什麼時至今日才突然宣告這些位址？華盛頓郵報的追蹤報導中引述美國國防部聲明，表示美國軍方希望「評估、衡量並防止未授權使用國防部持有的 IP 位址」。鑑於來自境外勢力的網路入侵威脅不斷，國防部也希望能藉機「查找潛在弱點」，事先防堵利用休眠 IP 位址進行的網路攻擊。

Geoff 認為，國防部的舉動或許也可解讀為「不用則廢」。他解釋，若國防部手中大批位址因閒置而長期遭冒用，最終可能導致網際網路上將冒用者視為位址的真正主人。另外，雖然可能性極低，但若位址閒置太久，未來即使國防部想在公共網路上使用這些位址時，網際網路可能會不接受這些位址。當然，Geoff 強調，這個情境發生的可能性趨近於零。

宣告 IP 位址，即使沒有實際於公共網路中使用，也可以在路由系統中再次確認所有權，避免其他人冒用並藉此發動惡意攻擊。Geoff 認為這是最合理的解釋。他也不認為國防部的舉動暗藏什麼陰謀，事實上，他反而好奇為什麼國防部等到如今才發動。

根伺服器營運的挑戰

APNIC 文摘

https://blog.twnic.tw/2021/01/18/16682/

本 APNIC 文摘原標題為 The challenges of operating a root name server，由 NetNod 共同創辦人 Lars-Johan Liman 撰文。

根伺服器是 DNS 根區的存取入口，透過根伺服器，使用者得以進入 DNS。根伺服器也可看成 DNS 解析過程的起點，它會告知送出 DNS 查詢的人下一階段應該往哪裡去，或直接宣告使用者輸入的域名不存在。本文作者為 Lars-Johan Liman，是 13 座根伺服器之一，I-Root 營運方 Netnod 的共同創辦人。他分享 Netnod 的根伺服器營運心得，也列出維運根伺服器須面對的挑戰。

存取根區資訊是使用網際網路上任何服務的起點，而根伺服器是存取根區資訊最簡單、也最容易的方式。網際網路極端仰賴根伺服器，換句話說，根伺服器是網際網路整體運作順利的關鍵。

對 Netnod 而言，確保根區服務的穩定和準確性是最重要的目標。這包含幾個方面：

- **伺服器穩定：**透過「任意傳送法」（Anycast）技術，全球網路上多個互相連結的伺服器得以共享同一組 IP 位址。網際網路的路由系統會自動將使用者端的 DNS 訊務疏導至最近的伺服器。如果有伺服器突然故障，訊務會自動被導向其他正常運作的伺服器，不影響傳輸。Netnod 在所有關鍵環節都使用雙套系統，確保安全。
- **服務可及度：**Netnod 與全球許多網際網路服務供應業者有訊務交換的對接（peering）關係，即使單一路由故障，訊務

仍能順利到達 Netnod 的伺服器。

- **軟體多元性：**Netnod 的服務可以透過多種不同的軟體提供。即使某個軟體元件失效，也能立刻用其他軟體取代。
- **政策穩定：**Netnod 的職員積極參與所有 DNS 相關的論壇會議，而且樂於承擔責任、發揮影響力。諸如 IETF、ICANN，乃至網際網路工程指導小組（Internet Engineering Steering Group，IESG）和網際網路架構委員會（Internet Architecture Board，IAB）等，都可看到 Netnod 員工身居要職。
- **財務穩定：**維運根伺服器必須保持中立獨立。由於提供根區服務沒有任何報酬，維運方必須另循財源。Netnod 的方式是提供頂級域名註冊管理機構另一套收費的 DNS 服務，確保收入來源。如此一來，不僅用於維護根區營運的錢與服務本身直接相關，收入多元也確保 Netnod 本身的經營決策不受制於單一客戶。

如前所述，根伺服器總共有 13 座，由 12 個營運方負責維運。根伺服器營運方都是獨立運作，除了基本的技術大原則外，各營運方被賦予相當的彈性，可自行決定如何設置、提供服務。這種多元性也再次確保 DNS 的穩定和靈活性；即使某一座根伺服器的系統出了問題，其他根伺服器仍能照常運作、確保網際網路持續運行。

至於營運根伺服器的挑戰，至少包括：

- 設置伺服器：Netnod 在全球網際網路各處都設有伺服器，這也代表需要各種安排支援，包括尋找代管方、跨國運送、海關報通關、遠端指導當地代管方安裝主機等等。
- 時時調整伺服器以保有正確的 DNS 資訊，並確保伺服器即時且正確的蒐集、回報橫跨網際網路的連線數據。
- 確保 Netnod 使用的軟體確實提供所需的服務。根伺服器管理人員弄壞軟體的方式千奇百怪，有時候連軟體開發者都會

大吃一驚！

- 防禦各種類型的攻擊，包括持續性阻斷服務（DDoS）攻擊或其他針對不同弱點的攻擊。
- 提供完整清楚的資訊，確保全球網際網路社群都明瞭根伺服器系統如何運作。Netnod 的目標是確保所有可能影響根伺服器服務的決策，都基於事實而非誤解。

最後 Liman 強調，強化根區服務的最主要方式，就是增設更多的伺服器。Netnod 也計畫在非洲和亞洲逐步增設伺服器，同時改良技術平臺，持續簡化設置流程並降低成本。如此一來，Netnod 或可進一步在更多元、更不同的網路環境中裝置伺服器。另一方面，Netnod 也將繼續與其他根伺服器營運方合作，改善整個系統的透明度和當責。

物聯網變成「廢物」聯網？

APNIC 文摘

https://blog.twnic.tw/2021/03/10/17117/

本 APNIC 文摘原標題為 The Internet of Trash，由 APNIC 首席科學家 Geoff Huston 撰文。

美國的《物聯網網路安全改善法》（IoT Cybersecurity Improvement Act of 2020）於去年 12 月正式立法，法案要求國家標準暨技術研究院（National Institute of Standards and Technology，NIST）與其他機關單位合作，建立管理安全弱點、修補漏洞，以及設定身分管理等裝置使用安全守則。

本文作者 APNIC 首席科學家 Geoff Huston 以美國的法案為起點，從頭檢視物聯網如何逐漸淪為「廢物」聯網（Internet of Trash），這個可能未來將造成的問題，以及我們應如何設法解決這些難題。

我們的世界正以驚人的速度數位化，而無限增長的連網裝置是推進數位化的重要動力之一。目前估計全球網路使用者將達到 46 億人，連網裝置數量則將超過 300 億。

不僅是裝置本身，裝置搭載的服務和功能其實都包含在「物聯網」中。從汽車、電視、居家保全系統、天氣站、視訊鏡頭、攝影機、空調系統、延長線、燈泡到門鈴，都可能是物聯網的一環。不僅一般消費者個人使用或居家環境，工作場所、醫院、工廠、農場，以及各種運輸設施和設備，也都在數位化的進程中，被納入無所不在的物聯網。

在這廣袤的物聯網裡，某些裝置在消費者心目中，廠商理應負起「售後服務」的責任，如定期更新、發布修補漏洞版本等。如 iOS、

Android 都會定期更新，利用這些作業系統平臺的應用程式也都會定期或不定時更新。

然而，物聯網中有另一大部分使用電池、比較不「智慧」的裝置。隨著技術進步，業者開始把半導體放進過去沒想過的產品裡，但這些裝置有了電腦運算能力後，壽命也從原本的 15 年減至 5 年左右。根本問題在於「可充電電池」和「高性能」在尺寸有限的智慧型裝置中難兩全，研發人員最後也只能雙手一攤，告訴你若電池沒電，裝置就不再「智慧」。

這一類型的裝置，業者往往在售出產品後就銀貨兩訖，版本更新、修補漏洞等責任都全權落在消費者身上。但是，對消費者而言，只要我的相機還能照相、印表機還正常運作，我何必管什麼版本更新或安全漏洞？

當然，對網路安全有些認識的讀者就能了解，問題不在於相機或印表機是否「智慧」。問題在這些連網裝置內建的運算功能可能有弱點，而這些弱點一旦遭惡意人士發現利用，印表機很可能在一派正常、忠實列印所有文件的同時，成為駭客的攻擊跳板、工具，甚至淪為大規模網路攻擊的幫凶。2016 年由 Mirai 變種殭屍網路主導、癱瘓美國部分地區網路的大規模 DDoS 攻擊就是不敢或忘的慘痛教訓。

當然，「裝置未更新導致重大網路安全威脅」的責任，難以清楚地歸在消費者或業者的頭上。裝置未能或難以更新有各式各樣的原因，有些硬體意外的體質硬朗，可以順利運作超過 30 年，業者推出更新版本的年限該有多久？難道裝置都已停產還得繼續更新韌體嗎？更別說有些產品可能活得比出產廠商還久，這種情況下又該由誰負擔維修責任？

這或許也是美國政府推出法令的原因。然而，姑且先不論國家司法管轄權和商品全球流通性之間存在巨大落差的問題，單一政府

的立法規範，是否真有辦法解決這些問題？

對業者而言，在產品停售後還持續版本更新已實屬難得，雖然理想的最長年限可能達到停售後 7 年，但連 Apple 都沒有這種耐心。iOS 10 於 2016 年底推出，2019 年 7 月就是最後一次版本更新了。Android 的情形更糟糕，因為他們將更新的責任轉嫁至裝置廠商身上，連行動網路業者都必須負擔部分更新。結果是物聯網中使用 Android 系統的裝置，可說是幾乎或完全沒有安全保障。

由於缺乏明確規範，業者提供版本更新的年限完全依各自方便行事，越來越多人傾向比照電池裝置的作法，一方面縮短裝置的使用年限，一方面無所不用其極地誘使消費者每年汰換裝置，直接躲掉軟體更新的麻煩。然而，這造成另一個更大的問題——電子垃圾數量持續激增，物聯網淪為「廢物」聯網。

我們無法假裝視而不見「廢物」聯網的問題，但光是「誰」該負責解決這個問題，就又是另一個眾人爭執不休的難題。作者批評過去科技產業奉為圭臬、臉書創辦人馬克．祖克伯「快速行動、破除窠臼」（move fast, break things）的名言。若奉行此原則的結果是整個業界持續不負責任地製造大量短命的連網裝置，作者認為，這已可視為產業性的集體犯罪性疏忽。

最後作者作結，「廢物」聯網是科技產業市場失靈的結果，若業界持續缺乏矯正此類陋習的意志，則除了政府介入別無他法。

APNIC 2021 年行動計畫主題：線上參與

APNIC 文摘
https://blog.twnic.tw/2021/06/09/18691/

本 APNIC 文摘原標題為 Exploring APNIC's 2021 themes: Online Participation，由 APNIC 執行長 Paul Wilson 撰文。

今年 3 月舉辦的 APNIC 51 期間，APNIC 執行長 Paul Wilson 介紹了 APNIC 今（2021）行動計畫的四大主題。參考 2020 年度 APNIC 問卷調查結果及社群意見，APNIC 執行理事會訂出 2021 年行動計畫的四個主題：

- 次世代註冊管理服務
- 線上參與
- 未來發展培力
- APNIC 組織韌性

本篇文章為系列第二篇，未來將陸續發布新文章，說明四大主題分別的詳細內容，以及對 APNIC 會員、社群可能產生的影響。

APNIC 社群如同所有網際網路社群，幅員遼闊但緊密相連。網際網路也一直都是 APNIC 社群互相溝通協作的重要工具。隨著科技持續進步，線上活動也發展出更多可能。APNIC 會議一直都支援遠端參與形式，提供包括線上直播、即時字幕和聊天室等功能。因應疫情，今年選舉也改成全面線上舉行。

不只是會議，APNIC 的訓練課程也逐步線上化，APNIC 線上學院（APNIC Academy）平臺提供的課程和研討會種類和數量皆與日俱增，教育訓練工作坊和實作線上實驗室也不遑多讓。

APNIC 秘書處始終盡力打造線上服務、支援線上參與交流，

但也不避諱仍有改善空間。事實上，早在 2019 年的戰略規劃期間，COVID-19 疫情尚未延燒全世界時，APNIC 執行委員會（Executive Council，EC）就認定線上參與的重要，並將持續改善 APNIC 社群線上參與經驗訂為 2020 至 2023 年的重點目標。

COVID-19 疫情自 2020 年開始延燒全球，線上參與也從此成為唯一參與社群活動的方式。繼 2020 年 2 月澳洲墨爾本的 APRICOT 會議後，所有 APNIC 實體會議都取消，訓練課程和會議都轉至線上。許多當地社群的活動也大受影響，大多地方網路維運社群（Network Operating Group，NOG）聚會都因此取消或延期，APNIC 因此協助舉辦「從家中連結」（Networking From Home）系列活動，希望藉此多少彌補活動取消造成的空缺。

於 2020 年底籌備 2021 年活動規劃時，COVID-19 疫情短期之內不會結束，甚至可能延長至 2021 年後的態勢已相當明顯。這也代表「新常態」仍是線上形式，APNIC 秘書處也因此應該做好萬全準備，持續支援並改善所有會員的線上參與經驗。這也是「線上參與」成為 2021 年行動計畫四大主題的原因。

為了進一步協助 APNIC 社群的交流和線上參與，秘書處自認尚有許多改善空間。值得慶幸的是，全球疫情下大部分活動都移至線上，許多創新線上參與工具和服務也相應而生。無論是會議、專業交流、一般社交或進階協作，都得利於這些新的應用程式而得以順利進行。

另一方面，APNIC 秘書處也有多項改善規劃。如改善網站使用者經驗，確保使用者能更輕易找到並吸收資訊，以及無障礙使用經驗強化。APNIC 線上學院也持續更新，不只更新課程內容，也新增了線上技術支援的功能。

去年廣邀社群專家與談的線上即時社群媒體活動將持續，APNIC 部落格也將定期更新，持續提供高品質。APNIC 更首次舉

辦全面線上的英才計畫（Fellowship），為了協助獲選的優秀學員們能充分享受、參與年底的 APNIC52，相關訓練課程現在就已經展開。

不僅如此，秘書處還建立了一個專屬 APNIC 社群的線上交流協作平臺，希望透過這個目前尚未命名的平臺，以更有效、更靈活的方式促進社群成員的凝聚力。此平臺將首先向 APNIC 線上學院使用者開放，希望往後能慢慢推廣至其他層面，包括鼓勵社群成員們放棄過時的 mailing list 方式，轉往更實用、更有效率的線上交流工具。

歡迎所有社群成員一起加入這個改善線上參與的過程。APNIC 成立了「使用者回饋小組」（User Feedback Group），所有想為改善 APNIC 產品服務盡一臂之力的社群成員都可以參加。只要在 apnic.net/your-say 填寫資料，APNIC 秘書處會盡快聯絡你，協助完成後續使用者回饋小組的加入事宜。

Ethos Capital 收購 Donuts

國際瞭望 撰輯

https://blog.twnic.tw/2021/02/23/17032/

去（2020）年收購.ORG 註冊管理機構 PIR（Public Interest Registry）未果的 Ethos Capital，在今年 1 月 22 日由聯合首席執行長 Erik Brooks 及 Fadi Chehadé 共同對外宣布，該公司已決議收購註冊管理機構 Donuts 之股份，以提高持股比例。

根據 Donuts 在同日發布之聲明，Ethos Capital 係透過收購投資組合公司（Portfolio company）Abry Partners 持有的 Donuts 股份來達成此項目的。早在 2018 年時，Erik Brooks 及過去曾擔任 ICANN 執行長的 Fadi Chehadé，便主導過 Abry Partners 對 Donuts 的收購案，隨後二人離開 Abry Partners，另外成立私募股權公司（private equity company）Ethos Capital。去年 Ethos Capital 試圖以 11.35 億美元的價格收購 PIR，以取得.ORG 註冊管理機構的經營權，然而此項交易未能獲得 ICANN 的批准，最終以失敗收場。

Donuts 為鞏固其市場地位，在去年底甫收購另一家大型註冊管理機構 Afilias，可推測 Ethos Capital 也在幕後參與了這場交易。本次收購 Donuts 明顯可以看出，在.ORG 交易案失敗後，Ethos Capital 的投資者積極渴望將資金投入其他的域名市場當中。

根據媒體 DOMAIN INCITE 的報導，作者認為此案將會再度引起業界關注，然而此次交易不同於.ORG，不具有特殊的非營利意義，應當不會面臨相同程度的監管審查及社群反應。而網路社群對於此案最關注的，莫過於未來域名註冊費用是否會隨之調漲了。

參考資料：

1.http://domainincite.com/26198-breaking-failed-org-buyer-ethos-capital-buys-donuts

2.https://domainnamewire.com/2021/01/22/breaking-ethos-capital-acquires-donuts/

Verisign 宣布.com 價格上漲至 8.39 美元

國際瞭望 撰輯

https://blog.twnic.tw/2021/03/19/17251/

Verisign 於今(2021)年 2 月 11 日宣布,自今年 9 月 1 日起,.com 域名註冊及續約的批發價格將從現行的 7.85 美元提高至 8.39 美元。這是.com 價格自 2012 年以來首次調漲,當時美國政府商務部(Department of Commerce)係依據與 Verisign 的長期合約凍結了註冊費(Registration Fee)。

根據 Verisign 在去年 3 月與 ICANN 簽訂之協議,ICANN 同意 Verisign 在每次續約 6 年期間的第 3 年到第 6 年,可逐年提高域名價格 7%,惟須提前 6 個月發出價格調漲通知,此外,Verisign 自今年 1 月 1 日起 5 年內,每年應額外支付 ICANN 400 萬美元的年費。

Verisign 基於上述協議提高價格,也意味著.com 域名的批發價可能在 4 年內逐步上漲至 10.26 美元左右。實際上,受理註冊機構可自行訂定域名的註冊價格,然而許多受理註冊機構提供給客戶的價格遠低於 8.39 美元,因此域名註冊人在今年底前肯定會面臨到價格調漲的情況。

去年度由於受到 COVID-19 疫情影響,提高了小型企業上網的機會,助使 Verisign 從中獲利,並反映在該公司去年第四季度及全年度的業績表現。事實證明 COVID-19 為域名產業帶來意外的收獲,但相對的,未來當疫情趨緩後的經濟復甦對於該產業就未必是件好事了。

參考資料：

1.https://domainnamewire.com/2021/02/11/breaking-verisign-announces-com-price-hike-to-8-39/

2.http://domainincite.com/26283-verisign-upgrades-its-cash-printing-machine-but-warns-post-pandemic-could-go-either-way

通用頂級域名（gTLD）權利保護機制簡介

國際瞭望 撰輯

https://blog.twnic.tw/2021/09/20/19675/

誰有權依法註冊什麼域名？誰才是特定域名的合法持有者？這些問題常是域名爭議的來源。當域名爭議涉及法律保護商標時，自 1999 年啟動的統一域名爭議處理政策（Uniform Dispute Resolution Policy，UDRP）是歷史最悠久，也最多人熟悉的爭議解決管道。

ICANN 於 2012 年開放新通用頂級域名（new gTLD）申請回合，gTLD 的數量從不到 20 筆激增至超過千筆。這表示商標權利所有人名下商標被註冊成域名的風險大幅提升，風險處理開銷也將因此飆升。為了減緩相關風險及開銷，許多新的權利保護機制（right protection mechanism，RPM）相應而生，包括：統一快速中止爭議處理流程（Uniform Rapid Suspension Dispute Resolution Procedure，URS）；利用全球商標資料中心（Trademark Clearinghouse，TMCH）資料庫所提供的保護措施如日出期註冊（Sunrise services）及商標維護（Trademark Claims）通知服務；以及**授權**後爭議處理流程（Post-Delegation Dispute Resolution Procedure，PDDRP）。

本文將分別簡介上述權利保護機制。在那之前，先簡短介紹僅能在新申請 new gTLD 字串期間使用的權利保護機制：法律權利反對意見（Legal Rights Objections，LRO）。

法律權利反對意見（LRO）

本機制由世界智慧財產權組織（World Intellectual Property Organization，WIPO）和 ICANN 共同設計完成，提供商標所有人及國際政府組織在 new gTLD 申請期間，針對可能損及其法律權利的 new gTLD 字串申請提出正式反對意見。所有 LRO 都將交由獨立仲裁委員會，根據申請字串的外觀、發音、涵義、反對者是否正當取得及行使商標權利字串，以及申請人的申請意圖等原則逐一審理並做出判決。在 2012 年申請回合期間，負責提供此仲裁服務的是 WIPO 仲裁暨調解中心。

根據 WIPO 網站資料，2012 年申請期間總共收到 69 筆 LRO。所有審理結果也都公開記錄於 WIPO 的 LRO 專屬頁面。

統一域名爭議解決政策（UDRP）

如前所述，統一域名爭議處理政策（UDRP）是歷史最悠久的域名爭議處理管道，所有受理註冊機構皆須遵守 UDRP。在 UDRP 下，大部分基於商標的域名爭議，應經協議或仲裁解決爭議後，受理註冊機構才可以取消、中止或轉移域名。此外，也有人選擇逕行法律訴訟管道，另一種可能是在爭議處理達成協議後，不滿結果而轉向仲裁或法律訴訟。若遭投訴的域名有濫用行為，例如：網路蟑螂（cybersquatting），商標權利人可在向爭議處理服務提供商提出投訴時，同時提出 UDRP 申請加速行政處理程序。

UDRP 服務提供商包括：阿拉伯域名爭議處理中心（Arab Center for Domain Name Dispute Resolution，ACDR）、亞洲域名爭議處理中心（The Asian Domain Name Dispute Resolution Centre，ADNDRC）、加拿大國際網際網路爭議處理中心（Canadian International Internet Dispute Resolution Centre，CIIDRC）、捷克仲裁法院網際網路爭議仲

裁中心（The Czech Arbitration Court Arbitration Center for Internet Disputes）、美國國家仲裁協會（The National Arbitration Forum，NAF），以及世界智慧財產權組織（WIPO）。

統一快速中止（URS）

統一快速中止（URS）僅適用於 new gTLD 的域名爭議案件，目標是針對具明顯商標侵權情形的案件，提供比 UDRP 更經濟快速的投訴管道。提供 URS 的服務提供商共有三家，分別是亞洲域名爭議處理中心（ADNDRC）、位於義大利的 MFSD srl，以及美國國家仲裁協會（NAF）

全球商標資料中心（TMCH）

全球商標資料中心（TMCH）是 ICANN 指定成立的中央資料庫，存放已註冊、法院認證，以及法律或協議保護的商標。TMCH 本身並非一種權利保護機制，而是權利保護機制如日出期註冊（Sunrise Registration）及商標維護運作必須仰賴的資料庫。TMCH 由 ICANN 委託管理諮詢公司德勤（Deloitte）負責維護，為服務不熟悉 TMCH 商標登錄流程的商標所有人，TMCH 網站中也提供服務代理商清單，權利人可以委託代理商登錄及管理 TMCH 資料庫中的旗下商標。

日出期註冊（Sunrise Services）

商標持有人可以在域名開放大眾註冊前的日出（Sunrise）期間，優先註冊持有商標的相關域名。所有 new gTLD 註冊管理機構都應開放至少 30 天的日出期註冊。

商標維護（Trademark Claims）

日出搶註結束後便進入商標維護期，在此期間雖然域名已開放大眾註冊，但若有人註冊的域名符合 TMCH 資料庫中登錄的商標，其將會收到通知，提醒此域名是註冊商標；同時，商標持有人也會收到通知。商標維護期一般與大眾註冊同時開始，將維持至少 90 天。

授權後爭議處理程序（PDDRP）

若權利人因特定 new gTLD 註冊管理機構行為導致權利受到侵害，可透過「**授權**後爭議處理流程」（PDDRP）提出投訴。PDDRP 共有 3 種類型，分別是：商標**授權**後爭議處理流程（Trademark Post-Delegation Dispute Resolution Procedure，TM-PDDRP）、註冊管理機構限制事項處理流程（Registry Restriction Dispute Resolution Procedure，RRDRP），以及公共利益承諾處理流程（Public Interest Commitments Dispute Resolution Procedure，PICDRP）；上述仲裁程序都由 ICANN 委任的外部單位負責。

1. **商標授權後爭議處理流程（**TM-PDDRP**）**

若註冊管理機構發生在 new gTLD 頂級域名或第二層域名侵犯商標權利的情形，受害者可訴諸 TM-PDDRP。透過 TM-PDDRP 提出投訴的至少 30 天前，商標所有權人必須通知註冊管理機構相關侵權情形，並表達會面處理此議題的意願。

2. **註冊管理機構限制事項處理流程（**RRDRP**）**

若 new gTLD 註冊管理機構以社群名義申請並取得 new gTLD 字串，則註冊管理機構協議（Registry Agreement，RA）當中會有社群 TLD 特定的相關條款。任何社群 TLD 宣稱代表之社群，若因註冊管理機構違反 RA 相關條款導致權益受損，便可透過此 RRDRP

提出投訴。投訴人必須先經由 ICANN 一般投訴管道向 ICANN 履約部門提出投訴；若投訴結果未能滿足投訴人，才能進一步利用 RRDRP 提出投訴。

3. **公共利益承諾處理流程（**PICDRP**）**

若註冊管理機構未符合 RA 第 11 條規範（Specification 11）中的公共利益承諾，則可循 PICDRP 提出投訴。投訴人必須先經由 ICANN 一般投訴管道向 ICANN 履約部門提出投訴；若投訴結果未能滿足投訴人，才能進一步利用 PICDRP 提出投訴。

根據 ICANN 網站，TM-PDDRP 的仲裁服務提供商共有 3 家，分別是亞洲域名爭議處理中心（ADNDRC）、美國國家仲裁協會（NAF），以及世界智慧財產權組織（WIPO）。然而自 2012 年推出後，TM-PDDRP 的投訴案件為零。

所有通用頂級域名權利保護機制審核政策發展流程（Review of All Rights Protection Mechanisms in All gTLDs Policy Development Process，簡稱 RPM PDP）

定期審視特定機制的運作流程，檢查流程可信度及成效，是確保機制持續有效的不二法則。自 1999 年實施以來，UDRP 從未經歷過任何類似的審核。許多新的 RPM 隨著 2012 年 new gTLD 申請回合出現，理應亦定期檢視這些機制是否如預期運作、發揮功效。

有鑑於此，通用域名支援組織（Generic Names Supporting Organization，GNSO）理事會於 2016 年 1 月啟動 PDP，召集工作小組檢視所有運作中的 RPM。本 PDP 分成二個階段，第一階段將檢視 2012 年後建立、適用 new gTLD 的 RPM，第二階段則聚焦於行之有年的 UDRP。

RPM PDP 工作小組已於 2020 年 11 月完成第一階段工作並發布

結案報告。今（2021）年 1 月，GNSO 理事會也以絕對多數通過此報告並轉呈董事會。ICANN ORG 於今年 4 月公告 RPM PDP 結案報告並開放公眾意見徵詢，募集社群對結案報告內容的建議及想法。公眾意見徵詢已於今年 5 月底結束，點此可參考所有募集到的社群意見。

RPM PDP 第一階段結案報告共提出 35 項建議，如前所述，建議皆針對 2012 年後誕生的權利保護機制，包括 URS、TMCH 及旗下日出搶註及商標維護服務，以及 TM-PDDRP。

工作小組將這 35 項建議分成三大類，分別是建立新政策或流程的建議（15 項）、修正既有運作方式的建議（10 項），以及維持現狀的建議（9 項）。另外，小組在第一階段工作期間發現蒐集量化資料實屬不易，甚至導致工作進度遭拖累。RPM PDP 的順利進行仰賴有效且足量的資料，因此，除上述建議外，報告中亦提出針對資料蒐集整體方式的 1 項建議。

董事會目前尚未就 RPM PDP 的結案報告達成決議，若董事會決議通過此報告，註冊管理機構及 ICANN 認證的受理註冊機構，包括 URS、TMCH 及 TM-PDDRP 的服務提供商，都必須遵守根據上述建議訂定的新政策。

2021 全球域名報告的 8 項重點資訊

國際瞭望 撰輯

https://blog.twnic.tw/2021/03/23/17406/

InterNetX 及 Sedo 於 2021 年 2 月共同發布了《2021 年全球域名報告》，其中 8 項值得關注的資訊如下：

1. 除美國外，比起.com，許多國家更喜歡使用本國 ccTLD，這種情況遍見於歐洲多國，其中以荷蘭為最。根據統計，該國每 10 萬居民中約有 35,000 筆註冊域名。
2. 每年仍有許多域名被註冊，註冊總數呈現緩慢成長。在 2020 年 9 月，.com 域名註冊總數達到 1.5 億，而現在是 1.53 億，去年有將近 3,800 萬個新的.com 域名被註冊。目前使用最多的域名是.com、.org 以及.net。
3. 域名使用數量驚人，其中.com、.org 和.net 使用率最高。
4. 根據 InterNetX 的域名銷售資料庫，the 是域名領域中出現頻率最高的單字。
5. Sedo2020 年出售的域名比 2019 年更多，報告第 37 頁的圖表顯示，Sedo 域名總銷量增加了 26%。
6. 2020 年，由 Sedo 銷售的.com、.net 及.org 售價中位數下降，其原因可能有二：一是 Sedo 取消了 2019 年的最低銷售費用，因此更多低價域名被出售，二是有更多到期域名被銷售。.com 的售價中位數從 630 美元跌至 332 美元，平均價格從 2,693 美元降至 2,223 美元。
7. Sedo 每週都會向 Domain Wire 等部落格發送售價超過 2,000 美元的銷售清單。然而，此清單僅包含售價 2,000 美元以上

的域名，而去年中位數售價為 435 美元，由此可知，清單不代表實際銷售狀況，許多售價更低的便宜域名未被納入。此外，清單中通常未列出金額最高的售出域名，去年 Sedo 售出的域名中就有 14%是未公開交易，而這些交易的金額占了去年 Sedo 總銷售額的 3 分之一。

8. 最後，Sedo 在 2020 年的銷售額中有三分之二都是時價售出（buy now transaction）。

參考資料：

https://domainnamewire.com/2021/02/23/8-notable-takeaways-from-2021-global-domain-report/

EPDP Phase 2A 推出結案報告，EPDP 終於結束？

國際瞭望 撰輯

https://blog.twnic.tw/2021/10/04/20096/

背景介紹

「通用頂級域名註冊資料臨時條款加速版政策制定流程」（Expedited Policy Development Procedure on the Temporary Specification for gTLD Registration Data，簡稱 EPDP）於 2018 年 6 月成立，第一和第二階段分別於 2019 年 2 月及 2020 年 7 月結束。

EPDP 第一階段的任務是建立新的註冊資料目錄服務（Registration Data Directory Service，RDDS）政策，也就是「如何管理註冊人資料」及「可以公開哪些註冊人資料」。根據結案報告建議，註冊人姓名、電話、地址、郵遞區號等個人資料應遮罩，電子郵件則由電子表格或匿名電子郵件取代。

EPDP 第二階段的工作範圍則包括：（1）非公開註冊資料標準化存取／揭露系統（System for Standardized Access/Disclosure to Non-Public Registration Data，SSAD）、（2）臨時條款附錄中的議題，以及（3）第一階段推遲的議題。

所謂的 SSAD，是一個供第三方申請驗證並提出資料要求的管道，此機制的用意是讓具合法目的之第三方，取得所要求的非公開註冊資料。EPDP 第二階段結案報告最終提出的 SSAD 是一個「混合模型」（hybrid model）：以集中管理方式接受揭露請求，但審核請求及揭露與否的最終決策由受理註冊機構（registrar）各自負責。

由於時程限制，EPDP 第二階段依舊未能徹底研議所有預定討論的議題。有鑑於此，若干 EPDP 工作小組成員要求通用域名支援組織（Generic Names Supporting Organization，GNSO）理事會延伸第二階段，啟動第二階段 A（EPDP P2A）流程。

EPDP P2A 結案報告重點

EPDP P2A 僅探討二個議題：（1）是否應區分註冊人資料屬於法人或自然人，並揭露法人資料；（2）同一註冊人的多筆註冊資料採用同一筆匿名電子郵件信箱的可能性，以及相關政策建議。

EPDP P2A 工作小組已於今（2021）年 9 月 2 日完成結案報告並提交 GNSO 理事會。報告中提出四項建議，所有建議都獲得工作小組的共識支持[1]。以下簡要說明四項建議的重點：

1. 必須（MUST）建立一個用以區分註冊人為法人或自然人，以及／或是顯示該筆註冊資料是否含有個人資料或非個人資料的欄位。ICANN ORG 必須與技術社群協調合作，建立在 RDDS 中使用此欄位的必要標準。如合約方（Contracted Parties）[2]欲區分註冊人為法人或自然人，可以（MAY）使用此欄位。未來 SSAD 必須支援此欄位的應用。
2. 欲區分註冊人為法人或自然人的合約方應（SHOULD）遵守下列原則：
   (1) 註冊人應可自行選擇自然人或法人身分。
   (2) 除非註冊人知情同意公開，或基於 GDPR 其他合法依據得以公開，否則必須確保公開 RDDS 中遮罩自然人資

[1] 這裡的「共識支持」指「Consensus」。根據 GNSO 工作小組指導原則（Working Group Guidelines）第 3.6 節，Consensus 的定義為「大部分同意，僅少數人不同意」。

[2] 指與 ICANN ORG 簽有合約的註冊管理機構（registry）及受理註冊機構。

料。

(3) 建議受理註冊機構在 RDDS、SSAD 或內部資料庫，使用建議 1 中的欄位處理相關資料。

(4) 受理註冊機構須清楚說明法人及自然人的定義，確保註冊人了解自稱法人的代表意義及後果。

(5) 若註冊人自稱法人且確認輸入資料中不含個人資料，則受理註冊機構應在 RDDS 中公開此資料。

(6) 註冊人（資料主體）應能輕易修正任何可能錯誤。

3. 未來 ICANN 內相關資料控制方（controller）及處理方（processor）在根據 GDPR 第 40 章建立行為守則（Code of Conduct）時，應將上述原則納入考量。

4. 如合約方欲於公開 RDDS 中揭露假名化（registrant-based）或匿名化（registration-based）[3]的電子郵件信箱，應參考 EPDP 就此議題取得的法律諮詢建議，以及資料保護當局的相關指南。

EPDP P2A 工作歷程

筆者身為 EPDP P2A 工作小組成員，認為結案報告執行摘要中〈主席的話〉不僅完整描述小組的工作歷程，也充分呈現小組在過程中遇到的挑戰。以下段落以〈主席的話〉為骨，筆者的參與心得為肉，希望讀者可藉此一窺自今年 1 月開始，為期 8 個月的 EPDP P2A 工作小組旅程。

EPDP 第一、第二階段工作都極度勞心勞力，其中工作小組也

[3] 工作小組在 EPDP P2A 中，使用「同一註冊人」（registrant-based）取代過去使用的「假名化」（pseudonymized），並以「同一註冊」（registration-based）取代「匿名化」（anonymized）。唯本文為方便中文讀者理解，仍使用「匿名化」及「假名化」。

面對無數挑戰及艱難的協商過程。鑑於前二年的經驗，不免令人憂慮在這之後啟動的 P2A，成員也難以達成任何共識。然而，隨著本工作劃下句點，我們還是成功就報告中的所有建議達成共識，雖然結果並非大家都完全認同的「全體共識」[4]，但在小組成員立場迥異，以及缺乏實體會議、時程限制等諸多挑戰下，這樣的結果已足以感到驕傲。

如前所述，主席最終判斷報告中所有建議皆獲小組共識支持，此判斷也未受小組成員的強烈反對。然而，多方妥協的結果總是「最完美的不完美」，沒有任何一方會對結果完全滿意。有些成員仍堅持報告中建議的強度不夠，另一派則認為部分建議毫無必要。在最後一場會議中，也有成員主張他們只支持某些建議中的特定部分，對主席視所有建議為一體，直接判定整份報告具小組共識支持的決定頗有微詞。

也因此，若希望深入了解所有參與利害關係團體的完整立場，屆時報告發布後，請務必閱讀報告中來自各團體的〈少數意見聲明〉。

EPDP P2A 是 EPDP 所有階段中，唯一因為全球疫情而無法舉辦實體會議的工作階段。缺少了面對面討論、協商的機會，對上這個不同團體立場涇渭分明、難以找到共同點的議題，對 P2A 的工作無疑是極大挑戰。主席在報告中也建議 GNSO 理事會未來規劃任何 PDP 時，必須審慎考慮缺少實體會議對政策工作的具體影響。

在 P2A 中，主席、副主席及 ICANN ORG 支援職員想到的補救方案，是在正式工作會議之外，另外舉行小型、僅限部分團體代表參與的私下討論會議。這些小型討論針對成員提出的痛點，或認為有折衷可能的議題，分別邀約團體僅一名代表出席發言（可另派一

[4] Full Consensus，意指「沒有任何人在最終檢視階段提出反對」。

位代表列席旁聽），由具溝通協調專業的 ICANN ORG 職員主持，希望這些不錄音、不留存紀錄的私下小會議，可以多少彌補缺少實體會議中，休息時間閒聊或走廊上交流的遺憾。

在〈主席的話〉中，主席也解釋他最後做出「所有建議皆獲共識支持」判斷的原因。P2A 接近尾聲時，小組成員的任務是審閱 ICANN 支援職員撰成的結案報告內容，並指出報告中「完全無法接受」的部分。最後二週的 4 場工作會議中，我們逐一檢視並調整、修正這些段落，依序化解了所有「完全無法接受」的部分。雖然主席曾考慮過判斷為「全體共識支持」，但由於多數團體都已表示會提出〈少數意見聲明〉，而這也代表成員並不全然同意報告所有內容，因此主席最後仍判斷為「共識支持」。

RDDS 爭議就此結束？

隨著 P2A 完成結案報告，這個因 GDPR 而起，雖名為「加速版」，卻連綿不斷持續了 4 年的政策發展流程，似乎也終將告一段落。然而，註冊資料目錄服務自過去便是充滿爭議的議題，主張應公開越多資料越好的一方，反覆強調註冊資料對執法、網路安全及保護使用者至關緊要；反對公開的合約方不願觸法；非營利團體則希望捍衛註冊人隱私。目標如此截然相反的對立，似乎永遠不可能取得各方皆滿意的折衷結果。

事實上，P2A 就是部分團體不滿意第一、第二階段結果，爭取繼續討論特定建議的產物。而 P2A 的最終建議與原本建議本質上相去不遠，可想而知，原本要求啟動 P2A 的團體仍不會滿足。在 P2A 的多次工作會議中，部分團體就不斷提出「未來若特定法案通過應立即重啟 EPDP」，或甚至直接建議繼續「第三階段」。另一方面，經 GNSO 理事會判定非屬 EPDP 工作範疇的註冊資料準確度議

題，也已另外成立議題範圍界定小組，隱隱有下一個 PDP 出現的態勢。

EPDP P2A 的結束，究竟是否代表 ICANN 內對註冊資料目錄服務的爭議及辯論就此結束？答案似乎不言而喻。

打造更數位包容的網際網路

國際瞭望 撰輯

https://blog.twnic.tw/2021/09/13/19765/

全球通用（Universal Acceptance，UA）是 ICANN ORG 的重點工作項目，也是 ICANN 2021 至 2025 財政年度戰略計畫中的目標。為了達成此目標，很重要的一項工作是提升大眾對 UA 的認識，了解 UA 面臨的挑戰，並為深受挑戰的利害關係人提供緩解方案。有鑑於此，ICANN 線上學習平臺 ICANN Learn 最近新推出「介紹全球通用」（Introduction to Universal Acceptance）線上課程，希望進一步推廣全球通用。

過去二十幾年來，域名系統（Domain Name System，DNS）因新通用頂級域名（new generic top-level domain，new gTLD）及國際化域名（Internationalized Domain Name，IDN）的推出而持續擴張。目前市面上有超過 1,200 筆 new gTLD，其中也有使用不同文字、字符，長度不一的各種字串（如：.дети、.london、.engineering）。除此之外，更有超過 60 筆國碼頂級域名（country code top-level domain，ccTLD）都有自己語言的 IDN。頂級域名數量的增加及 DNS 的擴張，不僅鼓勵創新及增加消費者選擇，也降低了全球各地不同語言使用者使用網際網路的障礙。

然而，目前仍有許多應用程式、裝置或系統不支援使用 IDN 的域名或電子郵件信箱。這也是為什麼 ICANN 及網際網路社群始終致力推動全球通用（UA），希望使用不同語言文字的域名及電子郵件，都能獲得一樣的待遇，使用者得以自由選擇域名或信箱的語言。

在 ICANN Learn 最新上架的「介紹全球通用」課程，目標對象包括網際網路社群、技術開發人員、電子郵件服務業者、政府及立法單位。上完本課程者，將具備 UA 及相關挑戰的基礎知識，也會了解符合 UA 的社經益處。無論是希望在當地或全球推廣 UA 的人，或希望將服務系統改成符合 UA 的技術人員，都將受益於本課程。

全球 UA 程度越高，我們就能幫助越多不同語言的網路使用者、增加越多的消費者選擇、拓展企業商機、提升電信業者優勢，也更能協助政府及立法人員及人民溝通。越多人認同並參與 UA，我們就能越快實現 UA。若希望進一步參與此工程，你可以：

- 完成「介紹全球通用」課程；
- 加入 UA 討論 mailing list（UA-Discuss mailing list）；
- 參與 UA 推廣工作小組；
- 將你的服務改成 UA 友善系統（參考資源）。

參考資料：

Sarmad Hussain (2021.8.11). Learn How You Can Help Build a More Digitally Inclusive Internet. ICANN Blogs. 檢自：https://www.icann.org/en/blogs/details/learn-how-you-can-help-build-a-more-digitally-inclusive-internet-11-8-2021-en (Aug. 20, 2021)

Afnic 發布新的域名註冊規定

國際瞭望 撰輯

https://blog.twnic.tw/2021/10/20/20256/

法國的 ccTLD 註冊管理機構 Afnic 日前更新其域名註冊規定，使得政府更容易刪除.fr 域名，並禁止註冊可能假冒政府相關網站以進行網路釣魚的域名。

法國在 2020 年 12 月 3 日施行的第 2020-1508 號法律（稱為 DDADUE 法），允許「競爭、消費者事務和詐欺控制總局」（General Directorate for Competition Policy, Consumer Affairs and Fraud Control，DGCCRF）指示註冊管理機構暫停被認為用於詐欺的域名，Afnic 已將這項規定納入新版域名註冊規定當中。

除此之外，Afnic 也禁止使用「-gouv」作為第二層域名結尾的字串，包括其國際化域名（Internationalized Domain Name，IDN）。由於法國官方政府單位的域名是以.gouv.fr 結尾，這樣可避免有心人士註冊外觀相似的域名，使公民誤以為連線到合法的政府網站。

未來，Afnic 收到 DGCCRF 的禁制令之後，將會在 48 小時以內阻斷、刪除或轉移指定的域名。這項做法與鄰近的英國類似，當地的消費者保護機構與.uk 註冊管理機構 Nominet 達成協議，以刪除用於仿冒及盜版等活動的域名。

參考資料：

1. Kevin Murphy (2021.9.13). France gets more domain takedown powers. DOMAIN INCITE. 檢自：http://domainincite.com/26990-france-gets-more-domain-takedown-powers (Sep. 24 , 2021)

2. Afnic (2021.9.9). As of 15 September 2021, the registration of domain names ending in -gouv.fr will be prohibited. Afnic. https://www.afnic.fr/en/observatory-and-resources/news/changes-to-the-registration-rules-for-the-fr-tld-and-application-of-the-ddadue-law/ (Sep. 24 , 2021)

.au 禁止使用者註冊奧運相關域名

國際瞭望 撰輯

https://blog.twnic.tw/2021/09/02/19604/

國際奧林匹克委員會（International Olympic Committee，簡稱國際奧會）於 2021 年 7 月 21 日宣布，2032 年的奧運將於澳洲布里斯本（Brisbane）舉行，一週之後，澳洲國碼頂級域名（Country code top-level domain，ccTLD）註冊管理機構 auDA 隨即發表部落格文章，要求使用者停止註冊與奧運相關的域名，因為這些域名將無法使用。

auDA 在該篇文章中提到，自從國際奧會宣布此項消息之後，便湧入多筆註冊包含「olympics」或相關變形字的域名，然而這些字串均被列入 auDA 的保留清單當中，只有澳洲奧委會（Australian Olympic Committee，AOC）才能使用，其他人在未經政府許可的情況下，即使是做為域名的子字串也不被允許。

依據.au 的授權規則第 2.6 條，基於下列三個主要原因會將域名列入保留清單：

1. 包含澳洲法律限制或禁止的單詞、單詞的縮寫，或是由多個單詞首字元組成的縮寫。
2. 包含澳洲或其領土的名稱或縮寫，包括「Australia」一詞。
3. 可能會對.au 及全球域名系統的安全、穩定及完整性構成威脅。

澳洲於 1987 年公布的《奧林匹克徽章保護法》（Olympic Insignia Protection Act），限制基於商業目的註冊域名，其中包括以下文字：Olympic、Olympics、Olympic Games、Olympiad，以及 Olympiads。

就奧運會而言，AOC 是唯一可以自由註冊「olympics」相關.au 域名的組織，讓公眾確信他們正在與一個值得信賴的官方奧運資訊來源互動。

參考資料：

1. Kevin Murphy (2021.7.28). Olympics: Australia preemptively blocking Brisbane 2032 regs. DOMAIN INCITE. 檢自：http://domainincite.com/26900-olympics-australia-preemptively-blocking-brisbane-2032-regs (Aug. 6, 2021)
2. auDA (2021.7.28). .au reserved names… why can't I register that domain name? auDA. 檢自：https://www.auda.org.au/blog/au-reserved-names-why-cant-i-register-domain-name (Aug. 6, 2021)

零方資料及極化政治：大數據時代的政治倫理

國際瞭望 撰輯

https://blog.twnic.tw/2021/03/12/17131/

隱私未來趨勢與零方資料

美國市場研究公司 Forrester 預測[1]，在 2021 年，企業對於敏感個資的需求日益增多，企業將應用大數據進行管理，並透過其分析員工表現，相對的，針對企業使用個資的監管法規亦將增加，企業必須強化內部規範使自身合規。在此情況下，消費者也擔心個資遭到濫用，因此傾向與「具道德意識」的企業接觸並向其提供個資。

隨著消費者隱私意識高漲，第三方 Cookie（third-party cookie）[2]逐漸被停用，迫使企業更積極於直接從客戶端蒐集資料，預估各大企業將投入更多資源及技術於蒐集「零方資料」（zero-party data），並與資安、風險及隱私等相關業者合作。隱私規範日益嚴格雖能保障消費者權益，但也代表個資被蒐集的情況日益氾濫，尤其「零方資料」更是一種能使企業牢牢掌控消費者習性甚至人格特質的重要資訊。

零方資料[3]是消費者為了獲得個人化服務及廣告，主動分享給企業的個資，例如：某人明確表示在娛樂頻道中僅看美劇，或是在

---

1 Forrester Research. Predictions 2021: Privacy becomes an imperative in a year of transition. ZD Net 2020/10/30

2 關於 Cookie 的介紹可參閱：資安趨勢部落格。什麼是 Cookie？如何管理 Cookie，防範網路隱私外洩?. 2020/03/09

3 極詣數字營銷。零方数据（Zero-party Data）究竟是什么？ 2019/07/17

寵物頻道的推薦問卷中表示喜歡貓勝於狗。簡言之，零方資料透露出人們對於消費品項的偏好及情感，而消費者為了取得自己所偏好的服務，通常願意主動提供這些資訊給企業。零方資料具有準確及合法的特性，並由消費者主動提供，一般而言，不需要特別去解釋消費者的偏好，且主動提供的特性使企業蒐集個資更可能合規，不僅能使企業提供更為客製化的服務，違反個資法或 GDPR 的可能性也比較低；然而，若相關資料被有心人士取得，可能會深化極化政治的情況。

極化政治：概況及發展

不同黨派的支持者通常具有不同偏好[4]，以美國為例，典型的民主黨支持者往往支持民權、女權、同性戀、少數族裔及新移民權利、愛貓多於愛狗等，而共和黨支持者則支持開放槍枝、部分具有種族意識、反移民等等。

在《極端政治的誕生》（Prius or Pickup?: How the Answers to Four Simple Questions Explain America's Great Divide）一書中，作者引用了生物政治學家的實證研究[5]，說明不同黨派的支持者不僅受到社會文化或經濟教育的影響，生理反應也是影響因素之一，例如：受到驚嚇時，反應較強烈者是保守派，較溫和者是自由派。而生理因素塑造了不同黨派者的世界觀差異，並反映在消費偏好當中，例如：通常共和黨支持者更喜歡以皮卡（Pickup Truck）作為代步車款，而支持環保的民主黨通常喜歡 Prius。因此，若有心人士掌握零方資料，則有可能透過相關分析理解消費者的偏好，進一步製造不實訊

4 Marc Hetherington, Jonathan Weiler, & Scott Merriman. Prius or Pickup?: How the Answers to Four Simple Questions Explain America's Great Divide. Chapter 1.

5 王宏恩（2019 年 9 月 3 日）。〈釐清兩極化政治與世界觀的因果〉。風傳媒。

息或陰謀論強化其認同。

零方資料推升政治兩極化

零方資料某種程度上能彰顯消費者的世界觀，這些資料若被有心人士取得，再搭配時下氾濫的不實訊息或內容農場，將使極化政治的情況日益嚴重，加上政黨為了鞏固票源，有時會往更極化的方向前行，政黨透過重新定位自我，讓支持者的世界觀及政黨傾向變得更加一致。

政治極化的結果不僅是對問題的解決方法存在重大分歧，甚至對於問題本身也缺乏共識，雙方對於彼此看法產生困惑並認為對方無法溝通，進一步產生更嚴重的衝突。在極化政治的持續發展下，有心人士更能利用陰謀論與不實訊息達成特殊政治目的。若資訊量充足，零方資料可呈現廣大消費群眾的不同世界觀，要處理世界觀造成的政治分裂危機實屬不易，內心深處的衝動及傾向如今已投射至政治傾向之中。

結語

若從商業角度看待零方資料，企業能透過它掌握消費者偏好，提供更適切的服務，但從政治學的角度看待零方資料，其可能是為極化政治推波助瀾的因素，若讓偏狹的黨派及社群媒體取得零方資料，可能讓壁壘分明的對立方更加沉浸在同溫層的溫暖中，民主政治中與不同意見者溝通的元素亦日益淡化。當人們臣服於意識中的恐懼時，其將追求安全及保護，而非堅持民主信念中的溝通及對話。民粹領袖可能就隨之而起[6]，他們會挑起民眾的恐懼，讓選民

[6] Marc Hetherington, Jonathan Weiler, & Scott Merriman. Prius or Pickup?: How the Answers to Four Simple Questions Explain America's Great Divide.

認為寧可追求安全也不要造成遺憾。

一般民眾對於複雜的重大政策（例如：稅收）其實關心度不足，然而，在種族、文化及安全等能展現自我世界觀的議題時，卻相當堅持，也讓持不同世界觀者看起來更像是「外星人」。個人生活上的選擇及政治偏好密不可分且會互相強化，當零方資料被大量蒐集，個人世界觀較有可能被全面性揭露，因此，個資蒐集已不僅涉及個人隱私及國家監控，對於民主價值及社會分化亦有不小的影響力。

Chapter 3.

世界經濟論壇 2021 年度全球風險報告：數位落差與對演算法的依賴

國際瞭望 撰輯

https://blog.twnic.tw/2021/03/26/17412/

數位落差

《2021 年度全球風險報告》[1]第二章指出，數位落差的擴大將進一步削弱社會凝聚力，對數位科技及資訊的日益依賴，彰顯出各國政府監管制度與制定相關法規能力的差距。根據統計[2]，國家之間及國家內部的「數位技術落差」正在擴大，高收入國家的網路覆蓋率可達 87%，然而，低收入國家卻不到 17%。此外，在各國國內，不同社會經濟地位者獲得數位資源的機會亦有甚大差距。地緣政治的分裂深化了各國敵意並加劇了數位落差，目前仍有 23%的國家禁止或審查新聞，同時限制該國公民對重要數位資源的存取權限。

此外，許多國家的資訊保護措施不足，儘管近 80%的國家已實施電子商務及資訊保護的法規[3]，但仍跟不上數位化的速度。目前，提供公共數位服務的權力已掌握在業者手中，這使得資源分配更為不均，政府需要透過政策及監管工具縮減數位落差。

當務之急

歷經 COVID-19 疫情肆虐，政府減少數位技能差距的公共支出

1 World Economic Forum. The Global Risks Report 2021 16th Edition
2 World Economic Forum. The Global Risks Report 2021 16th Edition
3 World Economic Forum. The Global Risks Report 2021 16th Edition

及決策能力將受到限制，此種情況遍見於中低收入國家，面臨收入損失或破產風險的雇主可能也缺乏為員工提供財務支持的能力。疫情使不具數位能力的弱勢勞工生活情境更為嚴峻，對這些勞工而言，當務之急是保住既有工作或參與就業培訓。數位能力差距的擴大可能塑造新的弱勢階級。

究竟新興科技的採用是促進個人及社會福祉，抑或擴大技術持有者及未持有者之間的能力落差，是政府部門亟須思考及面對之議題。儘管科技的日新月異使得生產力得以提升，若要確保在數位化轉型的過程中降低社會分裂的風險，政府必須主動進行創新管理，例如：堅持資安及隱私、增進新技術對社會及人權影響的理解、獎勵科技創新，以及在基礎教育中加入數位素養的課程以縮小數位落差。根據 WEF 的《就業前景報告》（The World Economic Forum's Future of Jobs Report）[4]，數位化已使勞工對線上學習及數位技能（如資料分析、電腦科學及資訊科技）產生濃厚興趣，在 2020 年第二季度，雇主提供的線上學習機會增加了 5 倍，數位服務能克服因 COVID-19 導致的健康風險及經濟不平等。

被數位資源排除的勞工將錯過因數位經濟所創造的教育及就業機會，根據前述的《就業前景報告》，截至 2025 年，將產生 9,700 萬個新興就業機會，被排除在數位經濟之外的勞工將面臨生計危機，進一步導致社會分化及弱勢勞工的相對剝奪感[5]，形成社會對立。

以美國為例，目前網路安全公司 Fortinet 已免費提供包含技術操作教學的網路安全課程[6]，美國國家網路安全聯盟執行總監 Kevin

---

4 World Economic Forum. The Future of Jobs Report 2020. 2020/10

5 關於相對剝奪感的概念介紹，詳參 MBA 智庫。

6 Bradly Barth. Free cyber career training coursework emerges as a perk in tough times. SC Media 2021/01/18

Coleman 表示，網路安全產業是當前不景氣中的好機會，雖然付費課程可能更加專業並具契約保障，但目前美國需要更多財政援助及經濟措施，因此免費協助是受到歡迎的。免費課程能使人們獲得網路安全技能，並提升從事相關產業的可能性，解決因技能差距或疫情等導致的失業問題；IBM 旗下的 SkillsBuild 數位平臺也與 WEF 合作，利用網路安全培訓課程擴大網路資源。美國因既有小政府[7]傳統，私人企業承擔提供公共服務的角色，因此，科技企業主動提供公共培訓。各國政府或可參考，與不同利害相關者合作，結合專業人才提升數位培訓，以弭平數位落差。

對演算法的依賴可能導致更深刻的社會裂痕

對演算法的依賴將使社會不平等加劇，可能會損害個人福祉並加劇社會裂痕，演算法本身可能內建既有社會歧視[8]，例如：運用演算法做出的刑事判決可能會反映出社會上對弱勢團體的歧視，若不解決演算法內建的偏見，其導致的社會分歧可能會在短時間內不斷擴大。

因疫情之故，個人對數位經濟的依賴日漸加深，掌握演算法的科技企業因此得以坐大，此趨勢可能進一步使消費者無力對抗企業，從而失去與之協商及個資使用的主導權，演算法使用戶有可能面臨針對性的政治操弄、隱私侵犯、網路犯罪、經濟損失以及心理或人身傷害的風險，而這些風險通常來自於科技平臺上的不實訊息、陰謀論或帶有歧視意涵的不適切內容。作為對上述情境的回應，各國政府普遍增加消費者保護法規並嘗試強化對數位市場的監

7 關於美國小政府主義的介紹可參考維基百科。

8 MandyLi. 人權在網路世界中危機重重？演算法掌控社會的隱私與歧視挑戰。Inside 2020/12/01

管。近期，歐盟通過《數位服務法》[9]，根據該法，歐洲科技巨頭必須嚴格審查平臺，並有義務刪除非法及有害宣傳內容，若不遵守這些規則，企業將被處以全球年營業額的 6%罰款。

不僅歐盟作出回應，美國國會也通過相關法規，賦予業者對平臺言論更大的監管責任。美國在拜登政府上任後，民主黨議員也開始與白宮商討如何對付社群平臺爭議言論的處理方式[10]，以約束平臺上的不實訊息及煽動性言論。整體趨勢是政府透過法規使科技企業擔負更多道德責任。除了政府推動監管外，平臺業者也開始自發的發布相關準則。例如：維基百科（Wikipedia）基金會於 2021 年 2 月 2 日發布第一個全球行為準則[11]，以回應輿論長期對於維基百科無法應對平臺上的騷擾言論，以及缺乏言論多樣性之批評。新規範所禁止的相關內容包括：線上及線下的騷擾行徑、仇恨言論、使用侮辱性或具刻板印象字眼進行人身攻擊、暴力威脅言論、在不同文章中追蹤某人以批評其言論、將不實訊息或帶有偏誤的資訊引入文章內容。

綜合討論

數位落差及對演算法的依賴皆是報告中所著墨的重大風險，目前大量數位資源已被科技巨頭掌握，政府除強化科技巨頭責任並訂定監管規範外，也須注意數位技能培訓以縮減數位落差，甚至將其納入社會福利政策之中，才能有效抑制風險。然而，分裂網路及政府管制亦有可能加劇數位落差，根據歐亞集團發布的《2021 全球

[9] 羅昀玫（2020 年 12 月 16 日）。〈歐盟擬新法規 美中科技巨頭面臨拆分、天價罰款威脅〉。鉅亨網。

[10] Nandita Bose, Jarrett Renshaw. Exclusive: Big Tech's Democratic critics discuss ways to strike back with White House Reuters 2021/02/17

[11] Elizabeth Culliford. Exclusive: Wikipedia launches new global rules to combat site abuses. Reuters 2021/02/02

風險報告》[12]，預期各國將加強數位主權及跨境資料流通的管理，未來網路分裂及地緣政治的割裂仍會加劇，因此，要如何在捍衛網路主權及網路安全的同時縮減數位落差，是對各國政府治理效能的嚴峻考驗。

最後，雖然透過政府強制或業者自願性措施能降低因演算法導致的社會裂痕，但此類措施也產生限制公民自由、訊息審查及通訊中斷的風險，跨國科技企業已形成一股超越政府的力量，其具有能與政府法規抗衡的政治能量，因此相關監管能否發揮作用，仍須持續觀察。

[12] Eurosia. TOP RISKS FOR 2021 2021/011/04

婦女歷史月：介紹 ICANN 的傑出女性

國際瞭望 撰輯

https://blog.twnic.tw/2021/05/07/18236/

3 月是美國婦女歷史月，為了共襄盛舉，ICANN 特此撰文介紹三位傑出女性，分別代表三個 ICANN 不同的多方利害組成結構：社群、董事會及 ICANN 組織。這三位女性分別是國碼域名支援組織（Country Code Names Supporting Organization，ccNSO）主席 Alejandra Reynoso、ICANN 董事 Merike Käo，以及 ICANN 政策研究及利害關係部副理 Karen Lentz。

ICANN 社群：Alejandra Reynoso

Alejandra 擁有資訊科學碩士學位，於 2011 年加入瓜地馬拉國碼域名（.gt）註冊管理機構。身為研究及技術開發人員，Alejandra 負責.gt 註冊管理功能的技術及資訊系統全部業務。除了母語西班牙語，Alejandra 還精通英文及葡萄牙文。2011 年，Alejandra 透過英才計畫（Fellowship）參與 ICANN41 新加坡會議，就此加入 ccNSO，擔任過工作小組成員及主席。她在 2015 年 ICANN64 神戶會議獲拉美地區成員推派，成為 ccNSO 理事會成員，並於 ICANN70 獲選成為 ccNSO 主席。

Alejandra 認為，更多的女性參與是維繫 ICANN 社群多元的關鍵，多元才能確保多樣不同的觀點，進而促成更豐富有意義的政策討論。而 ICANN 能做的，是打造互相尊重、重視專業的環境，讓每個人都能平等發聲。

Alejandra 視母親為最佳榜樣，認為是母親開放、先於時代的進

步觀念，鼓勵她勇於追求夢想。她也強調，任何盡力實現夢想、牽成他人的女性都是無名英雄。

ICANN 董事會：Merike Käo

Merike 是安全與穩定諮詢委員會（Security and Stability Advisory Committee，SSAC）駐董事會聯絡人。她現職人工智慧對話技術公司 Uniphore 的資訊安全長，之前則是資安顧問公司 Double Shot Security 的創辦人暨執行長。Merike 擁有超過 25 年網際網路技術部署及安全戰略規劃的資歷，在 90 年代，她發起並領導思科系統（Cisco Systems）的史上首個安全專案，也是思科第一本安全專書 Designing Network Security 的作者。

Merike 擁有豐富長久的全球網路治理經歷，她是國際電機電子工程師協會（Institute of Electrical and Electronics Engineers，IEEE）長期成員，參與網際網路協會（Internet Society）草創過程，也積極參與網際網路工程任務組（Internet Engineering Task Force，IETF）。她自 2010 年起成為 SSAC 成員，精通英文、德文及愛沙尼亞語。

對於「更多女性參與 ICANN 的重要」，Merike 認為女性視角與女性獨有的文化性別經驗，能增加政策討論的層次深度。對女性參與者而言，有女性擔任領導職位、作為學習榜樣更是至關重要。Merike 指出，女性參與 ICANN 的一大障礙，是她們往往擔負家中照護者的責任。未來 ICANN 會議若逐漸走向線上配合實體的混合形式，或許能減輕女性參與 ICANN 會議的負擔。她也讚許社群自主發起的「DNS Women」連線，認為這提供女性彼此交流、建立社交網路的大好機會。

對 Merike 而言，對自己誠實、嚴以律己、負責、樂於助人且不畏艱難的女性，都是最佳榜樣。她的母親便擁有以上特質，而母親也是她勇於投入技術領域的關鍵。

ICANN 組織：Karen Lentz

Karen Lentz 於 2003 年加入 ICANN，擔任通用頂級域名（generic top-level domain，gTLD）註冊管理機構聯絡人。任職 ICANN 期間，她的工作包括註冊管理機構合約修訂、政策實施、權利保護機制，她也參與撰寫 gTLD 申請指南。Karen 大學雙主修英文及政治，更分別取得寫作及新聞碩士學位。她目前職務包含政策及審核建議實施、議題研究分析，同時也參與國際化域名及全球通用相關專案。

Karen 認為擁有越多觀點、越多技能及經驗，多方利害關係模式的運作也會更順暢。這也是 ICANN 必須鼓勵更多女性參與的原因。她指出，提供新進者參與指引、積極鼓勵各種背景投入 ICANN，是達到以上目標的最佳方式。

Karen 的榜樣也是自己的母親。在她心目中，母親是無私助人的體現。但她也不忘強調，眾多女性在這艱難的時局中互相幫助，共同抵禦疾患、種族歧視、暴力及各種難關，這些無名英雄都值得我們作為榜樣。

參考資料：

https://www.icann.org/en/blogs/details/celebrating-women-at-icann-31-3-2021-en

國際化域名加速政策發展流程：徵求參與者及觀察員

國際瞭望 撰輯

https://blog.twnic.tw/2021/07/01/19101/

ICANN 通用域名支援組織（Generic Names Supporting Organization，GNSO）理事會今（2021）年 5 月底決議成立國際化域名（Internationalized Domain Name，IDN）加速政策發展流程（Expedited Policy Development Procedure，EPDP），並於 6 月公開徵求 IDN EPDP 工作小組成員。本工作小組的目標成果是針對以下二項議題，向 GNSO 理事會提出政策建議：

1. 所有通用頂級域名（generic top-level domains，gTLD）的定義及異體字（variant）的管理方式。
2. 如何在未來更新合約方須履約遵守的 IDN 實施指南 4.0 版提案。

考量 EPDP 的工作內容及其章程要求，GNSO 理事會決定依「代表制＋開放」的模式組成 EPDP 小組，這表示 IDN EPDP 小組將由成員（member）、參與者（participant）、觀察員（observer）三種參與類型組成。採用此參與模式是希望在確保 EPDP 小組工作效率的同時，仍能提供廣大 ICANN 社群成員參與機會。

成員將由 ICANN 社群內各團體指派限定人數擔任，這些小組成員將主導 EPDP 的議題討論，亦有權參與結案報告中政策建議的共識表決。有關哪些團體可以指派多少代表的相關細節，請參考 IDN EPDP 章程。

參與者也可以參加所有 IDN 的工作會議並自由發言，但不能

參與最終的共識表決。根據章程，工作小組成員必須具備包括 IDN 專業知識，對 ICANN 政策及相關流程、註冊管理服務及受理註冊服務也都應有適當了解。參與者最好也具備以上知識，亦應參與所有 EPDP 工作會議，並在需要時提出意見。

觀察員可以訂閱 IDN EPDP 工作小組 mailing list，但僅能閱讀、無權回覆。觀察員也不可參與工作小組會議。

ICANN71 期間，本 EPDP 亦於 6 月 14 日舉辦了一場推廣議程「GNSO IDN EPDP Community Outreach Session」，議程中首先由 ICANN 職員 Pitinan Kooarmornpatana 介紹 IDN 在 ICANN 中的發展，接著由長期參與 ICANN 內 IDN 相關工作流程的社群成員 Akshat Joshi 及 Edmon Chung 分別介紹何謂「根區標籤生成規則」（Root Zone Label Generation Rules，RZ-LGR），以及何謂 IDN 異體字。有興趣進一步了解的讀者，可以點此觀看議程錄影。

參考資料：

ICANN (2021.6.3). Participate or Observe: Expedited Policy Development Process on IDNs. ICANN Blog. Retrieved from: https://www.icann.org/en/announcements/details/participate-or-observe-expedited-policy-development-process-on-idns-3-6-2021-en (Jun. 18, 2021)

New gTLD 申請回合：下一步

國際瞭望 撰輯

https://blog.twnic.tw/2021/08/27/19586/

實施評估流程（Operational Design Phase，ODP）是去（2020）年底由 ICANN ORG 正規化的機制，董事會就政策建議報告做出決議前，可以指示 ICANN ORG 啟動 ODP，取得更多背景資訊及相關評估，做出更完善的決定。新通用頂級域名未來申請政策（New gTLD Subsequent Procedures Policy Development Process，簡稱 SubPro）工作小組已於今年完成結案報告，董事會目前正在研議啟動此報告的 ODP。

SubPro 光是社群的政策討論制定就耗時 5 年，今年終於完成的報告篇幅長達 400 頁，內含 100 項政策建議，還不包括加總超過百條的過去建議確認事項及實施指導原則，以及小組最終無法達成共識的棘手議題。

如前所述，董事會正在研議啟動 SubPro 的 ODP。在此期間，ICANN ORG 除了提供董事會 SubPro 政策建議及複雜議題的背景資訊，也同時評估 ODP 應涵蓋的項目，包括技能需求、時程、系統條件、財務考量等因素，基本上就是 ODP 的前置作業。

ODP 的最終目標是提供董事會完整務實的實施評估報告（Operational Design Assessment，ODA），報告中會針對諸如風險、預期開銷、資源需求、時程安排及其他實施事項，提供完整的分析評估。董事會將參考實施評估報告、公眾意見及其他相關材料，最終就 SubPro 結案報告的政策建議達成決議。

目前 ICANN ORG 端的 ODP 前置作業已幾乎完成，只要董事

會正式決議啟動 ODP，就可以開始後續工作。對此進展有興趣的讀者，未來可以從此頁面追蹤工作進度。

參考資料：

Karen Lentz (2021.7.29). Next Steps Toward the Next Round. ICANN Blogs. 檢自：https://www.icann.org/en/blogs/details/next-steps-toward-the-next-round-23-7-2021-en (Aug. 6, 2021)

少了網路，我們將無法實現永續發展目標

國際瞭望 撰輯

https://blog.twnic.tw/2021/08/13/19323/

網際網路協會（Internet Society，ISOC）網路發展專案小組的資深副總裁 Jane Coffin，在 2021 年 7 月上旬參加了聯合國「永續發展高階政治論壇」（High Level Political Forum on Sustainable Development，HLPF），她認為這是一個討論如何從 COVID-19 疫情中持續復甦的絕佳機會，也能藉此突顯出網路的不可或缺。

Coffin 表示，她難以想像如果沒有網路，人們要如何在疫情下維持生活，研究人員在防止 COVID-19 疫情傳播以及合作開發疫苗時，也都會面臨到更大的挑戰。受惠於網路，讓許多人得以選擇居家工作，或是遠距學習。

然而，目前世界上仍有將近一半的人口無法使用網路，原因林林總總，可能是基礎設施不足，或無法負擔上網的服務費用，也可能是因為缺乏相關的數位技能。隨著網路及數位技術日漸重要，如何加緊腳步讓這些人口也能上線，成為更加急迫的問題。

聯合國的永續發展目標（Sustainable Development Goals，SDGs）正是考量到這一點，在過去曾呼籲到了 2020 年時，最低度開發國家也能達到網路的普及及近用，時至今日，這個目標顯然還很遙遠。

ISOC 認為，網路乃是為了大眾而存在，亦認同聯合國秘書長提出的數位合作地圖當中以人為本之做法。近年來，ISOC 深刻體認到，這項努力需要仰賴多方利害關係人的參與、由下而上的治理模式，同時以社群為基礎漸進提升，這也是經濟及社會進步可持續的關鍵。

ISOC 呼籲各國政府應創造一個有利的環境，讓政府的利害關係人、民間社會組織、企業，以及技術社群成員，得以共同努力尋找創新的解決方案，進而拓展我們邁向網路普及與近用的康莊大道。

參考資料：

Jane Coffin (2021.7.7). We Can't Achieve the Sustainable Development Goals without the Internet. Internet Society. 檢自：https://www.internetsociety.org/blog/2021/07/we-cant-achieve-the-sustainable-development-goals-without-the-internet/ (Jul. 16, 2021)

A4AI 發布「永續網路近用報告」

國際瞭望 撰輯

https://blog.twnic.tw/2021/08/02/19278/

目前世界上仍有將近一半的人口無法使用網路，如何讓這群人能夠順利連上網路固然是一項重責大任，但是，我們是否同時思考過其背後所隱藏的環境成本，例如：將產生多少碳足跡？對於全球氣候又會造成什麼樣的影響？

可負擔網路聯盟（Alliance for Affordable Internet，A4AI）於 2021 年 6 月 22 日發布「永續網路近用報告」（Sustainable Access Report），分析了政府單位如何將氣候問題納入其寬頻政策，並審視不作為的後果，同時對於如何打造更環保的網路提出政策建議，內容涵蓋新基礎建設的建構、營運及使用。

- **建構：**網路建設對於解決數位落差至關重要，特別是在農村及偏鄉，然而，用於提供網路建設的工具及技術將決定這項基礎建設對於環境的整體影響。
- **營運：**當基礎建設完工後，網路的營運便成為金融及環境永續性的問題，並行基礎設施（parallel infrastructure，例如電網）的可用性也相當重要。
- **使用：**透過消除網路使用的社會障礙，例如：阻礙婦女及女童使用網路的性別規範，政策制定者可以調整評估網路碳足跡與每位網路使用者碳足跡規模之間的平衡。

A4AI 透過「永續網路近用報告」向社會傳遞：某些政策決定將有助於打造更環保的網路，今天我們所做的選擇，將影響未來十年的網路。點選此連結即可閱讀完整版報告。

參考資料：

Alliance for Affordable Internet[A4AI] (2021.6.22). Report: Sustainable, Universal Access to the Internet. 檢自：https://a4ai.org/research/sustainable-access-report/ (Jul. 9, 2021)

視訊串流是否會增加碳排放？

國際瞭望 撰輯

https://blog.twnic.tw/2021/09/17/19784/

根據國際能源署（International Energy Agency，IEA）的統計資料，2020（去）年 2 到 4 月全球各地實施 COVID-19 相關警戒限制的高峰期，在視訊會議、線上遊戲、串流媒體及社群媒體的推波助瀾之下，全球網路流量激增近 40%。IEA 表示，若按照這個速度，到了 2022 年時，網路流量將會增加一倍，此外，預計在 2025 年時，行動上網的用戶量將可從去年的 38 億人口躍升至 50 億。

所有的網路活動都需要靠電力驅動，人們也擔憂這是否將導致地球暖化加速惡化。然而，問題的全貌比想像中更複雜。英國環境顧問公司 The Carbon Trust 今年 6 月的研究就發現，觀看影片的碳排放量大約等同於煮開電熱水壺 3 次，而且畫質高低對碳足跡的影響微乎其微。另一方面，IEA 則指出，線上遊戲及影音串流服務儼然成為消費者網路訊務主要來源，進而提高了人們對於資料中心的需求。專家指出，媒體串流業如何邁向更環保的未來，將取決於企業使用的能源類型，以及如何設計自家產品。

根據 IEA 分析，資料中心在 2019 僅使用 1%的全球總電量，儘管資料中心的總需求增加了 60%，但估計到 2022 年為止所需電量將保持不變。IEA 研究員 George Kamiya 表示，這是因為與其他產業相比，資料中心通常更加節能，且越來越多企業使用再生能源。

根據英國知名科學研究所皇家學會統計，數位科技所產生的溫室氣體排放量僅占全球的 1.4%至 5.9%，相較之下，交通工具就占了大約 25%。Kamiya 表示，減少線上休閒活動並無法阻止氣候變

遷，若過度關注於此，反而會轉移人們對於其他可實際減少碳排放行為（例如：減少開車或搭飛機）的注意力。我們需要各國政府實施強而有力的氣候政策，以實現整體結構性的減碳，此外，也可以善用如人工智慧等數位科技，預測及改善家中的用電方式。

參考資料：

Lin Taylor (2021.6.16). Climate change: Is video streaming pushing up harmful emissions? World Economic Forum. 檢自：https://www.weforum.org/agenda/2021/06/coronavirus-pandemic-streaming-video-calls-data-environment-emissions/ (Aug. 20, 2021)

IETF 進化史

國際瞭望 撰輯

https://blog.twnic.tw/2021/08/12/19325/

過去 50 多年來，網際網路工程任務組（Internet Engineering Task Force，IETF）這個集合體制定了無數網路協定，成功打造今日的數位網路設備及服務全球市場。起始於 1969 年，這個當初由網路研究人員鬆散組成的智庫，現在已是全球最具影響力的標準制定組織。

喬治亞理工學院山姆能恩國際事務學院（Sam Nunn School of International Affairs）國際策略、科技及政策中心（Center for International Strategy, Technology, and Policy，CISTP）特聘資深研究員 Anthony Rutkowski 特別撰寫「The IETF Evolution」一文，透過爬梳 IETF 歷年會議紀錄，了解 IETF 的參與人口組成變化，如何反映科技及市場幾十年來的劇烈改變，以及 IETF 如何與時俱進。他特別聲明，文章目的並非作為「IETF 正史」，僅希望透過回溯紀錄，成為一個墊腳石，供更多人進一步了解、剖析 IETF 的參與人口組成。

如 Rutkowski 所述，歷史事實在不同的詮釋角度下，也可能顯得截然不同。本文摘要翻譯 Rutkowski「The IETF Evolution」一文，其中陳述的觀點、立場及價值判斷，也請讀者自行斟酌理解。

起始（1969-1986）

1969 年 4 月，一群高級研究規劃局（Advanced Research Projects Agency，ARPA）的網路研究人員之間，開始流傳「徵求意見稿」

（Request for Comments，RFC）文件，這群人及 RFC，就是 IETF 的雛形。這個由 Steve Crocker 領頭，自稱網路工作組（Network Working Group，NWG）的鬆散組織，成員主要來自 2 家私人企業及 2 所大學，再加上 ARPA 資訊處理技術辦公室（Information Processing Techniques Office，IPTO）的主任。

到了 1971 年，NWG 的成員已擴充到涵蓋 7 家私人企業及 7 所大學，也陸續成立處理如資料管理、網路圖像、電子郵件及各式協定等不同議題的子工作組。但在這之後的 15 年，NWG 並未繼續擴張，成員仍以國防高級研究計劃署（Defense Advanced Research Project Agency，DARPA）相關研究人員為限，RFC 也僅在此群體內公開流通。

同一期間，許多其他重要的網際網路組織也陸續誕生，包括由時任 ARPRANET 專案經理 Vint Cerf 在 1980 年成立的網際網路設定控制委員會（Internet Configuration Control Board，ICCB）。ICCB 在之後幾年被網際網路諮詢委員會（Internet Advisory Board）取代，最後正式定名為網際網路架構委員會（Internet Architecture Board，IAB）。

初期架構及使命（1986-1990）

在 1986 年 DARPA 閘道演算法及資料架構任務組（Gateway Algorithms and Data Structures Task Force）的第四屆會議中，以「找出並解決國防部網際網路運作及短期規劃的工程問題」為目的成立了 IETF。因此契機，NWG 以 IETF 之名組織化，受到的支持也顯著成長。這個史上第一次的 IETF 會議（IETF#1）共 21 人參與，與會者由來自 13 個不同美國政府單位及來自學界、業界的承包單位組成。

草創之後，IETF 在短短幾年內以驚人的速度成長。其中，美國國會透過國家科學基金會（National Science Foundation，NSF），投入 250 億美金鉅資提拔國內網路研究、標準制定、網路應用研發呈現等產學業界，加上 NSF、NASA 與教育部都致力推動 TCP/IP 協定及應用，也是 IETF 得以迅速茁壯的重要關鍵。

除此之外，IETF 也逐漸擺脫「僅為國防部網路計畫服務」的狹隘任務，廣邀民間企業、其他政府單位，以及不同網際網路標準制定組織參與。到了 1987 年 7 月的第 6 次 IETF 會議（IETF#6），諸如 Cisco、HP、IBM 及 NASA 都在出席名單內。

在這之後，由國家科學基金會網路（National Science Foundation Network，NSFNET）主導，橫貫美洲大陸、使用 TCP/IP 的網際網路基礎建設也進入建設白熱期，更規劃繼續發展並連接全球網際網路。IETF 因此成為與會者交流技術、討論新興應用，合作探討如何結合並連貫現有及未來網路協定的重要場域。

重要改變及成長（1990-1998）

IETF 在 1990 年登上了世界標準制定的舞臺。1990 年 2 月，世界上主要的網路標準制定組織在美國維吉尼亞州弗瑞德里克斯堡（Fredericksburg）舉行第一次全球高峰會，討論標準組織如何趕上科技及市場變化的速度。會議期間，國際電信聯盟（International Telecommunication Union，ITU）秘書長邀請當時的 IAB 主席 Vint Cerf，向與會者介紹 IETF 的標準制定流程。IETF 開放參與、流程透明、紀錄公開的參與模式前所未有，也因此廣獲關注。

第 23 次 IETF 會議（IETF#23）於 1992 年在聖地牙哥舉行，會議中花了許多時間介紹 IETF 如何從 DARPA 下的小型團體，演變成廣納網路研發、營運、經銷及研究人員的開放國際社群，共同為

了網際網路的順利運作而努力。本次會議人數已經成長至 529 人，參與者更不再侷限於美國境內，共有 43 名來自 14 個不同國家的外國人參與會議。從會議紀錄中也可看出，越來越多電機及電信系統服務的供應商開始積極參與 IETF。

1994 年，IETF 發表了「IETF 之道」（The Tao of IETF）。文件中將 IETF 定義為「鬆散、自行集結，為了網際網路及相關技術的進化工程提出技術及其他貢獻的一群人」。2001 年上述定義將「網際網路及相關技術」改成簡單的「網際網路科技」，到了 2006 年，又再度簡化為「鬆散、自我集結，為網際網路科技的進化工程提出貢獻的一群人」。2012 年，此定義正式以網頁形式公告，可預期未來仍將持續跟著時代演化。

巔峰時期（1998-2007）

無論在參與人數、業界投入程度，或新市場的創造來說，1998 到 2007 年期間都可視為 IETF 的巔峰。在這期間，以 TCP/IP 為基礎的網路建設及商機急速成長擴張，眾人所熟知的網際網路泡沫（dotcom bubble）及隨之引起的電信泡沫（telecom bubble）都發生在這時期。在景氣一路走高的 1998 年，第 43 屆 IETF 會議參與人數達到 1,551 人，分別來自 27 個國家、共 546 個組織。網際網路商業設備及服務供應商更是積極參與 IETF，尤其當時 TCP/IP 技術大量應用於支援電信服務，許多電信業者也因此常出現在 IETF 會議。然而，狂熱投資的泡泡在 2001 年破裂後，這些一時踴躍參與 IETF 的業者也逐漸消失。

這期間的另一個重點，是 IETF 逐漸確立其作為網際網路倡議者的政治理念。2004 年發布的 IETF 使命宣言（IETF Mission Statement），至今仍是約束 IETF 工作及變革的基本原則。宣言中，

IETF 表示網際網路並非價值中立，IETF 也不是。IETF 希望網際網路能造福共享其「開放公平」理念的社群，並擁抱去集中化、邊緣使用者權利、開源共享等符合 IETF 核心價值的技術理念。

成員延續及演化（2007-present）

自 2007 年至今，IETF 的參與人口經歷 20 多年的波折及成長，如今已進入穩定時期。許多不同的組織單位把 IETF 當成推動自家商品或服務的平臺，繼 Cisco 之後，華為已成為最踴躍參與 IETF 的組織，亦有許多企業固定出席 IETF。以全球地區分布而言，來自中國的參與人口急遽成長，目前已成為 IETF 非美籍參與人數第一名。

全球疫情之下，2021 年的 IETF#100e 共有來自 68 個國家、498 個組織的 1,329 人線上與會。即使全面轉為線上會議，數據顯示無論是參與人數最多的國家或企業，以及與會者國際分布，都和實體會議沒有顯著差異。尤其線上形式免除了旅途開銷，許多企業反而可以派更多員工參與會議。

IETF 個人參與者

自從在九〇年代脫離國防部計畫及 NSF 資金後，IETF 的風格相較其他業界標準制定組織始終獨樹一幟，以個人身分、而非代表公司出席的參與者比例很高，而且聲量及權力絕不亞於企業代表。

以個人身分參與 IETF 的這些人背景十分多元，從由企業出錢贊助、為出資者謀取情報或參與標準制定的電腦科學家或獨立顧問，分享研究或探詢工作機會的學者研究員，到獲補助出席的弱勢或偏遠地區成員。雖然個人參與者是 IETF 重要的一部分，但如上述受贊助出席的「獨立顧問」，個人參與者究竟是否誠如其所宣稱

的代表「個人」，或是以「個人」名義為企業喉舌，尤其 IETF 做出的決定足以影響市值百億的網際網路市場，這些難以確認的個人參與者身分，不免為整個組織及決策流程蒙上一層不透明的疑慮薄紗。

IETF 的國際化

1992 年後，IETF 的非美籍參與者人數大增，其中以 1995 至 2010 年期間成長最快，達到整體參與人口的四成。這些人大部分來自少數幾個歐洲國家及日本。自 2010 年起，中國參與者成為非美籍參與人口的大宗，並穩定占整體人數近一成。整體而言，即使非美籍的參與人口增加，但以國家數而言，仍然侷限於少數國家。換句話說，名義上為了拓展多元包容，刻意輪換會議場地、在世界不同地區舉辦會議的努力，並未轉換成實際的 IETF 參與人口多元包容。

未來展望

大部分以志願協作為主要工作模式的組織，都會定期檢視成員組成，藉此改善組織的作為及使命，IETF 也不例外，最近 IAB 的 RFC 五十年（Fifty Years of RFCs）即為一例。IETF 主席最近也啟動諮詢流程，徵集針對 IETF 組織效率及改善需求的意見。

30 年前，IETF 還年輕時，是個力求改變，樂於與其他歷史更悠久的標準制定組織合作的團體。如今，隨著 IETF 邁向不惑之年，也面臨如何避免結構僵化、持續聽取社群意見、改善透明度並防止少數利害團體獨大等課題。Rutkowski 建議，再次開始積極與其他組織協作，也許是可以考慮的解決之道。

參考資料：

Anthony Rutkowski (2021.5.26). The IETF Evolution. CircleID. 檢自：https://www.circleid.com/posts/20210526-the-ietf-evolution/ (Jul. 16, 2021)

ICANN 域名系統安全威脅防治計畫：進度報告

國際瞭望 撰輯

https://blog.twnic.tw/2021/08/11/19538/

網域名稱系統（Domain Name System，DNS）濫用始終是 ICANN 社群中討論最激烈的熱門議題。過去幾年來，ICANN ORG 也積極透過各種方式支援社群防治 DNS 濫用。去（2020）年開始，ICANN ORG 啟動組織內跨部門的多功能專案，目的是協調、強化 ICANN ORG 方面 DNS 濫用防治的多項支援工作。

究竟如何定義 DNS 濫用，ICANN 社群目前仍未底定全體共識同意的定義。ICANN ORG 在協助社群防治 DNS 濫用的相關工作上，主要使用政府諮詢委員會（Governmental Advisory Committee，GAC）及基本通用頂級域名註冊管理機構協議（Base gTLD Registry Agreement）定義的 DNS 安全威脅，也就是釣魚、惡意軟體、殭屍網路及網址嫁接。ICANN ORG 也將垃圾郵件視為安全濫用的一種，但只有在「郵件名稱為濫用域名」時才適用。

如前所述，ICANN ORG 專案的主要目標是支援社群防治 DNS 安全威脅。本專案有三大主要支柱：

- 作為值得信任的資訊來源：提供研究、資料及專業意見，協助基於事實的社群討論。
- 提供工具：研發工具以支援社群的 DNS 安全威脅防治工作。
- 執行合約規定：透過稽核及投訴調查，執行註冊管理機構協議、驗證受理註冊機構協議及 ICANN 共識政策。

ICANN ORG 於今年 7 月 22 日舉辦了「ICANN 的 DNS 安全威

脅防治專案」線上說明會，請到 ICANN 履約部門、全球域名暨戰略部門（Global Domains and Strategy，GDS），以及技術長辦公室（Office of the Chief Technology Officer，OCTO）代表，介紹各自進行中的專案及行動，包括合約執行及稽核、域名濫用活動報告（Domain Activity Abuse Reporting，DAAR），以及「域名安全威脅辨識、蒐集與通報」（domain name security threat identification, collection and reporting，DNSTICR）系統。ICANN 亦爲本專案設置專屬網頁，有興趣的讀者不妨前往瀏覽，7 月 22 日線上說明會的影片亦已上傳至此處。

參考資料：

Russ Weinstein (2021.7.19). Update on ICANN's DNS Security Threat Mitigation Program. ICANN Blogs. 檢自：
https://www.icann.org/en/blogs/details/update-on-icanns-dns-security-threat-mitigation-program-19-7-2021-en (Jul. 30, 2021)

浩瀚無垠，奔向宇宙：太空與網路安全

國際瞭望 撰輯

https://blog.twnic.tw/2021/09/24/20010/

太空領域與網路安全的重要性已備受重視

自美蘇冷戰後，美國一直在太空領域獨占鰲頭，但近年來中國也積極參與太空領域，並研發出國產的「北斗衛星導航系統」，試圖與美國競爭。根據 BBC 報導[1]，中國開始啟用「天宮號」空間站，並計畫於 2021 及 2022 年再發射「問天號」及「夢天號」實驗艙，進一步擴大空間站。除中國外，俄國也有建造太空站的計畫，目標在 2030 年啟用[2]。世界大國已開始在太空領域彼此競爭，此情況不僅將產生製造更多太空垃圾的風險，衛星、太空船及其他太空資產的網路風險亦將隨之增加。

前美國總統川普於 2020 年發布的《第五號太空政策命令》（Space Policy Directive-5）[3]確認網路安全原則適用於太空，並提及針對太空基地站或相關系統的特殊威脅，例如偽造傳感器資料或破壞傳感器系統；駭侵或干擾指揮及控制基礎設施；以及未經授權的有心人士透過安全漏洞竊取關鍵軟硬體權限。

太空無疑已是大國兵家必爭之地，美國太空司令部（U.S. Space

---

1 BBC News 中文（2021 年 6 月 26 日）。〈中國啟用天宮空間站 美國擔心太空主宰地位受威脅〉。檢自：https://www.bbc.com/zhongwen/trad/world-57600910 (Aug. 25, 2021)

2 自由時報（2021 年 4 月 22 日）。〈競爭外太空！俄羅斯宣布建造國家太空站 計畫 2030 年啟用〉。檢自：https://news.ltn.com.tw/news/world/breakingnews/3507564 (Aug. 25, 2021)

3 文件連結：https://fas.org/irp/offdocs/nspm/spd-5-fs.pdf

Command，USSPACECOM）亦開始思考如何落實太空網路安全。由於美國公共建設民營化之傳統，保護關鍵基礎設施的常見做法是建立威脅資訊共享機制。該部指揮官 James Dickinson 將軍表示，目前正評估考量適合的模式[4]，2019 年成立的「太空資訊共享暨分析中心」（Space Information Sharing and Analysis Center，Space ISAC）便是一例，2021 年更有 24 間太空相關企業及科技巨頭（如微軟）宣布加入。

據 Dickinson 將軍表示，太空司令部已安插網路司令部（United States Cyber Command，USCYBERCOM）人員，同時與美國國家偵察局（National Reconnaissance Office，NRO）保持聯繫，就聯合行動、規劃網路安全演習及太空軌道及技術問題進行磋商。

儘管政府已開始重視太空安全，但目前美國大眾普遍缺乏安全意識，Dickinson 表示，絕大多數美國人仍不了解許多地面業務仰賴衛星軌道上的系統或硬體，包括 GPS 衛星導航系統、ATM、信用卡以及大型現場直播都與太空基地臺系統相關。因此提升大眾及產業的太空網路安全意識，是整合支持及資源的第一步。

衛星為重中之重

目前最重要的太空資產是衛星，其用途包括軍事、民用、商業等，例如：電訊、廣播電視及 GPS 導航系統皆須仰賴衛星，軍用衛星經常用於偵察、導航及通訊；政府衛星主要用於氣象及科學考察；民用衛星的用戶包括學術研究機構及業餘廣播[5]。由此可見，

[4] Derek. B. Johnson (2021.7.27). The military is mulling how to share cybersecurity threat data for space. SC Media. 檢自：https://www.scmagazine.com/analysis/threat-intelligence/the-military-is-mulling-how-to-share-cybersecurity-threat-data-for-space (Aug. 26, 2021)

[5] BBC News 中文（2011 年 4 月 11 日）。〈圖解資料：太空衛星知多少〉。檢自：https://www.bbc.com/zhongwen/trad/china/2011/04/110408_satellite_50_years

公民生活的各層面多仰賴衛星，因此，衛星若遭受攻擊將造成嚴重後果。

美國太空發展局（Space Development Agency，SDA）局長 Derek Tournear 於 2021 年 4 月 14 日表示，對衛星而言，相較於飛彈攻擊，網路及供應鏈攻擊更令人擔憂[6]。Tournear 於華盛頓太空企業圓桌論壇（Washington Space Business Roundtable forum）發表談話指出，擁有數百顆衛星的擴散網路，使衛星系統能抵禦飛彈等地面武器攻擊，但網路攻擊可透過破壞供應鏈系統使大量衛星停止運作，只要供應鏈系統遭駭侵，整體衛星網路都將被癱瘓。

為保衛 SDA 衛星網路，該機構將與其他國防單位合作，發展用於衛星的加密及其他安全設備。SDA 將與安全設備供應商合作，也將接受非美國廠商的報價，但供應鏈設備來源是一大關鍵，政府必須謹慎權衡，SDA 強調，關鍵零組件或飛行計算機（flight computer）[7]等設備須由國內供應商提供，目前國防部特別擔憂由中國製造的零組件或軟體，它們可能是敵國進行網路攻擊的媒介。

保護衛星網路安全

根據外媒 Security Magazine 分析[8]，衛星網路安全包括衛星本體

(Aug. 26, 2021)

6 Sandra Erwin (2021.4.14). DoD space agency: Cyber attacks, not missiles, are the most worrisome threat to satellites. SPACENEWS . 檢自：https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites/ (Aug. 26, 2021)

7 飛行計算機為一種精細複雜的電腦系統，可協助計算飛行器的燃油消耗、風阻、航行時間等項目。詳細資料參考維基百科：https://en.wikipedia.org/wiki/Flight_computer

8 Thorsten Stremlau (2021.4.19). The vulnerability of satellite communications. SECURITY. 檢自：https://www.securitymagazine.com/articles/94689-the-vulnerability-of-satellite-communications (Sep. 10, 2021)

及地面基地站。持有衛星的組織必須了解存在哪些漏洞，目前許多組織仍使用傳統衛星通訊，這些衛星的網路安全系統不易更新，在更新時須完成測試，確保系統升級不會干擾或影響其他關鍵系統功能。

功能較弱的加密系統及老舊的網路設備是常見的衛星網路漏洞，隨著衛星通訊技術演進，網路安全技術也隨之提升，包括可信賴運算（Trusted Computing，TC）、加密金鑰、結構單元（Building Block）等技術皆可使用，網路安全基礎設施能讓從基地站發送至衛星的資料在每個發送階段進行驗證，以防止駭侵攻擊。此外，良善的網路衛生、限制存取權限、乾淨供應鏈及第三方風險管理，以及確保網路及實體措施的安全，將是保護衛星安全之關鍵[9]。最後，衛星產業可參考美國國家標準暨技術研究院（National Institute of Standards and Technology，NIST）提供的網路安全框架（NIST Cybersecurity Framework）採取網路安全措施。

與一般網路安全原則相同，政府及相關廠商須針對衛星網路攻擊進行預防、偵測及回應，確認關鍵資產並採取風險緩解措施。一旦發生網路安全事件，衛星部門的資訊科技（information technology，IT）及營運科技（operational technology，OT）團隊須依 SOP 流程降低負面影響。

儘管有上述機制，但牛津大學研究人員 James Pavur 於 2020 年黑帽安全會議上指出[10]，他可輕鬆利用市價 300 美元的電視衛星接

---

[9] Mark Holmes (2021). The Growing Risk of a Major Satellite Cyber Attack. Via Satellite. 檢自：http://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/ (Sep. 10, 2021)

[10] 陳曉莉（2020 年 8 月 7 日）。〈安全研究人員：衛星網路含有可被竊聽的安全漏洞〉。iThome。檢自：https://www.ithome.com.tw/news/139281 (Sep. 10, 2021)

收設備攔截衛星通訊。由於各地資通訊服務多仰賴衛星連接，衛星須盡可能將資料在最大範圍內傳送給各地用戶，因此往往以未經加密的方式加快傳播速度，Pavur 認為這是衛星網路的最大漏洞，且衛星網路攻擊影響層面可能橫跨國家，必須審慎看待。

結語

目前全球約部署 2 千顆通訊衛星，但在 2030 年可能會增加到 1.5 萬顆[11]，隨著衛星日漸普及，衛星製造商及網路服務供應商應正視網路安全議題並加以改善。此外，預期世界大國將持續建設更多太空基地站，隨著太空旅行魅力日增，首間太空旅館將於 6 年後問世[12]，代表太空網路安全將更加重要，可持續觀察各國提出的太空網路安全政策及相關議題。

[11] 陳曉莉（2020 年 8 月 7 日）。〈安全研究人員：衛星網路含有可被竊聽的安全漏洞〉。iThome。檢自：https://www.ithome.com.tw/news/139281 (Sep. 10, 2021)

[12] Momo Chi（2021 年 3 月 14 日）。〈首座太空旅館預計 2027 年問世！主題餐廳、電影院、SPA 等豪華設施全都有！〉。LaVie。檢自：https://www.wowlavie.com/article/ae2100285 (Sep. 10, 2021)

南極洲將有高速網路可用

國際瞭望 撰輯

https://blog.twnic.tw/2021/12/28/21342/

每年 10 月至隔年 2 月，共有超過 1,000 名科學家前往位於南極洲、由美國國家科學基金會（National Science Foundation，NSF）營運的麥克默多站（McMurdo Station）進行研究，研究範圍涵蓋氣候到海洋科學。

麥克默多站為南極的研究發揮核心作用，但其缺乏大多數科學實驗室的基本配備——高速網路，因此，今（2021）年 NSF 正計畫為南極洲建造一條連往紐西蘭或澳洲的光纖電纜，完成之後，南極洲的研究及日常生活將被改變。

目前在南極洲工作的科學家主要依靠低頻寬衛星與外界通訊，NSF 技術開發經理 Patrick Smith 表示，麥克默多站每人平均可用的頻寬甚至比典型的美國農村家庭更少，科學家通常須將資料儲存於硬碟內以便攜帶，而非輸出資料讓同僚進行即時分析，造成研究進度緩慢的窘況。

今年 6 月，NSF 贊助一個為期三天的研討會，與會者討論光纖電纜將如何改變南極洲的情況，包括它將如何影響研究、教育及麥克默多站科學家的福利。今年 10 月，研討會主辦人發布一份報告，介紹關於未來南極電纜的關鍵節點及潛在路線，以及如何利用電纜在南極洲蒐集更多科學資料的方法。與會者表示，光纖電纜將有助於研究人員直播日常工作、天氣預報將可獲得改善、可即時分析衛星影像、促進網路安全，未來亦可擴大科學家的研究範疇。

此外，光纖電纜可蒐集震測資料（seismic data），或在電纜中增

設感應器以持續觀察南極海的氣溫及氣壓，進而了解氣候變遷速度。明尼蘇達大學冰川學者 Peter Neff 指出，目前針對南極海的觀測很少，隨著溫度上升，此種持續而即時的觀測可增進科學家對氣候變遷的理解。

除擴大研究機會外，高速網路將使科學家更容易與家人、境外同事及大眾取得聯繫。南極電影製片人 Ariel Waldman 表示，透過高速網路，大眾可身歷其境看見南極洲科學家的工作日常，使研究者與南極境外的人們進行即時互動，並對科學傳播產生重大影響。然而，儘管高速網路將帶來諸多好處，也可能影響南極科學站的既有文化。Neff 解釋，由於長期與世隔絕，南極科學研究站逐漸形成緊密連結的社群，完全連網可能會改變未來科學家之間的互動情形，以及其對實地研究的關注程度。

參考資料：

Jasmine Hicks (2021.11.23). High-speed internet could be coming to Antarctica. The Verge. 檢自：
https://www.theverge.com/2021/11/23/22765471/antarctica-internet-mcmurdo-station-research (Dec. 2 , 2021)

AFRINIC 及網路號碼註冊系統的穩定性

國際瞭望 撰輯

https://blog.twnic.tw/2021/10/07/20086/

非洲網路資訊中心（African Network Information Centre，AFRINIC）正與一間立案於塞席爾、名為 Cloud Innovation 的企業（負責人為 Lu Heng）進行訴訟，由於此案廣受矚目，且可能影響網路號碼註冊系統的整體穩定，ARIN 執行長 John Curran 特別撰文提供本案詳情，也表達 ARIN 將全力支持 AFRINIC。

2020 年，AFRINIC 完成註冊管理機構稽核後，要求 Cloud Innovation 提供非洲網路號碼資源的使用資訊，經審查後，AFRINIC 認為資源使用未符合當初的申請目的，因此將撤銷對 Cloud Innovation 的授權。Cloud Innovation 主張 AFRINIC 未具此權力，並向法院提起訴訟，要求凍結 AFRINIC 的帳戶，此舉可能將阻礙 AFRINIC 營運，並對非洲乃至全球的網路號碼註冊系統構成傷害。

Lu Heng 過去曾透過 Cloud Innovation 從 AFRINIC 獲得 620 萬個 IPv4 位址，2013 年，亦透過另一間企業 Outside Heaven，試圖向 ARIN 申請超過 100 萬個 IPv4 位址，但 ARIN 基於二項理由拒絕其申請：第一，Lu Heng 在申請階段多次拒絕向 ARIN 提供相關資訊；第二，Lu Heng 所提供的資訊具誤導性且前後矛盾。此外，Lu Heng 在美洲地區並未持有任何商業機構，且根據他的陳述，顯然 IPv4 位址將用於美洲地區以外的商業活動。

類似的戲碼再次上演，ARIN 發現 AFRINIC 授予 Cloud Innovation 的網路號碼資源幾乎都在非洲境外使用，顯然 Cloud Innovation 並未依當初申請目的運用資源，根據註冊服務協議，AFRINIC 有權收

回網路號碼，並使資源能真正裨益於非洲網路社群。

全球區域性網際網路註冊中心（Regional Internet Registry，RIR）在 2015 年成立聯合 RIR 穩定基金（Joint RIR Stability Fund），以維持 RIR 的長期運作，當 RIR 向基金求助，基金能提供超過 200 萬美元的財務及業務人力支援。若 AFRINIC 依據基金提出支援請求，ARIN 將堅定支持 AFRINIC，並採取必要措施，以確保非洲網路社群及全球網路號碼註冊系統在訴訟期間不受影響。

參考資料：

John Curran (2021.8.27). AFRINIC And The Stability Of The Internet Number Registry System. ARIN. 檢自：https://teamarin.net/2021/08/27/afrinic-and-the-stability-of-the-internet-number-registry-system/ (Sep. 10 , 2021)

ICANN 及 TWNIC 合作交流論壇——如何參與 ICANN 多方利害關係治理模式

文／NII 產業發展協進會研究員 陳曼茹

https://blog.twnic.tw/2021/06/08/18869/

2021 年 4 月 15 至 16 日期間，TWNIC 及 ICANN 共同於臺北舉辦合作交流論壇（ICANN APAC-TWNIC Engagement Forum）。本次為自 2019 年來第二屆 ICANN 與 TWNIC 合作交流論壇，目的是集合多方利害關係人及國際網路社群，針對域名、IP 位址及網路安全等主題，提供探討議題、互通有無的機會，也期許藉此場合，加強深化臺灣網路社群與國際多方利害關係人的連結、共同面對全球網路重要議題。

論壇第二天下午，我國資歷最深的 ICANN 參與者，臺灣網路治理論壇（TWIGF）理事長吳國維主持「如何成為 ICANN 多方利害關係社群一員」議程。吳理事長不僅是我國參與 ICANN 的先驅，也是唯一擔任過 ICANN 董事的臺灣人，可說是主持本議程的不二人選。

為了儘量展現 ICANN 的多方利害關係樣貌，本議程也請到來自不同利害關係團體的代表，包括現任 ICANN 董事 Akinori Maemura、我國參與政府諮詢委員會（Governmental Advisory Committee，GAC）代表林茂雄副司長、現任位址支援組織（Addressing Supporting Organization，ASO）理事的詹婷怡律師、代表.TW 參與國碼域名支援組織（Country Code Names Supporting Organization，ccNSO）的臺灣網路資訊中心（TWNIC）副執行長丁綺萍，以及 ICANN 職員 Mary Wong。我身為通用域名支援組織（Generic Names

Supporting Organization，GNSO）下非營利團體利害關係人（Noncommercial Stakeholder Group，NCSG）成員，也擔任與談人並分享自身參與 GNSO 的經驗。

如何成為 ICANN 多方利害關係社群一員

議程中，主持人希望所有與談人簡介自己所屬的利害關係團體，並說明如何參與該團體。

Akinori 是由位址支援組織（ASO）推派至 ICANN 董事會，今年是他董事任期的第 5 年。ICANN 董事會的組成乃 ICANN 多方利害關係架構的縮影，由代表 ICANN 組織的 ICANN 執行長及各支援組織（Supporting Organization，SO）、諮詢委員會（Advisory Committee，AC）代表組成，並有 8 個席次由提名委員會（Nominating Committee，NomCom）遴選指派。為深度了解 ICANN 社群內部所有議題，董事會內亦設立委員會，包括一般議題（如財務）或特定 ICANN 議題（如當責機制）。Akinori 是董事會內技術委員會主席，負責在關乎 ICANN 轄下單一識別碼系統運作的技術議題上，向董事會提供專業建議。

如前所述，ICANN 董事會組成多元，成為董事的管道也不只一條。有些董事是由所屬 SO 或 AC 推派，有些則獲 NomCom 提名擔任，而不同 SO 及 AC 內部的遴選推派流程也不盡相同。

交通部郵電司的林茂雄副司長是我國政府參與 ICANN 代表團的主席，也是我國的 GAC 代表。林副司長說明，GAC 主要由國家政府及跨國政府組織組成，所以要成為 GAC 成員，必須任職於國家機關，並非任何人都可加入。作為諮詢委員會，GAC 僅對董事會提出建議，無權制定政策。但是，林副司長強調，GAC 提出的共識建議有其重量，根據 ICANN 章程規定，董事會必須審慎考量

GAC 共識建議，唯有超過六成以上董事會成員反對時，董事會才可以否決 GAC 建議，且必須清楚解釋原因。

林副司長也呼籲，雖然不是所有人都可以參與 GAC，但 ICANN 內部議題繁多，若任何人對這些討論有興趣，都可以在網路上找到資料進一步了解。若在鑽研之下發現有臺灣可協助、或應該發聲的議題，歡迎隨時與他聯繫，他非常樂意為我國民眾在 GAC 會議中提出意見。

身兼律師及數位經濟暨產業發展協會副理事長的詹婷怡，是 ASO 中位址理事會（Addressing Council，AC）成員。AC 由全球 5 個區域網際網路註冊管理機構（Regional Internet Registry，RIR）各自推派 3 名代表組成，臺灣屬於亞太地區，參與 AC 代表則由亞太網路資訊中心（Asia Pacific Network Information Centre，APNIC）指派。APNIC 每年會由執委會指派一名任期一年的代表，其餘二名任期二年的代表則由社群投票選出。詹副理事長在去年獲 APNIC 執委會指派，今年任期將於年底結束。

ASO 的職責是向董事會提出關於 IP 位址運作、分配及管理的全球政策建議。ASO 在 ICANN 董事會中占有二個席次，與談人之一 Akinori 就是由 ASO 推派擔任董事。詹副理事長分享，由於 ASO 推派的董事其中一位任期將於年底屆滿，AC 今年擔負選出下任董事的重責大任，常有必須參加的臨時會議。

TWNIC 是我國國碼頂級域名（country code Top Level Domain，ccTLD）.TW 的註冊管理機構，也代表我國參與 ccNSO。ccNSO 歡迎所有 ccTLD 的營運管理方加入，分享經營經驗、探討技術協作，並向董事會提出 ccTLD 相關政策建議。TWNIC 副執行長丁綺萍表示，TWNIC 一直都是 ccNSO 的活躍成員，也認為對 ccTLD 營運方而言，ccNSO 是非常有用的交流平臺。

Mary Wong 現在雖然是 ICANN 職員，但他其實有豐富的

ICANN 社群參與經驗。他是 NCSG 的元老成員之一，也曾代表 NCSG 擔任 GNSO 理事。他亦曾獲 NomCom 提名擔任 ccNSO 理事。他在 2013 年成為 ICANN 職員，現在是社群運作規劃及交流策略資深副理。

Mary 分享 ICANN 職員及社群成員的不同：ICANN 的多方利害治理結構，是社群透過由下而上、共識決的方式建立政策。ICANN 組織僅負責從旁協助，並在政策建議通過董事會決議後負責執行。多方利害關係的組成表示在同一議題上，不同團體的立場很可能截然不同，難以互相妥協或達成共識。Mary 表示，ICANN 職員在這種情況下絕不能發表自身意見，而應盡力協助社群成員找出共識解方。

我自 2018 年開始參與 ICANN 會議，2019 年底成為 NCSG 成員。加入 NCSG 並不困難，只須上網填寫申請表格，審核通過後便可成為 NCSG 成員。其他 GNSO 下團體，包括與 ICANN 具合約關係的註冊管理機構（Registry Stakeholder Group，RySG）及受理註冊機構（Registrar Stakeholder Group，RrSG）團體，代表不同企業利益的企業團體（Business Constituency，BC）、智財權團體（Intellectual Property Constituency，IPC）及網路連線服務供應業者團體（Internet Service Providers & Connectivity Providers，ISPCP），雖然都有不同的入會條件並需要繳交會費，但只要符合資格並願意繳費，都不難加入。

持續、深度且有意義的參與才是關鍵

雖然成為團體一員的門檻不高，但持續、深度且有意義的參與卻很困難。我目前是政策制定流程（Policy Development Process，PDP）工作小組成員，隨著 PDP 進入收尾階段，每週一次的會議加碼為

二次。不僅會議時間是平常人準備入睡的晚上 10 點到 11 點半，會議之間還有很多「功課」要做：工作小組成員必須閱讀大量由 ICANN 職員提供的參考資料及草擬文件，提出所屬利害關係團體的立場建議，有時自身團體內部還可能意見不合，必須透過無數信件往返協調疏通。更別說疫情之下，所有討論都只能透過線上會議或文字進行，少了「見面三分情」，本來就具高度爭議的議題，更難以在各方意見中取得共識。

當然，參與 ICANN 的方式有很多種。有的人選擇只偶爾關注有興趣的議題，有的人可能只在 ICANN 會議期間參與，也有人不參與工作小組，僅在公眾意見徵詢時提出意見。我完全同意每個人都應該依自己時間及能力可負擔的程度，決定如何參與 ICANN。但我也相信亞太社群，包括臺灣人，都應該更積極、更深度參與 ICANN。

呼籲亞太地區網路社群積極參與 ICANN

你有過看到 ICANN 舉辦線上說明會的消息，想要參加卻因舉辦時間而卻步的經驗嗎？是的，大部分 ICANN 線上說明會的時間都非常不利臺灣人參加，尤以凌晨 2 點到清晨 5 點的時段最常見。這是因為 ICANN 社群組成以歐美人口為大宗，為服務多數，會議自然訂於歐美時區友善的時間。不僅 ICANN ORG 舉行的說明會，許多工作會議、SO 理事會通常也都訂於類似時段。

不友善的時區導致亞太社群難以參與會議，因此缺乏深入瞭解議題的機會。對議題理解不深又導致人們對會議興致缺缺，加入討論的意願更加低落。而這哀傷的惡性循環自 ICANN 成立起就是亞太社群共同的困境，至今未能改變。時區不友善的問題對年輕人更嚴重。大部分的資深社群成員若非已退休，也任職組織或公司高

層，相對工時自由。相反的，無論身處職場或仍是學生，年輕人都缺乏類似的時間彈性，也因此更難以投入參與。

這也是為什麼我認為深度參與非常重要。唯有更多亞太社群成員積極參與 ICANN，達到人數優勢，開始掌握會議時間的決定權，上述的惡性循環才有可能停止。我深切期望，在不久的將來，我們能推動改變，看到越來越多來自亞太地區的成員，包括年輕人，共同參與 ICANN，而總有一天，我們能在 ICANN 中發揮影響力的同時，支援更多亞太成員投入 ICANN。

去中心化域名的缺點及如何解決

國際瞭望 撰輯

https://blog.twnic.tw/2021/10/14/20142/

去中心化域名（Decentralized Domain Names）具備了中心化域名系統的功能，同時可避免後者中心化架構衍生的單點故障風險及中央監管。然而，現實和理想之間是有差距的，尤其現行域名系統長期得利於網路效應[1]，因此有必要以更現實的觀點理解去中心化域名。去中心化域名的幾個主要缺點包括：

- **即使有可用的方案，也難以說服使用者轉而使用去中心化域名。**理論上，轉向使用去中心化域名很簡單，只要在瀏覽器安裝擴充程式即可。然而目前為止，仍沒有任何域名系統替代方案（無論集中化或去中心化），成功吸引足夠的使用者並達到一定規模。New.net 即為一例。New.net 是有別於現有 DNS 的另一個集中化域名系統，用戶僅須在瀏覽器安裝 NewDotNet 外掛程式，即可拜訪使用 New.net 域名的網站。但基於雷聲大雨點小、惡意軟體疑慮及法律糾紛等原因，New.net 在 2012 年銷聲匿跡。去中心化域名的替代方案則如 NameCoin，NameCoin 的應用完全獨立於 ICANN 和傳統的 DNS 之外，使用者可以直接在區塊鏈上註冊域名，域名解析則是透過瀏覽器擴充程式進行。然而，目前 NameCoin 仍缺乏有意義的實質應用。

[1] 網路效應（network effect）：指一產品因使用者的數量增加而其價值亦隨之增加的效應。電話、傳真機、電腦作業系統等都是很好的實例。（資料來源：https://terms.naer.edu.tw/detail/1283049/?index=2）

- **真正做到去中心化的解決方案極其稀罕：**並非所有聲稱去中心化的區塊鏈技術都能達成去中心化效果。舉例而言，任何人都可開採加密貨幣，並聲稱加密貨幣為去中心化，然而，供應加密貨幣的權力卻完全掌握在發行者手中。換言之，去中心化技術並不能保證去中心化之結果。如果註冊管理機構或受理註冊機構代表的單點故障風險，只是被其他集中節點取代，那所謂的「替代方案」實際上並沒有解決任何問題。
- **去中心化的特性可能遭有心人士濫用：**去中心化協定的特性之一，是任何人一旦在協定中新增資料，其他人就無法刪除這筆資料。若某個去中心化協定遭有心人士用來鼓吹兒童虐待或仇恨犯罪，即使其他用戶毫不知情，協定本身也將引起各國執法機關的注意，因此蒙上污名，進而失去使用者。
- **去中心化技術所費不貲：**能同時達成**去中心化**與**被廣泛使用**二大條件的區塊鏈技術通常都要價不斐。

大部分的開發者都對去中心化域名的這些缺點心知肚明，也積極想方設法改善現況，如建立社群機制以踢除不良分子等。但重點是，即使去中心化域名看起來充滿無限可能，現在就認為它將取代傳統 DNS，仍然言之過早。

參考資料：

Jeffrey Gabriel (2021.8.23). The Dark Side of Decentralized Domain Names. CircleID. 檢自：
https://circleid.com/posts/20210823-the-dark-side-of-decentralized-domain-names (Sep. 17 , 2021)

ICANN「域名安全威脅資訊蒐集與通報」專案執行成果

國際瞭望 撰輯

https://blog.twnic.tw/2021/10/08/20076/

COVID-19 疫情自一年半前開始肆虐全球，有心人士也抓準此機會將人誘導至各種惡意網站。為因應此情形，ICANN 技術長辦公室（Office of the Chief Technology Officer，OCTO）發起「域名安全威脅資訊蒐集與通報」（Domain Name Security Threat Information Collection and Reporting，DNSTICR）專案，專門通報 COVID-19 相關的域名系統（Domain Name System，DNS）安全威脅。

在諸多使用通用頂級域名，特別是用當地語言且僅適用當地脈絡的網站中，辨識出哪些是釣魚或惡意軟體網站並不容易。DNSTICR 採取的做法，包括在新域名註冊中搜尋 COVID-19 相關詞語，量化明顯的惡意域名，並通報域名受理註冊機構。點此了解更多細節。

2020 年 4 月，COVID-19 相關的新域名註冊達到高峰，單日註冊量高達 5,543 筆。但註冊量在 5、6 月急遽下滑，此後的曲線始終平緩。

在 2020 年 5 月至 2021 年 8 月間，總共 210,939 筆疫情相關域名註冊，這些大部分都是平凡無害或沒有通報紀錄的域名，僅 6.1%（12,860 筆）域名曾遭通報。若進一步將範圍限縮至通報資訊可信或具多筆通報紀錄，則總共只剩下 3,791 筆域名（1.8%）。

這個數據顯示，被標為「可疑」的域名，並不等同證實具實際濫用情形的域名。

其他 DNSTICR 發現的趨勢包括：一開始的域名註冊喜使用 corona 一詞，後來逐漸被 covid 取代。在觀測的 18 個月中，以含有 covid 的域名註冊量最高，占總註冊量的四分之一。其他與疫情有關連的域名，註冊量也隨時間有所不同。如僅占總註冊量 4%、含有「疫苗」的域名在 2020 年 11 月開始攀升，並於 2021 年 1 月中達到高峰。

這個趨勢和疫情中網路常見相關用語的變化趨勢相同，Google 搜尋趨勢也呈現類似結果。

DNSTICR 是個長期專案，會隨著變化多端的 COVID-19 全球疫情持續演進。OCTO 未來也將定期向 ICANN 社群報告專案最新進度，不久後也將發布包含更多細節的完整報告。

參考資料：

Siôn Lloyd (2021). An 18 Month Summary of ICANN's DNSTICR Project. ICANN Blogs. 檢自：
https://www.icann.org/en/blogs/details/an-18-month-summary-of-icanns-dnsticr-project-2-9-2021-en (Sep. 10 , 2021)

網路治理的機會與挑戰
Opportunities and Challenges of Internet Governance

作　　者　財團法人台灣網路資訊中心

內容撰輯　Ali Abedi、Azhar Khuwaja、Cameron Steel、
Geoff Huston、George Michaelson、Kathleen Moriarty、
Lars-Johan Liman、Paul Wilson、Satoru Tsurumaki、
Stephen Strowes、Ulrich Speidel、
林方傑、黃士洲、鍾欣紘
國際瞭望專案團隊：
梁理旋、許嘉雯、鄭琦馨、陳曼茹、戴匡

出 版 者　財團法人台灣網路資訊中心
地址：臺北市松山區八德路四段 123 號 3 樓
電話：02-25289696
傳真：02-25287756
網址：https://www.twnic.tw

發 行 人　李育杰

總 編 輯　黃勝雄

主　　編　丁綺萍

責任編輯　呂愛琴

企劃編輯　李曉陽

執行編輯　湯序平

編　　輯　吳沛真

封面設計　王嵩賀

電子書製作　周妤靜

電子書發行及銷售　秀威資訊科技股份有限公司

出版日期　中華民國 111 年 5 月

ISBN　9789860624748（epub）