數位韌性與科技倫理

財團法人台灣網路資訊中心　著

目 次

推薦序一

2022 年 8 月 27 日數位發展部正式成立，主要職掌為促進全國通訊、資訊、資通安全、網路與傳播等數位產業發展、統籌數位治理與數位基礎建設，並促進數位經濟發展及加速國家數位轉型，打造穩固、先進與安全的網際網路環境。為了達到這樣的目標，本部由三個面向來完成「全民數位韌性」這個核心任務，而三個面向即為應變韌性、產業韌性跟社會韌性三個面向。

首先，「應變韌性」是當我們面臨不論網路攻擊或自然災害之各種危機時，都能有效應對。像去(2022)年 8 月美國眾議院前議長裴洛西歷史性訪臺期間所發生的網路攻擊，即是要試圖破壞公眾對我們民主制度的信任，結果未能成功。此外，我們為了加強應對像是 AI deep fake 等新興威脅，組織了公部門和民間的資安能量，實施零信任原則、進行攻防演練。2023 年我們也整合衛星業者，運用多重網路備援應變，連結陸地、海洋和天空，以確保在緊急情況下，關鍵基礎設施的無縫運行。

其次的「產業韌性」是我們對各行各業數位轉型的承諾，以培育堅韌的產業生態。臺灣擁有高度先進的 IT 產業、世界一流的半導體供應鏈，以及應對網路威脅的豐富經驗。而 TWNIC 也在這方面耕耘多年，其藉由 TWCERT/CC 提供企業資安事件通報、諮詢及協處服務，讓企業主在事前、事中、事後都能做好資安防護；並建立跨國網路安全情資共享管道，提升整體資安聯防與應變能力。

最後，「社會韌性」的意涵在於結合全球民主網絡，將權力賦予公民社會。我們相信，數位素養需要有見識和辨別力的公民。我

們不能僅限於制定保護措施，更要擁抱「參與、進步、安全」的三位一體，通過群眾智慧的力量開創新局，人民和政府全民守望相助，才能有最縝密的防備。

台灣網路資訊中心出版《數位韌性與科技倫理》一書，從網路政策、網路技術兩個方面，探究數位資訊時代下，政府應如何在面對資料治理議題的同時，避免資訊與網路安全的威脅及挑戰；對網路使用者而言，如何保護網路隱私、辨識新型態的網路風險；對政府及網路平臺業者而言，如何設計合宜的控管機制及傳輸架構，並在這些過程遏止極端內容並保有使用者的隱私，也都是「數位韌性與科技倫理」所需面對的課題。

資訊及通訊科技技術（ICT）、物聯網（IoT）、感測器、雲端服務、人工智慧（AI）、區塊鏈、5G 等技術紛紛引領新世代技術的發展，讓人類的生活更加智慧與便利，但創造可觀的數位經濟之同時，也衍生了隱私權及資訊安全問題。台灣網路資訊中心期待讀者們能透過本書，看見屬於臺灣的機會，以及面臨的挑戰，共同打造具有韌性且安全的數位環境及意識。

數位發展部

部長 唐鳳

推薦序二

資訊科技的快速發展及數位轉型的迫切需求，我們進入了一個全新的數位化時代，「數位韌性」與「科技倫理」也成為關鍵的議題。日益頻繁的網路威脅陰影下，保護個人隱私，乃至於國家數據安全和系統穩定性變得至關重要。TWNIC 於 2023 年出版《數位韌性與科技倫理》一書，即在此趨勢下，探討了個資保護、網路攻擊、DNS 系統、5G 網路等主題，不僅呼應政府推動的數位韌性政策，也與臺灣科技的未來發展、規劃息息相關。

人工智慧、元宇宙引發了全世界廣泛的討論和實踐，為人類描繪出充滿可能性的未來，然而我們也因此面臨了更加複雜的倫理問題。如本書所討論的，如何糾正演算法系統中的偏見與安全漏洞？如何監管人工智慧，避免其侵犯個人隱私？共享數據是元宇宙虛實無縫的重要基礎，但在個資保護與科技發展之間應當如何取得平衡？這些因應數位科技而生的問題，都可能大幅影響社會環境與文明發展，需要我們深入思考並制定相應的對策，以確保科技發展能夠符合人類的倫理價值。

多年來，TWNIC 一直致力於促進臺灣與國際網際網路組織之交流與合作，並積極推動跨域信賴機制以提升網路安全。自 2019 年起，出版一系列的電子書供大眾免費下載閱讀，如《網路治理與資訊安全》、《新世代的網路治理》、《網路治理的機會與挑戰》等；2023 年同樣期盼《數位韌性與科技倫理》的付梓，能喚起社會大眾對於新興數位議題的重視與關注，並促進各方交流、合作的契機。從技術、政策、創新、倫理面向以洞悉當前發展與未來趨勢，每一個見解的分享，每一個參與討論的聲音，都是催生變革的珍

貴種子。期盼社群共同耕耘，將為虛擬數位網路世界，開闢千畝良田。

財團法人台灣網路資訊中心

董事長暨執行長 黃勝雄

網路政策

歐盟數位服務法：迎向網路規範的新里程碑

謝國廉／國立高雄大學財經法律學系教授

https://blog.twnic.tw/2023/01/11/25347/

前言：數位服務的貢獻與風險

本文將聚焦歐洲聯盟（the European Union）部長理事會（the Council of the EU）於 2022 年 10 月通過的數位服務之單一市場法（Regulation on a Single Market for Digital Services）及其帶來的影響。各界將此法簡稱為數位服務法（Digital Services Act，DSA）。

1990 年代中期迄今，創新的數位服務（innovative digital services）改變了人類溝通、聯繫、消費和商業經營的方式，並提升了經濟、社會和環境發展的永續性（sustainability）。近 3 年來疫情的發展，更凸顯出數位科技對現代生活的重要性。然而，藉由各項數位服務所提供的資訊，亦造成了許多問題。有時資訊的內容或許未必違法，但卻可能造成具體的損害。此等資訊包括了非故意散布的錯誤訊息（misinformation）和故意散布的假訊息（disinformation），特別是：

1. 具有誤導性質的公共衛生資訊；
2. 消費詐騙（consumer fraud）資訊；
3. 其他網路犯罪（cyber-crime）資訊；
4. 違法的仇恨言論（hate speech）；
5. 或來自外國有目的性的政治操作（targeted influence operations）。

至於散布上述資訊的目的，主要包括獲取不法經濟所得（例如：網路詐騙）、傷害公眾利益（causing public harm），或者是政治上的目的（political purposes）。

DSA 立法前的背景、主要考量及立法目的

就歐盟關於網際網路的法規規範而言，2000 年的電子商務指令（*e-Commerce Directive*）毫無疑問是一項關鍵的立法。電子商務指令對於歐盟乃至於世界其他各地的社會和經濟轉型（societal and economic transformation），皆帶來了深遠的影響。不過，電子商務指令雖架構了網路商務活動的法規範框架，但並未課予數位平臺具體的義務。回顧當時歐洲電子商務的發展，歐盟立法機關訂定電子商務指令時，相關的數位服務業尚處於發展初期，因此嚴格的法律措施或較重的義務，或將扼殺電子商務的發展，因此不難想像的是，當時歐盟僅以電子商務指令構建了框架式的規範。

由於創新的數位服務帶來了新的風險與挑戰，電子商務指令已不足以處理相關的爭議。在數位服務法立法前，歐洲議會（the European Parliament）於一份不具法律拘束力的決議（resolution）中，指出了以下 3 大問題。

1. 數位平臺的法律責任不明：由於電子商務指令僅為框架式的規範，因此該指令並未針對數位平臺的法律責任作出明確的規定。
2. 平臺使用者的權益保護不足：舉例來說，數位平臺使用者的權益遭平臺或第三人侵害時，歐盟相關法規並未提供使用者迅速而有效的救濟管道。
3. 對於歐盟人民基本權利（fundamental rights）的保護不足：舉例來說，歐盟基本權利憲章（*Charter of Fundamental*

Rights of the European Union）第 8 條明文保護個人資料（personal data），但數位平臺或第三人未得同意便取得個人資料甚至以各種方式加以利用的情況屢見不鮮。

根據上述歐洲議會的決議，歐盟應針對以下事項訂定統一的法律規範：

1. 線上的違法內容；
2. 明確的平臺通報責任；
3. 平臺應負擔運作透明化的責任（transparency responsibilities）：近 10 年來，數位平臺的營運資訊不透明的情況，經常為人詬病。舉例來說，提供線上廣告乃是許多平臺營利的主要方式之一，但實際上，平臺是否確實按其與廣告主的契約投放線上廣告，在平臺與廣告主資訊明顯不對稱的情況下，廣告主往往難以主動地進行有效的稽核。
4. 平臺的責任豁免（liability exemptions）條款：舉例來說，按此等豁免條款，若數位平臺已採取有效的措施預防他人利用其平臺服務散布假訊息，則日後他人散布假訊息時，平臺得豁免其法律責任。
5. 主管機關的責任

DSA 有 2 項主要的立法目的。首先，DSA 以創造更安全的數位空間為目的，以確保數位服務使用者的基本權皆能受到保障。其次，DSA 的另一項立法目的為建立公平的競爭環境，以強化歐洲單一市場中數位服務產業的創新、發展和競爭力。

DSA 的規範對象：各類線上中介業者（online intermediaries）

DSA 的規範對象，乃是各類線上中介業者，包括：

1. 提供網路基礎設施的中介業者，例如：網路連線服務提供者

（internet access providers）；

2. 網頁代管服務業者，例如：提供雲端服務的業者；
3. 超大型線上搜尋引擎業者：界定標準為擁有 4,500 萬以上歐盟使用者的線上搜尋引擎業者。就消除違法線上內容而言，此等業者應負更大的責任。
4. 聚合出賣人與消費者的線上平臺業者：除線上商店外，應用軟體商店（app stores）和社交媒體（social media）平臺亦在規範之列。
5. 超大型線上平臺業者：界定標準為擁有 4,500 萬以上歐盟使用者的線上平臺業者。由於此類平臺較可能散布違法內容並對社會造成損害，因此為主要規範對象。

DSA 的規範重點

DSA 的規範重點，主要有以下 3 項。第 1 項規範重點為：打擊非法線上商品、服務或內容的措施。此項規範的內容較多，主要包括以下 7 項重點：

1. 平臺得與專業的民間監督機構（被稱之為 trusted flaggers）合作。
2. 平臺應有追蹤商業使用者的能力：此規定的目的在於，確保數位平臺擁有確認提供違法內容的使用者的能力。
3. 中介平臺應主動啟動調查與法遵（legal compliance）的程序。
4. 主管機關有權命令平臺處理非法內容的問題。
5. 中介業者負有「透明報告義務」（“transparency reporting obligations”）：按 DSA 的規定，中介業者除了應報告受主管機責令處理非法內容的次數外，亦應應報告主動調查的次數。

6. 平臺對於頻繁提供明顯違法內容的服務使用者，應暫停提供服務。
7. 若平臺發現嚴重的犯罪行為（serious criminal offence），應立即通知主管機關。

DSA 的第 2 項規範重點為：賦予數位服務使用者和公民團體新的權利，以對抗數位服務業者並尋求救濟。DSA 賦予此新權利的主要目的，在於幫助數位服務使用者和公民團體對抗數位服務業者，並取得有效的救濟方式。舉例來說，按 DSA，服務使用者和公民團體有權挑戰平臺處理疑似違法內容的決定。此外，針對涉及疑似違法內容的紛爭，DSA 對於法院外的爭端解決機制（an out-of-court dispute mechanism）和司法救濟（judicial redress）的機制，皆有明確的規範。就解決紛爭所耗費的時間而言，院外機制所需的時間往往較短，因此其重要性並不亞於司法救濟的機制。

DSA 的第 3 項規範重點為：建立評估及降低風險的機制。首先，超大型的線上搜尋引擎業者和超大型的線上平臺業者，應負擔風險評估的義務，並進一步採取防止使用者濫用數位服務的作為。其次，此 2 類業者應尋求外部獨立單位的協助，就業者的風險管理系統（risk management systems）進行獨立的稽核工作（independent audits）。此外，業者應將其所發現的公共安全或公共衛生危機，迅速通報政府機關。再者，業者應就未成年人的保護建立新的防護機制。值得注意的是，無論是公共安全、公共衛生的通報義務，或是未成年人保護的義務，皆為昔日法制中所未規定的義務。除此之外，針對利用敏感個人資料（sensitive personal data）以鎖定特定人進行廣告投放（targeted advertising）的行為，DSA 亦有所限制。

結論

首先，DSA 的立法凝聚了歐盟立法者和各會員國專家的智慧與心血，極有可能成為國際上數位服務法制的典範，其重要性或堪比歐盟「一般資料保護條例」（the General Data Protection Regulation）在個人資料保護法制中的地位。其次，DSA 以具體且詳細的方式，界定了受規範的數位服務提供者，釐清了昔日各國相關法規中受規範對象未臻明確的問題。此外，平臺與專業機構的合作機制、業者的報告義務和第三方的獨立稽核制度，皆為以往數位服務法制所未有的規定。再者，作為數位服務的主要提供者，超大型線上搜尋引擎業者以及超大型線上平臺業者，未來將就消除線上違法商品、服務和內容，負擔極大的法律義務。總體而言，在西元 2000 年數位服務業發展的初期，歐盟各界唯恐嚴格的法律將扼殺產業的發展，但近年來已形成對數位平臺採取嚴格管制的共識，而此共識已然透過 DSA 的制定而成為明確的法律規範。

《資料法》與歐盟的資料治理策略

羅心妤／東海大學資訊管理學系

https://blog.twnic.tw/2022/09/15/24262/

《資料法》[1]的介紹

《資料法》（Data Act）將確保工業資料在「充分尊重歐洲規則的情況下」共享、儲存和處理。這將保障數位環境的公平性，刺激資料市場的競爭性，開闢資料創新的機會，並使所有人都更容易獲得資料。其提案包括：

- 允許連網裝置的使用者訪問自身生成的資料，並與第三方共享，以提供售後市場或資料驅動的創新服務。
- 預防資料共享合同被濫用或權力失衡。《資料法》將保護中小企業免受於談判中較強勢那一方的不公平條款影響。
- 明定公部門訪問和使用私部門資料之特定條件，例如：在洪水和火災等公共緊急情況下。
- 允許客戶在不同的雲端資料處理服務提供商之間有效切換，並建立防止非法資料傳輸的保障措施。

《資料法》完全符合並以《一般資料保護規則》（General Data Protection Regulation，GDPR）規則為基礎。尤其適用於「資料可攜性」的權利，該權利允許資料主體在提供競爭服務的控制者之間傳輸資料。此法將加強「物聯網」的這一權利，以便消費者可以訪問和移植產品生成的任何個人和非個人資料。

---

[1] European Commission. (2022). Data Act: Commission proposes measures for a fair and innovative data economy. 檢自：https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 (Aug. 21, 2022).

《資料法》的生成背景：歐洲資料戰略[2]

資料戰略的重點是將人放在開發技術的第一位，並建立一個單一的資料市場，確保更多資料可用於經濟和社會，同時控制生成資料的公司和個人。公民和企業將多方受益資料驅動的應用程式。例如：改善醫療、降低公共服務成本、提高能源效率等。

歐洲資料戰略旨在：

- 資料「治理、訪問、重複使用」的相關立法。例如：為了公共利益而要求企業對政府資料共享。
- 透過高價值的公共資料集並允許免費重複使用，使資料更廣泛地被利用。
- 開發資料處理基礎設施、資料共享治理機制，以蓬勃發展資料共享，並聯合節能和雲端基礎設施。
- 鼓勵資料處理服務的市場建立，並確立雲端規則的適用監管框架，從而實現安全、公平和有競爭力的雲端服務。

《資料治理法》於 2021 年 11 月由共同立法者同意，作為其資料戰略的一部分。該法建立了促進公司、個人和公部門共享資料的流程和結構，而《資料法》作為其延伸，澄清了誰可以從資料中創造價值，以及在哪些條件下創造價值，是歐洲資料戰略的關鍵支柱。

《資料法》的多方效益[3]

在個人方面，消費者和企業將能夠訪問其裝置的資料，透過獲得更多資訊，促使消費者能夠做出更好的決定，例如：購買更高品

---

[2] European Commission. (2022). A European Strategy for data. 檢自：https://digital-strategy.ec.europa.eu/en/policies/strategy-data (Aug. 21, 2022).

[3] European Commission. (2022). Data Act: Questions and Answers. 檢自：https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114 (Aug. 21, 2022).

質或更可持續的產品和服務，為綠色交易目標做出貢獻。

在企業方面，商業和工業參與者將擁有更多可用資料，並從競爭性的資料市場中受益。服務提供商將能夠提供更個性化的售後服務，同時也可以將資料結合開發全新的數位服務。例如：汽車或機械車主可以選擇與保險公司共享其使用所產生的資料。這些資料來自多個使用者，也可以幫助開發或改進其他數位服務，例如：流量或事故高風險地區。

在政府方面，《資料法》旨在釋放私營公司在公共利益或特殊情況下的資料價值，它將大幅改善循證決策，特別是對洪水和火災等危機的有效和快速反應。例如：在新冠肺炎流行期間，來自行動網路營運商的彙總匿名位置資料，對於分析病毒傳播的移動性至關重要，為新疫情的預警系統提供資訊，並採取正確措施應對危機。

在永續方面，將提高商業和製造效率，應導致減少廢物、能源消耗和二氧化碳排放。例如：物聯網裝置可以幫助農民分析即時資料，就所需水資源做出更明智的決策。

結語

《資料法》釐清歐盟在資料處理的關鍵問題，包括：誰可以使用和訪問生成資料的不明確；中小企業往往無法公平地與產業巨頭談判資料共享協議；雲端和邊緣服務之間切換的障礙，以及無法有效整合來自不同部門的資料。資料治理新規則將讓更多資料可重複使用，預計到 2028 年將創造 2,700 億歐元的額外國內生產總值，除此之外，政策也兼容「歐洲人權價值」與「綠色交易等永續議題」。歐盟在資料治理政策中洞察市場及權衡利弊的能力，值得各國政府借鏡。

健康資料的使用條件：歐盟個資保護機關意見與臺灣現況

周冠汝／台灣人權促進會數位人權專員

https://blog.twnic.tw/2022/12/19/25174/

日常使用手機應用程式紀錄運動與健康狀態，生病時就醫留下的資料和醫療影像，電子化及雲端服務讓健康資料更容易被儲存及分享，健康資料被用於個人未同意或難以控制的情境也數見不鮮。世界醫師會於 2016 年修訂通過《台北宣言》，確立醫療人員蒐集建立的健康資料庫應遵循的倫理原則，其中涵蓋有效同意的要件、資料治理措施、個人可要求撤回資料，及可不受報復地取消同意等權利。臺灣超過 20 年來的健保資料目的外利用，也在今年迎來憲法法庭判決。

而在經由 App 或網頁蒐集的健康資料途徑中，近年也陸續出現個人敏感資料遭分享給第三方的例子。根據數位人權團體隱私國際（Privacy International）於 2019 年的調查顯示，其所分析的法國、德國、英國的 136 個熱門心理健康網站，超過 7 成含有行銷目的的第三方追蹤器；其中更存在將憂鬱症測驗的回答與結果分享給第三方的網站。今年，在美國推翻保護墮胎權的「羅訴韋德案」（Roe v. Wade）後，Mozilla 仍在多款懷孕、月經週期 App 中，發現蒐集大量個資並廣泛分享的情況。

歐盟個資保護機關如何看待健康資料？

歐盟資料保護委員會（European Data Protection Board，EDPB）

與歐盟個資保護監督機關（European Data Protection Supervisor，EDPS）今年公布針對「歐洲健康資料空間」規範提案的聯合意見書。意見書指出，保健 App 以及數位健康應用程式產生大量日常生活的資料，其中具有推論出更多個人資訊的可能，比如飲食習慣可能透露宗教信仰；另一方面這些應用程式的資料品質並不如醫療器材，將這類資料用於診療照護，可能引發診療不平等的風險。因此 EDPB 與 EDPS 建議，排除保健、行為等應用程式產出的資料從事二次利用，不輕易將此資料與醫療資料連結。若政策制定者欲保有原先設計，必須強化個人可決定是否同意二次利用，以及保健應用程式產出的哪些資料可分享。

不同於原始蒐集資料的用途，二次利用意旨將資料用作有別於最初蒐集的目的。比如促進研究、協助政策制定都是健康二次利用的常見用途。EDPB 與 EDPS 指出，「歐洲健康資料空間」規範中的二次利用目的不夠明確，並建議應進一步闡述各項二次利用目的，並將之限縮在與公共衛生或社會安全具有實質關聯的部分。目前政策制定者的提案中，只要合乎發展產品或服務、訓練演算法或應用服務「有助於」公共衛生或社會安全，即可使用電子健康資料從事二次利用，目的太過寬泛。在二次利用的資料最小化上，也存在規定不清的情況。

關於誰可以取用健康資料，EDPB 與 EDPS 認為不應無差別給予所有「健康領域專業人員」權限，因此類別定義涵蓋多項不同職業與責任。EDPB 與 EDPS 建議，應就執行特定任務所必要的範圍，來界定誰有權限使用健康資料。

由於政策制定者的提案中出現原創名詞「非個資的電子健康資料」，EDPB 與 EDPS 在意見書中強調，實務上結合「非個資」資料，可能推論出個人資料，從而提升個人被識別的風險。尤其是處理健康資料。

臺灣健保資料目的外利用的挑戰

說起「非個資的健康資料」，臺灣曾在 2020 年發生健保署將 350 萬死者健保資料歸戶後，存放到企業平臺的事件，並計畫進一步開放給產業利用。當時對於死者健保資料不是個資的解釋為，個資法僅保護自然人，而逝者資料自不在保護範圍。然而，健保資料一定程度涉及病史等於親屬有關、可間接識別在世者的資料，在此解釋下，仍應屬於保護範圍。再加上在缺乏其他法律的規範下，健保資料在個人過世時，原始蒐集目的已消滅，也不存在開放給他人利用的基礎。

同樣缺乏明確法律授權與規範目的外利用的情形，也出現在 2019 年衛福部公布的〈全民健康保險資料人工智慧應用服務試辦要點〉，越過當事人同意，也未有事後退出設計，逕行將醫療影像資料供產業利用。

臺灣超過 20 年涵蓋全人口的健保資料庫目的外利用，也在今年 8 月憲法法庭判決中宣告違憲。依照判決，健保署須在 3 年內完成修法或制定專法，規範將健保資料對外提供的範圍、目的與監督措施。若三年內未完成修法，個人可依判決要求停止資料目的外利用。很可惜的是，判決並未明確說明，在修法的三年間，已然侵犯資訊隱私權的違憲行為可以如何降低損害。健康資料有助於精準醫療、人工智慧、大數據等研究，那麼資料治理的腳步也應跟上，尊重資訊自主，完善個資保護制度，以合乎憲法保障基本權的方式，取得正當的研究成果。資料利用的信任來自個人可控，免於資料剝削並整體淪為「個資農奴制」的門檻，是健保資料乃至健康資料利用將處理的課題。

澳洲網路治理起源：談國碼頂級域.au 管理之發展

梁理旋／NII 產業發展協進會副執行長

https://blog.twnic.tw/2022/11/15/24916/

澳洲的網際網路治理發展起始於，為管理其國碼頂級網域名稱 .au 所逐漸形成由私部門非營利組織進行自律的治理方式。國碼頂級域（Country Code Top Level Domain，ccTLD）的管理不只是 DNS 技術課題，還是政治與經濟的爭辯。首先，ccTLD 代表的是一個國家的網路識別名稱，由政府來統籌管理似也名正言順；再者是域名註冊量擴張後，看似由少數人或組織所掌握的重要資源所涉及的商業利益越來越高時，也因此受到更多的關注。

本文透過回顧澳洲政府如何將澳洲 ccTLD 管理授權自一名學者移轉至目前的註冊管理機構的經過，說明澳洲建立起當今以多方利害關係人為基礎的網路治架構的起源。

代表澳洲的網路名稱為何是 .au？由誰來管理？

在網際網路創始之初，架構在 TCP/IP 通訊協定上的連網電腦數量越來越多，彼時參與網路發展的南加州大學教授 Jon Postel 為便利管理，設計出利用網域名稱系統（DNS）來管理 IP 位址和域名間對應的方式，來解決連網電腦 IP 位址難記的問題，並利用國際標準 ISO3166 所定義的國家代碼來為每個國家命名其各自代表的 ccTLD。在當時，包括澳洲在內的全世界沒有一個國家的政府有參與此 ccTLD 要如何命名的決策過程，換言之，Jon Postel 如同網

際網路界的上帝為每個國家訂出了命名規則，並沿用至今。

在沒有任何法源基礎下，代表澳洲的 .au 國碼頂級域也在 1986 年由 Jon Postel 直接授權（delegated）給澳洲墨爾本大學的 Robert Elz 教授個人，只因為 Robert Elz 與這群美國 DNS 架構的研究團隊一樣同為早期的網路架構研究者且彼此認識。

Robert Elz 在沒有商業利益的條件下，以自願性質提供並維運 .au 的域名註冊服務長達 15 年。澳洲政府因域名需求激增及越來越顯著的商業價值開始注意到 .au 的無政府狀態，也因此開始介入，也終於在 2001 年 9 月，澳洲的國碼頂級域名 .au 又再重新授權給目前的註冊管理機構 auDA。

原來的 .au 管理者為何不再受青睞？

自 .au 授權給 Robert Elz 後，澳洲的網際網路應用經歷了大規模成長，也大量增加了對 .au 域名的註冊需求；為滿足 .au 域名需求，Robert Elz 又在 .au 名稱架構下創建了 11 種不同的第二層域名，包括：asn.au、com.au、conf.au、csiro.au、edu.au、gov.au、id.au、info.au、net.au、org.au 和 oz.au 等。接著又為了紓緩超過負荷的龐大註冊量，Robert Elz 陸續將這些第二層域名移轉給不同的人或機構來協助管理，例如：.edu.au、.gov.au 在 1991 年移轉給當今的 APNIC 首席科學家 Geoff Huston 管理；.net.au 在 1994 年移轉給 ISP 業者 Hugh Irvine；而。其中商業利益最高的 .com.au 移轉最具爭議性：1996 年由 Robert Elz 透過一紙合約將管理權交給 Melbourne IT 公司。

Melbourne IT 在獲得授權後於 1996 年 11 月啟用了新的域名收費方式，原本希望針對 1997 年 3 月中旬前尚未支付費用的既有 com.au 註冊人，得以註銷其域名所有權，此政策當然引發這些既

有域名持有者的反對。位於伯斯（Perth）的一家 ISP 業者在當時即代表這些域名持有者提起了集體訴訟，而後聯邦法院也發出禁令要求 Melbourne IT 不得註銷這些域名。此一發展也成為澳洲網路治理從學術領域邁向法律及商業領域的轉捩點。此外，當時大量域名註冊需求在既有管理機構於技術營運面的不堪負荷，以及對完整域名管理政策發展的期待，都動搖著既有的 .au 管理運作模式。當時的澳洲政府、產業工會等團體都期待著可透過新的域名管理組織就 .au 域名產業進行更穩健管理。

另也參考 ICANN 在 2001 年 8 月所發布 IANA 有關 .au 重新授權報告，儘管 .au 在 Robert Elz 個人管理下發展良好，但為使 .au 發揮其未來潛力，其應由一個正式的、可對澳洲網路社群負責的組織來管理。這也如同美國商務部於 1998 年提出網路政策白皮書所指：「網域名稱越來越具有商業價值」，因此有關 DNS 政策和結構的決策「不能由未正式對網路社群負責的實體或個人做出」。

澳洲政府也因此成為第一個與 ICANN 建立正式關係的國家，ICANN 重新授權 .au 域名管理權移給澳洲政府正式認可的 auDA 組織。當時仍由通訊、資訊技術與藝術部部長負責指導澳洲的 DNS 政策，並依 2000 年的電信法修正案保留對 DNS 監管的權利。澳洲的域名產業也逐漸成為營運商業化且強調監管透明度的混合監管模式的試驗場，在此試驗場中包括產業、消費者團體、傳統監管機構、技術社群等積極參與其中，推動著域名產業朝向更可預測且客觀的監管方向發展。

auDA 接手 .au 管理後的改變是好或壞？

在 auDA 接手.au 管理職責後，原本捆綁在一起的註冊管理機構（registry）與受理註冊機構（registrar）功能被切分開，域名註

冊服務產業也因此引入了競爭，註冊管理功能應當由哪個機構來提供服務，也有機會採公開競標方式進行。倘若要衡量 .au 在重新授權後的績效，包括域名註冊數量增加、域名拍賣收益、域名價格降低、加值服務（例如：網站託管等）的選項增多等，都有不錯的數據可具體呈現。

澳洲的 ccTLD 網路治理安排是採取類似公、私部門混合監管之模式，政府將權力下放給 auDA，但仍保留重新授權 .au 的權利。有分析認為 auDA 監管成功的原因是對受監管對象的重視，使得產業願意積極參與監管決策且遵從決策結果。而 auDA 也成功運作了數個由多方利害關係團體代表組成的政策小組，包括用戶及消費者社群的觀點被納入 .au 政策考量中；這些小組成員則來自於廣泛社群，具備技術、工程、電信政策、智慧財產權及消費者保護等專業的志願者成員，大家共同訂出了受理註冊機構的行為守則等規則或政策。

綜合來說，auDA 獲得澳洲政府的支持，卻又獨立運作於政府體系；其職權來自於其作為 ccTLD 管理者的持續有效性，此有效性則展現在基於多方利害關係人共識所產出的政策或行為守則，且獲得域名受理註冊機構、域名經銷商等的支持。此也是目前可見、屬國家層級的多方利害關係人網路治理模式的成功案例之一。

參考資料：

[1] Williams, L. (2003, June). *Internet Governance in Australia: Modelling Self-Regulatory Structures in the Domain Name System*. Murdoch University Electronic Journal of Law. http://classic.austlii.edu.au/au/journals/MurUEJL/2003/16.html

[2] The Internet Corporation for Assigned Names and Numbers. (2001, August 31). *IANA Report on Request for Redelegation of the .Au Top-Level Domain*. Internet Assigned Number Authority.

https://www.iana.org/reports/2001/au-report-31aug01.html
[3] ITU (2003). *ccTLD Doc 47- Document for ccTLD Workshop*. https://www.itu.int/itudoc/itu-t/workshop/cctld/cctld047.pdf
[4] National telecommunications and information administration. (1998). *Statement of Policy on the Management of Internet Names and Addresses*. https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses

ITU 秘書長選舉結果對未來網路治理的意涵

梁理旋／NII 產業發展協進會副執行長

https://blog.twnic.tw/2022/11/04/24758/

國際電信聯盟（ITU）新任秘書長

國際電信聯盟（International Telecommunication Union，ITU）在羅馬尼亞首都 Bucharest 舉行 ITU 全會（PP-22）期間，由全體成員國選出由美國所推派的候選人 Doreen Bogdan-Martin 擔任 ITU 的新任秘書長。在總數 172 張選票中，Bogdan-Martin 一共獲得 139 張選票[1]，也成為自 1865 年就成立的百年老字號國際組織 ITU 的第一位女性秘書長。他的競爭對手是由俄國所推出的俄羅斯前電信部副部長 Rashid Ismailov，在這場選舉中他只有拿到 25 張選票。

Bogdan-Martin 將接替現任在位 8 年的秘書長趙厚麟（中國籍），預計在 2023 年 1 月 1 日正式開始任期 4 年 ITU 秘書長職務。在此之前，他已在 ITU 工作近 30 年且為現任 ITU 轄下三大局之一的電信發展局（ITU-D）局長。

美國國務卿 Antony Blinken 也隨即發布對 Bogdan-Martin 之祝賀稿[2]，其表示選舉結果不僅是反映出 ITU 成員國對 Bogdan-Martin

1 International Telecommunication Union (PP-22). 檢自：https://pp22.itu.int/en/elections/elections-results/?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news

2 Antony J. Blinken (2022). The Election of Doreen Bogdan-Martin as Secretary General of the International Telecommunication Union. U.S. Department of State. 檢自：https://www.state.gov/the-election-of-doreen-bogdan-martin-as-secretary-general-of-the-international-telecommunication-union/

在領導力及數位賦權等發展願景上的認可，更象徵著 ITU 已轉變成為更具包容性與代表性的組織。Blinken 除重申對新秘書長的支持外，也強調未來美國在國際多邊治理場域的領導功能，並承諾將與 Bogdan-Martin 共同為不能上網的 27 億人口努力。安全專家 Anthony Rutkowski 也指出[3]，秘書長在 ITU 組織中扮演著重要的協調與領導角色，而 Bogdan-Martin 也將為逐漸失去活力的 ITU 注入新的熱情。

ITU 的重要性

ITU 的重要性在於，其是目前唯一處理電信與資訊網路的全球層級政府間組織，其無線電頻譜的分配協調功能更為重要。因為秘書長有機會影響 ITU 組織的優先事項和資金運用方向，在這次選舉中，諸多國際主流媒體關注的是，這場由美國、俄羅斯推派代表競爭的選舉，是西方民主國家的開放網路與威權國家政府控制網路，兩種截然不同網路治理願景間的爭奪戰。即使從技術層面來看，網際網路關鍵資源的分配與協調，從來就不屬於以政府為主要參與者的 ITU 職權範圍，而是由非營利組織 ICANN 組織透過多方利害關係人模式來運作；但是包括俄羅斯、伊朗、中國等國家則多年來一直尋求擴大 ITU 職權範圍可涵蓋網際網路政策和基礎設施，並賦予政府更多權力來規範網際網路的使用方式。

《金融時報》的分析[4]中提到，這場競選戰是在國際對全球網際網路逐漸分裂的擔憂下進行。技術社群和公民團體擔心的是，越

[3] Anthony Rutkowski (2022). ITU Secretary-General Elect Doreen Bogdan-Martin. CircleID. 檢自：https://circleid.com/posts/20220929-itu-secretary-general-elect-doreen-bogdan-martin

[4] UN elections set to influence how nations shape the internet. 檢自：https://www.ft.com/content/f06d4dbe-a739-4dee-bccd-3b091788f112

來越多國家政府把限制公民連網或取得網路資訊視為具正當性的行為。俄羅斯殘酷對烏克蘭開戰，且將佔領地區的網路路由轉至俄羅斯電信、在俄國境內實施網路監控等諸多措施，也為這場外交選舉活動蒙上陰影。

對未來的展望與挑戰

Bogdan-Martin 的獲選，代表著這個世界上的大部分國家與地區，不認同由上而下、由政府所掌控的網際網路治理模式，不過其獲選也不代表威權體制國家網路控制願景的發展會就此打住。可以預見的是，未來新任秘書長將持續面對此一挑戰，並設法從不同的競爭提案中找出眾所期待的共通點與共識。

在 Bogdan-Martin 於 ITU 全會的大會堂中發表的當選演講[5]中，可感受到他接下此重責大任的兢兢業業，以及對 ITU 未來做出變革性貢獻的熱切。面對著全球不斷升級的衝突、氣候危機、糧食安全、性別不平等，以及 27 億無法上網人口等挑戰，Bogdan-Martin 認為 ITU 所代表的產業所展現出的創新能力，是未來解決這些挑戰的重要推力。他也承諾要建立更多夥伴關係，並提高 ITU 的透明度，以證據為基礎來解決問題。他也提及未來將推動 ITU 成為更具創新性的組織，團結包括國家政府、企業、大學等成員的力量，改善被排除在網路之外人們的生活，創建出可讓下一世代穩定成長的環境。

結語

演講中令人動容處是，他提及激勵自己堅持的力量是他的 4

[5] Acceptance speech of Ms Doreen Bogdan-Martin. 檢自：https://pp22.itu.int/en/itu_policy_statements/itu-sg-elect-doreen-acceptance-speech/

個孩子，並多次強調當今在 ITU 場域中所做出的決定與活動都將影響後代，而團結是必要且關鍵條件。要團結一群人已經不易，Bogdan-Martin 要面對的是團結一百多個國家迥異的觀點與立場，分歧的發生、理解與嘗試緩解會重大挑戰。

同樣身為一位母親，我能體會到 Bogdan-Martin 對改變世界現況的熱切（或為一種因焦慮轉換成而成的力量？），也期待 Bogdan-Martin 能引領 ITU 與網際網路社群間有更多的互動與理解，和緩對網際網路發展歧異願景，讓我們的孩子們，以及孩子的孩子們，能繼續擁有當今我們所享有、並視為理所當然，可暢所欲言且資訊自由流通的網際網路。

從國際法淺談網路攻擊之歸責疑義

林昕璇／中國文化大學法律學系助理教授

https://blog.twnic.tw/2022/11/03/24714/

網路攻擊概述

網路攻擊是現代戰爭依附於網路空間的新興產物，其法律意涵和責任歸屬的問題始終是一個待解的難題，有待更多國際法理論予以闡釋。

據美國執法部門的聲明，中國國家安全部所掌控之海南仙盾科技發展有限公司是似存有發動駭客侵入美國、柬埔寨、沙烏地阿拉伯等國家的電腦，尋找敏感的政府資料之情事，此外尚存試圖獲取紐澤西州一家公司的消防系統等意圖不甚明顯的網路間諜行為。問題在於，網路間諜活動與網路攻擊行為是否落入傳統國際互助協議所職掌之跨國網路之刑事犯罪行為，仍有很大的可議空間，故也加劇應由何人承擔起法律責任之歸責疑慮。

「歸責」的思考圖像

「歸責」（Attribution）一詞在網路安全涉及多種涵義。一般而言，「歸責」指涉者乃係確定對網路攻擊或入侵應負責的實體。而所謂應付擔責任之實體（responsible entity）之意涵界定上目前學說分為三個層面：（1）發動攻擊的機器；（2）在機器後面執行攻擊的個人；以及（3）指揮攻擊的個人或實體（individual or entity）。這三種面向看似互為獨立，其實互有關連。網路法學者 Kristen Eichensehr 在其發表之《The Law & Politics of Cyberattack

Attribution》一文中指出識別發動攻擊的機器此一行為在很大程度上是科技問題。從科技之角度以觀，除了將攻擊歸責於一台機器之外，更為棘手的毋寧是確定指揮或策劃攻擊的實體背後是否牽涉到政治和法律層面的隱藏成因。

必須先予指出者，鑑於所涉及技術的匿名性，將網路攻擊歸因於特定國家有其困難性。蓋儘管受害國最終可能成功地將網路攻擊追蹤至另一國的特定伺服器，但總體而言相當耗時費日。倘若指揮網路攻擊的實體是一個國家時，依循現行聯合國憲章及國際習慣法的規定，一國能夠要求另一國對武裝攻擊的網路攻擊承擔法律責任，是受害國在對責任國進行合法自衛時使用「主動防禦（使用武力）」的權利的一個重要樞紐。主動防禦包括攻擊侵略性電腦系統的電子設備，使該系統無法行動，進而阻止網路攻擊。有鑑於網路攻擊在行為態樣的千差萬別及隱匿性，以及聯合國安理會是否得以及時應對此類攻擊的不確定性，國家之間透過行使聯合國憲章 51 條所定之自衛權，進而將最初網路攻擊直接並最終歸因於另一個國家或該國直接控制下的代理人的解釋方向，應是頗為合理的論理。

美國政府對於網路攻擊的公開歸責模式

近年來，美國政府對於日益猖獗的網路攻擊行為的歸責模式，根據 Kristen Eichensehr 的研究，採取了四種形式分別為：（1）刑事起訴（criminal indictments）；（2）經濟制裁（economic sanctions）；（3）科技警報（technical alerts）；（4）官方聲明或者新聞稿（official statements or press releases）。其中美國司法部負責處理涉及刑事罪責之刑事起訴（criminal indictments）。美國政府第一次公開起訴網路敵意行為可追溯至 2014 年，彼時賓夕法尼亞州西區的大陪審團起訴了中國人民解放軍 61398 部隊的 5 名成員，起訴書指控其違反了聯邦《計算機欺詐和濫用法》《Computer Fraud and Abuse Act》

所處罰之包括共謀、未經授權進入電腦和造成電腦損壞罪名。以此對於駭客攻擊（hacking）和合謀駭客攻擊（conspiring to hack）包括西屋電器和美國鋼鐵在內的公司加以究責。

美國使用的第二種歸責機制是實施經濟制裁（economic sanctions）。制裁歸責是屬於財政部的職權範圍。2015 年發布的第 13694 號行政命令建立了一個新的網路制裁制度，允許財政部長封鎖「從事重大惡意網路活動（engaging in significant malicious cyber-enabled activities）」的個人財產，包括干擾重大基礎建設之電腦和參與重大網路盜取商業機密。2016 年 12 月，歐巴馬政府修訂該行政命令，將干預選舉納入其中。自此，美國政府迅速利用新的權利去制裁並因此指控俄羅斯情報部門、四名俄羅斯情報官員和三家公司干預了 2016 年選舉。

美國政府使用的第三種歸責機制是國土安全部（Department of Homeland Security，DHS），其機制乃透過網路安全和基礎設施安全局（Cybersecurity and Infrastructure Security Agency，CISA）發布的科技警報（technical alerts）。警報旨在提供科技資訊，如公告大眾周知存在惡意軟體（malware），以幫助系統管理員防範惡意活動。當科技警報指控之惡意活動背後的具威脅行為人是外國政府時，就會出現以警報來歸責之情形。

美國政府用以歸責外國政府的最後一種機制是發布公開聲明（issuance of public statements）或新聞稿（press releases）。例如：美國國土安全部（DHS）和國家情報總監（Director of National Intelligence，DNI）曾共同發表聲明，指摘 2016 年民主黨全國委員會遭駭客攻擊的原因經調查後歸責於俄羅斯政府。在通常情況下，這種透過發布新聞稿的歸責通常會是美國政府一系列歸責和回應行動中的第一個行為，抑或作為美國政府發動後續司法追訴之預告行為。

各國歧異立場加劇法規範整合之困難性

值得注意者，除了對政府行為者追究法律責任外，各國尚且就與歸責相關的證據問題試圖凝聚共識。其中，尤以 2015 年 U.N. Group of Governmental Experts（GGE）的聲明，包括巴西、中國、印度、俄羅斯、美國和英國等獲致最廣泛的支持共識。上述位列 GGE 談判回合的國家皆同意，在網路安全背景下，「對組織和實施針對國家的不法行為之指控應有證據支持」（accusations of organizing and implementing wrongful acts brought against States should be substantiated）。惟這份聲明並未精確釐清為成立系爭指控須達致何種舉證責任的門檻和程度。

Kristen Eichensehr 在前揭文章[1]中饒富深意的指出，中國、俄羅斯和其他國家繼續提倡網路攻擊的指控必須有充足的證據予以證立的觀點。從中美近年來網路空間的競逐以觀，中國和俄羅斯在接受指控後，自然希望迫使指控國（accusing countries）儘可能揭露更多資訊，蓋一旦揭露的證據和事實愈多，愈可能暴露美國的執法部門和情報部門平時因應這類介於政治與法律的灰色事務的情報來源和途徑。此外中國、俄羅斯及其盟國也可能慮及若要求提供指控的證明歸責方法（substantiating attributions）將因控訴成本提高而導致指控國降低其訴諸公開歸責的意願。

對於舉證責任的猶疑，展現在美國和英國向來主張國際法並不要求揭露證據來支持指控的立場。美國國務院法律顧問 Brian Egan 即曾表示：「儘管有些國家提出了相反的建議，但在採取適當行動之前，沒有任何國際法律提到有義務要揭露歸責所依據的證據。」這意味是否舉證據以支持網路攻擊之舉證只是個政策選擇，而非來

[1] Kristen Eichensehr, The Law & Politics of Cyberattack Attribution 67 UCLA L. Rev. 520 (2020).

自國際法的強行義務。這個立場鮮明地與上述中方與俄羅斯的主張站在對立面，並且得到英國、法國與荷蘭的支持。

不容諱言的，對於網路敵意行為的規則目前各國於舉證責任上存在分歧。在《塔林手冊 2.0：適用於網路行動的國際法》（Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations）[2]中，試圖重申適用於網路空間的現行國際法，各國在法規範存在的問題上立場容有不同且存在模糊不清的界定空間。塔林手冊提出的結論則是「儘管[提供證據]可能是為了避免政治和其他緊張局勢，但當前仍欠缺足夠的國家慣行（State practice）和法律意見（opinio juris）以獲致結論，證立此義務在國際法上存在既定性、強行規定的基礎淵源」。前揭立場說明各國在對網路攻擊訴諸法律究責之舉證責任的共識凝聚上，尚待更多的學說與理論填補空白。

[2] Int'L grp. of experts, nato coop. Cyber def. ctr. of excellence, tallinn manual 2.0 on the international law applicable to cyber operations (Michael N. Schmitt & Liis Vihul eds., 2017).

聯合國任命 IGF 領導小組：Who, What & How

梁理旋／NII 產業發展協進會副執行長

https://blog.twnic.tw/2022/10/14/24481/

網路治理論壇領導小組（IGF Leadership Panel）成立

聯合國秘書長 António Guterres 在 8 月 16 日宣布任命 10 位高階專業人士為第一屆網路治理論壇領導小組（IGF Leadership Panel）成員，以實踐其所提出的「數位合作藍圖（Roadmap for Digital Cooperation）」之規劃。該小組也定位為具戰略性、賦權的多方利害關係人團體，以支持與強化 IGF；也因此，小組的專家將會處理戰略性及急迫性議題，並加強 IGF 後續可能行動，促進 IGF 討論的影響力。

這 10 名小組專家透過公開徵求提名而來，最後由聯合國秘書長任命，並平均分配於政府、私部門、技術社群、公民社會團體，以及一般使用者等 5 類多方利害關係人作為代表。這 10 位領導小組成員的任期為 2 年，更精準地說，是 2022~2023 年 IGF 期間。除了這 10 位專家外，另有 5 名當然成員，包括 IGF 的多方利害關係人諮詢小組（Multistakeholder Advisory Group，MAG）主席、聯合國秘書長的技術特使，以及 2021-2023 年三年的 IGF 主辦國代表，依序為波蘭、衣索比亞及日本。

IGF 領導小組成員遭受批評

在去（2021）年 11 月公開徵求小組成員提名時，就有公民團

體公開批評，新的領導小組將惡化 IGF 的階級意識，也背離了 IGF 成立之際所主張的多元包容、鼓勵由下而上的多方利害關係人參與之初衷，而領導小組所做出的決定也可能會凌駕更廣泛的社群觀點。在相關論述中也強調，IGF 本是讓不同利害關係人平等聚集在一起討論與網際網路有關公共政策議題的一種模式，也因此和其他制定規範或標準的其他聯合國機構不同，IGF 應當更著重於過程，而不是結果，當重點被放在領導小組上時，無助於擴大決策參者的基礎，反而讓領導小組的決定有更高的可能性會成為決策者的政策偏好。

今年 8 月聯合國於 Twitter 宣布小組成員清單的訊息回應中，還包括對由政府發號施令全面封網的衣索比亞部長也入榜的不以為然。喬治亞理工學院的 Milton Mueller 教授則再度發表文章認為，聯合國因本身是個政府間組織，自然無法精準掌握由下而上多方治理模式運作的概念，他更批評該份領導小組名單所提出人選是聯合國的空降部隊，以為只要將五類型的利害關係人中各自指派相同數量的代表即是多方模式。Mueller 教授更認為這些成員的指派是是社會影響力、性別與區域平衡等因素考量後的結果，而非因為這些人士具有發展成為全球集體行動的想法（當然，Vint. Cerf 除外）。在當前複雜的數位政治與經濟交錯網路體制下，此小組無助於全球治理進展。

IGF 領導小組成立宗旨

曾擔任聯合國 IGF 主席特別顧問的外交基金會（Diplo Foundation）創辦人 Jovan Kurbalija 則提出領導小組應成立的理由：解決 IGF 自 2006 年成立至今逐漸弱化的地位。他描述 IGF 在 2006 年成立之際，是唯一討論全球層級網路治理議題的場域。但

這些年來，國際上各式委員會、小組、論壇、倡議、聯合聲明等問題解決機制如春筍般冒出，加上如資料保護、人工智慧及網路安全等高關注問題亟待處理，不少技術組織也開始涉及政策討論。在此同時，IGF 卻停滯不前，無法演進成為公民、企業與政府共同關注網路政策議題的場域，探究最主要原因是，許多決策者不知道 IGF 為何？即便知道 IGF，也多將之視為每年召開一次的會議而已。

Kurbalija 認為 IGF 最獨特之處在於，其同時具備聯合國的內在及全球社群的參與。IGF 更可作為所有政策制定者的單一入口，特別是對於發展中國家或弱勢族群來說，可以不必花大量資源去關注不同的國際倡議之討論。而領導小組在此過程中，可透過這些人士本身就具備的聲譽，扮演「IGF 銷售員」角色，擴大 IGF 的政策足跡。此外，在當今數位技術跨越健康、貿易或環境等不同領域之際，領導小組更可協助 IGF 與諸多不同的技術或商業社群進行介接。

結語

當然，IGF 的改革非一蹴可幾，領導小組也只是邁向進化版、亦即所謂的 IGF Plus 的其中一環。其中，IGF Plus 是聯合國在 2019 年中所發布「數位互賴時代」（The Age of Digital Interdependence）報告中所提出的建議：希望在原有 IGF 基礎上，透過設置如諮詢小組、合作加速小組，來強化 IGF 所產出建議可實質運用於公眾討論或決策制定參考當中。

目前我們尚不可知這些被指派的 15 位領導小組成員，將如何在預計於 11 月底在衣索比亞召開的 2022 IGF 年會中（或後）發揮作用，但至少一直以來引起不了太多國際媒體關注的 IGF 年會及其產出（如 IGF Message），可藉由這群高知名度的代表們取得更多的關注，並有機會將相關討論帶至決策者或政策制定者的眼前。

無解的域名衝突？

莊舒歆／東海大學資訊管理學系

https://blog.twnic.tw/2022/09/07/24175/

域名衝突（name collision）

在說明域名衝突前，我們要先了解企業內部網路以及域名系統架構。

隨著網路蓬勃發展，許多企業開始申請網域並架設網站，2011 年 6 月網際網路名稱與數字位址分配機構（Internet Corporation for Assigned Names and Numbers，ICANN）批准了新通用頂級域名（New generic Top-Level Domains，new gTLD）[1]，2012 年開放各企業與機構註冊，ICANN 在當年收到了 1930 個域名申請，截至 2022 年 6 月已核准了 1,241 個[2]。且數量可能會持續增加。

企業內部網路（Local Area Network，LAN），是指交換器會將內部許多電腦連結在一起，使它們可以共用網際網路、檔案和軟體等資源。使用者不僅可以透過區域網路內使用，在外部也可以透過 VPN 對企業內部網路進行存取。

域名系統（Domain Name System，DNS）的架構是採用階層式的分散式處理模式來分類，類似樹狀目錄結構（Tree Structured Directory）。在架構最頂端的稱為根網域（root domain），從根網域

1 ICANN. (2011). ICANN Approves Historic Change to Internet's Domain Name System. 檢自：http://www.icann.org/en/announcements/announcement-20jun11-en.htm

2 ICANN. (2022). Completed New gTLD Program. 檢自：https://newgtlds.icann.org/en/program-status/statistics

向下分出不同的分類網域，每個網域下又可再建立主機名稱，主機名稱下再延伸出子網域，如此不斷重複。這整個結構空間稱為網域名稱空間（Domain Name Space）。

綜合上述，可以知道企業內部自訂主機名稱擁有內部域名，內部域名選擇了原頂級域名中不存在的名稱。但後來出現的新頂級域名與之重複，就稱為域名衝突。域名衝突的問題其實早在新通用頂級域名問世前就發生了。但由於新通用頂級域名數量龐大，引發衝突的可能性和影響範圍將會更大。

衍生問題

使用企業內部網路，當域名衝突發生時，我們在外部瀏覽器上查詢域名，仍會在企業內部網路；同樣的，輸入內部域名使用企業內部服務，DNS 解析可能會導引至外部網站。

域名衝突會造成下列問題：

- 無法存取公司內部的服務。例如：無法使用企業電子信箱。
- 在企業伺服器內部中使用縮寫路徑時，無法與其他伺服器連接。
- 區域網路內的終端用戶無法存取頂級域名。
- 組織內伺服器會試圖存取組織外伺服器，導致資訊洩露；也造成公司使用的主機名稱洩露給外部。

以 Corp.com 的故事使我們更了解域名衝突衍生問題。

在企業內部網路的微軟電腦，是統一透過 Active Directory（AD）來驗證同個網路上的其他主機。AD 能使一台在 ABC.example.com 上的 Windows 電腦，要存取內網名叫「drive」的磁碟時，只需輸入路徑「\\drive\」就能存取。早期 Windows Server 2000 系統預設的 AD 路徑為「corp」，許多企業就在這基礎上建立了更龐大的網路。

如果一台受 AD 管轄的企業筆電，帶到公司外上網，筆電會試圖存取專屬於公司的網域名稱「corp」，但實際跑到網際網路上以 corp.com 為名的網域。所以任何控制 corp.com 的人都可以被動地攔截來自數十萬台電腦的公司與企業通訊內容。JAS Global Advisors 是長期研究 DNS 域名衝突[3]的公司，2019 年他們架設了網域為 corp.com 的網站，大約 1 小時就接到 1,200 多萬封信，包含企業機密文件。他們還分析了試圖連接 corp.com 的資料流，發現大多是要登錄各公司內網和共享文件。也就是掌控 corp.com 就能輕易掌控各企業網路、進入企業內網，擁有一個由企業組成的殭屍網路（Zombie Network）。只要企業 AD 的網路名稱，使用的不是公司所屬的網域名就會有風險。

解決辦法

2013 年 RFC 6762[4]建議各企業可將內網取名為.corp，後來證明這是件危險的舉動。2017 年 ICANN 開始了域名衝突分析計畫（Name Collision Analysis Project，NCAP），將「.corp」這類字串貼上高風險標籤並永久擱置，包含.mail、.home 等，並調查造成域名衝突的根本原因，回顧過去文件持續研究域名衝突的影響。但目前域名衝突問題沒有辦法完全根治，全世界的企業內網數量無法計算，企業需要多加注意內網所使用字串。ICANN 對頂級域名申請嚴厲的審查制度有利緩解此問題，但在效率上卻可能趕不上域名衝突的發生。

---

3 JAS Global Advisors. (2014). Mitigating the Risk of DNS Namespace Collisions. 檢自：https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf

4 RFC 6762. https://datatracker.ietf.org/doc/html/rfc6762

NCAP 研究團隊表示：「若是沒有經過龐大社群的仔細審查，不經過協調就毫不猶豫地使用網域名稱空間，就會持續造成域名衝突，降低整體網際網路的穩定及安全」。[5]

結語

目前各網際網路社群已將域名衝突視為需致力解決的議題。域名衝突影響的不只是企業，也可能衝擊到一般家庭，家中設定路由器或是家電所使用的網址，如果有部分字串也成為了頂級域名，可想而知那有多危險。ICANN 後期致力於嚴格審查頂級域名申請，引起部分的申請者抗議，認為有些機構能一開始就拿到域名，他們現在卻要等上好幾年的時間才可以使用或被告知不能使用，浪費了許多時間與成本。但我們都清楚知道，為了網路安全這是有必要的。

域名衝突的狀況到現在仍然持續增加，已演變為一個棘手的問題。企業自身需確實檢查內網域名設定，才能真正保護企業網路安全並為網際網路社群助一臂之力。

[5] ICANN. (2022). Challenges with Alternative Name Systems. 檢自：https://www.icann.org/en/system/files/files/octo-034-27apr22-en.pdf/

美國提出《服務條款標籤化、設計和可讀性（TLDR）法案》

羅心妤／東海大學資訊管理學系

https://blog.twnic.tw/2022/03/08/21912/

常見的網路協議

在使用軟體或進入網站前，常會跳出各式各樣的協議，複雜的內容讓人混淆不清它們真正的目的，而使消費者在無形中喪失了應保有的權益，以下介紹三種常見的協議[1]：

1. 最終用戶許可協議（End User License Agreement，EULA）：針對用戶安裝或造訪軟體時，提供了使用軟體的許可權，旨在保護公司對該程式碼的所有權。
2. 服務水準協議（Service-level agreement，SLA）：規定了服務內容，包括：正常運行時間保證、責任歸屬、信用或退款政策等，可以將其視為客戶服務政策。
3. 服務條款協議（Terms of Service，TOS）：則涉及公司向用戶提供的服務（例如：訂閱、造訪網頁），它定義了用戶使用該服務時的協議及需遵守的規則。

這些冗長且複雜的協議中通常會隱含對消費者不利的免責條款，例如：TOS 通常允許相關公司隨意訪問、存取和使用個人訊息，包括與第三方共享數據。

---

[1] Megan (2018). The differences between a EULA, TOS and SLA. 檢自：https://odinlaw.com/the-differences-between-a-eula-tos-and-sla/ (Feb. 13 , 2022)

接連的「個資外洩」及「濫用用戶個人訊息」事件促成 TLDR 法案

去年 4 月，在駭客網站上可以發現 5.33 億 Facebook 用戶數年前的隱私訊息。因為 Facebook 和其他社交媒體網站多年來收集的大量資訊，其中包括 106 個國家／地區的電話號碼、全名、位置、生日和電子郵件地址，雖然 Facebook 宣稱洩漏案在 2019 年已被解決，用戶卻未曾被告知個人資料外洩。

去年 10 月，前臉書產品經理弗朗西斯・豪根（Frances Haugen）在離開該社交媒體公司後仍多次在國會作證，概述了她公開發表的一系列洩密事件，包括：操縱輿論、影響青少年心理健康、挑撥紛爭等，引發軒然大波。

除此之外，亞馬遜因違反其 GDPR 數據保護規則而被歐盟處以創紀錄的罰款、Google 被指控通過使用「cookies」在未經使用者同意的情況下追蹤用戶資訊，大型公司接連的洩密風波，促使民主黨和共和黨議員共同推動 TLDR 法案。

TLDR 法案的目的

網路用語中，「TLDR」代表「太長了；沒看」（Too long；didn't read），雖然新推出的法案顯然參考於該用語，但它實際上是服務條款標籤化、設計和可讀性法案的首字母縮寫詞（Terms-of-service Labeling, Design and Readability）。目標是讓消費者更容易理解他們正在使用的網站條款。

TOS 通常跨越多個頁面，其中充滿了令人困惑的專業法律術語。當協議越長越複雜，普通人閱讀的可能性就越小。2012 的一項研究發現，一名美國人若是要閱讀完一年內所使用網站的所有服

務條款，需要花費 76 個工作天[2]。

長期以來，令人眼花撩亂的服務協議條款迫使消費者只許同意所有條件，否則完全失去對網站的訪問權限，這聽起來並不像是「協議」而是「規定」。更嚴重的是，若直接跳到「接受所有條款」可能會使用戶的隱私和個人數據面臨風險。TLDR 法案的推動議員之一，Lori Trahan 在聲明中提到，目前的服務條款協議沒有談判，沒有替代方案，更沒有真正的選擇。

TLDR 法案摘要

TLDR[3]法案要求網路公司提供「易於閱讀的 TOS 摘要」來解決這個問題，讓消費者在不必分析法律條文的情況下獲得訊息。這些規定將適用於要求用戶接受 TOS 內容的大型商業網站和應用程式。雖然小型企業將獲得豁免，但目前尚不清楚究竟如何定義小型公司與大型公司。

如果該法案通過，將要求大型公司的 TOS 需符合以下摘要[4]：

- 正在蒐集哪些類型的消費者訊息。
- 蒐集的數據對於公司為消費者提供服務是否為必要關聯。
- 消費者數據如何與第三方共享的圖表。
- 消費者是否可以刪除他們的數據以及如何刪除的說明。
- 使用該服務的消費者的法律責任，包括他們對其內容的權

---

2 Keith Wagstaff (2012). You'd Need 76 Work Days to Read All Your Privacy Policies Each Year. 檢自：https://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year/(Feb. 13, 2022)

3 117th Congress 2D Session H. R. (2022). 檢自：https://trahan.house.gov/ uploadedfiles/tldr_act.pdf(Feb. 13, 2022).

4 Senator Ben Ray Luján (2022). Luján, Cassidy, Trahan Introduce Bill to Inform Consumers, Increase Online Transparency. 檢自：https://www.lujan.senate.gov/press-releases/lujan-cassidy-trahan-introduce-bill-to-inform-consumers-increase-online-transparency/(Feb. 13, 2022).

利、強制仲裁和集體訴訟豁免。

- 將過去三年的數據洩露事件列表。

結語

美國參議員 Bill Cassidy 說，使用者不應該透過自行梳理條款中的專業法律術語，來了解自己的資料將如何被使用，早就應該強制業者提供易於理解的條款摘要。

然而，TLDR 僅解決了網路上大量數據的一小部分，公司仍能在其他的隱私權政策上巧立名目以訂定更多更細節的數據使用方式，期望 TLDR 能成為打擊不公網路協議的序幕，明定透明化制度，並進一步讓消費者能夠參與、選擇自身數據的使用權，並將成功模式應用至其他隱私權相關協議。

RPKI：回顧 2021 年

Dave Phelan

https://blog.twnic.tw/2022/05/01/22890/

本 APNIC 文摘原標題為 RPKI—2021 retrospective，由 Dave Phelan 撰文。

2021 從很多方面來說都令人失望，疫情仍未消失，國際旅遊仍充滿限制，很多人也還是必須在家工作。但 2021 年還是有好的地方：無論有沒有疫情，網路營運者都在繼續布建資源公鑰基礎建設（Resource Public Key Infrastructure，RPKI）。

全球疫情讓我們學到的事之一，就是網路的靈活韌性是讓世界繼續轉動的關鍵。而這份我們仰賴的靈活韌性，部分來自於全球路由的穩定，確保訊務封包不被轉向、挾持而順利前往預定目的地。

本文回顧 2021 年的亞太地區的 RPKI 整體概況並說明觀察結果。在這之前，作者首先解釋 RPKI 的基本運作原理。

網路營運人員希望將自己設置的路由方向分享給全世界，同時確保這些路由方向驗證有效。這就是 RPKI 框架的作用。

網路維運人員可以利用加密憑證擔保他的前綴 X.X.X.X 來自自治系統號碼（Autonomous System Number，ASN）YYYY，任何來自其他 ASN 的相同前綴都應視為無效。他也可以指定最大長度（maximum length）以涵蓋多筆前綴，如指定 61.45.248.0/21 最大長度/24，這就包含/21、2 筆/22、4 筆/23 和 8 筆/24。這是「路由來源授權」（Route Origin Authorization，ROA），也是 RPKI 框架的第一步。

其他網路維運人員將根據另一方設定的路由方向採取行動；若

發現有前綴被以 ROA 未指定的方式使用，他們就不能把這些前綴納入自己的路由表。這是第二個步驟，路由來源驗證（Route Origin Validation，ROV）。

框架的最後一塊拼圖，則是負責驗證的獨立軟體。這些驗證軟體解密路由來源的加密憑證後，產出路由器能辨讀的結果。路由器因此不需額外花費處理效能解讀加密憑證，僅需專注做好一件事：傳送封包。

了解 RPKI 框架的基本運作原理後，就可以開始回顧 2021 年的 RPKI 境況。

跟過去幾年比較起來，（惡意或意外的）路由事件數量和影響力都下降。APNIC 自 2008 年開始觀測紀錄路由事件，而 2021 年僅觀測到 4 起路由挾持，全部看起來都是維運失誤，而且只有未實施 ROV 的少數維運方和網路交換（Internet Exchange，IX）上的路由因此受到影響。

ROA 觀測資料分析

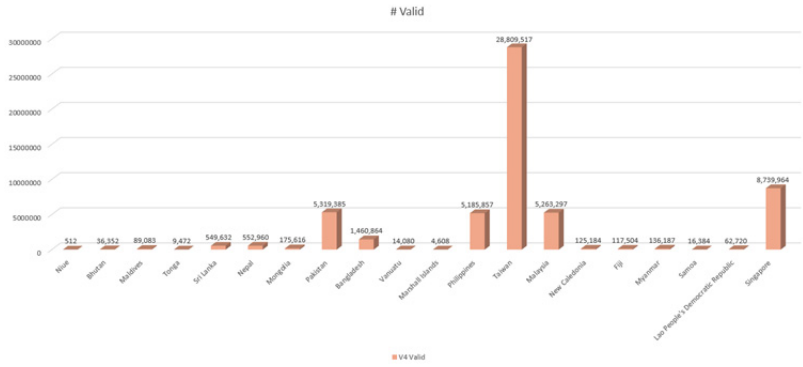
過去幾年來，全球路由表的規模急劇成長。2021 年的全球 IPv4 路由表成長約 6.3%，包含 92.2 萬筆路由。RPKI 方面，有效路由則成長 9.9%。這數字是個好消息，表示執行來源驗證的網路越來越多。

然而，無效 ROA 的比例也從 2020 年底的 0.07 成長至 0.2%。大部分的無效原因是不符最大長度或無效的自治系統（AS）。「找不到」（Not Found），也就是 ROA 不存在的情形也下降了 5.26%，但有效前綴比例並沒有因此上升。後者可能有很多原因，但最主要的可能是持有者沒有簽署新取得的發派資源，或是現有 IPv4 的空間被分散。

在亞太地區，發配空間約有 0.16%的淨成長，有效 ROA 的比例則從 40.97%成長至 50.55%，與全球趨勢差不多。亞太地區的無效 ROA 僅上升 0.11%，「找不到」ROA 則下降了約 10%。若進一步細看亞太地區內分布，東南亞和大洋洲地區表現最佳，來自這兩個地區的有效 ROA 成長幅度拉高了亞太地區的整體平均。

全球最多有效路由的前 20 名亞區中，有 9 個來自亞太地區。在這之中，哪些國家表現最傑出？在被結果嚇到之前，請記得比例不代表一切；若一個國家的網路需求僅需/23 或/22 的空間就能滿足，那達到 100%也就相對容易。當然，這也不代表我們就可以忽視小規模網路的努力。

如下圖所示，臺灣是亞太地區有效 ROA 比例最高的國家。除此之外，巴基斯坦、菲律賓和馬來西亞也都有顯著成長。



ROV 觀測資料分析

ROV 的觀測資料相對難取得，原因有許多，上游供應業者是最主要的因素。簡而言之，終端網路是否執行 ROV，端看他們使用的上游業者是否執行 ROV。

回顧完 2021 年 RPKI 觀測資料，最主要的教訓有 3 個：

1. 鄰接路由表（Adjacency Routing Information Base，Adj RIB）很重要

Randy Bush 去年在 RIPE 83 分享，某些型號較舊的路由因記憶體不足，無法儲存過去執行 ROV 後得知的無效路徑，每次執行邊界閘道協定（Boarder Gateway Protocol，BGP）都必須重新發送路由更新請求，鄰近路由因此必須反覆回應請求而大幅浪費處理器效能。（Randy Bush、Mark Tinka、Philip Smith 和 Kayur Patel 正在審核中的 IETF 草案文件中對此問題有更詳盡的解釋。）

根據 Randy 等人的發現，此問題有幾個解決方案。首先，路由應保留完整的 ADJ-RIB-IN。若沒有 ADJ-RIB-IN，則 BGP 排除無效路徑後，路由應保留此路徑但標註無效（ADJ-RIB-DROPPED）。最後，若路由器無法做到上述兩個方案，則不應執行 RPKI。

2. 荷蘭國家網路安全中心（NCSC-NL）揭露 RPKI 驗證軟體弱點

去年 11 月荷蘭國家網路安全中心（National Cyber Security Centre，NCSC-NL）透過多方參與的協調弱點揭露（Coordinated Vulnerability Disclosure，CVD）過程，發現並揭露多個 RPKI 框架和驗證軟體的弱點。這些弱點包括：有些驗證軟體碰到無效 ROA 資料就會程式崩潰、有些碰到資料庫含有太大位元數的 IP 位址就會程式崩潰、有些處理逾時值的方式很奇怪，有些則容易遭受造成記憶體超載崩潰的 gzip-white-space 攻擊。

目前大型廠商都已經釋出修補上述弱點的更新版本，但並非所有弱點都可透過軟體更新解決。這篇 IETF 草案文件建議在來源憑證上添加擴充程式，定義子物件和路徑的最大數值以建立某些限制。

3. APNIC 介面—MyAPNIC

APNIC 的會員操作介面 MyAPNIC 也可能是亞太地區無效 ROA 增加的原因之一，特別是因為 MyAPNIC 中關於 ROA 的最大

長度欄位的預設格式，常容易造成使用者誤解。目前 APNIC 已移除此預設格式，若使用者不確定應如何填寫最大長度欄位，可以直接詢問客服，進一步避免誤會後填入錯誤資訊並導致 ROA 失效的可能。

參考資料：

https://blog.apnic.net/2022/04/04/rpki-2021-retrospective/

網路治理：展望 2022

陳曼茹／NII 產業發展協進會研究員

https://blog.twnic.tw/2022/02/09/21792/

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。自 2013 的第一篇文章開始，到今（2022）年剛好屆滿十年，回顧十年來的網路治理演變，其認為某些層面其實宛若十年前的境況重演。

2013 年 Kleinwächter 發表本系列第一篇文章時曾寫到，自冷戰結束近 25 年後，世界再次走向兩極分化；然而，如今的隔閡與敵意並非來自不同「主義」之間的對抗，而是雙方對自由、人權、創新，以及政府管制角色的想像差異。

同樣的論述套用至十年後的今日，似乎並無違和。Kleinwächter 指出，這種兩極對立在去年達到新高。去年底華盛頓的民主峰會聚集近百個國家政府，探索集結新盟友以加強保護人權、強化多方利害關係模式以促進網路發展。另一方面，上海合作組織去年 9 月塔吉克峰會的討論，則聚焦於新跨國協議強化網路安全的可能，以及如何加強政府對國內網際網路的控制。

2022 年的網際網路會朝哪個方向前進？是益趨分化裂解，還是再度確認自由、開放、安全及民主，鼓勵無國界交流及大膽創新的網際網路？Kleinwächter 坦承，由於四大議題面向呈現的趨勢及信號都相當混雜，實在難以做出明確預測。

議題面向一：網路安全

在網路安全的範疇中，有三個議題是多方勢力拉鋸的主戰場。

首先是聯合國下第二次召集，負責探討網路空間中國家行為與「資通訊技術及使用安全」的開放式工作小組（Open-Ended Working Group，OEWG）。OEWG 首次會議於 2021 年結束，雖然與會代表都同意，國家政府在網路空間的行為應受國際法及聯合國規章規範，但對數位世界中「使用武力」與「自衛」的定義仍缺乏共識。另一方面，OEWG 顧名思義，應可邀請非國家政府代表參與，但小組成員始終無法就非政府單位的交流或諮詢形式達成協議。

第二個議題是網路犯罪。聯合國中甫成立的網路犯罪特設委員會（An open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes，Ad Hoc Committee），目標是 2023 年 9 月第 78 屆聯合國大會前，完成網路犯罪聯合國公約的撰寫。多年來，西方國家一直積極推動布達佩斯網路犯罪公約，然而這則歐盟議會於 2001 年擬定的公約，僅獲約三分之一的聯合國成員簽署。中國、印度及巴西等國因未參與公約撰寫而不願簽署，他們更支持俄羅斯「透過聯合國機制擬定新公約」的提案。西方國家則害怕聯合國體制的新公約將弱化布達佩斯公約的規範，加上民主與獨裁國家對「惡意內容」的看法南轅北轍，若新公約有任何內容管制相關條文，將加劇雙方衝突。

數位軍備競賽是最後一個議題。特定傳統武器公約大會（Convention on Certain Conventional Weapons，CCW）自 2014 年便設有專家小組，討論致命自動武器（lethal autonomous weapon systems，LAWS）的議題。聯合國秘書長多年來都主張應禁止 LAWS，如「廢止殺手機器人」（Stop Killer Robots）等非營利團體也致力聚集民意，希望阻止「無人機戰爭」的未來。然而許多國家，

包括中國、俄羅斯、土耳其、以色列及美國都無意支持立法禁止LAWS。而在聯合國仍缺乏實際行動的同時，諸如中東地區、葉門、利比亞等地區的國家內戰都已見 LAWS 的使用，更造成嚴重的連帶損傷。

議題面向二：數位經濟

數位經濟面向下有 4 個主要議題，分別是：數位稅、數位貿易、平臺管制及永續發展。

數位稅議題在 2021 年有突破性的進展：去年 11 月，經濟合作暨發展組織（OECD）稅基侵蝕與利潤移轉（Base Erosion and Profit Shifting，BEPS）包容性框架（Inclusive Framework）下 140 個國家中，共 136 個國家就「全球利潤分配稅制」及「全球最低稅負制」的兩大支柱達成共識，預計於 2022 年簽署公約，2023 年便能付諸實行。

數位貿易的前景則沒那麼樂觀。WTO 內雖對終止 1998 年的凍結電子傳輸課徵關稅備忘錄（the moratorium on customs duties on electronic transmissions）具普遍共識，但原訂於 2020 年舉行的第 12 屆部長會議因疫情延至 2022 年，對協商進度不無影響。雖然主導電子商務協商小組的聯合主席（澳洲、日本、新加坡）對 2022 年達成協議深具信心，但美中貿易戰及討論已久的 WTO 改革，都為此展望蒙上一層陰影。

在網路平臺管制方面，全球大致都已同意壟斷不是好事。數位經濟的「贏者全拿」機制促成寡頭經濟，來自中國與美國的巨頭公司制霸全球產業，對國家經濟、中小微型企業及創新都造成負面影響。越來越多政府相信，反托拉斯法能有效將數位經濟的未來導回正軌。歐盟於 2021 年擱置的數位市場法（Digital Market Act，DMA）與數位服務法（Digital Service Act，DSA）預計 2022 年通過實施，

此兩法是否能引發 2018 年通用資料保護規則（General Data Protection Regulation，GDPR）的同等效應，值得拭目以待。

即使近年來科技持續發展，全球已有近 50 億人口上線，數位差距仍存在，世界上許多地區仍缺乏基本的資訊基礎建設。我們需要來自各界，尤其是私部門付出更多精力，才有可能在 2030 年前達成永續發展目標。今年特別值得關注的相關討論，是 6 月的國際電信聯盟（International Telecommunication Union，ITU）電子通訊發展會議（Telecommunication Development Conference，WTDC），此會議將由衣索比亞政府主辦。

議題面向三：人權

全球疫情下，能夠使用網際網路是當代基本人權，以及 2012 年聯合國人權理事會（Human Rights Council，HRC）的「人類在線下享有的權利，在線上應受同等保障」決議，都驗證為真。過去幾年來，HRC 言論自由、隱私及集會自由特別報告員發表多份報告，詳列如大規模監控及網路言論管制等數位時代的全新人權挑戰。然而，面對挑戰，我們在數位時代應如何捍衛及推廣人權，報告卻都沒有給出任何具體建議或行動方案。

新興科技如物聯網及人工智慧的發展，也引發許多可能撼動人類基本尊嚴的本質性問題。2021 年 11 月聯合國教科文組織（United Nations Educational, Scientific and Cultural Organization，UNESCO）巴黎會議中，通過「人工智慧倫理」建議，是難得的里程碑。建議中呼籲企業及政府應加強保護措施，包括改善資料保護規範、賦予使用者對自身資料的知情與控制權，並強化全球執法機關的個資保護執法能力。建議中更明令禁止使用人工智慧執行社會信用評分及大規模監控。雖然 UNESCO 產出的建議並無法律強制效力，但 UNESCO 成員，包括俄羅斯及中國都支持此建議。

議題面向四：科技

自 2000 年代初期開始，「寫程式」與「立法」的人之間，由於缺乏彼此理解及溝通，隔閡也日益擴張。聯合國秘書長 António Guterres 在 2019 年柏林 IGF 的演說就坦承：「即使在最先進的國家，政策制定人才也缺乏技術專業。……在業界勇往直前、打破陳規的同時，政策制定者往往袖手旁觀」。這在全面數位化的世界裡是很大的問題。寫程式的人必須了解，他們的工作成果有連帶的政治、社會甚至經濟影響；立法的人則應理解技術如何運作，避免訂出無法實行或適得其反的法規。兩者應如何負責、對誰負責，又該運用什麼機制確保透明度及當責，也都是值得探討的問題。

Kleinwächter 強調，技術網路治理（Technical Internet Governance，TIG）與政治網路治理（Political Internet Governance，PIG）雖然彼此連結，但兩者不可混為一談。2005 年聯合國世界資訊社會高峰會（World Summit on Information Society，WSIS）突尼斯議程（Tunis Agenda）區分網際網路的「發展」（development）與「使用」（use），此概念日後被用來形容網路治理的兩種層面：「網路的治理」（Governance OF the Internet）與「網路上的治理」（Governance ON the Internet）。

TIG 就是「網路的治理」，範圍侷限於全球網際網路的關鍵基礎資源。Kleinwächter 認為網路關鍵基礎資源就像空氣，沒有所謂的「中國空氣」或「美國空氣」，只有乾淨的空氣，或被污染的空氣。他更主張，若硬要將 IP 位址、域名或根伺服器等關鍵基礎建設資源拖入地緣政治紛爭，爭執誰才有權訂定管理網路基礎資源的標準，就像是污染網際網路，沒人能因此得到好處。

即使如此，仍難以阻擋國家政府將手伸入網路的欲望，加上諸多國家掌握數位未來發展方向、躋升領導地位的野心，「標準戰爭」

很難就此消停，今（2022）年 3 月預計於日內瓦舉行的 ITU 世界電子通訊標準化大會（World Telecommunication Standardization Assembly，WTSA），就是一個值得關注的地緣政治角力場合。

打造維護網路和平的永續機制

網路安全毋庸置疑是當代網路治理的首要議題。借鑒歷史，無論是工業革命、第一次世界大戰，或終結第二次世界大戰的原子彈，科技的發展時常伴隨著益發殘酷的戰爭與無法挽回的死傷。若未來有任何戰爭的可能，網路無疑將是最主要的戰場。要避免新興科技淪為戰爭工具，需要全體人類共同努力。Kleinwächter 認為，2020 年代的網路安全需要嶄新思考，發展「新的多方利害關係外交」。唯有創新、跳脫框架的創新思考，才可能促成因應未來數位挑戰的解決對策。

Kleinwächter 身為共同發起人，集結多方利害關係人的獨立智庫「網路空間穩定全球倡議」（Global Commission on Stability in Cyberspace），過去幾年陸續提出許多想法，也廣為諸如巴黎倡議、歐盟法規及聯合國報告等採納。但他呼籲，我們需要更多、更新的思維。若未來有個新的倡議連線，成功訂出條款，打造維護網路和平的永續架構，那這個組織得到諾貝爾和平獎也不為過。

團結力量大

Andrew Cormack

https://blog.twnic.tw/2022/09/01/24159/

本 APNIC 文摘原標題為 Strength together > weakness apart，由 Andrew Cormack 撰文。

事件應變及安全團隊論壇（The Forum of Incident Response and Security Teams，FIRST）定期舉辦年度會議，宣導全球電腦安全事件通報團隊（Computer Security Incident Response Team，CSIRT）互助協作的重要。今年的年度會議於 6 月 26 日至 7 月 1 日於愛爾蘭都柏林舉行。本篇為作者 Andrew Cormack 針對會議期間，與本次會議主題「團結力量大」（Strength Together）相關的場次留下的心得紀錄。

信任還是互惠？

今年 FIRST 會議的主題是「團結力量大」。Cormack 提到，自 1999 年他首次參與會議開始，大家都同意合作的基礎是「信任」。然而，信任極難定義，律師、電腦科學家和心理學家對信任的解讀都不一樣。他於是開始思考，是否可以從別的角度去看待安全和事件應變。

Cormack 分享，他開始加入全球事件應變社群時，為了盡快融入、不冒犯他人，花了很多時間觀察別人。他因此發現大部分的關係其實是建立在「如果花時間在你身上對我有好處，我就願意花更多時間」。這種合作關係可能會催生信任，但實際基礎仍是互惠。

有些人可能認為「信任」和「互惠」只是語意上的差異，但

Cormack 認為這個區分很重要。誠如會議中 Wendy Nather 的專題演講所指出，一個組織下一次遇到的安全慘案可能來自另一個他完全沒聽過的單位——某個無名軟體程式館、某個安全供應鏈中的廠商，或某個僅是基於組織周邊功能需碰到資料的處理者。在這個全球服務供應商會因為網路攝影機遭駭而停擺的世界，「團結力量大」的概念需要大幅擴及那些我們沒有建立信賴關係的人或群體。在緊急事件中，「是否值得信任」的標準或許太高了。Cormack 認為，「其他人或團體知道對方」是更適當的基準。

他更指出，在艱困時期，動輒提出「信任」或「社會責任」，反而可能弱化合作的重要。贏得信任難，失去信任卻容易。當合作事關組織營運，失去合作關係的後果將難以承擔。會議中，某場座談提到「社會責任」應是分享資訊的動機。但 Cormack 認為，如果資訊共享只仰賴責任感，就容易面臨相關預算遭刪減的困境。他強調，合作是「必要」，不是選擇。

歐盟執委會的 NIS 2 草案中表明，有效的網路安全合作現在無論對個人、組織、經濟或整體社會都至關緊要。Cormack 呼籲大家儘速正視合作之於改善整體數位環境的必要，否則很快我們都將共同蒙受其害。

安全不足是所有人的問題

Wendy Nather 的專題演講也提及安全貧窮線，並說明為何在貧窮線上的人應該和位於線下的人一樣憂慮。保護系統和資料的安全需要資源（工具和人力）、懂得有效運用資源的專業人才，以及充分發揮影響力以克服障礙的能力。

但市面上現有的指南、工具和實例，目標讀者都是安全貧窮線上的人。這在安全威脅會影響整個數位環境的現在是個問題。當代

網路安全威脅已經不適用「躲避飢餓的熊」的比喻，而是「污染」；也可以說，每個人身後都有一頭熊。就算單一組織的安全防護做得再好，也可能因他們自己都不知道有在使用的軟體或服務，或完全無關的裝置而受害。在供應鏈安全事件頻仍的當代，協助改善他人的安全也是在保護自己。

Cormack 認為，要達到「保護他人就是保護自己」的境界，應超越「提升意識」，而開始提升「能力」。小型組織無力負擔頂級的安全軟體或人才，而對兼職的系統管理人員而言，提供所有進階安全選項的操作介面可能無助於辨識、解決問題。開源軟體聽起來很棒，但若算進請專業人力安裝、設定並營運的開銷，其實也不便宜。對於「最基本的安全工具有哪些」這個問題，可以出現 4 種到 31 種的答案。Cormack 觀察，最基本的要求應該是「支付卡產業資料安全標準」（Payment Card Industry Data Security Standard，PCI DSS），但對很多只使用市售安全工具的小企業，就連這可能都是強人所難。

「污染」的比喻彰顯未來風險，無論是信譽或安全的威脅，都是大家一同承擔。若個人使用者對數位系統和服務失去信任，所有人都將連帶遭殃，絕不僅限於出問題的那一方。過去幾年來，政府開始幫忙處理「普通」的網路安全威脅，而不再局限於國家級的高級威脅。

作者最後呼籲所有位於安全貧窮線上的人，開始思考可以如何付出；諸如協助他人減少事件、協防應變或記取教訓，都可以進一步幫助改善整體的安全和信心。

參考資料：

https://blog.apnic.net/2022/08/08/strength-together-weakness-apart/

太平洋的海纜政治

Geoff Huston

https://blog.twnic.tw/2022/07/01/23456/
https://blog.twnic.tw/2022/07/07/23460/

本 APNIC 文摘原標題為 The politics of submarine cables in the Pacific，由 Geoff Huston 撰文。

網際網路誕生早期，曾有一種天真的理想主義，認為網際網路可以超越廉價的政治遊戲。這種想法的最佳範例是 John Perry Barlow 在 1996 年發布的《網路空間自由宣言》（Declaration of the Independence of Cyberspace）。然而，當網際網路成為電信產業主流，這些早期的理想終將幻滅。通訊產業涵蓋大量活動，市值高達三兆美元，這個產業的高度政治化無可避免。

通訊科技早期的政治角力集中於大西洋。如歐洲採用泛歐數位行動電話系統（GSM）技術，美國則擁抱分碼多重進接（Code Division Multiple Access，CDMA）系統。起初 Nokia 是行動通訊業界唯一龍頭，歐洲因此佔上風。然而，隨著智慧型手機成為主流，Apple 的 iPhone 和 Google 的 Android 主導市場，形勢又轉回美國手中。

近幾年來，太平洋地區成為角力的主要場域。

包括美國、澳洲、紐西蘭，以及最近期的加拿大，都宣布國內通訊服務，尤其是 5G 行動通訊網路建設，將限制使用中國供應商。若干中國最大的科技和電信公司，最近幾年都遭美國及西方國家基於國安因素抵制。此類政治緊張關係不僅限於行動通訊和寬頻網路。太平洋地區的海纜也深受此政治地緣拉鋸影響。

海纜模型

在電信時代，投資海纜是控制開放的過程。海纜建設通常由數個電信公司組成集團，成立一個負責海纜建設營運的事業體，並由參與公司擔任股東。海纜的路線反映這些股東的最大共同利益。這條纜線可能是單一纜線系統或分段式系統，也可能是支援多條點到點服務的多點纜線系統。

過去海纜營運之所以大多透過集團形式，主要是因為電話世界供應和需求的不對等。人口增加、不同形式的雙邊貿易增加，以及相關服務的價錢漲幅是影響電話通訊需求的主要因素，而此需求成長缺乏彈性漲幅。供應面而言，電纜系統固定成本極高，但海纜容量變動成本相對非常低。基於以上，最經濟實惠的做法，就是建造當下傳輸技術能支援的最大容量系統。

若新海纜一次就把系統容量提升到完全不同的等級，會破壞市場和價格，導致泡沫化循環。另一方面，即使供應方有能力大幅提升海纜容量，若需求維持微幅成長，則難以確保新海纜系統的財務穩定。

集團承包海纜工程的模式是為了弭平供應與需求的不對等。多家公司持股的海纜公司在高容量海纜布建完成後，會依需求微幅釋出容量，同時保持價格穩定。持股的各家公司會與海纜公司簽訂 15 到 30 年的合約租賃海纜容量（又稱不可廢除使用權，Indefeasible Right of Use，IRU），如此一來，此共同持股的集團事業體在負責提供各家公司海纜容量的同時，各家公司也有義務共同負擔海纜公司的營運成本。

在電話世界裡，此營運模型常使用「半迴路」模式。每筆 IRU 只擁有半個迴路的使用權，必須與另一筆半迴路 IRU 配對才能順利運作。這個模式有效確保兩家公司真正聯合並平等持有此完整

IRU。然而，在網路世界中，這種營運模式無法存活。自 1990 年代起，網路基礎服務需求的成長倍數已超過 11 位數，跟電話通訊需求的平緩成長曲線說是天壤之別。

電話海纜的半迴路 IRU 的配對營運模式也不符需求，在網際網路時代中，一家公司能獨自擁有整副迴路，甚至開始出現單一公司包辦海纜建設的案例。

然而，海纜系統還是有某些方面沒有改變：

- 地質。海纜斷線非常嚴重且代價高昂，能避免就避免。最理想的海纜路徑，應避開所有地理活動頻繁的深海地段。活躍海底裂谷帶、斷層帶，以及任何海底地滑好發的地帶都應盡力避免。一般而言，海纜應該建立於深海底，水域太淺容易導致海纜遭其他海上活動干擾。
- 距離。越短越好。在電話通訊中，只要端到端延遲低於 300 毫秒，就能確保通話兩端的體感即時。電腦對速度的要求則遠高於此，每一毫秒都很重要。也因此，海纜路徑越短越好。
- 國家領域和政治。國家司法管轄區域並不止於海岸，而會延伸至海域和海底。1982 年的聯合國海洋法公約（PDF）規定國家領海為平均海岸低潮線（又稱基線）起延伸 12 海里的水域。對沿海國家而言，基線出發延伸 200 海里的範圍，或 350 海里內的大陸棚地區，還可主張專屬經濟區。對海纜而言，這表示一旦海纜進入此區域，就必須要求專屬經濟區所有國的許可。除此之外，任何此區域內的建設工程或維修營運也都需要取得該國政府許可。

多年來，太平洋是所謂的「轉運區」，許多沿岸大國在此建造端對端纜線系統以提供互連。主要節點包括北美西岸、日本、香港及新加坡。

這造成太平洋中的「兩種速度」：大國之間有高容量、低延遲

的海纜互聯，其他太平洋國家則只能使用衛星系統。一直到非常最近，才開始出現為其他較小國家建立高速光纖連線的海纜計畫。

下圖為目前太平洋地區的海纜分布。

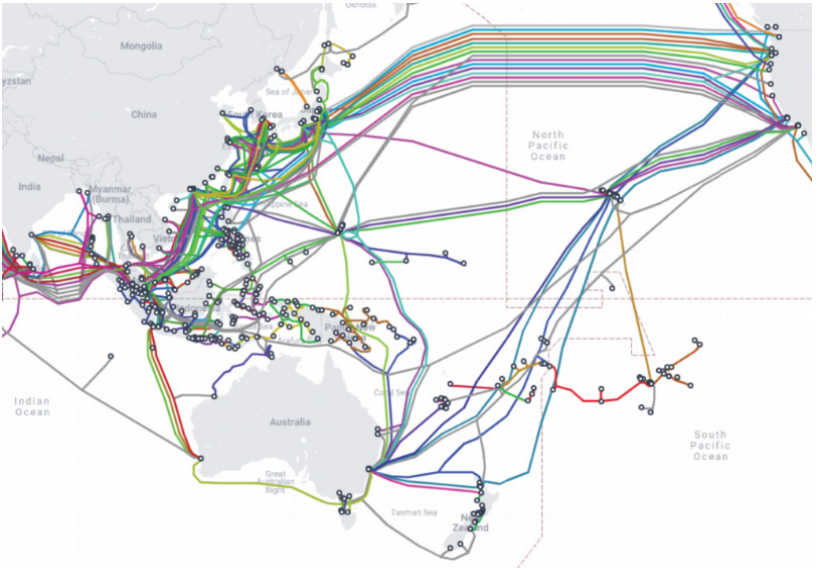


圖 1：亞太地區海纜建設

此地區的海纜連線主要據點為香港、新加坡和日本。許多海纜都位於南海並經呂宋海峽。新加坡扮演海纜東西間閘道的角色，除了少數例外，大部分跨太平洋海纜都使用日本和美國之間的路徑。

近期的太平洋海纜計劃

內容網路的興起及雲端服務轉型，大幅提升對電信服務供應容量的要求，也帶來擴建亞太地區海纜的機會。然而，此情形也揭露美國和中國之間某些未解決的衝突。以下作者透過近期的海纜提案，解析其中凸顯的中美衝突。

索羅門群島海纜

亞洲開發銀行 2012 年宣布將援助在 PPC-1 海纜上建立支線，連接索羅門群島與雪梨的建設案。由於建設工程進度緩慢，索羅門群島在 4 年後成立國有海纜公司，決定自己與廠商交涉，亞銀因此收手不再支援此計畫。2017 年 7 月，華為海洋宣布與索羅門群島簽訂合約，負責建設連接荷尼阿拉和雪梨之間的海纜。

但澳洲不想要來自中國的設備與自家網路連線。2018 年 8 月，澳洲政府宣布珊瑚海電纜計畫（Coral Sea Cable system），此計畫由澳洲公司 Vocus 負責，建立巴布亞紐幾內亞和索羅門群島至澳洲的海纜。此工程由法國公司 Alcatel Submarine Networks（ASN）擔任供應商，並於 2019 年 12 月完成建設。

東密克羅尼西亞電纜

世界銀行和亞銀在 2017 年宣布將延伸關島、密可羅尼西亞和馬歇爾群島之間的既有纜線（HANTRU-1），連接密可羅尼西亞的柯斯雷島、彭佩島、諾魯和吉里巴斯首都塔拉瓦。法國 ASN、華為海洋和日本 NEC 都參與競標此案。

2020 年底路透社報導，美國警告華為海洋以極低價格競標，可能為太平洋島國帶來安全威脅。報導中引用諾魯過去因相同顧慮而拒絕華為海洋的案例，指出所有中國企業都必須配合中國情報安全單位，以及太平洋地區可能因此受到的安全威脅。此建設案因此陷入僵局，最後於 2021 年中撤銷。

澳洲、日本和美國在 2021 年 12 宣布，將建立一條新纜線連結上述地點至 HANTRU-1，此情境宛若索羅門群島海纜事件重演。

太平洋光纖網路

此建設由 Google、Facebook 和中國鵬博士合資，希望建立當時（2018）容量最高、也是首條直接連接洛杉磯和香港的纜線。建設於 2018 年完工，但美國司法部以「國安法嚴重破壞香港自治，法律限制將容許中國在香港的登陸點收集美國通訊訊務」為由，禁止美國端與香港的連線。

2022 年初，美國聯邦通信委員會（Federal Communications Commission，FCC）核發許可，啟動連接洛杉磯、菲律賓巴萊爾和臺灣頭城的光纖纜線。

香港美國纜線（HK-A）

HKA 海纜原計劃建造 6 對光纖連線，連接香港、臺灣和美國。此建案由 Facebook、中國電信、中國聯通、RTI Express 和印度 Tata Communication 及澳洲 Telstra 合資。供應業者則是 ASN。此工程於 2018 年公告，但在 2021 年 3 月撤銷向 FCC 提交的海纜許可申請。

香港關島海纜（HK-G）

香港關島電纜系統於 2012 年提案，但於 2020 撤回向 FCC 提交的許可申請。

BtoBE

BtoBE 由中國移動、Facebook 和 Amazon 集資。此海纜預計連接新加坡、馬來西亞、香港和美國，建設供應商為日本 NEC。此提案在 2020 年 9 月撤銷向 FCC 提出的許可申請。

下一輪海纜建設

太平洋地區對更高容量網路建設的需求持續成長，但美國不核可連至美國電纜另一端落地中國或香港的情況一日不變，南海的國際衝突不解決，所有跨太平洋的海纜提案都必須經日本的北邊路線，或更往南經婆羅洲連結到新加坡。

Apricot

Apricot 計畫長達 12,000 公里，將縱貫西太平洋，連接日本、臺灣、關島、菲律賓、印尼和新加坡。此工程由 Facebook、Google、NTT、中華電信和菲律賓 PLDT 集資。建設供應商為 NTT。

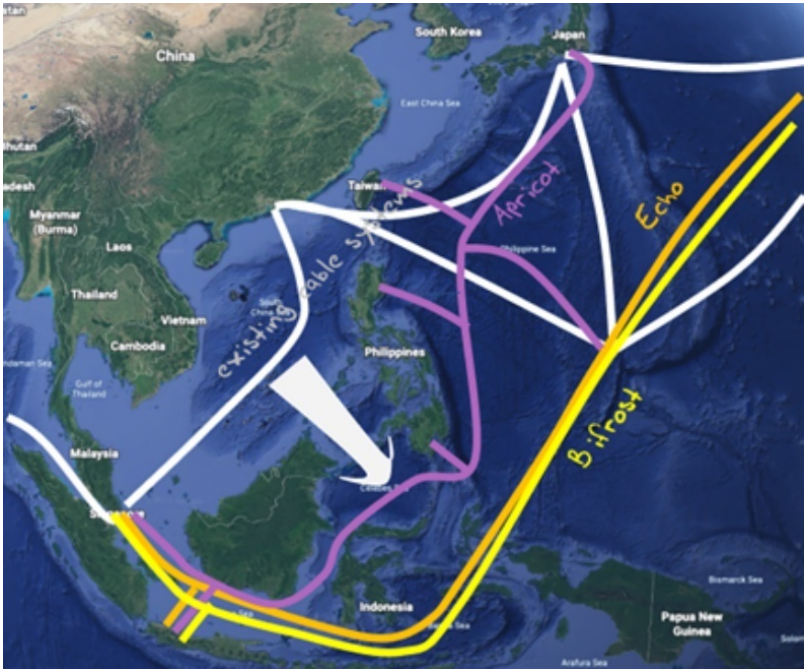


圖 2：跨太平洋海纜新建案

Echo

Echo 將連接新加坡、印尼和美國，並有分支連線連接關島。系統將由 NEC 供應，Google 和 Facebook 則各持有一半海纜容量。此海纜預計於 2023 年開始運作。這也是第一條直連新加坡至美國的海纜。

Bifrost

Bifrost 將連接新加坡、印尼、菲律賓和美國，並分支連接關島。此海纜建設供應商為 ASN，預計於 2024 年開始運作。

現在的問題是中國如何面對這些改變。這不只是海纜路線，或中國科技公司如華爲或中興未來如何自處的問題，更牽涉到中國的數位巨頭如阿里巴巴或騰訊，未來如何經營全球廣大數位市場的問題。

綜觀歷史，任何跨時代的新科技都會帶來劇烈的社會變動，推翻舊秩序的同時造成許多不穩定。在這種時候，作者認為，企圖預測未來其實無異於臆想猜測。

參考資料：

https://blog.apnic.net/2022/06/02/the-politics-of-submarine-cables-in-the-pacific/

發送方付費

Geoff Huston

https://blog.twnic.tw/2022/10/15/24649/
https://blog.twnic.tw/2022/10/23/24653/
https://blog.twnic.tw/2022/10/30/24657/

本 APNIC 文摘原標題為 Sender pays，由 Geoff Huston 撰文。

歐洲電信網路營運業者協會（European Telecommunications Networks Operators' Association，ETNO）在 2012 年 9 月向當年國際電信世界大會（2012 World Conference in International Telecommunications，WCIT-12）提出法規改革提案，建議應要求內容供應方為使用網際網路通訊基礎架構付款。

此提案激起不少反應，有些特別激烈，如民主與科技中心（Centre for Democracy and Technology）就措辭強烈地警告「ETNO 的提案將危及接取開放全球網路」，而這立場代表了網路業界多數心聲。

WCIT-12 並未因此提案作出任何改變。若不是因為韓國後來的舉動，這件事大概會持續在業界暗潮洶湧，但終究浮不上檯面。

韓國內容戰爭

2012 年時「智慧型電視」還是新產品，三星當時趁勢推出高畫質影片串流服務。而韓國電信（Korea Telecom，KT）的反應，是封鎖阻擋三星的串流服務使用 KT 的寬頻網路。國內最大電信業者和最大 3C 業者的戰爭，立刻引發大眾關注。

三星祭出「網路中立」原則，表示消費者使用網路服務的權利，不應受網路服務供應業者的主觀限制，進一步質疑「串流服務過度

浪費網路容量」的說法。韓國通訊委員會也介入，指出 KT 的行為「不恰當」。KT 因此退讓解除封鎖，而高畫質內容串流未來 10 年間在韓國及全球的成長從此勢不可擋。

但此事件並未因此結束。2021 年 SK 寬頻採取法律行動，指出公司客戶大量播放 Netflix 內容導致 SK 寬頻訊務負載大幅激增，主張 Netflix 應負擔部分成本。首爾中央法院判決 SK 寬頻依法應獲得補償，具體金額則交由 SK 寬頻和 Netflix 協商。

部分韓國立法人員曾公開批評內容供應業者不為造成大量訊務量付費。此議題在韓國的特別之處，在於部分本地內容供應業者本就必須付錢給韓國網路服務供應業者（ISP）以提供內容串流，也因此，這議題很容易就被塑造成「本土產業」和「不願入境隨俗的美國巨頭」的對立。

整個網路中立、互連和結算、終結壟斷、成本分攤和基礎建設投資經濟的議題因此重新浮上檯面。但這次議題主打的不是「網路中立」，而是更直接了當的「發送方付費」（sender pays）。兩者的原則相差無幾：網路供應業者希望消費者和內容供應業者都為內容傳遞付錢。

發送方付費

在此之前，讓我們先透過此論戰脈絡，了解「發送方付費」的歷史由來。

若某項服務聚集多種元素，通常有幾個特定模型，用來將此服務收益分配至不同元素的供應方。在「遞增付費」模型下，顧客個別直接付費給不同服務的供應方。此模式中，最終環節的服務供應方具極大優勢，由於顧客已付錢給前面所有環節，即使最終環節索取高額費用，為了不浪費其他已付出的金錢，消費者仍只能咬牙付費。

在其他不同形式的利潤分配模型中，也有由某指揮協調方依不

同環節付出的比例，分配每筆傳輸利潤的形式。在此形式中，指揮協調方可能要求傳輸發起方或服務託管方付費。

另外也有「計價保留」（bill and keep）模式，服務供應商都說好互相免費使用對方服務。如此一來，供應商在計算收費架構時，與其他服務相關的機會成本和收益都按「互撞免賠」（knock for knock）原則抵銷，只需考慮自身服務的成本收益。

最早的通訊方式「郵件」基本上是「收件人付費」，所有遞件環節的費用皆累計至信件送達後，由收件人支付。雖然也可在收件人付費後，再分配費用予所有環節，但更簡單的方式是承接方在信件轉手時付費給交件方，這樣一來，因為必須回收已經付出的成本，每個環節也更有意願確保信件送達。

19 世紀的英國皇家郵政提出兩項重大改革：大幅調降郵寄費用和改成「寄件人付費」，一方面促進郵政活絡，一方面改善收件人拒絕付款收件，造成郵局無法回收成本的困境。

電話系統也比照郵政系統的費用模式。發話人向本地電話公司支付全額，若必須經由其他業者建立通話，則需另外付費給連接另一端的業者。在此模式中，消費者為每筆傳輸付費，而這些費用成為所有參與業者的分攤收益。當然，這模式也有它的問題，如電信公司不滿自己為本地發出的通話負擔最多成本，卻必須平分收益，也有公司利用國內和國際通話的費用落差收穫不當利潤。

接下來 Geoff Huston 以韓國內容戰爭為引，闡述訊息傳遞網路收費架構的歷史演變。自網際網路開始，說明為何「發送方付費」成為近代網路爭議焦點。

網際網路的出現

最初認為至少以功能來看，網際網路跟電話網路差不多。然而，兩者之間的差異遠比相似之處更關鍵。

網際網路中沒有「撥叫」，也沒有可以確認距離和時長的「網路傳輸狀態」。封包的傳輸很隨興：可能會被傳送到目的地，也可能不會；可能會被中介方或其他人員攔截，也可能不會；可能會引發其他封包的傳輸，也可能不會。

網路不是免費的。歸結而言，是我們這些使用者在付費。以目前的網路收費架構而言，使用者向 ISP 付的錢包含「所有網路」接取費，不計距離、不計連線次數，更不計封包數量。與此差異最明顯的是計時或計量型的行動網路費用方案。

這種缺乏明確傳輸定義、與傳統零售大不相同的模型應如何收費，不同供應方又如何在提供無縫服務的同時平衡開支？

若兩個網路互連並交換訊務，有兩種可能：彼此互為顧客並為連線（接收或發送）付費，或是免費互連（peering）。如此一來，所有網路路徑的費用負擔被切成兩部分，一部分由發送封包端付費，一部分由接收封包端付費，兩端以「互連」點切割（如下圖）。除此之外，也有所謂的「付費互連」，意即互連雙方中，一方必須支付費用才能互連。

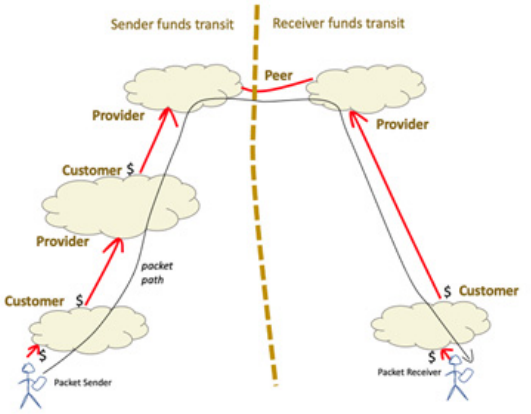


圖 1：網路路徑費用分攤方式

圖片來源：APNIC 部落格

天然壟斷：協商還是脅迫？

若所有潛在對手都面對難以克服的天然阻礙，某人或事物將自然而然具有「天然壟斷」的優勢，如位置優越的港口和廣播頻譜的專有授權。鑑於建置多重進接網路的高昂成本，寬頻網路業者也可視為一種天然壟斷。

然而，這跟「發送人付費」的概念，或是 ISP 和內容網路業者之間的協商又有什麼關係？

套用前述網路連線的邏輯和用語，ISP 認為內容串流業者應「付費互連」，花錢拜託 ISP 將內容傳遞至客戶端。但對內容業者來說，他們已經自負開銷將內容送到 ISP 門口，ISP 的要求形同敲詐。

若寬頻網路業者服務絕大多數國內人口，如德國由 3 家網路業者服務超過三分之二國家人口時，他們就具備強烈的談判優勢；內容業者若想接觸到用戶，就必須接受 ISP 的條件。

若內容業者談不到可以接受的條件，希望另謀出路呢？這並不是假設情境，過去就曾發生內容業者試圖透過其他外部互連或中轉網路連接到使用者，ISP 的對策則是一方面容許此連線，一方面刻意阻塞此連線，大幅降低內容傳輸的速度和畫質。

這種手段也落入網路中立的討論範疇。以消費者的立場而言，向 ISP 支付的費用應保證無差別取得任何來源的服務內容和品質，ISP 和內容業者的角力不應牽連到網路使用者。

最後 Geoff Huston 探討政府透過法律規範介入的可能，警告未來可能並不樂觀。

主管機關如何應對？

撇開雙方論點和網際網路中傳送內容的各種方式不談，在此角力中，規模更大、消費者更想要的一方才是最後贏家。若內容業者

擁有大部分消費者亟欲取得的內容，則 ISP 自然有壓力讓步。反之，若 ISP 佔據壟斷消費市場的絕對優勢，內容業者除非退出市場別無選擇，則後者也可能在面對其他內容業者願意付錢的競爭壓力下屈服。換言之，對雙方而言，企業規模越大、手中握有的消費者人口越多，就能在談判中佔上風。

主管機關要怎麼回應這情形？鉅細彌遺的規範條文很明顯不適合。若規範過於嚴格，則有業界不願繼續負擔成本建設寬頻網路的風險。然而，若完全撒手不管，放任巨頭濫用壟斷地位壓迫國內消費者和本地企業，也不利於國家經濟的長久穩定。

目前最流行的主管機關立場，可見於韓國案例中法院的聲明：「雙方應基於善意協調，我方對協調結果沒有任何要求，僅堅持雙方皆具備充分意願協調出互相同意且能履行的結果」。

相較之下，歐盟似乎希望能採取更強勢的立場。根據最近的媒體報導，歐盟委員會可能提出某種要求內容業者付費的架構，但也有評論擔憂此舉長遠而言將危及網路中立原則，進而導致網路落入單一企業手中。

許願需謹慎，願望會成真

如果內容平臺進一步互相併購，最終只剩下比今天更少的幾家超巨型業者，擁有的客群將龐大到足以在與網路業者的談判中佔據絕對優勢，又會怎麼樣？

這並非天馬行空。過去十年來深海纜線的版圖有極大變動，而當今大部分跨洲的海纜計劃，背後金主都是大型內容供應業者。目前八成以上的跨大西洋海纜是由內容供應業者，而非傳統電信業者經營。內容產業在此領域佔據的主導地位之高，同時握有海纜產業本質上就是一種壟斷。

沒有任何一家電信業者經手的內容，能達到足以發起新兆位元電纜計畫的量，電信聯盟也無意插手。更不用說，幾乎沒有電信業者具足夠的資本支持這類計畫。結果是內容業者成為自己的電信業者。最後一哩（last mile）網路接取市場又該如何自處？這市場具備足夠的使用量和競爭利益，保護其自外於超大規模兼超高利潤的內容市場嗎？舉例而言，Google 多年來就一直在美國開發這方面的市場。

消費者很可能樂見這樣的現象，因為這代表整體服務更無縫、品質更高，同時價格大幅下降。對主管機關而言，如果結果是更有效、可靠且價格低廉的數位基礎建設，又有什麼立場去規範或阻擋此轉變？雖然這在內容產業還沒完全發生，但我們早已眼見其他數位服務，諸如電子郵件、訊息軟體、文件管理到電子商務服務，經歷此合併過程。而過去主管機關對此從未發表任何意見。

若目前主管機關成功強迫內容產業和存取網路產業進行協商，進而導致內容產業乾脆直接入侵並佔據寬頻網路產業的主導地位，那還有所謂的存取網路產業嗎？還是存取網路也終將被內容業者的壟斷勢力吞併？對國家政府而言，國內的寬頻網路建設完全受海外內容巨頭業者的控制，無疑是嚴重的戰略危機。

另一個衍生憂慮，則是若事後反悔，我們能否重頭來過。借鑑歷史，一旦業界巨頭成功併吞所有競爭者並握有實質壟斷，他們將投注全部精力，也有更多資源持續鞏固此壟斷地位。奇異公司、JP Morgan 和標準石油都是至今仍健在的實例。數位巨頭無疑擁有同樣願景，而將接取網路納入麾下，將是邁向此未來關鍵的墊腳石。

英文俗諺如此道：許願需謹慎，夢想會成真。到時候，我們可能沒有工具或腦袋去適應那樣的未來。

參考資料：

https://blog.apnic.net/2022/09/09/sender-pays/

強化技術與非技術社群間的合作

Joy Chan

https://blog.twnic.tw/2022/09/29/24373/

本 APNIC 文摘原標題為 Boost cooperation between technical and non-technical disciplines at APNIC 54，由 Joy Chan 撰文。

APNIC 的特殊興趣小組（Special Interest Group，SIG）提供亞太地區網際網路社群開放的公共論壇，討論大家有興趣的關注議題。APNIC 中目前有 4 個 SIG，分別是路由安全（Routing Security）SIG、政策（Policy）SIG、國家網際網路註冊機構（National Internet Registry，NIR）SIG，以及合作（Cooperation）SIG。所有 SIG 都會在每年兩次的 APNIC 會議中舉辦會議，提供與會者參與網際網路號碼管理、路由安全、網路政策和治理，以及聽取亞太地區各國 NIR 重大消息更新的絕佳機會。

Cooperation SIG 都在做什麼？

Cooperation SIG 是探討高層次公共政策議題，並連結這些議題與實際網路運作的公開論壇，藉此加強網路運作人員和非技術領域的合作。Cooperation SIG 的目標是推動廣大技術社群和非技術網路社群之間的協作。

在 Cooperation SIG 論壇中，APNIC 秘書處會報告 APNIC 的推廣活動，並徵求與會者針對未來活動的意見和指導。Cooperation SIG 的成立宗旨是發展並釐清 APNIC 社群在公共領域相關議題的定位，包括在收到外部針對特定議題尋求 APNIC 社群立場時，負責整合意見並提出答案。

- APNIC 48 會議期間，Cooperation SIG 討論網路維運人員和電腦資安事件應變小組（Computer Security Incident Response Team，CSIRT）如何合作打擊線上濫用行為，並解決追究攻擊來源的問題。
- APNIC 49 的 Cooperation SIG 則聚焦於近年來發展「網路常規」（cyber norms）以支援並強化事件回應量能，進而防止不同司法管轄地區衝突的討論。
- APNIC 50 期間，Cooperation SIG 討論的是電信與合法監聽的議題，以及執法單位和網路服務供應業者的互動。
- Cooperation SIG 在 APNIC 51 探討網路維運人員在 COVID-19 疫情期間擴張的角色，以及因應疫情的調適。
- 永續發展及網際網路的環境影響，則是 APNIC 52 期間 Cooperation SIG 的討論主題。
- 在最近一次的 APNIC 53 會議中，Cooperation SIG 根據規模化、彈性、適應性和韌性四個面向，探討量測網際網路技術成功程度的新方式，並透過三種進行中的計畫，包括網際網路協會（Internet Society，ISOC）的網路的網際互連方式（Internet Way of Networking）、New IP 和歐盟的 DNS4EU，檢視此方式。

若對 Cooperation SIG 有興趣，希望了解更多或更深入參與，也歡迎加入 Cooperation SIG mailing list。

參考資料：

https://blog.apnic.net/2022/08/30/boost-cooperation-between-technical-and-non-technical-disciplines-at-apnic-54/

資訊安全

雲原生之軟體安全韌性

潘育群／華碩雲端數位專型事業處

https://blog.twnic.tw/2023/01/05/25320/

應用服務的「微服務化」及「容器化」

COVID-19 讓 IT 流程自動化加速進行，防疫政策導致企業必需分地、分流工作，在過去自動化能力不足的公司，更面臨了停工、缺料的風險，嚴重一點甚至會導致公司倒閉。IT 產業在這樣的變局之下，製造業系統和服務業上雲都是勢在必行。遠距視訊會議、同儕共同協作機制、產線自動化機制、IT 程序遠端監控與除錯等等，這些機制都讓「數位轉型」的策略，由過去謹慎的評估，搖身一變成為企業永續經營的關鍵抉擇。如果僅靠企業內部有限的 IT 人力資源，通常無法即時滿足企業營運需求，這時候仰賴可靠與穩定的雲端服務，就是一個最佳選擇，在過去幾年，企業其實已經加速上雲的進度，同時仰賴雲端服務協助監控效能與維護架構。

但是否僅將在地端機房的服務直接搬遷到公有雲就足夠呢？原本的程式碼架構，是否能隨著工作負載增加，提升基礎架構即服務（Infrastructure as a Service，IaaS）的資源，當尖峰負載降低時，減少 IaaS 資源的使用，達到用多少付多少（pay-as-you-go）、兼顧成本與服務最佳化的目的呢？很顯然地這些問題，都因為傳統穩態式的程式碼架構相對的巨大而不可切割，導致服務不具敏捷擴充性，在資訊安全更新或者功能迭代上都面臨了實際上的困難，為了克服此一挑戰，目前在積極發展中趨勢是將應用服務「微服務化」以及「容器化」。

雲原生（Cloud Native）

由於為雲而生的基礎環境設計逐漸地受到重視，雲原生（Cloud Native）就在這樣的環境中蓬勃的發展，過去的十年是雲端運算發展起飛的黃金十年。專注在傳統基礎架構（IaaS）雲服務上，未來十年的重點是雲原生基礎架構、微服務（Micro Service）、人工智慧（Artificial Intelligence，AI）以及因為高速 5G 網路串聯 IoT 設備讓行動邊緣計算（Mobile Edge Computing，MEC）茁壯的時代。雲原生是爲雲而生的新一代應用和資源架構模式，進一步減少企業研發成本的同時，也可以避免因為業務擴容需求，導致應用服務中斷的副作用。另一方面，隨着企業持續因為數位轉型，需要收集大量數據分析，也必須提供應用程式開發者更好、更敏捷的開發方式。在雲原生快速發展的趨勢下，未來數年將是業務領銜，直接要求應用的雲端計算資源，運用無伺服器的觀念（serverless），將 IT、AI 算力直接提供至客戶端，隨著萬物互連成爲可能，提供更即時與智能的 IT 服務給客戶，這將導致新的 IT 數據處理架構不斷的演變，引領雲原生時代的來臨。

過去穩態式的 IT，強調安全、穩定與性能，如資訊系統管理（Enterprise Resource Planning，ERP）、製造執行系統（Manufacturing Execution System，MES）、業務流程管理（Business Process Management，BPM）、E-Flow、管理監控（Business Activity Monitoring，BAM）、商業智慧（Business Intelligent，BI），到協作平臺的 OA、CRM；但是在許多企業面臨數位轉型的浪潮下，敏捷式 IT 開發方式，強調敏捷、彈性與靈活的數據化營運（Search Engine Marketing，SEM）、線上線下整合（online to offline，O2O）與 AI、物聯網（Internet of Things，IoT）則必須利用雲原生的特性來提供開發與營運環境。

如果提供業務服務的系統要升級，要如何平滑的調升硬體資源？如果升級失敗，或者負載處於離峰狀態，要如何調降硬體資源呢？同時兼顧線上業務持續運行不中斷。最理想的工作型態，是要能夠讓工作負載配合資源的提供，也就是供給與需求的曲線綿密的貼合在一起（如圖 1）。

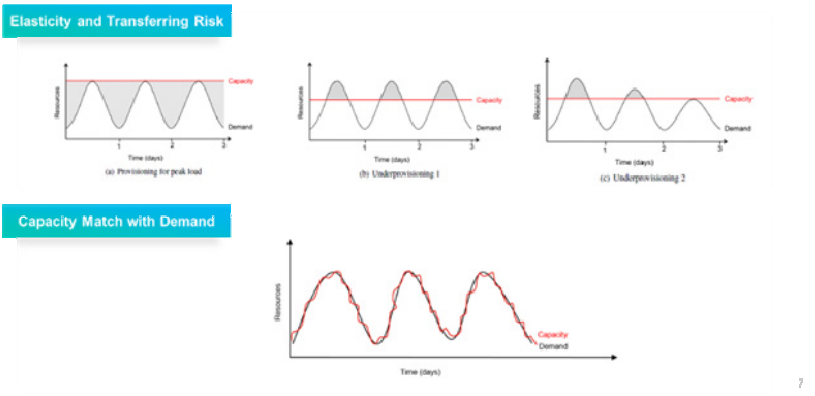


圖 1：工作負載與資源配置關係

雲原生的實際架構為「為雲而生、以應用為中心」，所以能夠適應業務量的變化。我們定義的雲原生平臺組成有 3 部分：一為應用服務微服務架構設計，二為 DevOps（Development and Operation），三為能夠隨著技術發展環境變化的底層平臺，例如：容器（Container），三者缺一不可。

眾所周知的 DevOps 與 CI/CD 循環圖，因為資安因素或者功能變更式不斷迭代與累加的，這個時候就是雲原生平臺要夠提供管理的功能。

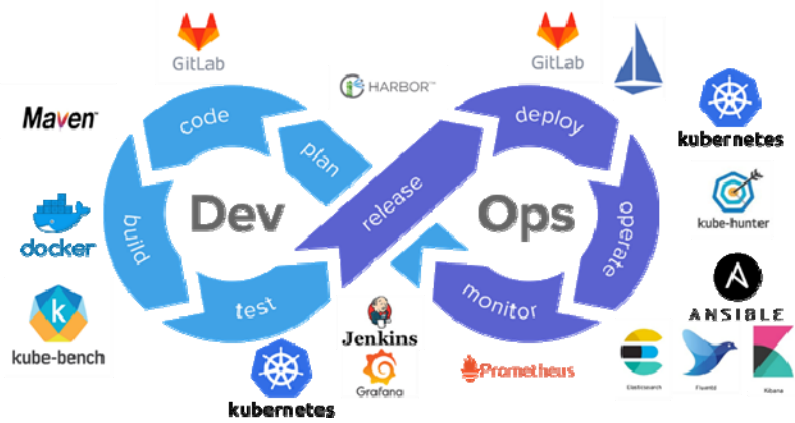


圖 2：DevOps 循環圖

	雲原生應用	傳統應用
佈署可預測性	擴充可預測性	擴充性不可預測
作業系統通透性	具備通透性	與作業系統不可分離
彈性能力	彈性調度	資源冗餘多 缺乏擴充能力
開發維運模式	敏捷性開發如scrum	瀑布式開發
服務架構	微服務解耦架構	單體架構
恢復能力	自動化維雲平台 快速恢復	手工恢復 恢復速度緩慢
資安防護	軟體工程安全性左移	高牆式保護

圖 3：雲原生應用與傳統應用的比較

雲原生的優勢

雲原生的好處引人注目，但是雲原生的架構在強調敏捷性的開發也引入了各種新型安全風險，現在的趨勢是參考 NIST 800-160 SSDLC（Secure Software Development Life Cycle）[12]，將安全性左

[1] NIST 800-64 Rev. 2 Security Considerations in the System Development Life Cycle.

[2] NIST 800-160 Vol. 1 Systems Security Engineering.

移的觀念導入 DevOps 的開發部屬循環中。如圖 4 中所示，在軟體開發生命週期的前期如開發概念（Concept）與開發（Development）階段就導入大比例的安全程序，我們稱為安全性左移；另一方面，考慮軟體的商業價值，對需要完成的安全檢測需求，則以最小可行性商品（Minimum Viable Product，MVP）的概念導入相關必要的資安程序，兼顧資安開發成本與軟體功能上的需求。

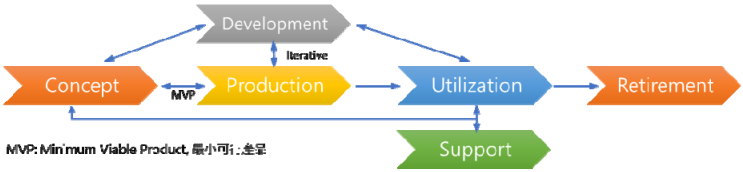


圖 4：ISO 15288:2015

在 SSDLC 的流程中，另外可以參考 NIST CSWP 04232020[3]所定義的平臺安全指引 SSDF（Secure Software Development Framework），如圖 5 中所規範之工具，與安全軟體開發程序整合。

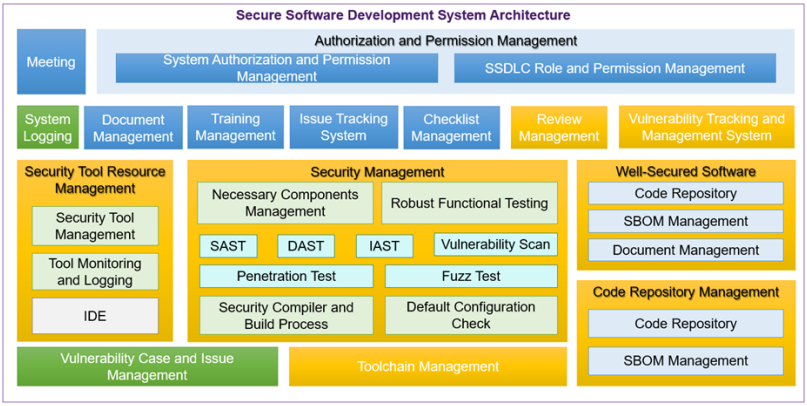
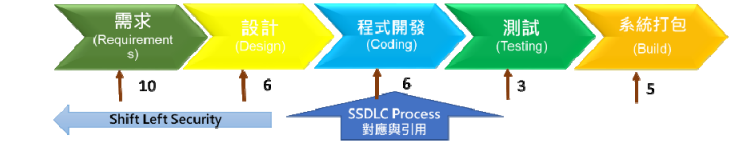


圖 5：SSDF 平臺架構圖

[3] NIST CSWP 04232020 Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF).



Agreement Processes (2)	Organizational Project-Enabling Processes (6)	Technical Management Processes (8)	Technical Processes (14)	
Acquisition	Life Cycle Model Management	Project Planning	Business or Mission Analysis	Verification
Supply	Infrastructure Management	Project Assessment and Control	Stakeholder Needs and Requirements Definition	Transition
	Portfolio Management	Decision Management	System Requirements Definition	Validation
	Human Resource Management	Risk Management	Architecture Definition	Operation
	Quality Management	Configuration Management	Design Definition	Maintenance
	Knowledge Management	Information Management	System Analysis	Disposal
		Measurement	Implementation	
		Quality Assurance	Integration	

圖 6：SSDLC 相關程序之對應及引用時機

在圖 6 中，可以看到 SSDLC 在軟體開發的生命週期每個階段中，都會有需多資安程序需要考慮，但是導入這些安全程序將會產生許多高昂的資安成本，因此可以依據軟體資安等級，動態選擇這些程序之進行的廣度與深度。

在 NIST 2022 的目標中，SSDF 將會考慮往以下 4 個方向：

1. 產出一個對應互動的線上儲存體，可以更容易使用提供主機之間讀取互通的格式。
2. 說明 SSDF 可以對應到 SDLC 開發流程，即可將 DevOps 延伸至 DevSecOps[4]，確保開發風險是可控的，包含了 IT、OT、IoT 的軟體、應用服務環境、韌體與硬體。
3. 特別是將 SSDF 的基礎套用在開源軟體上，提供軟體供應鏈安全。
4. 開發一個真實可以被展現 SSDF 與 SDLC 整合的平臺、安全軟體的開發模式、使用的程式語言與安全檢測的技術。

[4] https://blog.convisoappsec.com/en/is-your-software-supply-chain-secure

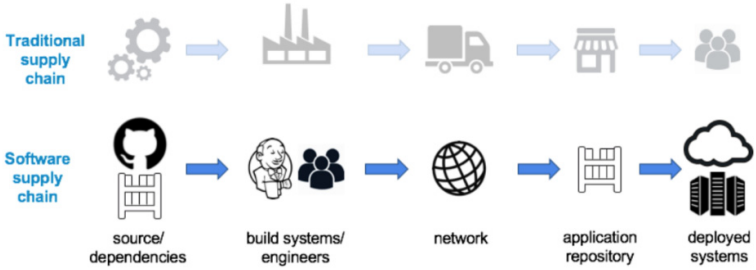


圖 7：軟體供應鏈管理

軟體供應鏈安全 SSCSP（Software Supply Chain Security Paper）的資訊是不間斷更新的，可以參考[5]。從軟體供應鏈管理的角度，要定期稽核軟體提供者（trust by verify），我們必須隨時謹記下面四個原則：

1. 確保所有的程序是一致且有受到品質管控。
2. 確認所有的資源都在流程（pipeline）的管理中，包含了人員、程式碼、流程的相依性與 IT 基礎建設。
3. 確保運作中的程式碼安全，不僅是在儲存設備中的程式碼，也包含在傳輸過程中的程式碼。
4. 確保最後運作中的軟體是充分完成資安檢查，依照規劃進行提供布署。

我們在 CI/CD 的流程中，如圖 7 依據軟體資安等級，參考 SSDF 所定義的安全軟體開發平臺架構，在開發流程中（Pipeline）加入了許多的資安檢核點，其中可以包含靜態應用程式安全測試（Static Application Security Testing，SAST）、動態應用程式安全測試（Dynamic Security Testing，DAST）、軟體物料清單管理（Software

[5] https://github.com/cncf/tag-security/blob/main/supply-chain-security/supply-chain-security-paper/CNCF_SSCP_v1.pdf

Bill of Material，SBOM）、交互式應用程式安全測試（Interactive Application Testing，IAST）等。因此實施安全性左移，做到原生的安全 Secure by Design，是將軟體安全因素 DNA 深植於軟體之中，由 DevOps 演變為 DevSecOps。

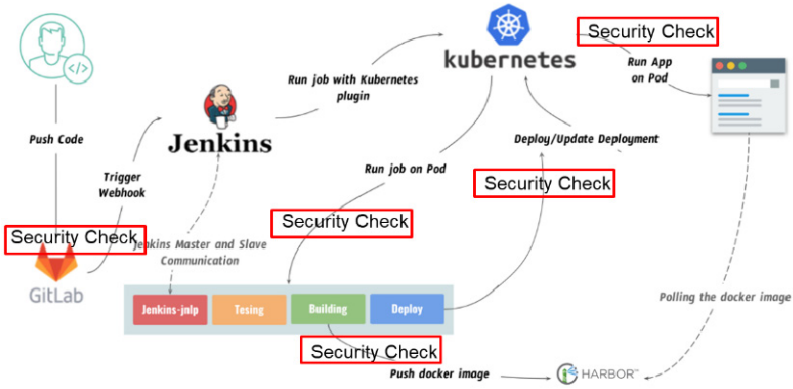


圖 8：CI/CD 整合 SSDLC

參考圖 8 中一個典型的 CI/CD 流程範例，我們在流程中整合了 SSDLC 中所規範的幾個資安檢核點，包括交付程式碼、在容器中執行時、將程式碼儲存到載體這些流程中，都需要資安檢核。

在本文中，過去軟體的安全作業與開發軟體的程序是分開考慮與執行的，軟體人員僅負責撰寫程式碼，軟體布署至生產環境之後，才由資安工程師檢查程式碼，或在運作的環境中建立高牆式的服務，這樣的軟體安全是沒有效率的。因應雲原生世代興起，應用快速布署在雲端環境中，如果在運作環境（production）才偵測到安全問題，必須更新已經撰寫與布署的程式碼，將造成嚴重的成本增加，也讓服務面臨了如零時差攻擊、持續性攻擊與勒索軟體此類的資安威脅之下。

結語

最後，我們要強調的是，DevSecOps 依據軟體商業價值，可能採用的流程與工具可以有許多彈性調整的空間[6]，所以這是一個安全的觀念與文化，其中包含了軟體的開發人員、基礎架構的 IT 團隊、安全專家以及參與軟體交付布署的人員都要進行教育訓練、團隊溝通，建立安全事件的處理流程劇本、並在流程中考慮資安稽核方式與產業合規性，導入雲原生架構中特別需要處理的 API 安全管理，這樣才能真正實現雲原生之軟體安全韌性。

[6] https://csrc.nist.gov/projects/devsecops

多重要素驗證的趨勢發展與分析

羅心妤／東海大學資訊管理學系

https://blog.twnic.tw/2022/12/20/25018/

多重要素驗證[1]的介紹

多重要素驗證（Multi-factor authentication，MFA），又譯多因子認證，是一種身分驗證的方法，它要求使用者要通過兩個或以上的驗證要素後才能獲得授權。MFA 透過將使用者訪問權與多種因素結合，讓常見的網路威脅變得難以成功，因此被認為是保護帳號與憑證的最佳安全方法之一。目前主要的 MFA 身分驗證類型分別為：

- 知識資訊（Something you know）：例如：使用者名稱、密碼
- 持有資訊（Something you have）：例如：獨立的裝置、身分證、提款
- 生物資訊（Something you are）：例如：臉部辨識、指紋辨識
- 位置資訊（Somewhere you are）：例如：IP 位址或地理資訊

MFA 需要符合兩種以上「不同類型」的驗證方法，假設使用指紋辨識與臉部辨識登入，則因為皆屬於「生物資訊」而不符合 MFA，最熟悉的方式莫過於在 ATM 提款時需要放入銀行卡片（Things you have）與輸入提款密碼（Things you know）。

[1] Seth Rosenblatt, Jason Cipriani (2015). Two-factor authentication: What you need to know (FAQ). 檢自：https://www.cnet.com/news/privacy/two-factor-authentication-what-you-need-to-know-faq/ (Nov. 7, 2022).

MFA 的優勢

1. 減少網路釣魚和身分盜用：MFA 需要兩種以上的驗證分法，使駭客更難破解與發動攻擊。
2. 對抗疲勞密碼：使用者為了方便記憶，會設置簡單、易猜測的密碼，或是於不同帳號中重複使用相同密碼，在無形中增加了安全風險。有鑑於此，許多應用程式開始規定複雜的密碼設置標準，迫使密碼已不再是「Something you know」。MFA 的驗證機制不僅可以防止密碼疲勞，也增加了安全緩衝，即使得到了使用者重複的密碼，也無法通過第二階段認證。
3. 簡化安全驗證過程：一次性密碼（one-time password，OTP）通過簡訊或語音發送時間敏感、唯一且隨機的代碼，從而保護基於 Web 的服務、私人憑證和資料。隨著愈漸頻繁的線上交易，MFA 將安全性與應用程式的便利性結合，使客戶能夠簡化登錄，同時保持高安全標準。

意想不到的新攻擊法：MFA 疲勞攻擊

雖然駭客可以使用多種方法繞過 MFA，但大多數都是通過惡意軟體或是網路釣魚攻擊。然而，一種運用社會工程（social engineering）的新方法在近幾個月開始蠻橫地蔓延，那就是「MFA 疲勞攻擊」，亦稱為 MFA 提示轟炸。

MFA 疲勞攻擊的第一步是獲取使用者的基本登入資訊，例如：電子郵件和密碼。一旦攻擊者通過了第一個登入步驟，第二步便是反覆傳送身分驗證確認訊息，希望另一端的人「按錯」或在訊息轟炸下屈服。雖然 MFA 疲勞攻擊不能保證成功，但做為相對簡單的攻擊手法，它可以很容易地規模化擴大攻擊範圍，加大成功的

機率。

駭客組織 Lapsus$運用類似手法在 2022 年攻破了微軟、思科、Okta 和 Uber 等多家國際知名企業[2]。Lapsus$竊取的內容並非皆為企業核心資訊，不會造成過大的實質虧損，然而由此風波所引起的「信任危機」，其傷害將難以估計，此事件也讓數千家組織處於高度警戒狀態。

如何防止 MFA 疲勞攻擊

1. 向客戶提供足夠的資訊、更改太過簡單的驗證要素[3]

根據微軟的研究，大約 1%的使用者會在第一次嘗試時接受簡單的批准請求。因此在驗證中增加「上下文資訊」來吸引使用者目光便能降低「按錯」的機率。例如：在確認通知中放入 IP 登錄位置的地圖資訊，有助於使用者了解登入的來源。此外，針對此類攻擊更有效的方法是調整驗證方式，例如：以輸入螢幕上的一次性密碼，以主動輸入內容替代被動按下選項。

2. 增加認證時的限制[4]

MFA 疲勞利用了「人性」在 MFA 的關鍵弱點，因此只要在登入時設立一些機制便能防範。例如：限制使用者的嘗試驗證次數、增加時間限制，便可以有效制止疲勞攻擊。

---

2 VERGE STAFF (2022). Lapsus$ cyberattacks: the latest news on the hacking group. 檢自：https://www.theverge.com/22998479/lapsus-hacking-group-cyberattacks-news-updates (Nov. 7, 2022).

3 Alex Weinert (2022). Defend your users from MFA fatigue attacks. 檢自：https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677 (Nov. 7, 2022).

4 Joe Köller (2022). MFA Fatigue: Everything You Need to Know About the New Hacking Strategy. 檢自：https://www.tenfold-security.com/en/mfa-fatigue/(Nov. 7, 2022).

3. 緩解登入疲勞－零信任、零密碼

除了源於駭客惡意訊息轟炸的「疲勞」，使用者在日常生活中頻繁收到驗證通知也會造成警覺性「疲勞」。擺脫欺詐性提示的關鍵步驟將是迎接「零密碼」，若是密碼不存在，便不會出現盜取密碼後的 MFA 疲勞攻擊。科技巨頭 Apple、Google 和 Microsoft 在今年 5 月[5]（2022）承諾擴大對 FIDO 標準[6]的支持，以加快無密碼登錄的可用性。

結語

隨著快速攀升的網路攻擊數量以及層出不窮的重大資訊洩漏事件，資訊安全的議題越來越受到重視，在開發新服務或新產品的同時，如何降低其中的資訊安全風險儼然成為重要的考慮因素。

企業可以採用雙管齊下的做法，一方面教育使用者資安知識，例如：如何應對攻擊；另一方面設計兼具簡單快速及安全穩定的驗證方式，抑或是讓產品採用更安全的機制。然而，完美的傳輸機制或安全協定不可能存在，企業必須透過不斷消除網路安全鏈中的關鍵弱點或已知問題，來探討出更合適於環境的新做法。

---

5 PRESS RELEASE OF APPLE. (2022). Apple, Google, and Microsoft commit to expanded support for FIDO standard to accelerate availability of passwordless signins. 檢自：https://www.apple.com/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/(Nov. 7, 2022)

6 FIDO Alliance Specifications Overview. (2022). 檢自：https://fidoalliance.org/specifications/

新型態的網路釣魚

羅心妤／東海大學資訊管理學系

https://blog.twnic.tw/2022/12/12/24997/

「網路釣魚」介紹

網路釣魚是指駭客試圖利用連網裝置欺騙受害者洩露敏感的個人資訊。一旦獲得資訊，詐騙者將使用或出售受害者的資訊來圖利。與去年相比，針對個人的全球勒索軟體攻擊增加了 38% [1]，而未能使用雙重身分驗證等安全工具可能面臨相對較高的風險。

通常網路釣魚不是專注於特定目標，而是將目標訂在在一個大群體中，因為群體中至少會有一名成員把自己放在「鉤子」上。他們透過包含惡意附件的電子郵件、社交媒體訊息、簡訊、電話、虛假網站等工具投下了龐大的網路，一旦潛在受害者開啟損壞的檔案或連結，詐騙者就會利用這個機會獲取個人或財務資訊，接著將惡意軟體下載到他們的電腦上，或是竊取他們的身分等等。

新興網路釣魚類型[2]

1. 語音釣魚（Vishing）

Vishing 是經典騙局的更新，涉及使用網際網路語音協議（Voice over Internet Protocol，VoIP）欺騙家人、朋友、親人、企業、政府

---

1 Grace Macej (2021). Phishing scams are taking advantage of crypto hype. 檢自：https://blog.avast.com/crypto-based-phishing-scams-avast?_ga=2.208117274.989264259.1652181898-1936466448.1652181898 (Jun. 26, 2022).

2 Grace Macej (2022). Which phishing scams are trending in 2022? 檢自：https://blog.avast.com/trending-phishing-scams-2022(Jun. 26, 2022).

官員等的電話號碼。詐騙者透過冒充這些號碼，試圖讓受害者洩露寶貴資訊、購買禮品卡或匯票、籌集保釋金、收取拖欠的稅款等。不幸的是，許多受害者往往是不熟悉技術的高齡者，他們容易相信與情感依賴相關的詐騙。

2. 性勒索詐騙

騙局通常從一封電子郵件開始，詐騙者表示他們擁有包含受害者的影像、電腦螢幕截圖以及其他的圖片和資訊，並威脅要將它們傳送給朋友、家人和僱主，或準備在各種社交平臺上傳播它們。如同語音釣魚一般，此詐騙取抓住不熟悉技術的受害者，並恐嚇受害者放棄有價值的自身資訊或帳戶資料。這些詐騙者幾乎是虛張聲勢，但許多受害者在面臨時間極短的曝光截止日期時，不敢冒著拒絕要求的風險。此外，性勒索因可能造成現實世界中災難性的後果，導致其中牽涉許多自殺案件。

2019 年南韓的「N號房事件」曾經轟動一時，近期 Netflix 上檔紀錄片《網路煉獄：揭發N號房》使此事件重新獲得大眾關注。N號房的初創者「Godgod」鎖定在推特（Twitter）上的國中少女，私訊佯稱已獲得她們的個資，當女孩們點進去附上的釣魚連結後，往往會出現推特或其他網站的重新登錄頁面，如果照樣填寫帳號密碼，加害者便會取得對方的個人照片、學校、住址、手機號碼等資訊，他們會駭入受害者帳戶取得受害者的個人資料及照片，並威脅受害者完成殘酷的性指示。

3. 加密貨幣詐騙

無論加密貨幣市場的長期表現如何，一個無可爭辯的事實是，詐騙者不會落後於加密貨幣的發展方向，它們使用網路釣魚攻擊來誘捕 NFT 投資者的情況並不少見。

加密貨幣詐騙主要的方式是，盜用主要加密貨幣發起人的推

文，滲透到圍繞加密貨幣構建的社群，推薦空投不知名 NFT，再用高額出價引誘至釣魚網站；或是透過一封電子郵件，表示有人將購買受害者的 NFT。那些看似合法的連結，將會連線到一個虛假的 NFT 平臺，受害者可能會無意中洩露加密錢包私鑰。

如何防範網路釣魚

網路釣魚最主要的預防方式，就是「有意識地識別資訊」，可以參考下列做法：

1. 確保電子設備設置為最新版本。
2. 盡量減少是使用密碼管理工具，以減少帳戶被盜用的可能性。
3. 使用雲端硬碟備份重要資料。
4. 與寄件人確認電子郵件，不要隨意點擊可疑鏈接或電子郵件的附件。

結語

詐騙者往往利用人性脆弱與貪婪的時候，或利用受害者對於資訊的不理解，攻防其心理，以進行詐騙。因此，若是剛開始進入不熟悉的領域，謹慎行事更是關鍵，不要隨意分享個人資訊，並避免訪問未知的點擊或可疑連結，每一次分心，都可能掉入等待已久的陷阱。此外，不斷提升資訊安全領域的新知，了解新型的犯罪手法，藉此提高自身的警覺性也顯得非常重要，期望網路釣魚的趨勢可以隨著民眾的認知提升而開始下降。

公用網路上的隱私安全

吳宜庭／東海大學資訊管理學系

https://blog.twnic.tw/2022/08/08/23941/

2022 年，我們處在一個網路非常普遍的時代，在萬物皆連網的情況下，你曾想過當你連接上網路瀏覽網頁或進行其他操作時是安全的嗎？

公用網路與私人網路

隨著新冠疫情的肆虐導致網路使用模式產生改變，人們逐漸習慣使用手機、電腦等電子設備進行上網，生活型態的轉變使得上網無所不在，在原有的工作型態下為了防止機密外洩，多數企業都會在網路邊界系統設有防火牆、偵測系統等多套措施，現今不論在家中、學校、公司甚至出門在外網路變得非常重要。

一般我們在咖啡廳、百貨公司或是飯店等公共場所所連接到的 Wi-Fi 熱點可稱為**公用網路**，對於許多人來說，在外能連接到免費網路似乎是個理想的選擇，但是當使用者連線至公用區域時，並不知道連在這個區域的其他使用者有誰，所以也不會意識到會不會因為使用了這個公用網路而使個資或是重要資料遭受到駭客偷竊。

在家中透過自己的路由器所架設的 Wi-Fi 或是組織中如學校，公司所提供的網路可稱為**私人網路**，私人網路通常是可控制的，想連接至私人網路必須要有存取權限才可連線，私人網路會有個管理者控管著所有連線者，以防範未知連線者的有意破壞。

公用網路有哪些不安全

公用網路的開放網域相對於私人網路來說可能會因為資安人員的不足或是防火牆設置不全導致入侵容易，並在其中植入惡意程式竊取個人資料，形成駭客最佳的入門管道。[1]公共 Wi-Fi 若遭受入侵後，可能形成攔截雙方之間的通訊的中間人攻擊（Man in the Middle attack）、以假 Wi-Fi 熱點收集到連接此設備的資料、利用特定電腦程式攔截封包或是 Cookie 偷竊與 Session 劫持等網路攻擊。[2]

VPN 是什麼

近期時常在 YouTube 平臺觀看的影片中出現某家 VPN 廠商的業配廣告，廣告中時常提到：「使用 VPN 可以保護您的線上隱私權並保護您的資訊不受駭客、網際網路服務供應商和其他第三方的影響」，然而這個 VPN 究竟是什麼呢？

虛擬私人網路（virtual private network，VPN）是在公共網路基礎設施（例如：全球網際網路）中建構的專用網路。專用網路的特點是他僅提供給授權用戶允許他們存取特定區域中各種網路相關的服務與資源。[3]

常見的 VPN 協議有：OpenVPN、點對點通道通訊協定（Point

---

1 教育部全民資安素養網（2021）. Wi-Fi 走到哪連到哪？一不小心就連到地雷啦！檢自：https://isafe.moe.edu.tw/article/2508?user_type=4&topic =9(Jul. 11, 2022).

2 Binance (2019). 為何公共 Wifi 是不安全的. 檢自：https://academy.binance.com/zt/articles/why-public-wifi-is-insecure(Jul. 11, 2022)

3 Paul Ferguson & Geoff Huston(1998). What is a VPN? 檢自：https://cpham.perso.univ-pau.fr/ENSEIGNEMENT/COMMUN/vpn_ferguson.pdf(Jul. 11, 2022).

to Point Tunneling Protocol，PPTP）、第二層隧道協定（Layer Two Tunneling Protocol，L2TP）、安全通訊端通道通訊協定（Secure Socket Tunneling Protocol，SSTP）與網際網路金鑰交換（Internet Key Exchange v2，IKEv2），簡略的 VPN 協議介紹如表 1[4]，VPN 透過加密隧道的方式連接使用者與遠端 VPN 伺服器，使用者可以從用戶端進入開放網路區域。例如：身在臺灣的用戶透過電腦或手機連接至位於美國的 VPN 伺服器，瀏覽網站時，這位用戶的位置就不再是原本的 IP 位置，而是 VPN 伺服器的位置。這種使用方式是大多人最常見的，也是所謂的「翻牆」。在部分國家因為法規政策的緣故 VPN 是被禁止使用。

表 1：VPN 協議介紹

VPN 協議	簡介
OpenVPN	目前被使用最廣泛使用的協議之一，為開源VPN協議，支持各種加密運算法所以有著高度的安全性。
點對點通道通訊協定（PPTP）	最早被廣泛使用的 VPN 通訊協議，但由於加密的安全性弱而有很多安全漏洞。
第二層隧道協定（L2TP/IPsec）	被廣泛使用建立通道連結，沒有加密或驗證身分技術，僅依靠 IPSec 加密技術。
安全通訊端通道通訊協定（SSTP）	微軟所開發 VPN 通訊協議，在增強隱密性和翻牆上皆很出色，但其他平臺上不易安裝使用。
網際網路金鑰交換（IKEv2/IPsec）	支援身分驗證和加密，傳輸占用的頻寬少、速度快，透過 IPSec 安全協議配合使用後，因此成為行動裝置傳輸通訊最可靠的 VPN 協定。

[4] Hacyber (2021).【VPN 協議】7 種通訊 VPN 協定比較. 檢自：https://hacyber.com/vpn-protocols/ (Jul. 11, 2022).

好的 VPN 應具有「無記錄」（zero logs）政策。安全的 VPN 只會記錄最少量的基本連線資料，如頻寬使用率、伺服器負載量或位置，這是用於優化服務而不能用於識別用戶。[5]

隱私的防範

雖然 VPN 可以保護上網的安全，也可以將內部網路延伸更遠的區域，但 VPN 的保護不是一定的，許多家廠商也曾遭受到駭客攻擊或是出現資安漏洞，如在 2019 年與 2020 年時數家資訊設備公司的 VPN 產品皆出現資安漏洞，這可能讓攻擊者不須驗證其身分即可進入單位的內部網路，竊取相關資訊。[6]

因此使用者除了使用 VPN 防止資料遭受到竊取外，在外選擇 Wi-Fi 使用時，應選擇有密碼保護的 Wi-Fi 進行存取；在瀏覽網頁時尋找鎖形圖示，盡可能使用「HTTPS」加密的網頁；留意不安全連線的警告等。並不是只有使用公用網路才有可能遭受資安威脅，許多中小企業所面臨到的攻擊也可能是來自簡單的地方，如：釣魚信件或是軟體未定期更新等，所以我們應該加強使用網路的安全觀念與注意來歷不明的連結，為自己的隱私做到有效的防護。

---

5 TWNIC. (2019). 如何選擇可靠的 VPN. 檢自：https://blog.twnic.tw/2019/12/06/5520/(Jul. 11, 2022).

6 TWNIC. (2020). 近期多家 VPN 設備資安漏洞，相關單位應立即檢視以降低資安威脅. 檢自：https://blog.twnic.tw/2020/01/31/6051/(Jul. 11, 2022).

淺談網路犯罪、網路戰與網路攻擊之分際線

林昕璇／中國文化大學法律學系助理教授

https://blog.twnic.tw/2022/11/11/24730/

網路犯罪側觀

一、概述

網路攻擊與網路犯罪的區分界線及法律評價，伴隨著網路活動的日益蓬勃發展，逐漸發展為重要法律議題。但網路攻擊、網路戰與網路犯罪三者間之概念內涵仍處於發展階段，因對於確切之界定範圍仍存在些許模糊地帶，亟待釐清。

雖然網路犯罪尚無完整明確界定，但現已存在一般性的定義為：「任何使用電腦、網路或硬體設備促成或實施的犯罪（any crime that is facilitated or committed using a computer, network, or hardware device.）」。相較於網路攻擊與網路戰，網路犯罪所涵蓋的範圍甚為廣泛，涵蓋網路詐騙、線上盜版、線上散布兒少色情、入侵電腦（computer intrusions）等。與網路攻擊不同，網路犯罪不以破壞電腦網路為前提，且多數不以政治或國家安全為目的。

二、網路犯罪之代表性行為態樣[1]

1. 惡意軟體攻擊

惡意軟體攻擊乃係網路犯罪分子透過惡意軟體攻擊電腦系

[1] What is cybercrime? How to protect yourself from cybercrime. 檢自：https://www.kaspersky.com/resource-center/threats/what-is-cybercrime (2022. Oct. 10).

統。而使得受惡意軟體攻擊的電腦會被用於其他非法之多種用途目的。其態樣包括竊取機密數據、使用電腦進行其他犯罪行為或對數據造成損害等。惡意軟體攻擊的代表性案件當屬發生於 2017 年 5 月之 WannaCry 勒索軟體攻擊事件。當時網路駭客利用程式透過網際網路對全球執行 Microsoft Windows 作業系統的電腦進行攻擊加密型勒索軟體兼蠕蟲病毒攻擊，涵蓋西班牙電信、英國國民保健署、聯邦快遞和德國鐵路股份公司等總計 150 個國家、共 230,000 台電腦受到波及影響，公私部門因此遭到駭客勒索支付比特幣贖金以重新獲得存取權限，並導致在全球範圍約 40 億美元的經濟損失。

2. 網路釣魚（Phishing）

網路釣魚活動係指發送垃圾郵件或其他形式的通訊，以誘騙收件人做出破壞其資訊網路安全的事情。網路釣魚活動訊息可能涵蓋指向惡意網站的連結，或者透過垃圾郵件誘使郵件接收者回覆機密資訊。

2018 年於俄羅斯世界盃期間瀰漫的「大規模網路釣魚詐騙」事件，具有高度爭議。事實背景涉及駭客發送給球迷的電子郵件，此等垃圾郵件試圖通過誘騙收件人得以免費前往舉辦世界杯的莫斯科來吸引，導致誤點擊這些電子郵件中的使用者的個人數據被盜。另一種網路釣魚活動稱為「魚叉式網路釣魚」，相較於大規模網路釣魚詐騙，是更具有針對性的資訊安全危害行為，試圖誘騙特定個人危害他們服務之組織企業的資訊安全。與大規模網路釣魚不同，魚叉式網路釣魚郵件通常經過精心設計，例如：他們看起來像是來自 CEO 或 IT 經理，使其看似像是來自可信來源的郵件，進而操縱網路使用者對網路系統輸入不實資料或程式以達到網路詐欺之效果。

3. 分散式 DoS 攻擊（Distributed DoS attacks）

分散式 DoS 攻擊（DDoS）則為駭客用以破壞計算機系統的典型網路犯罪態樣。DDoS 攻擊通過使用標準通信協議之一向系統發送連接請求的垃圾訊息，從而使系統不堪重負。進行網路勒索的網路犯罪分子可能會利用 DDoS 攻擊的威脅來索要金錢。或者，當另一種類型的網路犯罪發生時，DDoS 可能被用作分散注意力的策略。此類攻擊的一個著名示例乃係 2017 年對英國國家彩票網站的 DDoS 攻擊。網路駭客針對英國國家彩票發動 DDoS 攻擊。癱瘓彩票網站 www.national-lottery.co.uk 及使其移動應用程式離線，進而導致英國公民無法正常購買彩票，益彰顯駭客透過 DDoS 將為線上科技平臺的資安風險增添新的變數。

網路犯罪、網路攻擊與網路戰之區辨

從 Oona A. Hathaway, Rebecca Crootof 等學者所整理的彙整清楚凸顯了網路戰、網路攻擊與網路犯罪三者各自應具備之核心內涵[2]。從下表可知，第一、網路犯罪僅涉及非國家行為者所發動者為限。再者、其必須以透過電腦系統進而違反刑事法律為前提。相較之下，網路攻擊與網路戰則以側重基於國安或政治性目的，抑或者以影響層面必須達到「武裝衝突」之程度且必須在武裝衝突的情境脈絡下發端，始足當之。換言之，現代通訊的迅猛發展提供將傳統於實體法律場域所發生的各種法律行為態樣，移轉於虛擬空間的契機與條件，但卻也因此衍生諸多法律評價與概念解釋的灰色空間。

[2] Hathaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2012). The law of cyber-attack. Calif. L. Rev., 100, 817.

TABLE 1: Essential characteristics of different cyber-actions

	Type of cyber-action		
	Cyber-attack	*Cyber-crime*	*Cyber-warfare*
Involves only non–state actors		√	
Must be violation of criminal law, committed by means of a computer system		√	
Objective must be to undermine the function of a computer network	√		√
Must have a political or national security purpose	√		√
Effects must be equivalent to an "armed attack," or activity must occur in the context of armed conflict			√

圖 1：網路犯罪、網路攻擊與網路戰的區辨要素

資料來源：Hathaway et al. (2012).

FIGURE 1: Relationship between cyber-actions

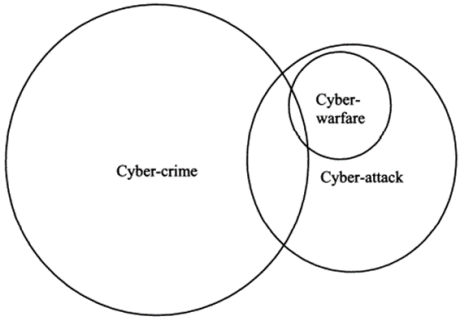


圖 2：網路犯罪、網路攻擊與網路戰之聯集圖

資料來源：Hathaway et al. (2012).

大多數網路犯罪不構成網路攻擊或網路戰（如圖 2 所示）。當非國家行為體的行為違反內國法或國際法而為犯罪時，這個行為只是網路犯罪（"An act is only a cyber-crime when a non-state actor commits an act that is criminalized under domestic or international law."）。Oona A. Hathaway, Rebecca Crootof 等學者於〈The Law of

Cyber-Attack〉一文中列出以下三項屬於網路犯罪但非為網路攻擊的例子：

1. 非國家行為體透過電腦網路，以政治或國家安全為目的，但不破壞電腦網路。如因在網路上發表政治意義言論而犯罪、個人出於政治性目的入侵銀行系統竊取資料。
2. 非國家行為體透過電腦網路實行非法行為，且破壞電腦網路，但非出於政治或國家安全之目的。如駭客破壞銀行系統以攫取金錢利益。
3. 非國家行為體透過電腦計算機從事非法行為，但不破壞電腦網路的功能，也不以政治或國家安全為目的。如散布兒童色情內容。

如圖 2 所示，如同某些網路犯罪既非網路攻擊亦非網路戰，某些網路攻擊既非網路犯罪亦非網路戰。以下兩種情況為在符合網路攻擊的定義下，僅該當網路攻擊（cyber-attack-only scenario）：

1. 國家行為體在非武裝衝突背景下所實施之未達武裝攻擊標準之網路攻擊。如 2011 年中國政府對法輪功網站的攻擊。
2. 非國家行為體所實施，未達武裝攻擊標準且不構成網路犯罪之攻擊，原因可能為法律漏未規定或未使用基於電腦的手段。

網路犯罪之行為主體必為非國家行為者，網路犯罪與網路攻擊之重疊處發生在非國家行為體以政治或國家安全為目的，透過電腦網路實施非法行為而破壞電腦網路時，若該行為上升至武裝衝突的程度則會構成網路戰。假設以一群人入侵美國國務院的伺服器，並出於對美國政府的蔑視而將該伺服器關閉。非國家行為體出於政治性因素入侵並破壞電腦網路，上述行為即同屬網路犯罪與網路攻擊。

同理可證，網路戰必構成網路攻擊。圖 2 中網路戰與網路攻擊之重疊包含兩種型態的攻擊：

1. 第一類包含任何於武裝衝突背景下實施的網路攻擊，但不構成戰爭罪或不使用基於電腦的方法，或兩者均無。
2. 第二類包含國家行為體實施與常規武裝攻擊（a conventional armed attack）效果相當之網路攻擊者。該使用武力可能為適法或不適法，但若行為主體係國家行為體，則不該當於網路犯罪。

結語

揆諸實際，網路攻擊以及現有法律（戰爭法、國際條約、內國刑法）的監管，戰爭法僅得於構成武裝攻擊或發生在武裝衝突背景下的網路攻擊提供的框架，實已對於物聯網世界中伴隨而生的資訊安全的法律規範體系構成挑戰。由 Oona A. Hathaway, Rebecca Crootof 等學者致力共著的《The Law of Cyber-Attack》一文從定義內涵的角度，將固有學說始終難以明確切割的網路犯罪、網路攻擊、網路戰做出如上文所討論之區辨要素及交集圖之切割，實有助於學理釐清長久存在的概念上的混亂和模糊地帶。

誠如學者積極呼籲應及早建立全新的、全面法律框架以更有效的應對網路攻擊。以美國為首的世界強權固然可藉由賦予內國刑法處理網路攻擊的域外效力（extra territorial effect）、採取國際法允許的有限度的反制措施處理戰爭法無法處理的網路攻擊。然而，從犯罪偵查的角度觀之，有鑑於所謂網路犯罪往往具備身分隱密、證據難以取得追索以及跨國管轄的本質特性。因此僅仰賴各國之內國法實已無法周延完整應對挑戰。在此基礎上，國際合作可謂提供國際間必須為網路攻擊、網路犯罪及網路戰的定義達成一致、同時釐清概念涵攝上的混亂，方得為資訊共享、證據蒐集和對涉案人員的刑事訴訟開展更廣泛的國際合作，構築穩健發展之基礎。

無密碼時代

吳幸芳／東海大學資訊管理學系

https://blog.twnic.tw/2022/09/08/24170/

何謂無密碼身分驗證

密碼能使人們在網際網路上的資訊多一層隱私，也同時成為資料安全保護機制中的一項弱點，根據 Verizon 2022 年的研究報告顯示[1]，超過 80%的數據洩露是由密碼薄弱或洩露所造成。由此可知，密碼可能被共享、猜測或竊取，導致資料外洩，無法完全的保護使用者資訊，逐漸出現密碼產生器（random password generator）、密碼管理員和多重要素驗證（Multi-factor authentication，MFA）等機制，以加強密碼的強度。

現今，無密碼時代正在發展，無密碼身分驗證能使使用者無需創建和輸入密碼或回答安全問題即可登入，但不代表使用者無須進行任何形式的身分驗證即可直接進入網站，仍須通過多種身分驗證形式，以證明是否為本人，例如：設備 PIN 或指紋辨識等。通常會與多重要素驗證或單點登錄（Single Sign-On，SSO）結合使用[2]，以改善用戶體驗、增強安全性並降低營運費用和複雜性。

無密碼身分認證之優點包含以下幾項[3]：

---

1 Verizon. (2022). 2022 data breach investigations report. 檢自：https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf (Jul. 04, 2022).

2 CyberArk (2022). Passwordless Authentication. 檢自：https://www.cyberark.com/zh-hant/what-is/passwordless-authentication/ (Jul. 05, 2022).

3 JumpCloud (2022). The Benefits and Challenges of Passwordless Authentication. 檢自：https://jumpcloud.com/blog/benefits-challenges-passwordless-authentication

1. 更強的網路安全環境

根據 SpyCloud 的研究報告顯示[4]，擁有多組外洩密碼的用戶中，有 64%會為多個帳戶重複使用類似的密碼，因此若密碼遭洩漏，攻擊者可訪問多個帳戶獲取機密數據，造成公司或使用者巨大損失。無密碼身分驗證可對最普遍的網路攻擊進行保護–網路釣魚，代表即使使用者收到網路釣魚電子郵件或連上網路釣魚網站，用戶並沒有密碼可以提供。加上創建虛假的一次性密碼（One-Time Password，OTP）、發送通知或指紋來進行身分驗證是相當困難的，種種因素皆提升用戶的網路安全環境。

2. 更好用戶體驗和更高的生產力

人的記憶有限，生成和記住數百個密碼是不可實現的，因為忘記密碼導致用戶不便，久而久之使用簡單的密碼便處處可見。況且根據 iProov 所發布的研究顯示[5]，消費者會因忘記密碼而放棄線上購物。使用無密碼身分驗證後，這些問題都迎刃而解，並且便捷的登入能夠減少用戶花在管理密碼上的時間，可用於其他更有意義的事物。

3. 降低長期成本

Forrester 報告稱[6]，美國組織每年用於與密碼相關的費用超過

(Jul. 05, 2022).

4 Business Wire. (2022). SpyCloud 2022 Identity Exposure Report: Majority of Consumers Have Poor Password Hygiene. 檢自：https://www.businesswire.com/news/home/20220302005209/en/SpyCloud-2022-Identity-Exposure-Report-Majority-of-Consumers-Have-Poor-Password-Hygiene (Jul. 05, 2022).

5 iProov. (2020). The End of the Password: 50% Of Young Consumers Share Their Log-in Details. 檢自：https://www.iproov.com/blog/the-end-of-passwords-iproov-consumer-survey (Jul. 05, 2022).

6 Forrester (2018). Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers. 檢自：https://www.keepersecurity.com/ assets/pdf/Keeper-White-Paper-Forrester-Report.pdf (Jul. 06, 2022).

100 萬美元。若使用無密碼身分身分驗證，長期下來可大幅降低成本。不再存儲密碼、重置忘記的密碼，也不再因資料可能外洩而煩惱。

FIDO

FIDO（Fast IDentity Online）聯盟[7]其使命為「身分驗證標準」，以幫助人們減少對密碼的過度依賴。FIDO 聯盟促進認證和設備認證標準的開發、使用和遵守。FIDO 協議為 FIDO 聯盟[8]所制定的一套網路識別標準，意在確保登入流程中伺服器及終端裝置協定的安全性。FIDO 協議使用公開金鑰加密技術、多重要素認證與生物辨識特性進行認證，來提供更強的身分驗證。同時 FIDO 聯盟也確保所有利用 FIDO 核心規範的產品能夠協同工作，以提升全球無密碼身分驗證的兼容性和標準化。

FIDO 聯盟目前發布三種用戶身分驗證規範[9]，分別為 FIDO UAF（FIDO Universal Authentication Framework）、FIDO U2F（FIDO Universal Second Factor）以及 FIDO2。CTAP（Client to Authenticator Protocols）是對全球資訊網協會（World Wide Web Consortium，W3C）的 Web 身分驗證（W3C's Web Authentication，WebAuthn）的補充規範，稱為 FIDO2。

以下為 FIDO 核心規範介紹：

---

7 FIDO. (no). Alliance Overview. 檢自：https://fidoalliance.org/overview/ (Jul. 06, 2022)

8 HENNGE (2021). FIDO 是什麼？無密碼時代的來臨. 檢自：https://hennge.com/tw/blog/what-is-fido.html (Jul. 06, 2022).

9 FIDO. (no). FIDO Alliance Specifications Overview. 檢自：https://fidoalliance.org/specifications/ (Jul. 12, 2022).

1. FIDO UAF

用戶安裝 FIDO UAF 堆疊（Stack）設備後，可以選擇在終端裝置上透過各種生物辨識等方式，例如：輸入 PIN、聲音辨識、指紋辨識，即可進行線上登入。結合生物辨識等認證途徑，提供使用者順暢的無密碼登入體驗。

2. FIDO U2F

FIDO U2F 允許雙因素驗證，用戶登入時需添加第二個驗證因素，以證明是否為本人，增強現有密碼基礎設施的安全性。該服務還可以在其選擇的任何時間提示用戶提供第二因素設備，例如：FIDO 安全密鑰。

3. FIDO2

FIDO2 由 WebAuthn 規範和 Client to Authenticator Protocol（CTAP）組成。FIDO2 通過嵌入式身分驗證，例如：生物識別或 PIN，或用外部身分驗證，例如：FIDO 安全密鑰、行動設備、可穿戴設備等，以支持無密碼、第二因素和多因素用戶體驗。

目前無密碼發展

今年 Apple、Google 和微軟已承諾[10]在未來一年正式支援 W3C 以及 FIDO 聯盟所制定的「無密碼登入」標準，希望能在不同系統的裝置之間，省去輸入密碼的步驟，利用生物辨識完成快速登入，無需密碼也作為帳戶恢復方法。三家科技巨頭公司也一同公告[11]

[10] The verge. (2022). Apple, Google, and Microsoft will soon implement passwordless sign-in on all major platforms. 檢自：https://www.theverge.com/2022/5/5/23057646/apple-google-microsoft-passwordless-sign-in-fido (Jul. 06, 2022).

[11] Apple. (2022). Apple, Google, and Microsoft commit to expanded support for FIDO standard to accelerate availability of passwordless sign-ins. 檢自：https://www.apple.com/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/ (Jul. 13, 2022).

未來為用戶提供兩種新功能，以實現更加無縫和安全的無密碼登錄：

1. 允許用戶在各種設備或新設備上利用 FIDO 進行自動登入，而無需為每個帳戶重新註冊。
2. 使用戶能夠在行動裝置上使用 FIDO 身分驗證，以登入附近設備上的網站或應用程式，不管所運行的操作系統平臺或瀏覽器為何。

結語

密碼的出現使資料不直接暴露在網際網路上，但也因此成為駭客攻擊的重點之一。無密碼身分驗證的出現，能讓我們擁有更強的網路安全環境、更好的用戶體驗和更高的生產力以及可降低長期成本。為了減少對密碼的依賴性，FIDO 聯盟發布三種用戶身分驗證規範 FIDO UAF、FIDO U2F 以及 FIDO2。Apple、Google 和微軟宣布在未來將支援「無密碼登入」標準，為使用者提供更流暢的登入體驗。無密碼身分驗證能改善密碼所帶來的問題，但若要全面使用無密碼登入，首先要改變的是使用者是否願意跨出舒適圈，嘗試使用「無密碼登入」。

物聯網所面臨的資安威脅

吳宜庭／東海大學資訊管理學系

https://blog.twnic.tw/2022/06/10/23311/

什麼是物聯網？

物聯網（Internet of Things，IoT）或稱萬物聯網（The Internet of Everything，IoE）是近年新興流行的科技趨勢，生活周遭的所有智慧產品皆有可能與網路互相連結。最早在 1999 年美國麻省理工學院的自動化辨識系統中心（MIT Auto ID Center）簡單地闡述了物聯網的涵義：「萬物皆可透過網路互連」。

而在 2005 年國際電信聯盟（The International Telecommunication Union，ITU）發布的物聯網報告[1]也提到：「將短距離行動接收器嵌入到各種附加的小工具和日常用品中，使其變得更加智慧，從而實現人與物之間以及物與物之間的新通訊形式。」

最初物聯網的實作在 1980 年代，由於一群程式設計師不想每次下樓到了可樂販賣機面前卻發現可樂已經售罄或是可樂不夠冰涼，進而將販賣機接上網路，並寫程式時時監控販賣機的可樂數量與可樂的溫度，因為人們的小偷懶，演進了物聯網最初的應用。隨著技術持續進步，從個人、家庭到社會領域，如：工業製造、農業生產、健康醫療、物流運輸，皆有物聯網的應用。

基礎的物聯網架構包含了感知層、網路層與應用層，藉由產品中的感測器蒐集資料並透過網路的方式將資料傳輸至雲端或本地

[1] ITU. (2005). ITU Internet Reports 2005: The Internet of Things. 檢自：https://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf(May. 07, 2022).

平臺，再利用軟體將資料進行處理後呈現給用戶，甚至可以結合人工智慧（Artificial Intelligence，AI）或機器學習更深入的分析資料，為將來的行為做些預測。

物聯網的安全隱患

物聯網的高速成長以及廣泛的應用同時也帶來了許多資安的威脅，在世界經濟論壇（The World Economic Forum，WEF）的一份報告[2]中指到：「網路安全將列為 IoT 技術的最大擔憂」。所有人皆可透過物聯網設備得到一些資訊，那也可能被有心人士鑽漏洞，或藉由誘導方式竊取到重要資訊。

根據 SonicWall 發表的《2021 年 SonicWall 網路威脅報告》[3]中提及：「醫療保健行業的物聯網遭到惡意軟體攻擊的比率增幅最大」，醫療保健的惡意軟體攻擊方式也與以往不同，惡意軟體透過盜版、破解版和未更新等弱點進而攻擊網站伺服器。

在 2020 年 Nokia 的威脅情報報告中也講述：「物聯網設備占行動網路受感染設備的 32.72%，及物聯網設備的漏洞之一在於駭客能否直接看到 IP 位址，透過 IP 位址的追蹤，物聯網設備感染病毒的機率就會升高。」[4]

今年（2022）年初，國外案例一名少年透過 Tesla 第三方開源

---

2 WEF. (2015). Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. 檢自：https://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf(May. 07, 2022)

3 Jessica Davis (2022). Healthcare sector saw largest increase in IoT malware attacks in 2021. 檢自：https://www.scmagazine.com/analysis/iot/healthcare-sector-saw-largest-increase-in-iot-malware-attacks-in-2021-report-confirms (May. 07, 2022).

4 Nick Wood (2020). Nokia warns IoT malware infection rate has doubled. 檢自：https://telecoms.com/507055/nokia-warns-iot-malware-infection-rate-has-doubled/ (May. 07, 2022).

軟體（TeslaMate）中的一漏洞，入侵 13 個國家中的 25 輛 Tesla 電動車，以遠端操作車輛並駭入車鑰匙軟體以獲取車主電子信箱，不僅如此，因為網路儀表板的安全漏洞導致許多用戶資訊及車輛資訊皆暴露在網路上。

而在近幾年來，因為 COVID-19 的緣故，人們比起過往任何時候都更依賴網路服務。而隨著科技的發展，物聯網設備日漸增加，分散式阻斷服務攻擊（Distributed Denial of Service attacks，DDoS）的攻擊對象日漸增加，透過 DDoS 控制眾多設備，並將其流量導向特定目標，迫使受害設備必須暫時中斷或停止服務。

結語

面對大量的網路攻擊，這些物聯網設備也必須制定相對應的安全方案及適當的保護特定的系統，每一個物聯網裝置與雲端設備的軟硬體更新與修補程式管理就更加重要，在帳號管理的部分也需要適當的維護與管理。

針對上述的舉例可列出以下的應對方法：

1. IP 位址追蹤：若企業使用經 NAT（Network Address Translation）處理的網路，將 IP 位址經過轉換則會使駭客不易追蹤，因此可望降低物聯網設備的感染率。
2. 智慧電動車：目前在設計智慧電動車時的安全性大多不周全，當資訊通訊介面整合時，所帶來的便利性更加了不少，但系統整合的複雜性也可能相對地提高衍生漏洞的風險，企業、國家皆在制定車聯網安全防護體系。
3. 個人周邊設備的防護：可以加強使用的密碼強度、確保周邊所有設備的軟體都是最新版，並且加強網路防火牆的設置。

隨著新興科技的發展，網際網路的影響範圍逐漸擴大，相對的應用領域也越來越廣闊，所有與物聯網技術相關的設備、場域也需

更加警惕來自各種不同的網路攻擊，不僅僅只有在設備上強調資安，每個人也需要建立更強的資安意識，以保護自身的重要資料，以免暴露在網上遭人威脅或被他人所侵害。

數位供應鏈的網路安全挑戰

吳幸芳／東海大學資訊管理學系

https://blog.twnic.tw/2022/06/09/23321/

何謂數位供應鏈

供應鏈[1]是一個全球供應網路，該網路包含產品從原材料採購到生產和交付給最終客戶的過程。傳統的供應鏈和供應鏈管理只關注生產和供應，而不是客戶需求，缺乏快速發現價值鏈上的問題，進而損害客戶滿意度和企業利潤。因此從傳統供應鏈中發展出的數位供應鏈（digital supply chain）[2]是動態的，利用先進的 IT 技術來快速適應不斷變化的環境，讓公司可以更快地交付產品，為客戶提供客製化服務。根據 McKinsey 研究[3]發現，大部分已將供應鏈數位化的公司可以將其收入提高 3.2%，年收入平均增長 2.3%。

數位供應鏈所使用的 IT 技術包含以下十項[4]：

1. 雲計算和軟體即服務（Cloud Computing and Software-as-a-Service，SaaS）

---

1 Investopedia. (2021). Supply Chain. 檢自：https://www.investopedia.com/terms/s/supplychain.asp (Apr. 30, 2022).

2 Oracle Netsuite (2020). Digital Supply Chain Explained. 檢自：https://www.netsuite.com/ portal/resource/articles/erp/digital-supply-chain.shtml (Apr. 30, 2022).

3 McKinsey & company (2017). Digital transformation: Raising supply-chain performance to new levels. 檢自：https://www.mckinsey.com/business-functions/operations/our-insights/digital-transformation-raising-supply-chain-performance-to-new-levels (May 9, 2022).

4 Reciprocity. (2021). Traditional Supply Chain vs. Digital Supply Chain. 檢自：https://reciprocity.com/blog/traditional-supply-chain-vs-digital-supply-chain/ (Apr. 30, 2022).

2. 人工智慧（Artificial Intelligence，AI）
3. 機器學習（Machine Learning，ML）
4. 自然語言處理（Natural Language Processing，NLP）
5. 大數據（Big data）
6. 商業智慧（Business Intelligence，BI）
7. 虛擬實境和擴增實境（Virtual reality and Augmented reality，VR/AR）
8. 機器人技術和機器人過程自動化（Robotics and Robotic Process Automation，RPA）
9. 物聯網（Internet of things，IoT）

這些技術提供自動化和提升預測分析能力，使公司能夠縮短產品上市時間、快速預測和解決問題、縮短規劃週期、改進決策制定並為所有利益相關者創造價值。

供應鏈網路安全問題

然而根據 McKinsey 研究[5]，只有 43%的公司使用數位供應鏈。借助數位供應鏈，雖然可以幫助公司提高收入、擁有更好的決策和更敏捷的流程，但數位供應鏈也伴隨著一些挑戰[6]，包含不連貫的系統、不良的用戶體驗、無法管理版權、過時的產品資訊等問題。其中，影響最大的問題是使用 IT 技術來支持整個系統運作時，所伴隨而來的網路安全風險問題。Gartner 為一家在美國從事資訊科

[5] McKinsey & company (2017). Digital transformation: Raising supply-chain performance to new levels. 檢自：https://www.mckinsey.com/business-functions/operations/our-insights/digital-transformation-raising-supply-chain-performance-to-new-levels (May 9, 2022).

[6] SoftwareONE. (2021). Digital Supply Chain 5 Common Challenges. 檢自：https://www.softwareone.com/en/blog/all-articles/2020/04/27/5-common-challenges-along-the-digital-supply-chain(May. 11, 2022).

技研究和顧問的公司，已將數位供應鏈風險定為一種新的安全威脅，並認列為 2022 年七大安全和風險管理的趨勢之一[7]。

以下為造成供應商網路安全問題的原因[8]：

1. 人為因素

人為因素常常是網路安全的漏洞，加上數位供應鏈上的組成成員可互相連線，因此無論是有意還是無意的疏忽皆會對整個供應鏈構成重大風險。例如：網路犯罪者通過手段侵入，獲得電子郵件系統的存取權限，了解工作原則和流程後，假裝是供應鏈的供應商，並誘使企業匯入大筆資金。美國證券交易委員會已發出警告，強調供應鏈中的商務電子郵件入侵（Business Email Compromise，BEC）攻擊加劇。

2. 缺乏供應商風險管理（Vendor Risk Management，VRM）

企業在選擇供應商時除了需事先對公司進行調查，了解供應商和第三方對環境帶來的風險，還必須嚴格的監控供應商流程，定期評估供應商的風險情形是否有所變化。

3. 第三方應用程式漏洞

數位供應鏈上企業也會採用第三方工具來構建產品和服務，例如：支付、分析、廣告等等行為會外包給其他企業進行，此舉動會為企業帶來風險，使保護數據隱私變得具有挑戰性。然而大多數的網站不會監督整合的第三方 JavaScript 指令，並且缺乏針對

---

7 Gartner (2022). Gartner Identifies Top Security and Risk Management Trends for 2022. 檢自：https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022 (May. 13, 2022).

8 Supply & Demand Chain Executive (2021). 5 Major Security Threats to the Digital Supply Chain in 2021. 檢自：https://www.sdcexec.com/safety-security/risk-compliance/article/21259409/knowbe4-5-major-security-threats-to-the-digital-supply-chain-in-2021(May. 14, 2022).

Magecart、表單劫持和信用卡資料劫持等攻擊的網路安全控制作法。

網路犯罪者發現可藉由攻擊數位供應鏈帶來高投資回報，因此越來越多的網路犯罪者利用小型公司的供應鏈漏洞作為訪問大型公司的手段。Gartner 預測[9]，到 2025 年，全球有 45%組織的數位供應鏈將遭受攻擊。

近年的供應鏈攻擊事件

SolarWinds 供應鏈攻擊事件是 21 世紀最大的網路安全漏洞[10]，SolarWinds 為一間幫助企業管理網路、系統和資訊技術基礎設施，提供網路設備監控系統管理以及其他技術服務的公司。2020 年 12 月被揭露 SolarWinds 所推出的 Orion 網路管理系統（Network Management System, NMS）遭到大規模駭客攻擊，攻擊方法是將惡意後門插入到 Orion 的更新程式中，再傳播給全球客戶。此攻擊事件引發重大影響，包括美國多個政府組織、資安業者與大型科技公司。

SITA 攻擊事件[11]影響全球主要航空公司，國際航空電訊協會（Société Internationale de Télécommunications Aéronautiques, SITA）專門向航空業約 400 名成員提供 IT 和電信服務，聲稱服務於全球

---

9 Gartner (2022). Gartner Identifies Top Security and Risk Management Trends for 2022. 檢自：https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022 (May. 13, 2022).

10 TechTarget. (2021). SolarWinds hack explained: Everything you need to know. 檢自：https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (May. 14, 2022).

11 Infosecurity. (2021). SITA Supply Chain Breach Hits Multiple Airlines. 檢自：https://www.infosecurity-magazine.com/news/sita-supply-chain-breach-hits/ (May. 16 2022).

約 90%的航空業務。SITA 於 2021 年 3 月坦承，旗下專門經營航空公司乘客處理系統的子公司 Passenger Service System（PSS）遭到駭客入侵，多家航空公司透過 SITA 的伺服器共享飛行常客的會員數據，造成大量的會員資料外洩。由航空公司組成的星空聯盟（Star Alliance）和寰宇一家（oneworld）當中皆有航空公司使用 SITA 服務，因此聯盟內的所有航空公司的常客數據皆遭洩漏，影響甚遠。

結語

供應鏈也因應資訊化趨勢逐漸發展成數位供應鏈，數位供應鏈可以幫助公司提高收入、擁有更好的決策和更敏捷的流程，但使用的 IT 技術同時擴大供應鏈的脆弱面，其中影響最大的為伴隨而來的網路安全風險問題。加上數位供應鏈上的組成成員可互相連線、存取可從近幾年的 SolarWinds 供應鏈攻擊事件與 SITA 攻擊事件得知，若資料外洩則會造成重大影響。因此，若企業想轉型使用數位供應鏈，需多加注意供應鏈網路攻擊問題。

調查日本的 DNS 濫用

Shoko Nakai

https://blog.twnic.tw/2022/08/08/23931/

本 APNIC 文摘原標題為 Investigating DNS abuse in Japan，由 Shoko Nakai 撰文。

日本電腦網路危機處理暨協調中心（JPCERT/CC）每天觀測 DNS 濫用事件及相關發展。如同其他 CERT，JPCERT 也會與當地及廣泛安全社群分享濫用事件特徵和趨勢，希望協助安全服務供應業者改善服務，DNS 服務供應業者則能因應採取措施。

本文作者今年 4 月出席亞太 DNS 論壇（APAC DNS Forum 2022）的「APAC 的 DNS 濫用：真實經驗觀點」（Real Life Perspectives on Regional DNS Abuse in APAC）場次，分享自身在亞太地區及國內經歷過的 DNS 事件，期望透過這些分享，共同強化減緩 DNS 安全威脅。

釣魚及域名挾持

由於難以透過外部觀察偵測，DNS 攻擊引發的安全事件通常很難調查或回應。JPCERT 身為協調中心，試圖透過歷史資料、受攻擊或被影響的組織資料，以及其他夥伴單位提供的資料，以了解整體狀況。事後調查所取得的攻擊事件細節，則用來防止未來類似的事件發生。

日本境內最常見的兩種 DNS 相關事件是釣魚網站和域名挾持。

JPCERT/CC 在 2021 年就收到 44,242 筆事件通報，其中超過半

數與釣魚網站有關。其中一件本文作者在亞太 DNS 論壇分享的事件中，攻擊者的目標是主機代管服務供應商。

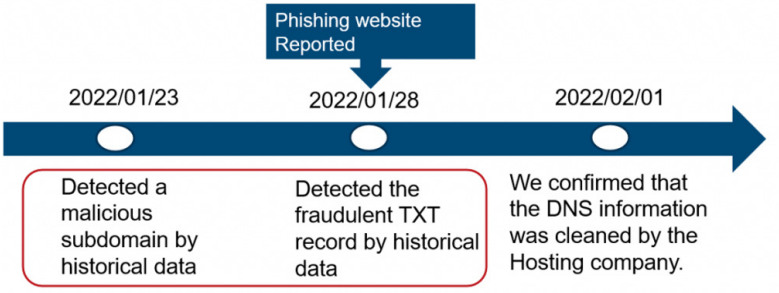


圖 1：釣魚攻擊時間線（從偵測發現到緩解）。代管主機公司一偵測到釣魚活動，馬上修正 DNS 資訊並通知相關網路服務供應業者（ISP）。

在此事件中，攻擊者改掉某個使用者的 DNS 資訊並註冊一個假的附屬域名，並在攻擊對象的主機上架設釣魚網站，同時 JPCERT 也發現增加寄件人政策框架（Sender Policy Framework，SPF）註冊資訊的惡意 TXT 紀錄。

JPCERT 推測攻擊者新增 SPF 紀錄是為了避免惡意郵件被發現。

作者在論壇中分享的另一個案例，是瞄準日本國內虛擬貨幣生意的域名挾持攻擊。

基於被動 DNS 資訊，作者與其 JPCERT 的團隊，分析攻擊者如何覆寫目標公司的域名伺服器（name server，NS）資訊，並控制改換該 NS 的路由，藉此竊取資訊。

調查中，作者團隊發現惡意的郵件交換（mail exchange，MX）伺服器。他們推測此攻擊的背後發動人假冒員工取得資訊，但他們目前仍不清楚攻擊動機。

主動積極面對 DNS 安全

DNS 營運方有很多方法能更積極地保全 DNS 免於攻擊。

在亞太 DNS 論壇的場次中，與談人都同意註冊管理機構鎖（registry lock）是保護域名最好也最簡單的安全預防措施。此功能可以鎖住所有域名相關資料，註冊管理機構和受理註冊機構欲更動資料時，也必須通過額外驗證程序。

該場次中，與談人也討論同時使用域名系統安全擴充（DNS Security Extensions，DNSSEC）及域名驗證技術，以偵測釣魚電子郵件及類似攻擊，會比其他設置難度門檻較高的電子郵件安全協定如 SPF、域名金鑰認證（DomainKeys identified email，DKIM）和域名為本的訊息驗證、通報及一致性（Domain-based Message Authentication, Reporting & Conformance，DMARC）等更有效。

參考資料：

https://blog.apnic.net/2022/06/30/investigating-dns-abuse-in-japan/

讓安全更簡單

Kathleen Moriarty

https://blog.twnic.tw/2022/08/12/23937/

本APNIC文摘原標題為Making security simpler for organizations big and small，由 Kathleen Moriarty 撰文。

過去幾年來，我們看到更多各種不同規模的組織單位面臨網路安全威脅，包括試圖找出侵入點以取得更大範圍權限的攻擊。雖然供應鏈攻擊並不一定比其他類型的攻擊更厲害，但此類攻擊帶來的危害不可否認日益嚴重。

越來越多包括美國行政命令、歐盟國家制令等政府命令要求內建安全和常態性管理。許多缺乏資源的組織單位往往選擇利用雲端代管環境達到安全目標，然而這些代管環境也需要安全控管資源。除此之外，不同平臺的控管機制也大不相同。

要求供應商內建安全機制的趨勢，也呈現安全管理規模化的機會。隨著安全概念向「零信任」轉型，安全管理也必須進入每個微小的環節。如何推動安全轉型並建立管理架構模式，將決定未來供應鏈管理的安全。

本文作者Kathleen Moriarty為網路安全中心（Center for Internet Security，CIS）技術長，在加入 CIS 之前，Kathleen 是網際網路工程任務組（Internet Engineering Task Force，IETF）的安全主任。投身協定演進研究的同時，他也找到讓安全更簡單的方法，並將發現集結成書《資安轉型：最佳化五種並行趨勢以減少資源流失》（Transforming Information Security: Optimizing Five Concurrent Trends to Reduce Resource Drain）出版。書中指出當代軟體和執行

系統安全架構的不足之處，包括使用外加安全產品的慣例。

有感於許多資源不足的組織單位難以建立有效的安全控管架構，Katheleen 最近發布的 CIS 白皮書《簡化安全》提出範例，說明如何有規模地自動化供應商安全機制的基礎控管區域。白皮書內容聚焦於資產管理、軟體資產管理，以及資產購入及後續管理的系統態勢安全保證。在規模化建置的前提下，文件中列舉有民主化安全機制潛力的技術、協定和開源專案。

Kathleen 在今年 3 月的 RSA 會議中，主持了一場「讓安全更簡單」的座談。與談人包括 Dell、RedHat、Cisco 及 Microsoft 代表，討論未來 5 年內如何促進內建安全規模化的轉型。其中特別值得紀錄的亮點包括：

- Dell 代表 Rudy Bauer 分享 Dell 安全元件驗證（Secured Component Verification，SCV）專案，加強確保使用驗證技術的供應鏈安全。此專案顯示供應商有能力確保產品符合既定政策及量測規範，進而確保產品售出後，無需購入方多餘的持續管理監控，程式啟動過程也值得信任且安全。
- Microsoft 的 Kay Williams 分享 Microsoft 在發現新弱點時，用來更新客戶機器的平臺。過去幾年來修補程式改善很多，供應商可以全面自動化修補過程，客戶方幾乎不再需要在自身環境進行分散測試。
- RedHat 的 Luke Hinds 表示，RedHat 持續和 SigStore 開源專案合作，開發用來簽署、發布軟體物料清單（Software Bill of Material，SBOM）開源程式碼。
- Cisco 的 Tony Jeffs 指出產品開發環境是入侵的管道之一，隨著威脅樣態演變，Cisco 了解到規模和敏捷度的重要。他認為必須結合中央化安全架構及隱私保護，確保這些層面的一致性。此過程應從自動化資產清單開始，建立一系列控管

原則，並在過程中自動化減緩風險。

這場座談以 Kay Williams 強而有力的發言作結。他表示：「安全如同淨水與清淨的空氣，一般個人應可視此為理所當然」。

Kathleen 認為這也應該是未來產品安全的基本，安全對所有人來說都應該變得更簡單。

參考資料：

https://blog.apnic.net/2022/07/18/making-security-simpler-for-all-orgs/

從網際網路核心追蹤 DDoS 攻擊生態系統

Marcin Nawrocki

https://blog.twnic.tw/2022/06/20/23282/

本 APNIC 文摘原標題為 Tracing the DDoS attack ecosystem from the Internet core，由 Marcin Nawrocki 撰文。

對網際網路而言，分散式阻斷服務（Distributed Denial of Service，DDoS）攻擊是重大且無所不在的威脅。一般而言，網際網路上約三分之一的活躍/24 網路，平均每兩年至少會遭受一次某種形式的 DDoS 攻擊。

反射性放大攻擊可以簡單且經濟實惠的發動 DDoS 攻擊，因此很受歡迎。傳統上會利用蜜罐（honeypot）誘捕觀察此類攻擊，刻意設置弱點吸引攻擊，並記錄所有攻擊活動。然而，蜜罐模式無法推斷哪些其他基礎建設也被作為放大器利用，以及被利用的程度，因此在評估如強度等攻擊概況上有所限制。

為了彌補此缺口，作者於柏林自由大學（Freie Universität Berlin）的團隊與荷蘭特文特大學（University of Twente）、漢堡應用技術大學（HAW Hamburg）共同開發在網路交換中心（Internet Exchange Point，IXP）流量資料樣本中，被動推斷 DNS 放大攻擊的方式。使用 IXP 樣本的挑戰在於區分正當訊務和攻擊訊務。但比起蜜罐，使用 IXP 資料可以從網路內部完整觀察被濫用的放大系統全貌，以及攻擊者有多擅長放大攻擊。

令人驚訝的是，IXP 和蜜罐偵測到的攻擊幾乎完全不同，僅有約 4%重疊。區區 3 個月內，作者團隊就發現 2,4000 筆蜜罐沒偵測到的新攻擊。

以下，作者分享團隊研究發現的關鍵洞見，以及保護 DNS 相應弱點的建議。

攻擊者特別愛用大型區域

首先，團隊調查攻擊者在最大化放大攻擊時是否查詢域名，或其中還有沒有尚未被使用的潛在威脅。

使用 OpenINTEL 資料，團隊推定 ANY 查詢的回應數量為 4 億 4 千萬域名（如圖 1）。此推定數量乃基於 DNS 中儲存的累積資源紀錄數量，並排除常見的軟體或協定限制（EDNS 的 4,096 位元和 UDP 的 65,536 位元）。

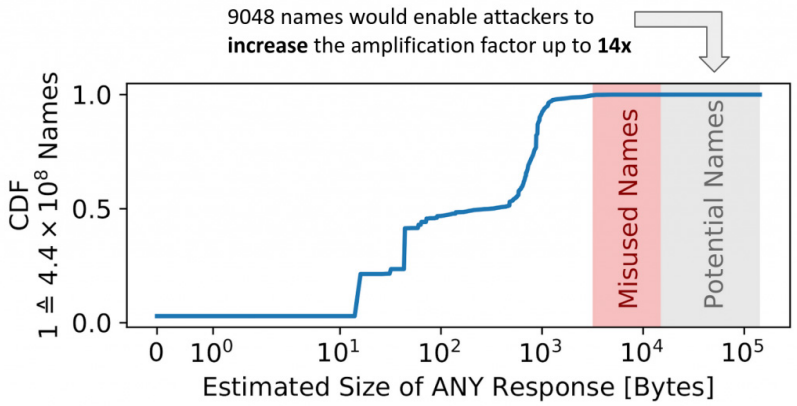


圖 1：ANY 回應的推估數量（位元）

紅色是在 IXP 中偵測出被用於攻擊的域名。整體而言，只有 9,048 筆域名的放大因素高於其他在濫用排名上更高的域名，大約佔所有域名的 0.002%（灰色區域）。這表示攻擊者在挑選域名時，只專注於放大效果，而不會選擇濫用性質更高的域名。

建議：盡可能限制區域大小！

ANY 查詢（ANY queries）仍然有效

分析 IXP 資料樣本的封包尺寸後，團隊得以確認攻擊達到有效的放大效果。圖 2 依不同域名，顯示 IXP 觀測到的實際回應數量頻率。

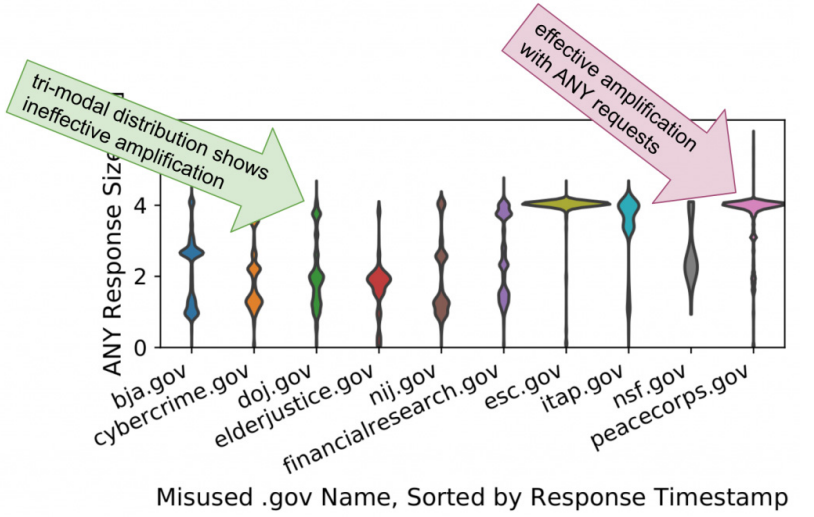


圖 2：濫用.gov 域名（依回應時間分類）

團隊將所有 DNS 查詢類型納入考量，但在攻擊中，僅觀測域名的 ANY 查詢。大部分域名都呈現雙重或三重的分散模式。

團隊觀測到接近理論限制的回應群集數量，證明攻擊者能找到仍允許 ANY 查詢的域名（及關連權威域名伺服器）和放大器。

不僅如此，更深入的調查顯示，域名快不能用時，回應數量也比較小。這顯示攻擊者會持續觀察當下有效的放大效果，並在效果減弱時改用新的域名。

建議：拒絕 ANY 查詢或強制執行 TCP 失效切換（TCP failover）。

不好的 DNSSEC 金鑰汰換（key rollover）容易吸引濫用

圖 3 中，虛線表示 DNS 建議的最大有用負載尺寸（4,096 位元）。團隊觀測到，預期回應數量會在域名遭濫用於攻擊中時改變，而且一旦數量下降，攻擊者就會轉向其他域名。

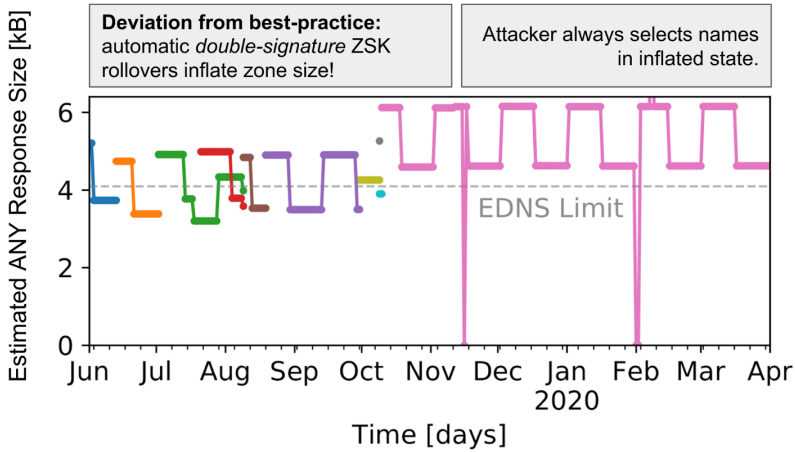


圖 3：從 OpenINTEL 資料推斷的域名 ANY 回應數量

回應數量達到高點後大概會持續兩週，如圖中顯示頂端平坦的部分。而這現象和域名系統安全擴充（DNS Security Extensions，DNSSEC）金鑰汰換（key rollover）有關。新的區域簽署金鑰（zone signing key，ZSK）推出時，由於多筆 DNSKEY 紀錄會同時出現，回應數量因此將提高。ZSK 替換通常是在軟體中自動執行，因此會如圖中呈現具有規律。

RFC 6781 中建議兩種替換方式：事先發布及雙重簽署。雖然有兩種方式，但事先發布一直以來都被當成實際上的標準做法（在 2020 年，事先發布的實際執行次數高達雙重簽署的 8 倍，也是大

部分 DNS 軟體商建議的方式）。

事先發布會以「待用」模式推出新的金鑰，也就是說此金鑰還不能用來簽署 RRset。這是為了讓解析器在正式啟用前先知道新金鑰。

雙重簽署則容許兩組啟用的 ZSK，並生成兩組（冗餘的）RRSIG 紀錄簽名。舊的 ZSK 因此可在任何時間退場。但這樣做的缺點，是區域中簽署數量翻倍，因此容易吸引濫用。

在 IXP 資料中，團隊發現因為金鑰汰換遭濫用的.gov 域名，都是使用雙重簽署方式。

建議：以「事先發布」模式進行金鑰汰換！

更多細節可參考作者團隊發布的研究論文 。

資料來源：

https://blog.apnic.net/2022/04/28/tracing-the-ddos-attack-ecosystem-from-the-internet-core/

網路技術

網路瀏覽器的演進史

莊舒歆／東海大學資訊管理學系

https://blog.twnic.tw/2022/12/16/25093/

瀏覽器的誕生

說到網路瀏覽器的起源，就一定要提到電腦科學家 Tim Berners-Lee，身為全球資訊網（World Wide Web）之父的他，設計並建構了第一個瀏覽器「WorldWideWeb」。為了避免與全球資訊網混淆，後期改稱為 Nexus。

Nexus 是當時瀏覽網際網路唯一的途徑，雖然被稱為瀏覽器，但更準確的名稱應該是「瀏覽器編輯器」，當時並沒有料想到網頁的開發會如此普及，考量到網頁設計也要有專屬介面供使用者使用，Tim Berners-Lee 與團隊為瀏覽網站設計了一套流程，用戶要依照固定程序將 URL 放入，就製作出一個客製頁面。詳細的教學與體驗網站能夠使我們更認識 Nexus。

市占率競爭

隨著開放的網際網路發展，許多瀏覽器如雨後春筍般冒出。較為知名的就屬 1993 年大受歡迎的 NCSA（National Center for Supercomputing Applications）Mosaic 瀏覽器，該瀏覽器由 Marc Andreessen 開發，Mosaic 瀏覽器可說是幫助 Web1.0 發展的大功臣，原本網際網路上寥寥無幾的網站，藉 Mosaic 操作直覺的特性及吸引人的介面迅速擴展。

Marc Andreessen 隔年推出瀏覽器 Netscape，增加了許多功能，

使其全球市佔率高達 80%且持續成長，Netscape 立志為所有作業系統的使用者提供跨平臺的使用體驗。因此，微軟開始認為自家販售的電腦要有預設瀏覽器，與 Spyglass 公司合作，該公司當時已高價收購了 NCSA Mosaic 瀏覽器，名稱改稱為 Spyglass Mosaic。取得 Spyglass 的授權後，微軟以 Mosaic 基礎推出了 Internet Explorer（IE）。

個人電腦販售後，微軟作業系統預設瀏覽器都是 IE，使其市佔率開始成長，而 Netscape 在推出更新版時，大幅度的強化 JavaScript 與其餘功能，導致穩定性變差，IE 順勢超越 Mozilla 公司的 Netscape。

這場市占率之爭，讓後起直追的 IE 成為瀏覽器霸主，2003 年市佔率更高達 95% [1]，而後期不斷更新 Netscape 再出售後，在 2004 年以 Netscape 原始碼推出 Firefox。2008 年 Google 推出 Chrome 瀏覽器。在當時，IE 對各家瀏覽器來說，是可望而不可即的存在，當時的 Google 執行長也因此反對開發網頁瀏覽器[2]。但其他高層並沒有放棄，基於 Firefox 開源程式碼推出了 Chrome，強調簡潔介面和速度成功打出一片天。

架構演進史

看完了精彩的歷史故事，我們來探討網路瀏覽器程式架構的演進。

---

1 Microsoft's Internet Explorer global market share is 95% according to OneStat.com. 檢自：https://web.archive.org/web/20210225175726/http://www.onestat.com/html/aboutus_pressbox15.html

2 Steven Levy (2008). Inside Chrome: The Secret Project to Crush IE and Remake the Web. 檢自：https://www.wired.com/2008/09/mf-chrome

單一程序（Single Process）

單一程序代表每次只能處理一個功能。瀏覽器是由多個功能模組組成，包括擴充功能、JavaScript 執行環境等，這多個功能都放在同一程序內。意味著，如果有個模組損壞，瀏覽器就無法運作了。除此之外，單一程序的瀏覽器每次使用後，沒有辦法把記憶體完全清空，隨著使用時間增加，記憶體占用比也會越來越高，瀏覽器就會出現卡頓情況。

多程序（Multi Processes）

Google Chrome 為多程序瀏覽器揭開序幕。為何 Chrome 出現時，瀏覽器霸主 IE 就此殞落？因為 Chrome 將需要運行程式碼的執行緒（thread）分別出渲染程序（Renderer Process）與擴充功能程序（Plugins Process）。當頁面渲染或者擴充崩潰時，只會影響單一頁面或擴充功能；也不會影響到瀏覽器的主程序，更重要的也可避免惡意擴充直接取得用戶數據。

目前的 Chrome 獨立出了更多的程序，獨立程序雖然能使我們有更安全、更流暢的體驗，但同時越多的程序就需要越多的記憶體資源，當我們開啟 Chrome 瀏覽器多個頁面時，可以注意到電腦的記憶體占用比非常高。面對消耗記憶體的問題，2016 年 Google 以服務導向架構（Services Oriented Architecture，SOA）概念[3]為設計目標，持續更新優化 Chrome。

結語

瀏覽器的快速更迭，令人感嘆科技的日新月異。提醒了我們因著許多人的無私付出，科技才能如此快速的進步。全球資訊網之父

[3] John Abd-El-Malek (2016). Chrome Service Model. 檢自：https://docs.google.com/document/d/15I7sQyQo6zsqXVNAlVd520tdGaS8FCicZHrN0yRu-oU/edit?usp=sharing

Tim Berners-Lee 的發明，完全以公共財公布，任何人都可以免費使用，造就了後續不論是瀏覽器普及和各式網路技術的蓬勃發展。早期瀏覽器的開放原始碼，締造了現今的網路瀏覽器，供所有人學習與共享。

網際網路是現代人不可或缺的服務，瀏覽器更是電腦不可忽視的工具，不論是一般使用者或網路開發人員，都需要珍惜所擁有的共享資源，共同維護前人所打造的網路環境。瀏覽器的功能與可能性還在不斷突破，演進的齒輪仍持續轉動著，就讓我們拭目以待未來的發展。

淺談內容傳遞網路（CDN）

吳宜庭／東海大學資訊管理學系

https://blog.twnic.tw/2022/12/14/25009/

內容傳遞網路（Content Delivery Network 或 Content Distribution Network，CDN）

在距今 20 多年前，隨著骨幹網路（Backbone Network）的擴增與訊息長距離傳輸需求增大，使得骨幹網路壓力越大且長傳效果愈差。在 1995 年，麻省理工學院（Massachusetts Institute of Technology，MIT）應用數學系教授帶領研究生與幾位研究人員嘗試使用數學邏輯解決網路壅塞的問題。

上述研究人員藉由數學演算法，處理內容動態路由配置，最終解決了網路使用者的困難，在後 MIT 史隆管理學院的學生加入團隊中，並開始實施商業計畫，於 1998 年成立一家科技公司「Akamai」並成為目前全球最大的分散式運算平臺之一，後續在其他地區亦有相同的科技公司紛紛成立，提供相似的服務，即內容傳遞網路（Content Delivery Network，CDN）。

CDN 系統架構

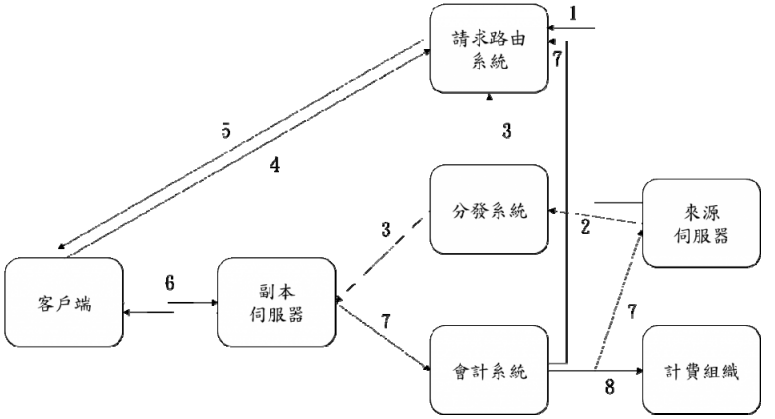


圖 1：CDN 系統架構

CDN 的系統架構圖如上，首先來源伺服器將 URL 名稱空間委託給 CDN 進行分發和將要交付的文件或物件傳送到請求路由系統，接著來源伺服器將要分發和下發的內容發布至分發系統中，分發系統會將內容移動至副本伺服器。系統透過回饋與請求路由系統互動，以協助客戶端請求的副本伺服器選擇過程。客戶端從他認為是來源的地方請求文件，由於 URL 名稱空間委託，請求實際上會被轉向請求路由系統。再來請求路由系統將請求路由到 CDN 中適合的副本伺服器，被選中的副本伺服器將請求內容傳遞給客戶端。

後續副本伺服器會將傳送內容的計費資訊發送到會計系統，會計系統會將計費資訊彙整統計與內容明細紀錄，以供來源伺服器與計費組織使用。統計資訊也可作為請求路由的回饋，最後計費組織使用內容詳細記錄、內容分發與交付過程中涉及的各方進行結算。[1]

[1] Gang Peng (2018). CDN: Content Distribution Network.

CDN 原先第一個重要用途是分發大量請求的圖形文件，如 GIF 檔，然而無論是在理論或是實務上，CDN 皆可以支援任何數位內容的交付包含各種形式的串流媒體。[2]為了能盡量縮短使用者與網站伺服器間的距離，CDN 會將內容來源伺服器（Origin Server）提供的內容儲存在最接近使用者的「邊緣」（edge）網路節點，讓使用者可以從最近的 CDN 所在區域更快速地獲取所需資料，進而達到優化網頁速度及效能的功效。

CDN 使用情境

若是在沒有使用 CDN 時，假設有一影音平臺架設在美國，成立初期使用者數量不多且大多數皆在美國，那所有使用者皆可直接向網站伺服器發出請求並快速取得資料。但是若網站使用者逐漸增加且區域逐漸擴展時，網路伺服器的承受程度也會隨之增加。最後距離網路伺服器越遠的使用者存取速度也會越來越慢，甚至面臨網路延遲和寬頻成本增加的問題，進而降低使用平臺的意願。

因此當平臺使用 CDN 時，CDN 會將網站伺服器回傳給使用者的快取（cache）並存在多個地理位置（Points of Presence，PoPs），且幾乎每個 PoP 都包含 CDN 節點（CDN nodes），可負責將快取傳輸給在 PoP 附近發出請求的使用者。

檢自：https://arxiv.org/pdf/cs/0411069.pdf

[2] M. Day, B. Cain, G. Tomlinson, P. Rzewski (2003). A Model for Content Internetworking (CDI). 檢自：https://www.rfc-editor.org/rfc/rfc3466# section-2.4

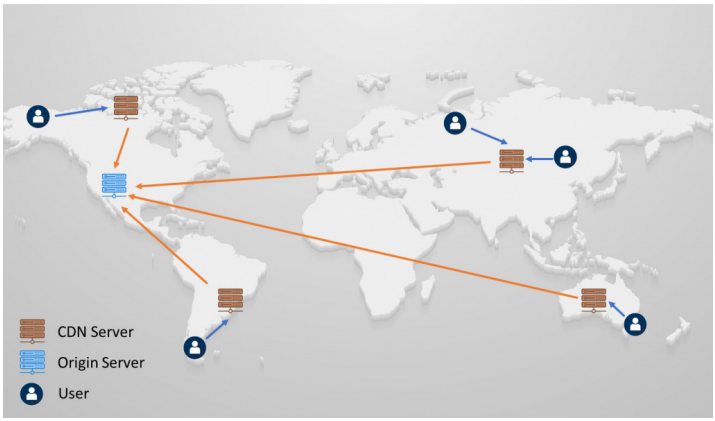


圖 2：CDN 系統架構

問題與資安疑慮

如今的網際網路已是一個複雜且相互依賴的巨大系統，許多平臺幾乎也會使用 CDN 服務，然而雖然 CDN 的承載量比一般傳統單一伺服器要多，當某個伺服器故障時，系統也可調用其他鄰近地區的伺服器服務，但若來源伺服器產生故障或其他意外情形發生時，則所有供應的服務也被迫中止，如：知名 CDN 業者 Fastly 因全球多個區域斷線，導致眾多網路業者 Amazon、Paypal、紐約時報及英國政府網站無法正常運作[3]。

從 2021 年至今中國資安業者安天（Antiy）長期追蹤印度駭客組織的網路攻擊，並表示駭客為了避免遭受追查，可能會濫用 CDN 服務來隱藏攻擊來源[4]。在 2020 年時，也曾經發生過全球 200 大 CDN 遭受 BGP 劫持，藉由破壞路由器內的全域 BGP 路由表（global

[3] 林妍溱（2021）. CDN 業者 Fastly 組態問題造成全球斷線，多家知名網站遭殃. 檢自：https://www.ithome.com.tw/news/144911

[4] 羅正漢（2022）.【資安月報】2022 年 7 月-印度駭客組織 Confucius 對巴基斯坦軍事機構發動攻擊. 檢自：https://www.ithome.com.tw/news/152206

BGP routing table），造成一組 IP 流量被導向不該去的目的地，Facebook、Google、Amazon 等大小型平臺所使用的 CDN 皆遭受影響[5]。

因此 CDN 的使用為使用者帶來許多便利，也增進網路服務提供的效能與擴展，但是使用的同時也應了解相對的風險並做好相對應的對策，以備不時之需。

[5] 林妍溱（2020）. 全球 200 大 CDN 發生 BGP 劫持，Google、Cloudflare、Line 皆被導向俄羅斯. 檢自：https://www.ithome.com.tw/news/136758

偏遠之星 Starlink

吳幸芳／東海大學資訊管理學系

https://blog.twnic.tw/2022/09/12/24270/

何謂 Starlink

太空探索技術公司（SpaceX）為美國一家民營航太製造商和太空運輸公司，Starlink[1]是由其所推出的一項透過低軌道衛星群（Low Earth Orbit，LEO），提供覆蓋全球的高速網際網路存取服務。雖然現今大多數衛星網際網路服務都來自與地球距離約 35,000 公里的靜止衛星，但 Starlink 是一個由多顆衛星組成，與地球距離約 550 公里且覆蓋整個地球的網路服務。Starlink 網際網路的工作原理是在真空中發送電磁波訊號，傳播的速度比光纖快許多，並且可以到達更多的地方。

根據 Ookla 2022 年第一季度報告顯示[2]，Starlink 過去一年在美國以及加拿大增長近 58%與 38%，Starlink 在墨西哥的服務是北美洲最快速的網際網路供應商，墨西哥的寬頻固網下載速度（40.07 Mbps）遠低於 Starlink。Starlink 在歐洲的服務也勝於絕大多數歐洲國家的寬頻網路，其中在立陶宛的下載速度最快，為 160.08 Mbps，其次是比利時（147.85 Mbps）、斯洛伐克（146.25 Mbps）、克羅埃西亞（136.00 Mbps）和奧地利（132.61 Mbps）。

---

1 SpaceX. (no). Starlink. 檢自：https://www.starlink.com/ (Aug. 12, 2022).

2 Ookla (2022). Here's How Fast Starlink Has Gotten Over the Past Year. 檢自：https://www.ookla.com/articles/starlink-hughesnet-viasat-performance-q1-2022 (Aug. 13, 2022).

Starlink 之優點包含以下幾項[3]：

1．更快的網際網路

SpaceX 所提供的服務絕對比傳統的衛星快。Starlink 的速度幾乎無法將其與傳統的衛星連接進行比較。

2．相對便宜

Starlink 的價格合理，在農村和郊區之價格比有線和衛星網際網路便宜許多。現今許多郊區消費者支付與城市居民相同的價格，但所獲得的網際網路速度慢上許多。

3．廣泛的可用性

無論身在何處，Starlink 都可以提供給每位客戶使用，其網路覆蓋範圍廣泛，並提供從南極洲到海洋中央的快速、無限制的網際網路。

Starlink 之缺點包含以下幾項[4]：

1．硬體安裝費用

對於許多用戶來說，硬體安裝可能會成為一項問題，Starlink 不提供使用其網路所需的設備安裝服務。因此，客戶必須自行安裝設備或聘請專業人員花費額外的費用。

2．不方便攜帶

與蜂巢式網路（Cellular network）相比，Starlink 相較之下不便攜帶。Starlink 的天線設計不便於攜帶，雖然可以安裝在房車或船的上方，但仍然不夠小，無法輕鬆攜帶。

---

3 Passwork. (2022). How secure is Elon Musk's Starlink? 檢自：https://blog.passwork.pro/how-secure-is-starlink/ (Aug. 13, 2022).

4 Ookla (2022). Here's How Fast Starlink Has Gotten Over the Past Year. 檢自：https://www.ookla.com/articles/starlink-hughesnet-viasat-performance-q1-2022 (Aug. 13, 2022).

3. 服務穩定性取決於天氣

衛星服務經常因雨水、風暴等天氣狀況中斷。

Starlink 的近期應用與所遇問題

自 2022 年 2 月 24 日俄羅斯對烏克蘭發動戰爭後，該國基地台大多數遭到嚴重破壞，受創傷的倖存者無法與親友連絡[5]，Starlink 的出現成為一條訊息生命線。烏克蘭空中偵察部隊也使用 Starlink，成功擊毀許多俄羅斯坦克、行動指揮中心和其他軍用車輛的無人機。烏克蘭的數位轉型部在戰爭開始前幾個月首次與 SpaceX 取得聯繫，部門顧問 Anton Melnyk 表示「Starlink 高階主管與烏克蘭數位部長 Mykhailo Fedorov 在 2 月底時對啟用該服務進行討論，幾天後俄羅斯入侵，使得 Starlink 的服務因不同的原因變得有吸引力」。

然而，目前 Starlink 的營運有其問題，Starlink 正在尋找大量新客戶，雖然這種趨勢對 Starlink 來說是正面的影響，但對訂戶是極其不利。許多客戶發現其連接速度[6]在過去幾個月裡隨著越來越多的用戶連接到 Starlink 的衛星網路而嚴重下降。根據歐洲天文台、美國政府等多家科學家機構，在太空探索核心期刊《天文物理期刊》通訊專欄發表文章：〈SpaceX 星鏈衛星對史維基瞬變設備觀測結果的影響〉（Impact of the SpaceX Starlink Satellites on the Zwicky Transient Facility Survey Observations）[7]表示，觀察出史維基瞬變設

---

5 Wired. (2022). How Starlink Scrambled to Keep Ukraine Online. 檢自：https://www.wired.com/story/starlink-ukraine-internet/ (Aug. 14, 2022).

6 Input. (2022). Starlink will be open to everyone in August—not that you'll want it. 檢自：https://www.inputmag.com/tech/starlink-will-be-open-to-everyone-in-august-not-that-youll-want-it (Aug. 16, 2022).

7 The Astrophysical Journal Letters. (2022). Impact of the SpaceX Starlink Satellites on the Zwicky Transient Facility Survey Observations.

備（Zwicky Transient Facility，ZTF）在近兩年裡，共出現超過 5,300 條星鏈衛星軌跡，美國天文學會將此比做光汙染，對於觀星者而言明顯汙染觀測主體。

與 Starlink 相關的新服務

夏威夷航空公司（Hawaiian Airlines）宣布[8]最早將於明年提供免費的 Starlink 服務，往返於夏威夷群島與美國大陸、亞洲和大洋洲航班上的每位乘客皆可使用高速、低延遲寬頻網際網路。Starlink 所提供的服務吸引整個航空業的關注，夏威夷航空公司並不是唯一一家參與 SpaceX 談判的航空公司，達美航空公司（Delta Airlines）目前正在探索使用 Starlink 提供機載 WiFi 的可能性，最近也進行一些機上測試。

今年 3 月中華民國國家通訊傳播委員會（NCC）通過「申請衛星通信頻率公告」草案，NCC 表示將開放其中一區段與既有電信業者協議使用，經過一連串申請與審驗後，才可提供服務，同時亦應落實保障消費者權益及配合通訊監察等相關監理規定。未來用戶只需安裝固定天線，即可接收衛星訊號使用衛星通訊服務。

結語

Starlink 透過低軌道衛星群，在真空中傳輸資料，提供覆蓋全

檢自：https://www.researchgate.net/publication/357897783_Impact_of_the_SpaceX_Starlink_Satellites_on_the_Zwicky_Transient_Facility_Survey_Observations (Aug. 16, 2022).

8 Hawaiian Airlines. (2022). Hawaiian Airlines to Offer Free, High-Speed Starlink Internet Connectivity on Transpacific Fleet.
檢自：https://newsroom.hawaiianairlines.com/releases/hawaiian-airlines-to-offer-free-high-speed-starlink-internet-connectivity-on-transpacific-fleet (Aug. 18, 2022).

球的高速網際網路存取服務，無論高山或海洋甚至飛機上都可以存取。根據 Ookla 2022 年第一季度的報告，Starlink 在各地的速度皆快於寬頻固網速度。儘管 Starlink 有著許多優點：包含更快的網際網路、相對便宜以及廣泛的可用性等，硬體安裝費用、不方便攜帶以及服務中斷取決於天氣等都是其缺點。Starlink 成為戰爭中通訊的重要元素，但也有天文學家發現其星鏈衛星軌跡會嚴重影響到觀測品質，未來 Starlink 要如何從中取得平衡為一關鍵問題。

5G 頻段對航空造成的影響

吳宜庭／東海大學資訊管理學系

https://blog.twnic.tw/2022/04/25/22693/

自 2020 年 7 月，3G PP 宣布 5G -Release 16 技術標準完成後，全球的電信業者也逐漸地投入更多有關 5G 網路的建置。隨著 COVID-19 的肆虐，加速全球各產業數位化的腳步，5G 在未來幾年內將取代 4G 標準，成為新一代通訊行動主流的技術，更進一步扮演催化社會重新思考生活、工作和玩樂方式媒介。

5G 網路

下一代行動網路聯盟（Next Generation Mobile Networks Alliance）針對 5G 網路做以下定義[1]：

- 每平方公里最多可支援 100 萬台裝置；
- 以 1G bps 的資料傳輸率同時提供給在同一空間的人員；
- 支援大規模感測器網路的部署；
- 頻譜效率應比 4G 較為強大；
- 覆蓋率高於 4G；
- 延遲性應顯著低於 LTE。

相較於先前的網路技術，5G 的各個優勢也使得它可應用的場景更加廣泛，在 2019 年 IEEE 的報告[2]中提及：「1G 網路僅有 2.4Kbps

[1] The Institute of Electrical and Electronics Engineers (IEEE). (2017). IEEE 5G and beyond technology roadmap white paper. 檢自：https://futurenetworks.ieee.org/images/files/pdf/ieee-5G-roadmap-white-paper.pdf (Mar. 13, 2022).

[2] Milo Medin and Gilman Louie (2019). The 5G Ecosystem: Risks & Opportunities for DoD. 檢自：https://apps.dtic.mil/sti/pdfs/ AD1074509.pdf (Mar. 13 , 2022).

的傳輸速率，但已突破早期的電話限制。2G 網路的後期使用了 GPRS 和 EDGE 技術，故當時傳輸速率高達 200Kbps。在 2000 年時，3G 網路的推出更是讓傳輸速度在靜止時可達 2 Mbit/s，而裝置移動時還有 350Kbps 的速度。當 4G 網路推出時，傳輸速度比 3G 網路快上 10 倍，擁有更大的頻寬提高了網路速度，也提高了網路的使用品質。而 5G 的資料傳輸速度、數量與延遲則取決於所使用的頻段及使用環境（定點或移動）。」

而目前全球發展的 5G 頻率範圍（Frequency Range，FR），由 3G PP 所定義的規格大致上可分為兩類，以 6GHz 頻段作為分界：一是頻率範圍介於 410MHz 至 7125MHz，稱為 sub-6GHz 或 sub-7 GHz 頻段；二為頻率範圍在 24250MHz 至 52600MHz 之間稱為「毫米波」也就是 mmWave 頻段，屬於 30GHz 至 100GHz 的高頻段。[3]

5G 頻段與航空業的關係

在 2021 年時，美國將 C 頻段（C-Band）3.7-3.98 GHz 進行拍賣，而航空業者認為，C 頻段的 5G 服務可能導致多數的飛機無法使用，使美國航班大亂，成千上萬名旅客滯留海外。美國聯邦航空總署（Federal Aviation Administration，FAA）也為此警告，因為無線電高度計使用 4. 2 GHz-4. 4 GHz 之間頻段運作，而美國 5G 網路使用的 C 頻段 3.7-3.98 GHz 與高度計運作頻率範圍太過接近，若兩者間有著相互干擾的情況，可能會使飛機在飛行時相關的安全儀器無法正常運行，聯合航空公司（United Airlines）執行長 Scott Kirby 表示：「FAA 為避免干擾造成的意外而制定規範，限制飛機在起降美國最大的 40 座機場時，禁止使用無線電高度計」。但此規範卻令

[3] Anritsu. 全球 5G 通訊頻段與運行模式. 檢自：https://www.anritsu.com/zh-tw/test-measurement/technologies/5G-everything-connected/5G-world-fre (Mar. 13, 2022).

航空公司認為未來可能影響每天約 4%的航班飛行。

各國 5G 制定與航空的差異

截至目前為止，針對歐盟在 2019 年時對 3. 4 GHz-3.8 GHz 的中頻段訂定標準，並在歐洲進行拍賣後，已有多國使用並無出現任何問題，在英國和歐洲，無線電高度計在不同的無線電頻率上運行，遠離飛機使用的無線電頻譜部分。而歐洲飛航安全局（European Union Aviation Safety Agency，EASA）表示，5G 干擾航空問題僅限於美國空域，歐洲區域並未偵測到不安全干擾。

美國 FAA 官員注意到了法國使用的 3.6-3.8 GHz 頻段，距離美國高度計使用的 4.2-4.4 GHz 較遠，法國 5G 使用的功率標準也遠低於美國授權的等級，即使美國降低了 5G 的使用功率，仍是法國的 2.5 倍[4]。

在南韓，5G 網路通訊頻率範圍為 3.42-3.7 GHz，且自 2019 年 4 月商轉以來，尚未收到無線電波干擾的訊息。而臺灣 5G 商用頻譜目前釋出 3.3-3.57 GHz，跟航空高度計使用頻段有相當的保護頻段（Guard Band）不會互相干擾，因此不受影響。

當局的因應措施與結語

針對其他國家例如：法國機場所規劃之緩衝區預留了著陸前最後 96 秒的飛行。法國的 5G 功率標準較低。在美國，即使是較低的全國性功率標準也還比法國高出 2.5 倍。而在法國，政府要求天線必須向下傾斜以限制有害干擾，但美國並沒有類似的限制。[5]

---

[4] Federal Aviation Administration. (2022). US-France graphic. 檢自：https://www.faa.gov/ sites/faa.gov/files/2022-01/US-France%20graphic_0.pdf (Mar.13, 2022).

[5] Federal Aviation Administration. (2022). US-France graphic.

因此 FAA 在約 50 個機場周邊地區效仿法國規定設置暫時性的緩衝區，限制緩衝區內的 5G 訊號，緩衝區範圍的寬度足以覆蓋著陸前最後 20 秒的飛行，且為了更精確的繪製出機場周圍訊號減弱區域的大小與形狀，進而縮小天線有效運行的區域。同時 FAA 開始確認那些飛機上的高度計能在 5G 訊號下安全運行，也需確認那些機場能使用全球定位系統（Global Positioning System，GPS）來引導飛機降落。

短期來說，美國電信兩巨頭 AT&T 和威訊通訊（Verizon）同意暫緩啟動各大機場附近的部分無線基地台，並同意設置緩衝區方法，以 6 個月為限降低干擾風險。長期來說，FAA 需要放鬆規範，在評估後核准使用無線電高度計，讓美國絕大部分的商業飛機，在許多有 5G C 頻段部署的機場執行低能見度降落。

檢自：https://www.faa.gov/sites/faa.gov/files/2022-01/US-France%20graphic_0.pdf (Mar.13 , 2022).

5G 雲端基礎建設的零信任原則應用

Kathleen Moriarty

https://blog.twnic.tw/2022/05/17/22998/

本 APNIC 文摘原標題為 Zero trust applied to 5G cloud infrastructure，由 Kathleen Moriarty 撰文。

美國國家安全局（National Security Agency，NSA）與網路安全和基礎設施安全局（Cybersecurity and Infrastructure Security Agency，CISA）最近發布由 4 份文件組成的《5G 雲端基礎建設安全指導原則》（Security Guidance for 5G Cloud Infrastructures），目標是加強雲端環境的安全。

任何提供安全多租戶（multi-tenancy）分離運算基礎建設的虛擬環境都適用此指導原則。本系列提出詳細的需求條件和指導原則，針對 5G 時代，雲端供應商或資料中心在代管解決方案和應用程式時應達到的安全層級，給出全方位的宏觀整體方案。

許多業界專家也參與本指導原則的撰寫，這些專家根據親身經歷，提出許多加強 5G 基礎建設安全的設計決策。指導原則包括以下 4 份文件：

1. 〈預防並偵測橫向移動〉（Part I: Prevent and Detect Lateral Movement）：偵測 5G 雲端中的惡意行為人，預防對方利用遭入侵的單一雲端資源感染整個網路。
2. 〈安全隔離網路資源〉（Part II: Securely Isolate Network Resources）：確保客戶資源之間有安全隔離，特別確保負責支援虛擬網路功能之容器網路堆疊（container stack）的安全。
3. 〈資料保護〉（Part III: Data Protection）：保護資料的傳輸、

使用及靜態安全。確保網路和客戶資料在資料處理流程所有階段（傳輸、使用中、靜態、銷毀）的安全。

4. 〈確保基礎架構的完整性〉（Part IV: Ensure Integrity of Infrastructure）：確保 5G 雲端資源必須驗證後才能更動。

強化 5G 基礎建設中的容器安全

指導原則中清楚指出，預防橫向移動及隔離網路資源的管控措施很重要。其中更點名容器（container）的設置和小節點群（pod）的安全，是在雲端代管 5G 建設中達成上述管控措施的重點關鍵。指導原則中亦建議參考網路安全中心（Center for Internet Security，CIS）的 Kubernetes 和 Docker 指標，依據資訊進行隔離和安全設定，進而達到以風險考量為本的管控。

除此之外，NSA 也發布針對 Kubernetes 的指導原則文件，可搭配 CIS 的 Kubernetes 指標使用，了解 Kubernetes 相關的更多安全設定細節。

對公共雲端內建安全措施的要求持續升高

隨著越來越多雲端供應業者採納指導原則中的建議，符合原則中的要求標準，代管環境的安全基本要求也會隨之提高。內建安全措施及規模化管理，再加上零信任租戶的做法，很可能成為常態。

5G 生態系統中的主要威脅向量

雲端和邊緣代管系統已被認定為 5G 生態系統中的主要威脅向量。這是因為雲端含有應用程式於網路核心處理的資料，又位於具高度運算能力的基礎建設之上，此集中特性特別容易招致攻擊。本指導原則中除為服務供應業者提供完整的指南，也列出相關服務應

符合的內建安全標準，供消費使用者參考，評估業者的安全措施是否足夠。

打造值得信任的基礎建設

過去幾年來，許多地方已培養出在維護系統完整性的同時，持續評估基礎建設信任度的能力。值得信任的基礎建設現在對很多組織都是基本需求。這些進展主要來自信任平臺模組（Trusted Platform Modules，TPM）和信任執行環境（Trusted Execution Environments，TEE）的廣泛部署，前者從信任源頭驗證並確保基礎建設值得信任，後者則透過依處理資料所需保護程度，分別提供執行代碼的方式，進一步鞏固資料處理流程安全。

保護資料

機密運算聯盟（Confidential Computing Consortium，CCC）正在開發保護資料執行中仍保持機密的長期方案。指導原則中也有提供短期之內保護並隔離資料的建議，市面上也有不同供應商的軟體開發套件（software development kits，SDKs）可供應用。

確保基礎建設的完整性

確保資料在傳輸和靜止狀態都保持加密乍看簡單，但實行上有很多地方需要注意。指導原則的第四份文件涵蓋一份詳盡的確認清單，用來完整檢視支援 5G 代管環境應提供的加密措施。過去的安全指南都聚焦於傳輸安全，不僅因為傳輸安全的要求行之有年，也因為它比靜態資料的保全策略更容易執行。然而，零信任架構清楚指出確保資料全程加密以防止洩露的重要。隨著零信任架構成為主流，對保護靜態資料安全的關心也大幅成長，更出現許多透過自動

化金鑰管理功能以達成靜態資料保護的新方案。

若成功符合本指南中的相關建議，服務供應業者將能提供滿足零信任要求、所有環節都加密的完整解決方案，服務使用者也將連帶受惠。

信任確保和零信任的其他參考資源

若讀者本身沒有深厚的技術背景，可能難以理解信任確保和 TEE 的相關主題和文件。作者任職的機構 CIS 最近發布名為「信任確保的簡單說明」（Trusted assurance simplified）的部落格文章，希望幫助讀者了解相關議題。

對很多人來說，達成零信任可能過於困難。本指導原則著重於支援 5G 基礎建設的雲端代管環境，但類似建議其實也適用於使用 TPM 和 TEE 硬體，且含有容器與小節點群的虛擬環境。這篇部落格文章以減少攻擊者的潛伏時間出發，說明零信任的重要。

參考資料：

https://blog.apnic.net/2022/04/18/zero-trust-applied-to-5g-cloud-infrastructure/

DNS 是否集中化？

Geoff Huston

https://blog.twnic.tw/2023/01/02/25232/
https://blog.twnic.tw/2023/01/09/25236/
https://blog.twnic.tw/2023/01/16/25248/

本 APNIC 文摘原標題為 Looking at centrality in the DNS，由 Geoff Huston 撰文。

域名系統（Domain Name System）在當代網際網路中扮演的角色舉足輕重。DNS 一開始是為了以人類可讀的方式標示網際網路傳輸目的地位置，後來成為客戶端／伺服器結構傳輸中的服務點名稱。以前一個域名只會連結一個 IP 位址，但這一對一的連結隨著 IPv4 地址耗竭而逐漸弱化。如今的位址空間高度分裂，但域名空間仍提供定義網際網路的關鍵參考框架。

有很多種方式可以回答此問題。Geoff Huston 本篇文章將聚焦於 DNS 中一個特定層面，也就是 DNS 域名解析運作。

DNS 域名解析是否集中化？這問題乍看之下很奇怪，因為 DNS 從設計上就是高度去集中化，所有資料庫都將內容分散放置在網際網路各處。DNS 的資訊模型包含資訊複本，藉由移除分散式資訊結構中的潛在單點失效，確保系統的韌性及規模。DNS 的查詢協定容許多種備用選項以強化域名解析的穩健，遞迴域名解析也包含靠近客戶端的快取儲存。這些聽起來都像是可以抵擋任何形式的合併集中、高度多元分散的資訊管理模型。

但現實是這樣嗎？

Geoff 從 DNS 解析量測方式談起，透過指標數據資料回答此問題。

市場集中指標

首先是用來形容市場集中化、市場支配優勢的指標。

- 澳洲消費者與競爭委員會（Australian Consumer and Competition Commission，ACCC）視掌握 70%以上市場的單一事業體為具有市場優勢。英國對「壟斷」的法律定義則是單一企業市占率超過 25%。
- 四大廠商集中率（four-firm concentration ratio）稍有不同，是看市場中前四大業者的市占率總合。實際也可能是前三或前五大廠商，但評估重點是寡頭集團的存在與否。若集中率超過一半，就能合理質疑市場集中。
- 賀芬達指數（Herfindahl-Hirschman Index，HHI）呈現產業中單一廠商的市占率，計算方式為將市場上前 50 大廠商個別產量占市場總產量的比例進行平方總和。通常賀芬達指數超過 25%即視為市場集中化，超過 10%則有「適度集中傾向」。

DNS 解析市場

註冊管理機構和頂級域名的一對一關係，代表企業市占率通常等於轄下 TLD 受歡迎的程度。另一方面，由於很難比較「握有上百萬個從沒用過的罕見域名」和「持有少數非常受歡迎的域名」，受理註冊機構市場的集中化問題因此較不明顯。

在此前提下，接著就可以利用前述指標衡量 DNS 域名解析市場的集中程度。

首先必須了解域名解析的本質。使用者端的應用程式欲解析 DNS 域名時，本地解析器會將查詢傳送至設定好的遞迴解析器，由後者向多個權威伺服器進行一系列查詢並找到適合的權威伺服

器，查詢到回應後再回傳至本地解析器。一般而言，DNS 域名解析有 2 步驟：「本地至遞迴」與「遞迴至權威」。

若進一步檢視這 2 步驟的市占率，則「本地至遞迴」中，域名為何並不重要，因為遞迴解析器本就必須提供所有域名的解析。所以要看的應該是使用或相互依賴性，如每個遞迴解析器收到的查詢數量，或不重複使用者（或不重複本地解析器）的數量。

使用者數量的指標則不適用權威伺服器，因為理論上，每一個權威伺服器都可以收到來自任何遞迴伺服器、代表任何一個使用者傳來的查詢。檢視每權威伺服器收到的總查詢數量可能更合理，因為就很多方面而言，受歡迎域名的多筆查詢，跟很多筆少見域名查詢一樣。在檢視權威伺服器業者的市場集中化時，域名本身不比伺服器營運方重要，所以需要連結權威伺服器與業者，並檢視每個業者經手的查詢數量。

前面介紹市場集中指標，並解釋 DNS 域名解析分為「本地至遞迴」及「遞迴至權威」2 步驟。接下來透過觀測數據資料分析，檢視遞迴解析器市場是否集中化。

為分析此問題，需量測每遞迴解析器的使用者數量分布。APNIC 依解析器的 IP 位址，將解析器分成幾個類型：

- 解析器和自治系統（Autonomous System，AS）及終端使用者（ISP 的遞迴解析器）相同。（sameas）
- 已知的公共 DNS 解析器。
- 解析器位址的地理位置與終端使用者的國碼相同。（samecc）
- 解析器位址的地理位置與終端使用者的國碼不同。（diffcc）

下圖為測量結果：

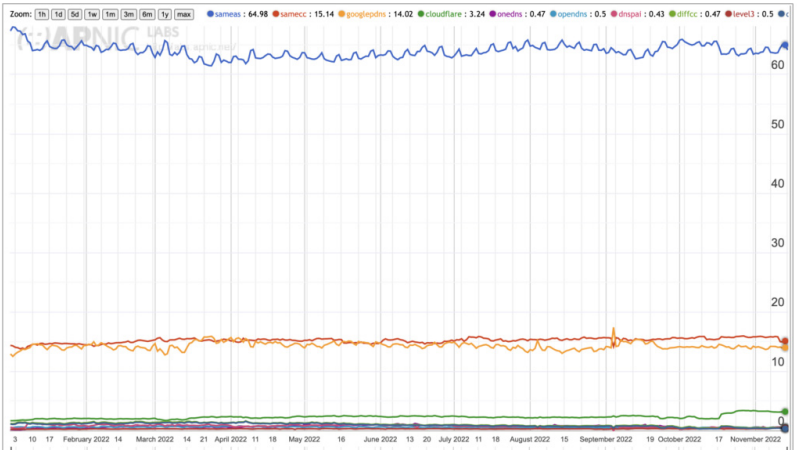


圖 1：遞迴解析器市占率

上述分類的使用者數量比例則如下表。將近三分之二的使用者將查詢傳送至自身 ISP，15%使用者將查詢傳送至位於本國的遞迴解析器，很可能是因為他們的 ISP 使用另一個 AS 的遞迴解析器。14%使用者利用 Google 的公開 DNS 解析器，3.2%使用 Cloudflare 的 DNS 解析服務，沒有任何其他公共 DNS 解析服務的使用者數量超過 0.5%。

解析器種類	使用者數量比例
Sameas	65.0%
Samecc	15.1%
Diffcc	0.5%
All Open Resolvers	20.0%
Google Public DNS	14.0%
Cloudflare 1.1.1.1	3.2%
OneDNS (China)	0.5%
OpenDNS	0.5%

DNSPAI (China)	0.4%
Level3	0.5%
114DNS (China)	0.2%
Green Team (Israel)	0.05%
Quad9	0.05%
Neustar	0.02%

所有公共解析器總共佔 DNS 解析市場的 20%，若比對此資料與每國相對市占率，就可比較公共 DNS 解析服務在各國的重要性如圖 2。

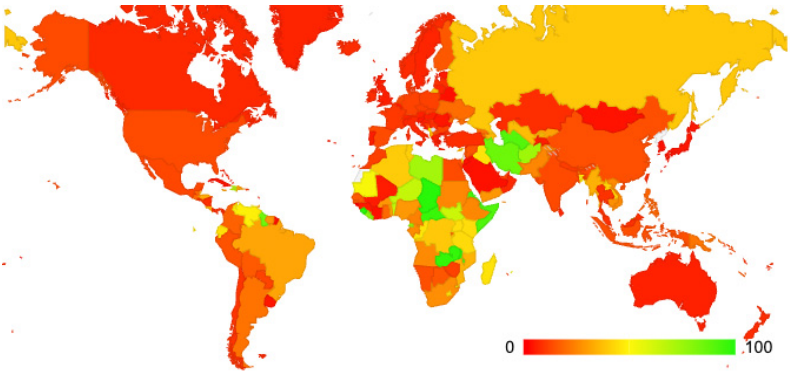


圖 2：各國公共解析器使用率

在部分非洲國家及蓋亞那、伊朗、阿富汗及土庫曼中，公共 DNS 解析服務是主流。換句話說，除了在非洲及少數中亞國家中，公共 DNS 解析器並不佔主導地位。

另一方面，從表 1 可看出 Google 的解析服務是第二名的 4 倍。若將以上各國使用率分布的比較套用至 Google 的公共 DNS(Public DNS，PDNS)，或可發現其他觀點。

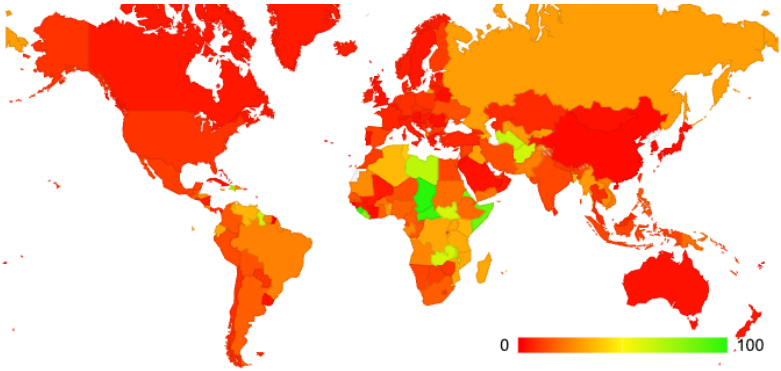


圖 3：各國 Google PDNS 使用率

圖 3 與圖 2 的分布情形類似，非洲中部與東部、伊朗及阿富汗以 Google 的 PDNS 為主。若觀察 Google 的 PDNS 使用者分布，則如圖 4：

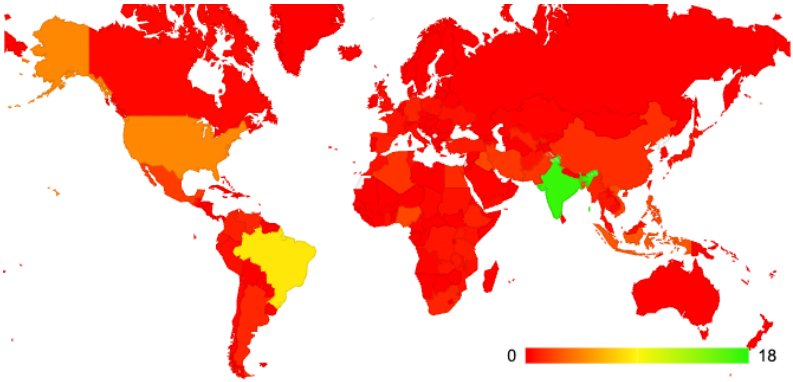


圖 4：Google PDNS 使用者分布

這裡則可看出，PDNS 使用者數量以印度和巴西最多，17%的 Google PDNS 使用者位於印度、8%位於巴西，5%位於美國。

直接使用 ISP 遞迴解析服務的使用者占 65%至 80%，公共解析器服務市占率僅 20%。由此可知，Google 在大部分國家的解析服務市場中不具主導地位。公共解析器在 DNS 遞迴解析市場中的 HHI 指標為 4%，Google 的 HHI 指標為 2%。因此，遞迴解析市場並未集中化。

若只看公共 DNS 解析，而不看 ISP 連帶提供的 DNS 服務呢？

- 單一事業體主導：Google 享公共 DNS 解析市場的 7%市占率。
- 四大廠商集中率：Google、Cloudflare、114 DNS 和 OpenDNS 總市占率達 6%。
- HHI 指標為 49%。

若只看公共解析器，則市場高度集中，且 Google 具主導地位。

限制條件及說明

基於 DNS 和量測使用者對象的本質，此結果有許多先天限制條件。

當本地解析器向 DNS 送出查詢，通常至少有 2 到 3 個遞迴解析器會收到同一筆查詢。本觀測中，在 6 成情況下，客戶端本地解析器的查詢會傳給至少 2 個遞迴解析器。

回應使用者查詢的解析器和所有「收到」查詢（但不一定有後續動作）的解析器不同，而本觀測數字呈現「收到」查詢的解析器數量。若只看「回應」查詢的解析器，則 Google 的市占率從 14%提升到 17%。這極可能是因為 Google 回應最快，而此高速來自其雲端平臺的高密度。

此實驗中還有一個無法觀測的因素。鑑於快取在 DNS 中的重要性，使用者數量大的解析器效能通常高於使用者數量較少的解析器。所幸使用 anycast 技術的極大型 DNS 遞迴解析複合架構足以抵銷此可能偏誤。

APNIC 的量測採廣大採樣調查，終端使用者包括 ISP 用戶、企業網路，和其他未明確分類的網路。若深入檢視圖 2 的每日用量數字，可看出週末用量上升，Google 則相反，週間使用量較高。換句話說，企業服務網路傾向使用公共 DNS 服務，而一般消費者的個人使用則仰賴 ISP 附帶的 DNS 服務。也可以說，上述呈現的市占率數字並不反映消費市場、企業或任何特別產業的 DNS 服務使用分布，而僅概括顯示 DNS 服務的整體使用分布。

除此之外，如 Apple 的私密轉送（Private Relay）服務等保護使用者隱私的服務使用率亦日益增加，也會導致觀測資料難以正確呈現使用者的位置和身分。

權威伺服器的環境與「本地至遞迴」截然不同，無法從不同權威伺服器的查詢資料看出「遞迴至權威」的查詢或使用者類型。這裡看的是各權威伺服器收到的查詢數量。

APNIC 與 Cloudflare 簽訂的的合作研究協議，取得 1.1.1.1 遞迴解析器的部分資料：雖然不知查詢來源身分，但可知道查詢內容（域名）。透過尋找離查詢域名最近的域名伺服器，APNIC 找出回應單筆查詢的域名伺服器及其 IP 位址和自治系統號碼（Autonomous System Number，ASN）。本數據資料不看權威伺服器實際收到的查詢數量，而是計算使用者取得來自此伺服器（無論是否來自遞迴解析器快取）回應的數量。

僅支援一個極受歡迎域名，或支援很多筆不常見域名的伺服器，收到的查詢數量都會很高，也因此伺服器業者的市占率不會相差太多。本觀測每 24 小時定點紀錄 Cloudflare 解析器收到的查詢，

分類查詢內容並自行解析以找到最近的權威伺服器，進一步找出 IP 位址和 ASN，最後依各 ASN 收到的查詢數量排序。

以 2022 年 9 月的資料舉例，共觀測到 26,971 筆不重複 ASN，其中前 50 名 ASN 擁有 89.2%查詢，顯示某種程度的集中現象。

從圖 5 的累積分布圖表，可看出此空間高度集中化的現象。

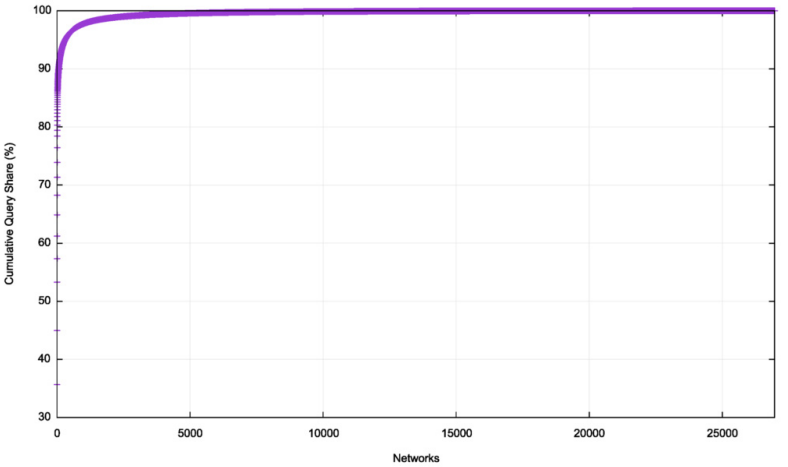


圖 5：權威伺服器累積分布

上述資料中的前十大權威域名主機如下表。

排名	ASN	伺服器收到查詢比例	累計	名稱
1	AS16509	35.7%	35.7%	Amazon-O2, US
2	AS13335	9.3%	45.0%	Cloudflare, US
3	AS15169	8.3%	33.3%	Google, US
4	AS21342	4.0%	57.3%	Akamai, US
5	AS8068	3.9%	61.2%	Microsoft, US
6	AS397239	3.7%	64.9%	UltraDNS (Neustar), US

7	AS714	3.4%	68.3%	Apple, US
8	AS31898	3.1%	71.4%	Oracle, US
9	N/A	2.5%	73.9%	NXDOMAIN
10	AS62597	2.5%	76.4%	NSone, US

如利用此資料，參考前述壟斷指標檢視 DNS 權威伺服器市場，結論如下：

- 單一實體主導：Amazon 市占率達 7%。
- 四大廠商集中率：Amazon、Cloudflare、Google 和 Akamai 總市占率達 3%。
- HHI 指數為 15%。

權威主機市場有「適度集中」現象。

限制條件和其他說明

1. 地理集中化

從以上觀測資料可看出，代管權威域名伺服器的前 10 大網路企業握有四分之三的「遞迴至權威」查詢流量，而這 10 家公司中有 9 家為美國公司，唯一的第 9 名不是公司，是根區伺服器系統。

2. 根伺服器問題

約 2.5%查詢的回應是來自根區的「NXDOMAIN」。然而，根據根伺服器營運方報告，根伺服器收到的查詢約 7 成都會導致「NXDOMAIN」回應。兩者之間似有矛盾，但通常只有遞迴解析器沒有快取紀錄或快取過期時，根區才會收到查詢。在遞迴解析器收到的查詢數量遠高於根伺服器的前提下，後者的 NXDOMAIN 比例相較之下遠高於前者亦合理。Cloudflare 資料的 NXDOMAIN 比例相較於一般 ISP 網路本來就偏低，也是另一種可能。

3. Amazon 與 Route 53

第一名的 Amazon-O2 和 AS16509 其實是兩組權威伺服器。Amazon 有自己的權威伺服器服務 Route 53，除此之外，很多人也利用 Amazon 虛擬服務營運自身權威伺服器。此資料中將兩者合併，可能造成讀者誤解。

4. 限制

本分析乃依據某一天僅 24 小時、來自單一公共遞迴解析器服務的資料。此樣本並非全貌，也可能有企業使用或瀏覽器使用偏誤。DNS 查詢數量也並非普世接受的市占率分析指標。

結論

以遞迴解析器而言，多數使用 ISP 附加解析服務的現象，抵消了公共 DNS 解析市場的高度集中化，全球市場在業者多元度上也相對平衡。

權威伺服器市場則不同，前四大業者掌握 57%查詢數量，HHI 指數則顯示有適度集中的現象。

公用基礎建設如 DNS 的市場高度集中可能引發多種顧慮，其中之一是若國家數位經濟僅仰賴少數或單一供應商，則會產生關鍵弱點。雖然這在權威伺服器市場是個問題，但在遞迴解析市場卻不是。

另一個集中化的隱憂則是獨佔或聯合壟斷，進一步導致哄抬價格或其他市場濫用行為。但這在遞迴解析市場完全不成問題，因為沒有 ISP 在為 DNS 解析額外向使用者收費。換句話說，對消費者而言，DNS 解析基本上是免費的。

權威伺服器服務的集中對使用者是否有潛在影響？有可能，但 Geoff 認為此議題不能自外於數位市場的獨佔競爭本質。數位時代的經濟環境和 19 世紀末的工業化時代大不相同，當時的反托拉斯

法也未必適用當代產業。他預計另外撰文深入研析此議題。

參考資料：

https://blog.apnic.net/2022/11/22/looking-at-centrality-in-the-dns/

個人意見：走入黑暗

Geoff Huston

https://blog.twnic.tw/2022/12/20/25037/

本 APNIC 文摘原標題為 [Opinion] Going dark，由 Geoff Huston 撰文。

很多人認為實用的大眾傳播工具，必須保護傳輸內容的隱私與完整性。郵政系統會緘封信件，電話系統中，大部分監聽都需在法院命令或合法監督下執行。大眾傳播系統要實用，就必須保護使用者的隱私。

網際網路也適用相同原則，只是過去從未嚴謹實施。隨著網路傳輸隱私興起，以隱私換取效率和速度的開放協定已成為歷史。現在所有公共網際網路上的網路傳輸，都必須以適當措施保護隱私。

另一方面，這樣的改變並非毫無連帶成本，Paul Vixie 在 NANOG86 的「走向黑暗：看不見私人管理網路導致的隱私及安全災難」（Going Dark: catastrophic security and privacy losses due to loss of visibility by managed private networks）簡報中，細數這些連帶成本。本文由 APNIC 首席科學家 Geoff Huston 介紹 Paul Vixie 簡報內容，並分享自身感想。

Paul 指出，要有效保護當代網站的安全，本質上必須觀察他者行為。由於無法挑選或排除任何終端、或驗證終端供應鏈，我們只能透過觀察終端傳輸的信號（封包或流量），來管理自身終端的風險。

Geoff 解釋，Paul 的意思是，並非所有網路訊務都友善無害。有鑑於此，大多數人選擇將網路分割成「家用」、「公司」等不同區

塊，並依各網路區塊的需求，過濾惡意不受歡迎的訊務。網路之間的防火牆無所不在，仰賴訊務監控保障網站安全乃當代網路環境的基本假設。然而，這個假設基礎越來越薄弱。

Paul 觀察，網際網路過去幾十年來遭當權者理所當然的濫用，迫使網路工程任務組（Internet Engineering Task Force，IETF）改革網際網路協定套組，將端對端加密融入網路運作。傳輸層安全協定（Transport Layer Security，TLS）及相關擴充 Encrypted Client Hello（ECH）、DNS over HTTPS（DoH），以及取代傳輸控制協定（Transmission Control Protocol，TCP）的 QUIC 等因此出現。

如此加密設定下，防火牆、監控點或任何型態的網路營運方，都無法繼續偵測因感染、入侵、軟體更新中毒或潛在設計疏失等上百種常見安全威脅，而出現的終端異常行為。Paul 擔憂，很多網路營運人員和安全設備業者都沒有意識到這個環境變化，當務之急是直接了當、立刻重整他們的觀念，為下個時代制定新的實用方案。

我們現在面對的問題，是攻擊者占極度優勢：防衛方須全天候捍衛整個空間，而攻擊者只需要找到在特定時間點存在的一個弱點，就可以發動攻擊。在這對攻擊方極其有利的不平等關係中，受害的是當代社會的整體結構。

現在的情況有一部分原因來自 2013 年 IETF 對史諾登事件的反應。RFC 7258 主張的「全面監控是一種攻擊」，不知不覺被扭曲成所有、任何形式的網路層訊務和傳輸監控都是攻擊。終端和其他終端的溝通應該完全隱密，任何人都不得從中竊聽。

無可否認，Paul Vixie 簡報刻意採極端觀點，將此情境與「惡意軟體也有權利」的論述類比。我們還保有辨識並封鎖「惡意」網路訊務的選項嗎？如果防火牆已經失去功用，我們該如何保護安全？我們有辦法透過大幅改革終端系統軟體以改變慘淡的現狀嗎？還是已經無力回天？

Paul 的結論是網站安全管理員面對越來越隱蔽的網路，必須做出不堪的抉擇。他們只能介入端對端模型，在網站上利用代理應用監控並限制進出網站的訊務。

這令人不安的現實還不是全貌。不只網路防火牆已無力過濾惡意軟體和行為，加密內容並未因此安全，只是能透視加密的人換了。現在變成終端應用程式幫我們決定誰可以看到我們的資訊，或更慘，我們只是將所有資訊奉送給監視經濟中的巨頭，還不設任何附帶條件。

在抵抗政府監控的同時，我們是否只是轉而擁抱在監控資本主義粉飾下，更狡詐的數位跟蹤模型？Meta 或 Google 等應用程式業者，是否能取得我們自己都無從得知、關於我們的第一手資訊？

Geoff 結語指出，他和 Paul 一樣感到悲觀。就像現在的世界一樣，此發展看起來難以善終。

參考資料：

https://blog.apnic.net/2022/11/04/opinion-going-dark/

IPv6：地理位置定位是關鍵

E. Marie Brierley

https://blog.twnic.tw/2022/12/15/25041/

本 APNIC 文摘原標題為 When it comes to IPv6, we need to be promoting location, location, location，由 E. Marie Brierley 撰文。

本文提筆初衷是比較 IPv4 的電信級網路位址轉譯（Carrier-grade Network Address Translation，CGNAT）的總擁有成本（total cost of ownership，TCO），但作者 E. Marie Brierley 表示抵擋不住自己的 IPv6 倡議熱情，最終僅聚焦於 TCO 中他最關心的其中一個重要因素：企業的 IPv6 部署不足。

全球 IPv6 部署是場漫長的戰役。電信業者和企業遲遲未轉換至 IPv6，促升多元轉接技術及運作上的變通做法彌補此真空。雖然許多人認為這種方式是最佳實踐，但 Brierley 明言，這充其量只是擴充做法，從未、也不應作為長程的 IPv6 轉換策略。

甚至有主張認為，這些變通作法並未促進真正的 IPv6 轉換，而反而延遲了轉換進程。

那麼，我們手邊有什麼工具，可以幫助大家逃出這個惰性導致的死胡同？

Brierley 提議，大家不僅需跳出資訊科技的框架思考，更需以遞增收益的觀點，檢視 TCO 如何延遲 IPv6 部署。

從行銷學習

對任何企業而言，首要考量都是收益。收益的生成、保護，及管理是基於多種可調整的因素累積遞增，而非仰賴單一要素。

若以遞增收益最大化的概念看待 IPv6 部署，就可以強化轉換至 IPv6 的提案說服力，同時擴大潛在決策者和投資者人選。在行銷領域中，具影響力的決策者有更多搶先採用新興科技的空間，更重要的是，他們亦握有預算。Brierley 指出，在仰賴 IP 的地理位置定位解決方案急速成長下，行銷的技術需求更與 IPv6 轉換不謀而合。

點擊率（click-through rate，CTR）和轉換率分別是數位行銷的 2 個關鍵效能指標，關乎顧客點擊的商品，以及最終是否完成購買。全球的平均轉換率始終低於 3%，這也表示此領域中任何增益改善都是無價。而更精準的定位廣告和網站內容的目標客群地理位置，就是可能的方法之一。

Brierley 住在美國內華達州，但他的 IP 定位常顯示周邊其他州，如約 700 公里遠的加州洛杉磯，兩州之間的社經文化更有天壤之別。

Brierley 住的地方遍布土狼、蠍子、印第安保留區及牧場，但不正確的地理位置定位，卻將他定位到海灘、比基尼和羽衣甘藍沙拉的城市。在建立對數位行銷企劃至關緊要的人口群像剖析時，這種錯誤地理位置定位會浪費大量成本。

GeoIP 資料供應業者 MaxMind City 去年指出，IPv6 的地理位置定位比 IPv4 準確約 9%，高於 2020 年的 7%。根據 Brierley 個人經驗，在與行銷人士討論 IPv6 轉換時，IPv6 在地理位置定位上的優勢馬上就能吸引對方的注意（可參考案例研究）。一旦計算過對收益的影響和浪費掉的成本，他們每個都變成 IPv6 傳教士。此類對話讓他們更容易與 IT 合夥，甚至資助 IPv6 轉換，也成為打破 IPv6 部署僵局的大好良機。

合作和使用者案例是關鍵

有些意見主張 IPv6 部署高峰期已過，業界應該向前看，宣布 IPv6 已死並轉向使用其他協定。Brierley 不同意此說法。但他也指出，如果我們仍無法就為何 IPv6 轉換如此漫長達成共識，或更重要的，同意一起推動 IPv6 轉換的跨領域合作戰略，那現在這惰性導致的僵局極可能繼續延長，直到下一個變革出現。

參考資料：

https://blog.apnic.net/2022/11/16/when-it-comes-to-ipv6-we-need-to-be-promoting-location-location-location/

2022 年國家網路區段可靠度研究

Alexander Kozlov

https://blog.twnic.tw/2022/11/10/24740/

本 APNIC 文摘原標題為 The 2022 National Internet Segment Reliability Research，由 Alexander Kozlov 撰文。

Qrator Labs 每年出版國家網路區段可靠度研究報告，至今已第七年。此報告針對特定自治系統（Autonomous System，AS）及 AS 斷線對國家連線的影響提出洞見。以下為 2022 年報告的精華摘要。

過去 12 個月的主要改變

每年可靠性排名都會出現令人興奮的變動，這通常肇因於相應地區電信產業的變化。相較於 2021 年，2022 年間：

- 4 個國家跌出 IPv4 可靠度前 20 名：泰國、臺灣、西班牙及美國。
- 瑞士在 IPv4 可靠度大跌 8 位到第 10 名，主要因為 AS6830 取代 AS3303 成為該國最關鍵的 AS。
- 日本跌至 19 名，相較去年下降 7 個名次。
- 新加坡上升 7 個名次、盧森堡上升 5 個名次。
- 愛爾蘭自 2019 年跌出榜外後，首次重返 IPv4 可靠度前 20 名。

IPv6 可靠度

到 2022 年 9 月為止，約 37%的 Google 用戶使用 IPv6，這實際上等於支援 IPv6 的 ISP 比例。然而，IPv6 的主要問題部分連線（partial connectivity）仍存在。

除此之外，囿於互連競爭、非全球化 IPv6 部署等諸多原因，IPv6 的網路能見度仍有限，如 IPv6 可靠度與部分連線比例的對比（圖 1）呈現。

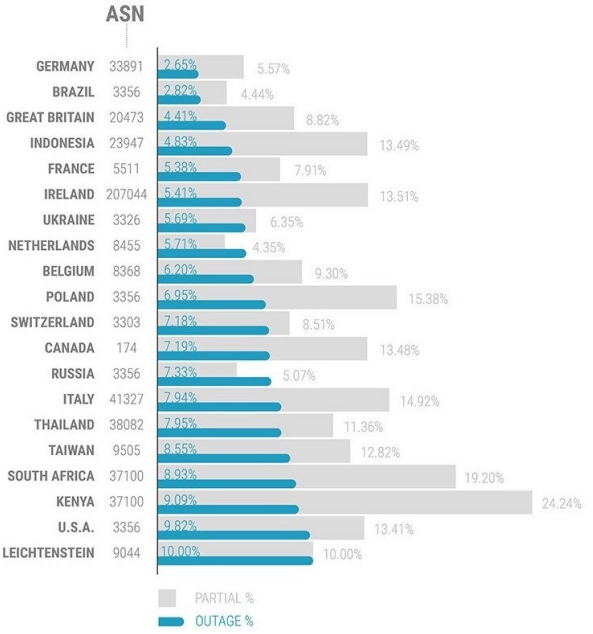


圖 1：IPv6 可靠度前 20 名國家分數

灰色代表部分連線比例，藍色代表斷線比例。比例越低可靠度則越高。

2022 年全球 IPv6 可靠度平均分數是 27.4%，相較於 IPv4 可靠度分數 26.7%，算是表現優異。

前 20 名中有不少國家部分連線超過 10%：印尼、愛爾蘭、波蘭、加拿大、義大利、泰國、臺灣、南非、肯亞和美國。列支敦士登的部分連線和 IPv6 可靠度都剛好是 10%。

若結合部分連線比例和「典型」可靠度比例（斷線），IPv6 可靠度表現最佳的國家是巴西（7.26%）、德國（8.22%）和荷蘭（10.06%）。最糟的是臺灣（21.37%）、波蘭（22.33%）和義大利（22.86%）。

根據 Google 的國家 IPv6 部署比例，2022 年 9 月前三名分別為法國（73.12%）、印度（69.16%）和德國（64.29%）。根據 Google 資料，所有其他國家比例都低於 60%。

另一方面，德法兩國都在 2022 年 IPv6 可靠度排名前五，但印度僅排到第 83 名，關鍵 AS（AS6453）可靠度 23.8%，部分連線分數為 7.38%。

寬頻網路和指標（PTR）紀錄

自 2019 年起，本報告試圖回答「一國的主要 ISP 對當地網路可靠度的影響力是否大於其他單位」的問題。實驗團隊的假設，是一國的主要 ISP（以客群或使用者人數而論）並不一定就是當地網路連線的關鍵。

為回答此問題，團隊分析反向 DNS 查詢使用的指標（pointer，PTR）紀錄。由於團隊已掌握全球所有國家的關鍵 AS，他們只需統計這些 AS 網路中的 PTR 紀錄，並與該地區所有 PTR 紀錄計算得出比例。此分析統計出以 PTR 為基礎的排名如圖 2：

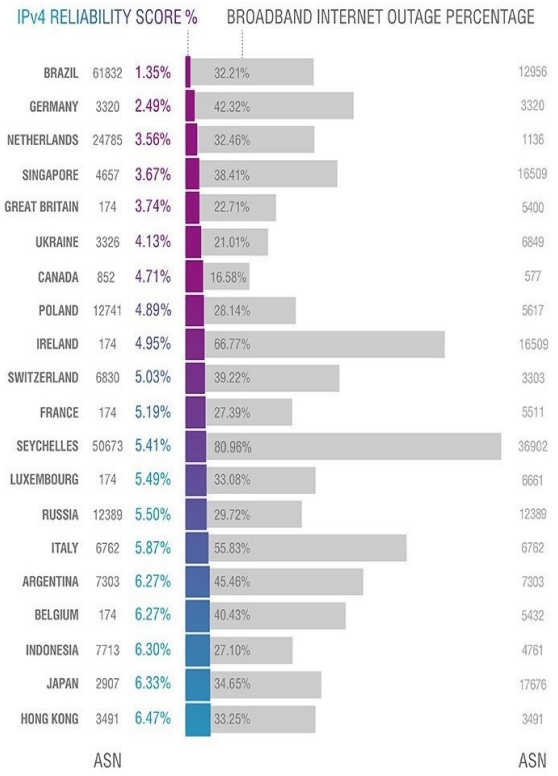


圖 2：2022 年 IPv4 可靠度排名（PTR-based）。

大多數案例中，不僅國家主要 AS 改變，比例也截然不同。在所有整體而言可靠（以全球網路可用性角度而言）的地區，單一 AS 斷線後，啟動 PTR 的 IP 位址隨之斷線的數字以數十倍激增。這可能意味國內主要 ISP 始終負責服務國內使用者。

因此，以上比例也可以代表在網路斷線時，將連帶受影響而離線（若無法及時轉換至第二大 ISP）的 ISP 使用者和顧客比例。以此角度而言，國家的網路可靠度明顯下降。

擁有兩家上游供應方可改善網路可靠度

報告的最終建議，無論對象是國家、城市、公司或終端使用者，要達到可接受的網路可靠程度，至少需有兩家上游供應方。

若有任何問題，歡迎寄信至 radar@qrator.net。

參考資料：

https://blog.apnic.net/2022/10/10/the-2022-national-internet-segment-reliability-research/

因應當代 DNS 挑戰

Moritz Müller

https://blog.twnic.tw/2022/08/25/24155/

本 APNIC 文摘原標題為 Addressing the challenges of modern DNS，由 Moritz Müller 撰文。

本文作者在荷蘭特文特大學（University of Twente）的團隊今年初與英國網路科技公司 sinodun 共同發表〈面對當代 DNS 挑戰：全方位教學手冊〉（Addressing the challenges of modern DNS: A comprehensive tutorial）。目標讀者是想更了解 DNS 的技術人員，本文將概略介紹手冊內容，並提出 DNS 目前面臨的挑戰。

了解 DNS 現況並非易事。大部分網路上的 DNS 教學都只介紹基本運作原理，只有極少數會提及如 DNS-over-HTTPS（DoH）或 DNS 集中化等當代發展。另一個問題則是以 DNS 為主題的正式文件，數量實在過於龐大。在 DNS 發展初期，定義此系統的 RFC 動輒高達百頁，至今更累積超過 200 份文件，相關說明高達 3,500 多頁。

作者團隊推出的教學手冊就是為了克服以上問題。本手冊基於作者團隊本身的 DNS 研究成果、營運經驗，以及他們對 DNS 相關 RFC 和學術研究的認識，說明當代 DNS 的樣貌，並指出 DNS 相關的關鍵安全議題。

手冊中列舉 DNS 實踐的最新進展，包括 DNS 訊息加密、DNS 基礎架構越來越集中化的現象，以及此現象如何影響 DNS 的功能和使用者、維運、開發和研究人員。手冊中也說明如何透過大規模量測觀察 DNS 的變化進展，並說明兩種不同的量測方式：從「外

側」查詢 DNS 的主動量測（如 OpenINTEL），以及搜集 DNS 伺服器上資料的被動量測（如 ENTRADA）。手冊中也說明如何設定量測及不同量測方式的優缺點。

除了當代 DNS 的實際運作現況外，手冊中也針對 DNS 的機密性、完整性和可用性，以及濫用因應等 DNS 的 4 大關鍵安全挑戰，提出現有的解決方案，並指出仍存在的挑戰。以下依序簡要說明：

機密性

DNS 訊息預設以明文傳送，而這造成很多安全和隱私問題。目前也有多種方式減緩這些問題，如所有主流開源解析器軟體業者都支援 QNAME 最小化，藉此減少 DNS 解析流程分享的資訊。也有利用 TLS（直接或嵌入 HTTP 或 QUIC）加密 DNS 訊息的技術。

當然，這些解方仍未臻完美。社群目前仍在找尋方法，讓客戶端自行發現，並與提供加密傳輸的解析器建立安全連線。另一方面，雖然 QNAME 最小化已相當普遍，但遞迴解析器的查詢機密性也仍是個問題。Oblivious DNS over HTTPS（OdoH）或 Apple 的 Private Relay 或可解決上述問題，但會影響效能。

完整性

原則上而言，DNS 數年前就已達到完整性要求。DNS 安全擴充（DNS Security Extensions，DNSSEC）在 2005 年就已標準化並安裝於上百萬筆域名和遞迴解析器。然而，DNSSEC 簽署在理想上應由送出請求的客戶端，而非遞迴解析器驗證。也唯有如此，無解析器 DNS（Resolverless DNS）等新技術才有可能實現。

另一即將出現的挑戰，是量子電腦及其可能對 DNS 訊息完整性帶來的威脅。量子電腦的發展或對 DNS 的實際影響都仍屬未

知，但作者團隊認為，現在就應該開始討論如何在量子世界中保護 DNS 安全。

可用性

由於在網際網路中扮演關鍵角色，DNS 中的資訊必須可以隨時供任何人使用。DNS 協定本身就有多個供維運人員加強 DNS 系統靈活性的方式，例如：他們可以把區域檔案複製放在多個域名伺服器上，以降低負載並加強可用性。遞迴解析器若遇到沒有回應的伺服器，就會自動找到另一個伺服器取得資訊。

但阻斷服務（Denial of Service，DoS）攻擊仍是威脅，而將 DNS 服務集中於少數供應方的因應方案，雖然表示供應方因此有更多資源投入於防範攻擊，但這也造成 DNS 生態系統集中化的問題。集中化不僅有隱私上的顧慮，更會擴大服務斷線的影響範圍。因此，我們仍必須持續尋找改善可用性又能避免集中化的解決方案。

濫用

濫用域名以發動網際網路上的惡意行為仍是一大問題。手冊中也提及偵測、減緩域名濫用的現行方案。然而這些解決手段並不長效，也無法防禦所有類型的攻擊。還有些 DNS 濫用的問題其實來自協定本身的設計，如仰賴 UDP 傳輸反而助長欺騙（spoofing）攻擊。DoH 和 DoQ 雖然某種程度上能解決這問題，但基於對效能的影響，仍無法大規模部署。

有時針對某一挑戰的解方，反而又造成新的問題。如加密 DNS 訊息是為了解決機密性的問題，但維運人員也怕這樣反而讓偵測 DNS 濫用行為變得更困難。

其他域名系統帶來的靈感

雖然 DNS 是網際網路上唯一普及的域名系統，但的確還存在別的域名系統。手冊中也檢視以區塊鏈為基礎，如 SCION 和 NDN 等其他域名系統，探討這些域名系統是否能應付 DNS 的挑戰，或帶來新的靈感。

點此可線上閱讀手冊全文，或下載 PDF 檔案。

參考資料：

https://blog.apnic.net/2022/07/29/addressing-the-challenges-of-modern-dns/

減少 IP 位址浪費

Seth Schoen

https://blog.twnic.tw/2022/07/14/23450/

本 APNIC 文摘原標題為 Cutting down on IP address waste，由 Seth Schoen 撰文。

本文作者 Seth Schoen 在今年 APRICOT 2022 APOPS 議程中，簡報了 IPv4 單播擴充專案（IPv4 Unicast Extensions Project）。本專案希望解放約 6 到 7%的 IPv4 位址空間，以回應 IPv4 位址稀缺的問題。

1980 年代 IPv4 剛萌芽時，某些決定讓一批位址變得「特別」，無法做為一般用途使用。即使這過去決策基於的緣由過去幾十年來都沒有發生，這些位址至今仍享受特別待遇。對 Schoen 來說，這也代表一批數量難以忽略的位址資源因此浪費了。

其中一種看待位址空間的方式，是關注 32 位元 IPv4 位址的位元模式，如何對應不同的位址類別（如圖 1）。

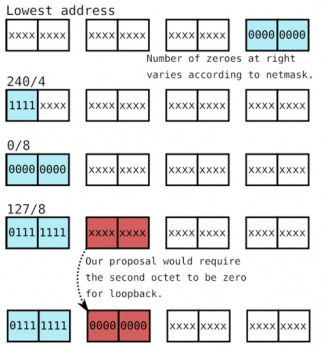


圖 1：Seth Schoen 及團隊希望開放的位址類型及範圍

如圖 1 所示，本專案希望開放的 IPv4 位址類別包括：

- 所有 IPv4 子網路中最低的位址（lowest address）
- 240/4（除 255.255.255.255 之外）
- 0/8（除 0.0.0.0 之外）
- 127/8（除 127/16 之外）

Schoen 的提案希望將這些位址定義為一般單播位址，而非過去的保留、無效或回送位址。上述目前不開放的位址當初都有各自不開放的理由，也因此，更動並開放這些位址也帶來不同的挑戰和機會。

挑戰與機會

開放最低位址，會移除所有本地網路中重複的的歷史廣播位址。此做法需要的變動最少，僅需當事人於本地網路中更改軟體設定即可。由於現行網路標準只在子網路中賦予最低位址意義，開放後可用的位址，本地網路外的外部主機也不需更改軟體設定，就可直接使用。這也表示，任何通過 EC2 連線測試（EC2 reachability test）可連接主機的人，都可以連接到其他網路中的.0（或其他最低號碼）。

此變動的好處極多，如每個大於/31 的 IPv4 子網路都將因此多出一筆位址。此做法亦無需位址政策實施程序，只要允許各單位做一個步驟，就可全面提升他們使用既有分配到 IPv4 區段的效率。

其他做法則需要 IPv4 目前使用的軟體變動，但 Schoen 指出，許多調整都已經很常見，如大多數主機就都已支援 240/4。目前 Linux 和 FreeBSD 都已經可支援最低位址開放所需的調整，OpenBSD 則多年前就已適用。

不少公司已經正在或考慮非正式地以私人位址空間擴充使用240/4，因為很多裝置已經容許此用法。將 240/4、0/8 和 127/8 作為可路由位址空間使用，無論是公開或私下，的確會出現政策問題（如這些區段分別能否、何時、如何正式作為公開或私人位址空間使用）。比起探討這些政策問題，Schoen 和團隊更著重在說服更多實施相關方更新軟體，最大化這些位址的相容性，如此一來，一旦網路社群就上述政策問題達成共識，便能立即啟用這些位址。

雖然 Schoen 和團隊希望隨著相容性問題解決，這些位址最終能在公共網路中使用，但他們也了解，正式或非正式地以私人位址空間使用這些位址，對網路營運方仍有價值。

針對此提案的反對和顧慮很多，有些人擔心現行系統很大一部分都已經在程式上寫死了必定視這些位址無效並拒絕。也有人擔心此提案將威脅或妨礙 IPv6 的部署。針對前者，Schoen 建議無論如何先開始動作，盡力最大化未來位址開放後，能利用的價值和空間。針對後者，他們則堅持這是偽命題——改善 IPv4 位址供給不應被視為對 IPv6 的攻擊，任何單位也不應因此就不部署 IPv6。

就算是已經大量部署 IPv6 的單位，也可能基於多種原因仍需要 IPv4 空間。Schoen 認為這樣的狀態還會持續很長一段時間，這也是他們積極推動開放這些 IPv4 位址的原因。

事實上，Schoen 的提案並非首創。如 APNIC 首席科學家 Geoff Huston 在解析 2021 年 IP 位址使用發展的文章（IP addressing in 2021）中，就指出此議題在過去 15 年內反覆出現，不乏希望直接開放此類位址（又稱「Class E」）使用的 IETF 草案，也有持反對意見，主張開放 Class E 將導致實施問題的草案。

Huston 進一步指出，開放 Class E 的提案總會默默沈寂。一方面可能是因為缺乏時間和資源投入此議題，也可能是普遍認為開放 Class E 難以彌補 IPv4 耗竭的現實，不如推動 IPv6。每過一段時

間，類似提案又會出現，但在數場內容雷同的辯論後，往往又消聲匿跡。

如對 Schoen 的提案有興趣深入了解，可點此觀賞他在 APRICOT2022 的簡報影片。

參考資料：

https://blog.apnic.net/2022/05/31/cutting-down-on-ip-address-waste/

邁向無解析器 DNS

Geoff Huston

https://blog.twnic.tw/2022/06/13/23299/
https://blog.twnic.tw/2022/06/23/23444/

本 APNIC 文摘原標題為 The path to resolverless DNS，由 Geoff Huston 撰文。

DNS over HTTPS（DoH）的徵求意見稿（Request for comments，RFC）RFC 8484 提到「server push」。RFC 中對「server push」模糊帶過，僅警告「必須加倍注意確保被推送（pushed）的統一資源識別碼（Unified Resource Identifier，URI），是客戶提出請求時會送往之處」。

Server push 其實是在描述「客戶端無需向伺服器提出 DNS 請求／查詢，HTTPS 伺服器便能傳送一或多個同時包含查詢和答案的區段」的可能應用。然而，對如此引人入勝的可能性而言，RFC 中的描述似乎過於模糊難懂。Server push 的做法，也跟我們熟悉的 DNS 大不相同。

本文首先說明傳統 DNS 及開放 DNS 解析服務的興起，接下來則敘述衍生的 DNS 隱私顧慮，以及相應而生的新興技術，無解析器 DNS 亦是其中之一。

「傳統」DNS

作者首先解釋傳統 DNS 的域名解析系統架構。

通常在描述 DNS 系統架構時，會提到 3 種基本組成元素：本地解析器（stub resolver）、遞迴解析器（recursive resolver）和權威

伺服器（Authoritative server）。

在這架構中，DNS 域名解析是由本地解析器將查詢傳至遞迴解析器，遞迴解析器再將查詢傳送至根區伺服器，並從頂級域名（Top-Level Domain，TLD）、第二層域名、第三層域名……逐層查詢後，取得回應再經遞迴解析器回傳至本地解析器。

當然，如果所有 DNS 查詢實際上都如此運作的話，那整個系統將遲緩不已。當代 DNS 之所以能順暢運作，主要是因為遞迴解析器會儲存快取，唯有快取中找不到資料時，才會將查詢傳至權威伺服器。換句話說，一個遞迴解析器越常被使用、收到的查詢越多、儲存的快取也越多，回應查詢的速度也越快。

傳統上，這種 DNS 遞迴解析流程會由網路服務供應業者（Internet Service Provider，ISP）負責。

Google 開放解析器服務的興起

然而，以 ISP 為基礎的 DNS 解析做法有些問題。使用者並不為每筆 DNS 查詢解析付費，也不會把解析效能當成選擇 ISP 的考量點。對 ISP 而言，這表示 DNS 解析是無法回收的成本，因此他們不願費心經營或提升 DNS 解析效能，有些業者更試圖透過別的方式用 DNS 解析牟利，如販售使用者的 DNS 查詢資料。當然，後者有嚴重的違害隱私疑慮，在某些國家已被列為違法。

瀏覽器也是傳統 DNS 架構逐漸式微的因素之一。諸如 URL 的普遍、可以直接在網址欄輸入搜尋文字等，不僅產生安全問題，當代使用者也因此越來越分不清楚域名和搜尋之間的差異。有些 ISP 在此發現商機；既然使用者無法分辨域名或搜尋文字，不如就跟搜尋引擎收錢，直接將「無此域名」（NXDOMAIN）的 DNS 查詢回應轉向搜尋結果頁面。

最受此手法影響的是 Google。Google 穩坐全球搜尋引擎龍頭多年，而且搜尋服務也一直是該公司的主要資本。Google 手中握有的搜尋資料，是精準側寫使用者並成功鎖定廣告投放目標的關鍵，而販售這些資料的收入也是 Google 最主要的財源。

於是，Google 自己開始提供免費開放解析服務。跟過去小型自建、不成氣候的解析服務不同，利用公司本身強大的網路基礎建設，Google 提供的 DNS 解析服務具全球規模，而且他們保證兩點：一是永遠忠實回傳 DNS 回應，二是 Google 不會利用這些 DNS 查詢作為廣告投放的資料來源，也不會在紀錄中儲存任何足以辨識個人身分的資訊。

Google 的 DNS 解析服務快速、管理完善、精準、不篩選資訊，而且完全免費。Google 也是最早響應、啟用 DNS 安全擴充（DNS Security Extension，DNSSEC）的業者之一。不言而喻，Google 的 DNS 解析服務大受歡迎，全球四分之一使用者的 DNS 解析環境都會用到 Google 服務，雖然只有 14%全球使用者真的以 Google 解析服務為第一首選。

Google 和其他開放 DNS 解析服務的不同，在於 Google 的商業模式支持其持續投入資金，維護並改善 DNS 解析服務。投資自家的 DNS 解析服務，實質上能強化釐清 DNS 解析和搜尋的差異，更有助於 Google 進一步鞏固其搜尋引擎霸主的地位。

DNS 隱私的興起

然而，公開 DNS 解析服務也帶來另一種隱私和資料完整性風險。不再使用 ISP 提供的遞迴解析器，代表客戶端本地解析器送出的查詢，必須經由公共網際網路抵達遞迴解析器。

本地解析器和遞迴解析器之間的 DNS 交流，使用未加密的用

戶資料報協定（User Datagram Protocol，UDP），無法防範竊聽或中途竄改。本地解析器基本上不會執行 DNSSEC 驗證，所以無法偵測發現遭竄改的訊息。DNS over UDP 也不執行任何類型的伺服器驗證，這表示，即使開放 DNS 解析器的位址被路由挾持轉向別的 DNS 解析器，本地解析器也不會發現。簡單來說，遠離使用者的 DNS 解析，會產生訊務遭妨礙或監聽等一系列的問題。

目前集中於本地—遞迴連線加密傳輸的技術包括：

- DNS over TLS（DoT）：利用 TLS 安全協定建立的加密通道傳輸資料（RFC 7858）。
- DNS over QUIC（DoQ）：利用 QUIC 安全協定建立的加密通道傳輸資料（RFC 9250）。
- DNS over HTTPS（DoH）：利用加密 HTTPS 安全協定傳輸資料（RFC 8484）。

這些做法的相同之處，在於本地解析器能夠驗證遞迴解析器身分，藉此減緩各種傳輸遭中途攔截的風險。這些做法能成功阻擋大部分的中途挾持轉向或竄改的威脅，但無法避免竊聽。

DNS over HTTPS

如果 DoT、DoQ 和 DoH 都可以有效防止本地和遞迴解析器因網路中轉被分開的問題，為什麼 DoH 還沒消失？

一種看法是 DoH 根本沒必要。雖然 DoH 有效將 DNS 查詢和回應藏在 HTTPS 訊務中，有心人士還是可以竊聽緊接的下一筆訊務以推斷原始的 DNS 交流。更全面的做法是把所有訊務都塞進一個加密通信中，就像 VPN 一樣，但如果已經使用 VPN 的話，DoH 其實沒有什麼額外的安全效果。

DoH 不只和網路訊務一起使用 port 443，還會使用通用 HTTP 快取控制，管理 DNS 回應的本地庫存。HTTP/2 和 HTTP/3 都支援

平行傳輸、重新要求回應和表頭壓縮，應用程式無需使用本地解析器，可以選擇將 DNS 查詢傳到任何自選的 HTTPS 伺服器。更重要的是，HTTP/2 和 HTTP/3 都含有 server push：

HTTP/2 容許伺服器在回應客戶端送出的請求時，連帶預先傳送（push）另一筆回應（和預期將收到的對應請求）。這在使用者知道客戶會需要多筆回應以完成原始請求時很有用。（RFC 7540）

HTTP/3 中也有類似功能：

Server push 是一種互動模式，容許伺服器在預期客戶端將提出請求時，事先將該筆查詢和回應同時推送（push）給客戶端。這種做法是用網路用量交換降低延遲。HTTP/3 的 server push 和 HTTP2 類似，但使用不同機制。

每筆 server push 都有伺服器指派的單一推送 ID。此推送 ID 是用來在 HTTP/3 連線的不同脈絡中指涉此「推送」（push）。（draft-ietf-quic-http）

這表示伺服器在回傳 HTTP 查詢回應時，可以同時將未查詢的 HTTP 物件打包傳送到客戶端。傳統上，這些物件可能包含 HTML 樣式表、圖片和其他元素，現在有了 DoH，物件中還可以多加上 HTTP 包裹的 DNS 回應。如此一來，客戶端可以直接使用 DNS 回應，無需再經歷 DNS 解析和衍生的延遲或隱私問題。

但客戶端仍面臨一個問題：他怎麼知道伺服器推送的是真實的 DNS 回應？雖然傳送路徑已經加密以防止第三方竊聽或偷換，但仍無法保證伺服器傳送的 DNS 資訊正確。當然，這種不確定性並非無解析器 DNS 所獨有。

目前唯一能解決此問題，確保來源真實的方案是 DNS 安全擴充（DNS Security Extensions，DNSSEC）。若查詢域名有 DNSSEC 簽署，則無論客戶端是透過 server push 或傳統的 DNS 解析流程取得回應，都可確認資料為真。

在傳統 DNS 解析流程中，若域名有 DNSSEC 簽署，客戶端還需經歷一系列驗證確認後回傳等繁瑣步驟，這會拉長整體解析時間，也因此本地解析器很少執行 DNSSEC 驗證。在 DoH 的 server push 模式中，上述驗證確認回傳等需要的物件，則都由伺服器這邊推送。後者顯然可以提升使用者體驗，但問題是使用者實際上也難以確認伺服器聲稱的 DNSSEC 簽署是否屬實。

為什麼無解析器的 DNS 引人興趣？

作者認為，這要從網際網路的經濟版圖變化談起。

現在的網際網路，是靠提供內容和服務創造經濟價值。奠基於通用基礎建設和協定層的免費穩定上，應用層持續開發商機並回收利潤。這造成的問題是通用基礎建設缺乏改善演進的動機，而應用層等不及底層架構跟上自身需求，於是把所有問題帶到應用層上，自行試圖在客戶端解決。

無解析器 DNS 就是此情境下的產物。這個做法不會改變 DNS 的通用基礎架構，只是改變應用程式使用 DNS 的方式，藉此強化應用程式對使用者經驗的掌控。

過去十年來，網際網路變得更快也更強健：

- 內容傳遞網路（Content Delivery Network，CDN）的應用把內容和服務帶到使用者身邊。
- 能善加利用平行傳輸的非封鎖式傳輸協定（如 QUIC）出現。
- TCP 和許多網路行為持續調整，創造更快、效率更高的網路傳輸。
- DNS 現在承載更多資訊（如 HTTPS 紀錄），所以服務可以更快啟動。

然而，在這些改善演化中，唯有 DNS 仍停滯不前。事實上，DNS 仍是遲緩、隱私洩露、不明原因失敗等諸多問題的來源。

無解析器 DNS 不會一次解決所有 DNS 的問題。這本來就是不可能的任務。但以 HTTPS 為基礎的應用程式和服務能因此取得大部分應用程式與服務品質的掌控權。它會比傳統 DNS 快很多。它可以大幅淡化客戶終端在傳統 DNS 解析流程中的角色。它也可能用來降低失敗頻率。基於這些原因，作者認為，無解析器 DNS 會是 DNS 演化進程中，值得關注的一步。

參考資料：

https://blog.apnic.net/2022/05/17/the-path-to-resolverless-dns/

利用 ccTLD 資料研究本地 IXP 影響

Terry Sweetser

https://blog.twnic.tw/2022/06/01/23295/

本 APNIC 文摘原標題為 Using ccTLD data to study the impact of local IXPs，由 Terry Sweetser 撰文。

研究網際網路路由資料常會發現有趣的趨勢。本文作者最近特別關注使用國碼頂級域名（country code Top-Level Domain，ccTLD）的網站和路由。網際網路協會（Internet Society，ISOC）研究多種脈絡下本地網際網路交換中心（Internet Exchange Point，IXP）的影響，而這鼓勵作者進一步探究兩者的交集。

作者已將研究結果整理成報告發布。此研究使用包含延遲、過路數（hop count）和自治系統號碼（Autonomous System Number，ASN）等技術性資料，但作者發現，ccTLD 使用富含網路工程師過去常忽視或避免的文化因素。也因此，本報告使用跨領域的研究方法進行研究。

資料揭露的重要發現之一，是商業和營運模式在這種等級的分析上很重要。以工程角度而言，營運模式指的是主機代管公司或網路如何建置、提供服務。

某些網路營運業者的營運模式，是他們本身的地理位置在離服務對象很遠的一兩處。對終端使用者而言，這表示他們無法享受低延遲；事實上延遲會很高，或他們會需要透過本地 IXP 存取目標網站，沒有任何好處。

上述模式的極端反例，則是營運業者部署多個 anycast DNS 及代理伺服器於多個 IXP。如此一來，他們能保持低延遲，對使用者

來說各種技術指標都很優異。

除此之外，還有兩種不同的營運模式。

大型雲端服務供應商標榜「把所有東西送到所有人眼前」、無所不在，但實際指標差距很大。他們的營運模式並非向客戶販售最佳化路徑；事實上，客戶可自行決定想採取的路徑。結果是 ccTLD 內容遍布網路中，不分地區、橫跨全球。

最後一種，也是最重要的營運模式，是在如日本、馬來西亞及印尼等國的當地組織。此模式裡文化因素特別明顯，網站都使用當地語言，域名使用當地 ccTLD，網站主機也都架設於本地的資料中心。

本地 IXP 尤其樂見最後一種模式。日本、印尼和馬來西亞的延遲表現指標分別是 6.17ms（91.34%）、10.78ms（89.62%）和 5.40ms（81.59%）。這些數字唯有良好的網際網路互連架構才能達成。

作者研究澳洲資料時，很驚訝地發現大部分澳洲網站（以域名數量計算）主機都設於海外，如新加坡、英國、美國及加拿大。Ng 和 Taneja 的 2019 年研究發現全球可依網路使用類似性，分成 5 個或 18 個群集。若進一步以 5 個群集的基礎分析，則可發現澳洲使用者瀏覽的網路內容來源，與上述主機位置一致。

Ng 和 Taneja 的 18 個群集分析中，東南亞和南亞地區的國家之間通常會因網路使用高度類似形成群集，但在此之中，新加坡的網路使用並不與東南亞地區類似，而更相近於西歐及美國。澳洲所屬的群集則包括紐西蘭、加拿大、葡萄牙和斯堪地那維亞地區。

網際網路的本地化是否是影響一國網路使用習慣的可能因素？資料顯示答案是肯定的。日本、馬來西亞和印尼的指標顯示這些國家的網路內容 8～9 成都是本地內容，而 ASN 來源分析更顯示，這些國家的本土企業都積極提供主機代管服務。

以印尼為例，有 42,909 筆 ccTLD 域名設置於超過 600 個本地 ASN 之上，僅 34,986 筆 ccTLD 域名設置於 75 個外國 ASN。印尼國內服務供應業者的總市佔率，以八比一的比例遠遠領先跨國企業和外國營運業者。這也顯示，在地化的概念在 ccTLD 資料中特別具有意義。

以 ccTLD 和 IXP 的宏觀角度而言，則可看出，本地互連和本地主機代管服務的技術維運不僅休戚與共，更仰賴當地企業、本土內容創作和本地網際網路使用者。

整體而言，真正加固這些元素彼此之間連結的，是內容和消費者之間的文化連結。兩者之間連結越緊密，營運模式符合活躍 ccTLD 的技術及文化需求的本地 IXP、主機代管基礎建設和網路服務供應業者，也將因此雨露均霑。

根據以上，作者向政府和發展單位提出簡單的建議：若想促成活躍的本地 ccTLD 使用，最重要的就是本地內容，以及連接所有國內網路營運業者的本地 IXP。

參考資料：

https://blog.apnic.net/2022/05/10/using-cctld-data-to-study-the-impact-of-local-ixps/

整體服務數位網路（ISDN）的終結

George Michaelson

https://blog.twnic.tw/2022/04/15/22710/

本 APNIC 文摘原標題為 The end of ISDN，由 George Michaelson 撰文。

澳洲的整體服務數位網路（Integrated Services Digital Network，ISDN）自 2018 年宣布階段性停止服務，2019 年開始逐步結束既有 ISDN 連線，此過程預計於今（2022）年完成。一旦結束，澳洲的 ISDN 將正式走入歷史。

在這值得紀錄的歷史時刻，本文介紹 ISDN 在網路發展史上的時代性意義，並說明 ISDN 為何不再實用。

ISDN 並非史上第一個高速網路，但是第一個全球廣泛布署的高速網路。ISDN 起源於國際電信聯盟電信標準化部門（ITU Telecommunication Standardization Sector）還是前身國際電話電報諮詢委員會（International Telegraph and Telephone Consultative Committee，CCITT）的時期，全盛期全球有 2,500 萬使用者。這跟當代網際網路的使用者人數比起來微不足道，但相較於同期間（1985 年前後）少於 1 萬人的最初代網際網路使用者，已經算是規模浩大。

就如同美國國防部高級研究規劃局（advanced research projects agency，APRA）的研究網路及相關網路協定，是成就當代網際網路的關鍵推手，成功大量製造並於全球布署電話線路的 ISDN，是電話領域的同等功臣。

ISDN 的歷史重要性必須從以下三點組成的脈絡中理解：實體

建設、電話和噪音，以及訊號處理編碼。

實體建設：銅質電話線路主場

如今大家都已習慣高速網路和光纖，很容易忘記銅直到最近都還是通訊線路建設的主要材料。對大多國家而言，實體電話線路是 50 到 70 年的公共建設投資，而且應由國營機關負責營運。

ISDN 就是在這個「電話實體線路要維持至少半世紀」的背景下誕生。而 ISDN 之所以成為當時通訊網路使用的技術，是因為它可以同時支援大頻寬（2Mb）和小頻寬（64Kb）。另一方面，建置電話網路基礎建設是以最便宜、製造成本最低的方式鋪建銅線，這表示銅質電路只有傳遞聲音時表現最好，若要再開發升級 ISDN 網路以傳送數位訊號，則需要投入工程成本。

升級 ISDN 之外的另一個選擇，是同時期的「數位用戶迴路」（Digital Subscriber Line，DSL）技術。DSL 跟信號技術的差別更大，而且隨著技術發展，註定需要汰換所有電話交換開關。這代表轉換至 DSL 的投資成本更高，風險也更大。

ISDN 相對保險，對電信業者而言，若僅考量中短程發展，ISDN 無疑勝出。ISDN 可以有效整合音訊電話、傳真和數位資料，也不需要發明新的位址系統。對當時認為電話將是通訊主流的世界來說，ISDN 是最合理的選擇。

電話與噪音

電話的基本模型，是通話兩端都有麥克風和喇叭。人類很擅長區分語音和噪音（所謂的雞尾酒會效應），一通電話能容忍的噪音極限也有已知的量測標準，也就是「量化失真單位」（Quantization Distortion Unit，QDU）。

同時間，人們發現，透過線路傳送 64Kbps 含有聲音編碼的數位訊號，會產生約 1QDU 的噪音和失真。換句話說，數位訊號跟直接傳送人聲的品質差不多，甚至更好。接著，人們又發現其實只需要 58Kbps 就能達到同樣的效果。當時決定以 64Kb 為標準，以容許 64Kbps 和 56Kbps 系統互相接軌，確保跨國通話連線。

然而，過不了多久，人們又決定改用數據機將數位訊號轉換成聲音了。銅質電話線路原本只是用來以類比訊號傳送聲音，然後被用來以撥接方式傳送音訊，之後又轉換用途，在 ISDN 中用來傳送低頻數位訊號。現在大家都有網路了，以數據機為主的電訊服務也成為主流，ISDN 相較之下就太貴了。一部分的原因在於，一般電信網路的本地電話服務都不會計時，但 ISDN 作為進階「數位」服務，無論通話距離都使用計時費率。因此，大家比起 ISDN 更偏好數據機連線，雖然對連線速度還是多有怨言。人們對連網速度的要求越來越高，但 ISDN 無法滿足此需求。

編碼與訊號處理

相較之下，與 ISDN 同期開發的 DSL 優勢盡顯。DSL 使用的頻率比一般聲音訊號更高，而且只要有分離器，就可以和一般電話一起使用。實測中證明，若把訊號頻率提高，就可使用既有的電話線路傳送數位訊號，用戶也可輕易連接網路。

但這需要能將高頻無線編碼解碼、植入除錯程式碼以解決噪音，以及同時處理多筆不同頻率的複雜訊號以增加頻寬的訊號處理能力，而且這種訊號處理必須能大規模執行。也就是說，要建置 DSL，整個業界都必須願意汰換現有設備，改用新的晶片、編碼程式和交換器設備。要讓業者情願投入如此資本，必須確定 DSL 會成為市場主流，將來不僅能回收成本還能賺錢。

「非對稱數位用戶迴路」（Asynchronous DSL，ADSL）因此雀屏中選。ADSL 可以限制上傳頻寬以擴大下載頻寬，避免噪音和串話。ADSL 還容許用戶同時使用電話和上網，不像數據機時代只能兩者擇一。在此同時，家用網路用戶數量激增，dot-com 泡沫吸引大筆資金湧入電訊產業，加上全球電訊市場的放鬆管制，ADSL 的商機明顯遠遠超過僅有 2,500 萬用戶的 ISDN，這也是整個產業決心轉向 ADSL 的關鍵時代背景。

結語

總結而言，聲音不再是主流服務，是 DSL 取代 ISDN 的主要原因。用來分開網路和電話訊號的分離器幾乎已成為歷史文物，因為很多人家裡已經不裝電話。至於銅質線路的未來，作者預測，除了可能限制僅傳送數位資料外，也可能作為複雜網路的本地迴圈、露天數位訊號傳送，或是後端同軸／光纖傳送，用來傳送 100Mb 以上的高位元訊務。

參考資料：

https://blog.apnic.net/2022/02/23/the-end-of-isdn/

域名伺服器和 DNS 解析器的多重意涵

Julia Evans

https://blog.twnic.tw/2022/04/01/22714/

本 APNIC 文摘原標題 The multiple meanings of ‘nameserver’ and ‘DNS resolver’，由 Julia Evans 撰文。

本文作者最近在編撰以域名系統（Domain Name System，DNS）為主題的雜誌，所以比平常人更常思索 DNS 詞彙的意義。其中特別引起他注意分別是「域名伺服器」（nameserver）和「DNS 解析器」（DNS resolver），這兩個詞在不同文脈下常有不同的意思。本文中，作者將試圖解釋這兩個詞可能代表的不同意涵，以及如何判斷文章中這些詞的意思。

域名伺服器的兩種意涵

域名伺服器有兩種類型，要判斷文章是在說哪一種，需要從文脈判斷。

意涵 1：權威伺服器

更新域名的 DNS 紀錄時，這些紀錄會儲存在名為「權威伺服器」（authoritative nameserver）的伺服器中。提到特定一個域名時，域名伺服器指的就是權威伺服器。以下是幾個文句範例：

- 更改域名的域名伺服器，以連接你的域名和 Wix。
- 幾乎所有域名都仰賴多個域名伺服器以強化穩定性；若單一域名伺服器失效或無法連線，還可以將 DNS 查詢送到其他伺服器。
- 遵循域名受理註冊機構網站中的指示，自行更新你的域名伺

服器紀錄。

意涵 2：遞迴伺服器，也稱為 DNS 解析器

這些伺服器會儲存 DNS 紀錄的快取。瀏覽器通常不會直接向權威伺服器傳送查詢，而是先詢問 DNS 解析器（也就是遞迴伺服器），由後者詢問權威伺服器並取得紀錄後，再快取儲存詢問結果。

在你瀏覽網際網路時，域名伺服器的意思就會是遞迴伺服器。以下是文句範例：

- 在某些裝置，如 Windows 10 中，要更改域名伺服器可能是需要無數點擊的痛苦過程。
- 你的 DNS 域名伺服器破壞了你的上網體驗嗎？此更新版本新增 1.1.1.1、1.0.0.1 和 9.9.9.9 域名伺服器。
- 更改你的網路設定，使用 8.8.8.8 和 8.8.4.4 作為 DNS 伺服器。

作者本人偏好使用「DNS 解析器」，主要是因為解析器的用法比遞迴伺服器更常見。

DNS 解析器的意涵

DNS 解析器可能是個函式庫，也可能是伺服器。雖然前文說解析器是伺服器，但某些時候解析器的確又是函式庫。

意涵 1a：本地解析器（Stub resolver，函式庫版）

本地解析器（可能是函式庫也可能是伺服器）本人不會解析 DNS 域名，它只負責將 DNS 查詢送到真正的 DNS 伺服器。以下首先說明函式庫版本的本地解析器。

舉例而言，libc 的 getaddrinfo 功能無法自行查詢 DNS 紀錄，它只會把查詢傳給在/etc/resolv.conf 中找到的 DNS 解析器。至於如何分辨；如果它是電腦作業系統的一部分且/或是函式庫，那就是本地解析器。

以下是文句範例：

- 解析器是在 C 函式庫中一套用來存取 DNS 的常式。這些是用來解析網頁位址的 DNS 伺服器，你可以列出最多三個，解析器會逐一嘗試，找出可用的伺服器。
- 若指令成功，你會收到「成功清除 DNS 解析器快取」的訊息。

意涵 1b：本地解析器（伺服器版）

本地解析器不一定一直都是函示庫。舉例而言，systemd-resolved 和 dnsmasq 都是本地解析器，但他們是伺服器。你的路由可能就是跑 dnsmasq。

這時候，本地解析器又稱為 DNS 轉寄站（forwarder）。判斷的方式：如果它是作業系統的一部分，或路由有在運行此功能，那大概就是本地解析器。

意涵 2：遞迴伺服器（伺服器）

如上所述，遞迴伺服器知道怎麼找到域名的權威伺服器。如果它是 unbound、bind、8.8.8.8、1.1.1.1，或由你的網路服務供應商（ISP）負責維運，那就是遞迴伺服器。

以下是文句範例：

- pfSense®軟體中的 DNS 解析器使用 unbound，一個具驗證功能的遞迴快取 DNS 解析器。
- 我們邀請你嘗試使用 Google Public DNS 作為你的主要或次要 DNS 解析器。
- 我在一家規模不小的行動通訊服務供應商工作，我們目前正在建置自己的 DNS 解析器。

最受歡迎的 DNS 伺服器詞彙

作者也稍微做了一個不是很科學的調查，計算最常見的 DNS 解析器 Google 查詢結果。以下是調查發現：

搜尋詞	Google 結果數
dns server	8,000,000
nameserver	4,200,000
dns resolver	933,000
public DNS server	204,000
root nameserver	42,000
recursive resolver	38,500
stub resolver	26,100
authoritative nameserver	17,000
dns resolution service	9,450
TLD nameserver	7,500
dns recursor	5,300
recursive nameserver	5,060

根據上述結果，簡單來說，當提到 DNS 伺服器的時候，最常意指的是域名伺服器和 DNS 解析器。其他如遞迴伺服器、權威伺服器、本地解析器相較之下都很少。

最後，作者表示，雖然整體而言這些詞的使用有些混亂，但他認為試圖解釋這些詞在不同脈絡的用法以釐清理解，還是比使用較不常見的同義詞彙好。

參考資料：

https://blog.apnic.net/2022/03/14/the-multiple-meanings-of-nameserver-and-dns-resolver/

位址意義演變

Geoff Huston

https://blog.twnic.tw/2022/03/11/22320/
https://blog.twnic.tw/2022/03/15/22324/

本 APNIC 文摘原標題為 Address semantics，由 Geoff Huston 撰文。

本文由 APNIC 首席科學家 Geoff Huston 撰文，從「位址」的意義談起，隨著網際網路技術及架構的發展進化，逐步探討 IP 位址的功能、相關技術和意義的演變。

在不同通訊系統中，無論是寄信時信封上的地址，撥打電話的電話號碼，或是在網際網路中傳送封包需要的 IP，縱使形式或指稱不同，但這些其實都是所謂的「位址」。

位址（address）通常包含 3 種元素，分別是身分識別（identity）、位置（location）和可聯絡性（reachability）。

身分識別和「獨特性」密不可分。理論上，正常運作的網路系統應指派專屬的單一位址給所有使用者；若否，則必須額外想方設法，解決多個實體使用同一位址可能衍生的衝突。以電話為例，一個號碼最好只能連通一支電話。

IP 位址在網際網路的架構中的角色類似電話號碼，但 IP 位址並非用來識別「電腦」，而是電腦連接網路的接口。也就是說，如果一臺電腦有多個連網接點，則這個電腦也會擁有多筆 IP 位址。

然而，只知道某個實體存在（有身分），卻不知道它位於網路中的什麼位置，在網路運作上等於沒有用。也因此，大部分的位址系統都會賦予每筆位址「識別身分」和「標示位置」至少兩種性質。

以電話號碼為例，國際電話號碼通用格式 E.164 可以用來標示號碼所在的國家及地區。IP 位址系統類似但更簡化，位址只分成網路和主機兩部分。同一網路中所有主機的 IP 位址會使用同樣的前綴，主機位址則各自不同。IPv4 容許自訂前綴長度，IPv6 則有更嚴謹的格式規定。從這角度而言，每筆 IP 位址都是網路識別碼和主機識別碼的串連，同時具有識別身分和標示位置的功用。

最後，位址當然必須包含某種「可聯絡」的資訊，用來協助網路中的其中一點連接另外一點。

在傳統的 IP 位址架構中，一筆 IP 位址必須能同時用來識別身分、標示位置，並提供網路要把封包傳送到哪裡的相關資訊。這種同一位址負擔多重角色的設計，有人認為是讓網路平臺得以極高成本效益運作的關鍵，也有人指出這是「意義過載」的典型案例，容易導致同一物件必須執行的某項功能，反而妨礙到另一項功能。

位址作為身分識別碼更深層的意義，在於位址和裝置之間因此具有獨一無二的連結。這在過去大型電腦盛行的年代很合理，但隨著客製化個人電腦成為主流，加上越來越多個人行動裝置進入網際網路，這樣的設計很快顯得不堪負荷。事實上，作者指出，位址系統的設計缺陷早在 1980 年代，網際網路商業化的時候就出現了。

回顧網際網路發展，作者更進一步點出，從撥接網路邁向大眾化開始，IP 位址的意義就已逐漸轉變。在撥接網路時代，使用者是透過撥打電話建立網路連線；線路另一端的服務供應商驗證使用者的登入資訊後，才會指派 IP 位址，在連線時間內，使用者都將利用這個指派 IP 位址上網。

這種作法是以「分時」（time-sharing）概念使用 IP 位址，使用者只在連網期間暫時使用獲指派的 IP 位址。接著出現了網路位址轉譯（network address translation，NAT）技術，以連接埠為基礎，讓多個本地裝置共享 IP 位址。

分時共享 IP 和 NAT 的技術，都在網際網路模型中引入間歇連線裝置的概念。這些裝置只有需要時才會連網，當然不能視為服務主機。於是，我們開始將連網裝置分成「客戶端」和「伺服器」兩種類別，客戶端需要時才連接伺服器，不必無時無刻連網，自然也不需除了連線登入帳密外的永久性網路識別身分（如 IP 位址）。

在這些 IP 共享技術流行的同時，IPv4 位址也逐漸枯竭，IPv6 因此誕生。

上述 IP 共享技術和 IPv6 之間最大的差異，在於前者只是被動新增的片面解方，後者則是 IETF 領導的組織力量，試圖預測未來業界需求，並提出滿足這些需求的技術方案。另一方面，驅動業界的兩大因素則分別是無止盡擴張、難以追趕的消費者需求，以及業者始終最重視的，如何降低服務成本。

作者特別指出，他不認為 IPv4 位址耗竭是 NAT 被大幅採用的主要原因；在 NAT 下，ISP 只需發給客戶端一筆 IP 位址，而由 NAT 轉換共享的多筆私人 IP 位址都由客戶端自行管理。對 ISP 而言，需要管理的 IP 位址越少就越省成本，換句話說，NAT 盛行單純是因為這樣最省錢。

總結而言，在網際網路發展的進程中，分時作法和 NAT 技術雖然起到改變 IP 位址意義的作用，但這並非因為業界有什麼先知灼見而刻意規劃執行的後果，只是在缺乏規範的市場中，生意人為了省錢而出現的慣例做法。

在前段中，作者分析「位址」的意義，IP 位址在網路系統中扮演的功能和演變進化，以及催生的相關技術發展，包括分時 IP、NAT 和 IPv6。接著將從 IPv6 談起，衍生探討近期網路發展，如何再度改變 IP 位址意義和功能。

IPv6 藉由微調細節，試圖重現 IP 位址在網際網路架構中的原始意義與功能。由於 IPv6 位元數更多，也有更多位元數可分派給

不同的連網存取介面。然而，對當時的業界而言，IPv4 位址枯竭的具體時間點仍未可知，相較之下，如何加快擴大網路基礎建設的規模，以跟上急速膨脹的連網客戶端數量和服務需求，才是真正的燃眉之急。

對業者而言，將網路分成客戶端和伺服器，且只有後者需要 IP 位址的方式習慣又好用，另一方面，服務層級的架構也在演進，現在客戶端與伺服器建立傳輸層安全協定（Transport Layer Security，TLS）時，可以附上欲存取的伺服器域名資訊，確保對方選擇回傳相應的 SSL 憑證。這代表特定服務與單一 IP 位址的連結不復存在；只有一筆 IP 位址的單一服務主機上可能搭載多種服務，同一種服務也可能被複製到多個各自擁有 IP 位址的服務主機上。

也因此，從 1995 到 2010 的 15 年間，IPv6 有充分的位址空間，供急速擴張的網路中所有終端和服務連結單一獨特的 IPv6 位址，但一來單一獨特的位址既非必要，二來從 IPv4 轉換至 IPv6 不符成本效益，整個業界都缺乏廣泛採用 IPv6 的實際動力。

在此同時，網際網路也非靜止不動。諸多根本性的改變仍陸續發生，而這些變化都對 IP 位址的角色具有深遠影響。

內容傳遞網路（Content Distribution Network，CDN）及雲端主導今日的網際網路。雖然缺乏實際公開數據，但作者聽聞，當今 7 成以上到 9 成傳遞至客戶終端的資料，都是影像串流。而 COVID-19 全球疫情促升的在家工作需求，也加倍促使企業將所有資料放到雲端，朝 CDN 的模式靠攏。

網路的角色也有大幅改變。若視網際網路為服務傳遞平臺，則網路的功能是將使用者瞬間移動到想要的服務所在。90 年代晚期的網路建設假設電腦運算和儲存很貴，而網路傳輸源源不絕又便宜。事後證明這假設是錯的，事實上，現在的電腦運算和儲存空間反而變得取之不盡又便宜。CDN 充分利用當代環境用之不竭的資

源，大批複製服務和內容後置於離使用者最近的雲端，大幅縮短傳輸距離，更進一步減少相關開銷和效能問題。整體而言，在 CDN 的世界中，網路服務更快、更便宜，也更有韌性。

如此一來，我們還需要獨特的位址嗎？在這個 CDN 主導的世界中，我只需要和本地 CDN 中的鄰居有所區別，何必在意其他 CDN 網路中其他數十億個客戶終端？獨特性有其成本，如今還有必要為了些微不使用 CDN 的服務，特地取得一筆專屬的 IP 位址嗎？

作者預言，隨著 CDN 繼續利用源源不絕的運算能力和儲存空間，服務和內容持續被移到離終端使用者近在咫尺之處，在全球位址基礎建設中，擁有獨一無二的位址將失去價值。

另一個網際架構變成今日樣態的原因，是沈沒成本。沒有人願意付錢升級既有的公共基礎建設，因為這些成本無法回收。於是，所有改變都是以繞道、跳過或鑽洞的方式進行，隨著時間過去，一個內含各種繞道鑽洞、由應用程式組成的上層架構形成，完全避開基礎建設全面升級的問題。在 IPv6 還因為沈沒成本而經過 20 年遲遲無法起飛的同時，諸如 QUIC、BBR、SVCB 和 HTPPS 等應用層技術的活躍，再一次證明應用層不想和基礎建設層有任何瓜葛。

作者認為，或許問題早已不再是何時才能從 IPv4 成功轉換至 IPv6。問題在於越來越多服務和應用程式企圖打造一個跟基礎架構層完全無關、壁壘分明的世界。作者感嘆，這就像當年使用 IP 封包跨國傳輸資料的網路出現時，對使用電路交換的電話通訊基礎建設不屑一顧一樣，十年河東，十年河西。

現在 IP 位址似乎只被當成暫時的通信期編碼代號，識別服務身分的重責大任都被轉嫁到域名系統。近來越來越多國家地區法規企圖將 IP 位址視為個人資料規管，作者多少感到諷刺，因為在網路裡，IP 位址通常只是暫時透過網路位址轉譯（network address translation，NAT）技術與某個客戶終端綁定，背後其實可能有數

百上千個人在共享這筆 IP 位址。

就連上述形容都已經又在改變。作者舉例說明，QUIC 使用的加密方式容許單一通信期綁定的 IP 位址變動，所以光是一個通信期間的 QUIC 通信期就可能有不只一筆 IP 位址。他總結，或許現在位址只剩下暫時標注不同封包流向的作用，過去的意義和功能都已流失。在今日的世界中，維繫網際網路的已不再是 IP 位址。

參考資料：

https://blog.apnic.net/2022/02/01/address-semantics/

東加王國：長距離通訊網路的脆弱

George Michaelson

https://blog.twnic.tw/2022/02/23/21775/

本 APNIC 文摘原標題為 Tonga and fragility of long-haul networks，由 George Michaelson 撰文。

最近東加王國火山爆發的事件，讓我們再次切身體會全球通訊遇到真實世界的嚴重天災時，是多麼不堪一擊。東加王國對外的通訊大部分都仰賴網際網路，而直至目前為止，東加王國的對外通訊仍未完全恢復。

東加的情況說明了常態性仰賴語音加載於網際網路協定（Voice over IP，VoIP）和即時訊息軟體，使用網際網路通話或視訊，將大幅削弱整體通訊系統的韌性。要和東加這種孤立島國建立即時通訊，除了網際網路以外，沒有什麼其他選擇。而當東加王國對外的唯一一條海底電纜失效，大部分人口也都因此無法與外界聯絡。

針對東加王國對外網路通訊斷線的原因，第一時間的主流猜測是電纜的登陸站停電，導致電纜無法運作。長期研究太平洋島國電子通訊的 Jon Brewer 在他的個人推特上說明，東加的海纜登陸站僅高海平面 1 公尺，而且所有關鍵設施，包括備用發電機都放在一樓。他推測，登陸站很可能被火山爆發引起的海嘯淹沒了。

Jon 在事件發生後持續更新推特，他引述紐西蘭先驅報（NZ Herald）的報導，分享電訊業者 Fintel 和東加海纜公司的事後調查結果，確認斷線原因是離岸 37 公里處的海纜毀損。來自其他媒體的後續報導，指出海纜似乎並非僅一處毀損。

海纜業者是利用一種叫做「光時域反射儀」（Optical Time Domain Reflectometer，OTDR）的儀器，量測源頭與毀損處之間的光反射延遲時間，進而判定海纜何處被切斷。即使海纜長達數千公里，OTDR 的檢測結果仍高度準確；也因此，目前應可確定海纜毀損是斷線的主因。

海纜修復船遍布全球各地，目前離東加王國最近的一艘位於巴布亞紐幾內亞。根據前述的紐西蘭先驅報報導，修復時程可能長達數週，甚至數月。

這事件再度顯示，天然災害導致通訊斷線並非空談，深海活動的確可能導致海纜中斷。2007 年的 APRICOT 暨 APNIC23 會議中，便曾因 2006 年底臺灣發生的恆春地震導致多條海底電纜中斷，而討論過此議題。當時包括臺灣、日本、中國及韓國之間的電信服務，以及這些地區連到美國、英國的電信服務都因此受到影響。

在架設海纜前，東加王國也建有衛星電子通訊的基礎建設。國內設有地球同步軌道衛星的地面站，但就像所有其他基礎建設一樣，必須仰賴國內電力。在 2013 年完成連結到斐濟的海底電纜之前，東加的網際網路和行動網路通訊都完全仰賴衛星，除了網速和延遲問題外，還常常可能因為天候不佳而有斷訊的問題。

不僅如此，衛星通訊還會受塵雲影響；宇宙塵會覆蓋衛星的碟形天線，削弱訊號。訊號減弱會影響網路頻寬，此時為確保連線品質穩定，就必須限制使用者人數。換句話說，若要讓多人使用網路，則網路連線品質和速度都會大幅降低。目前，東加王國的人民若使用衛星網路上網，可能常必須面對網路塞車、連線緩慢的問題。

根據「3-2-1」備份原則，備份時至少應 3 份，使用 2 種不同的備份方法，而且其中 1 份要存放異地。以東加王國的網路連線而言，他們的確有 2 種備份方式，分別是海底電纜和過去的衛星網路。雖然再接 1 條海纜可能會更好，但海纜並不便宜，而且以東加

的位置而言，要找到另一個負擔得起的連線端點並非易事。

在現實世界中，我們無法準備萬能的備用方案。有些災害的規模可能大到所有後備方案都失效。這對所有人都是個很好的警訊，有時候再怎麼努力規劃縱深防禦應變方案，在大自然的不可抗力下，人類仍束手無策。

最後，作者也代表 APNIC，真心祝願所有受此事件影響的人早日康復。

參考資料：

https://blog.apnic.net/2022/01/18/tonga-and-fragility-of-long-haul-networks/

Anycast 在 DNS 中的部署率

Raffaele Sommese

https://blog.twnic.tw/2022/02/21/21739/

本 APNIC 文摘原標題為 How widely adopted is anycast in the DNS?，由 Raffaele Sommese 撰文。

Anycast 技術能提升域名系統（Domain Name System，DNS）的效率，強化 DNS 靈活性以避免攻擊或失效，並有效擴大 DNS 域名伺服器基礎建設的規模。針對這些益處的相關研究不勝枚舉。然而，針對 Anycast 技術應用於頂級域名（TLD）和第二層域名（SLD）的研究卻很少見。本文作者來自荷蘭特文特大學（University of Twente），他的團隊與加州大學聖地牙哥分校（UC San Diego）的應用網際網路資料分析中心（Center for Applied Internet Data Analysis，CAIDA）以及荷蘭國碼頂級域名（ccTLD）註冊機構 SIDN 的研究團隊 SIDN Labs 合作，將 Anycast 於 TLD 及 SLD 的部署量化。研究發現，TLD 及 SLD 的 Anycast 部署率自 2017 年顯著成長，少數幾家大型網路營運業者的採用是主要原因。

DNS 的原始設計是樹狀結構，從頂端的「根」將權威逐步分配至延展的分支，進一步將承載的流量及傳送責任分散至整個域名空間。這種設計能避免全球系統因為單點失效而整體癱瘓。然而，在樹狀結構中，若連接頂端的任一分支失效，則此分支下的所有域名也都將無法連線。舉例而言，如果 Verisign 負責管理的.com 域名伺服器失效，則所有.com 域名也都會暫時消失於網路上。

為了避免這種災難，DNS 協定容許權威域名伺服器生成多個複本，共同負責域名空間中的同一分支。這些伺服器複本通常會被

分散至不同的地理位置，藉此強化 DNS 生態系統的靈活性。如此一來，即使其中某個伺服器默默失效，解析器也會自動將 DNS 查詢轉向其他複本，連線因此仍將正常運作。

隨著時間演進，網際網路的網路層亦發展出一套強化靈活性的機制，也就是 IP anycast。在此模型中，不同的網路被設定公告同一筆網路位址前綴，地理位置四散的伺服器複本因此會使用完全一樣的 IP 位址。當客戶端傳送封包至伺服器的 anycast IP 位址，此封包會被路由自動轉到最近的伺服器。若無法連線至最近的伺服器，路由會轉而連線第二近的伺服器。

作者分享團隊研究結果，指出 TLD 使用 anycast 的比例從 2017 年的 93%，至 2021 年成長至 97%，目前只有約 50 個 TLD 仍使用單點傳播（unicast）的權威域名主機。鑑於 TLD 在 DNS 基礎建設中扮演的關鍵角色，此結果對 DNS 的靈活性具正向效益。

利用 OpenINTEL 計畫提供的 DNS 資料，研究團隊進一步發現全球 DNS 基礎建設中，約 65%的 SLD 使用 anycast。2021 年間，一半以上有回應的 SLD 域名伺服器都使用 anycast，相較於 2017 年成長了 11.7%。

然而，研究結果也顯示提供 anycast 服務的業者高度集中，前 10 名組織就包辦了約 92%的域名部署率，其中 GoDaddy 就佔了一半。

有些讀者可能想知道，要不要使用 anycast 技術，是消費者（即域名註冊人）還是 DNS 營運業者（通常是受理註冊機構）的選擇？歐洲頗受歡迎的網路代管營運公司 OVH，提供每年 1.21 歐元的 DNS 域名伺服器 anycast 服務。團隊以 OVH 作為研究案例，發現幾乎所有 OVH 代管的 SLD 都使用 unicast。這代表若須額外付費，大部分消費者就不會選擇使用 anycast 服務。

團隊也發現，受理註冊機構在小規模市場（如 ccTLD）中通常

扮演關鍵角色。若比較荷蘭（.nl）和瑞典（.se）的 anycast 部署率，會發現後者高於前者，而原因就在於瑞典最大的受理註冊機構 Loopia AB 使用 anycast，荷蘭市占率最高的受理註冊機構 TransIP B.V 則僅使用 unicast。

最後，作者也提醒，改善 DNS 的靈活性絕非僅仰賴 anycast，而應搭配 DNS 中其他加強靈活性的機制，如多個網路系統、IP 和自治系統使用，才能真正強化 DNS 的靈活及韌性。

參考資料：

https://blog.apnic.net/2021/12/22/how-widely-adopted-is-anycast-in-the-dns/

趨勢議題

人工智慧治理思維演變、近期發展與課題

郭戎晉／南臺科大財經法律研究所助理教授

https://blog.twnic.tw/2023/01/12/25316/

光與影併存的人工智慧

人工智慧就字面意義而言泛指「非人類（機器）所表現的智慧」，人工智慧最常見的迷思，便是被誤解為屬於單一技術概念，然而人工智慧並非單一技術，世界智慧財產權組織（World Intellectual Property Organization，WIPO）表明人工智慧是眾多技術的結合運用，並被廣泛使用於諸多領域。在人工智慧關聯技術及實務應用持續推陳出新下，主要國家也高度關注人工智慧發展帶來的正反效益，並積極思考人工智慧應有的治理模式與可行監管作法。

人工智慧治理思維演變

一、由「外顯」技術到「內在」技術

根據 WIPO 的定義，人工智慧涉及的重要技術至少包括下列 6 者：（1）機器學習；（2）邏輯程式設計：（3）模糊邏輯；（4）概率推理；（5）本體工程；及（6）功能應用關聯技術，諸如電腦視覺、自然語言處理、語音處理等。

上揭技術可概分為「外顯」與「內在」兩類概念，多數人對於人工智慧的認識，具肉眼可見的「外顯」應用扮演重要角色，包括自駕車、無人機與醫療 AI 器材在內，人工智慧對一般民眾來說不再只是曾經聽聞或想像中的概念，而是真實出現在你我眼前，並擔心此等應用可能對民眾帶來的危害。因此早期針對人工智慧展

開的規範討論，自然而然地聚焦具可見外觀的人工智慧具體應用態樣。

二、由「管制性」行業到「不限」行業別

上述外顯應用大抵由管制性行業推動，PwC 曾在 2017 年指出人工智慧發展潛力最為顯著的前三名業態，分別為醫療照護、交通運輸及金融服務，全數為管制型行業。管制性行業顧名思義指基於行業立法，有著經營資格的要求或限制條件，因此早期針對人工智慧展開的規範討論，大抵是直接在行業固有立法基礎上進行討論。

但當人工智慧應用逐步深入各個行業別，同時人們對於人工智慧的關注不復侷限於外顯應用，進一步探討底層技術如演算法所帶來的相關風險時，由於存在此等風險的行業領域不以管制性行業為限，在不必然存在既有立法的前提下，也促使各國開始思考有無制定規範專法的必要。

三、由全然「自律」開始加入「他律」機制

人工智慧治理早期環繞自律機制展開，2014 年日本人工智慧學會設置了倫理委員會並發表「人工智慧倫理指引」，國際電機電子工程師學會（IEEE）也在 2016 年提出「人工智慧道德設計準則」，均強調希望透過「自律」方式，使得人工智慧的技術發展及具體應用獲得適當約束。在此一思維下，包括 GAFA 以及 IBM、DeepMind 在內的科技巨擘也紛紛提出本身的人工智慧自律規範，並嘗試發展自律監管工具。

產業引領的自律機制／軟法方案（soft law）雖有助於彌補人工智慧發展初期的監管真空（regulatory vacuum）問題，在人工智慧持續衍生過往未見的新興風險下，仍促使各國監管機關思考制定相應的法律規範。Google 及其母公司 Alphabet 的執行長 Sundar Pichai 亦在 2020 年 1 月親自撰文，表示商業公司不能急於發展人

工智慧技術，卻僅依賴市場力量來決定如何使用此一嶄新科技，來自公部門的監管規範仍有其必要性；Pichai 認為對於人工智慧此一嶄新應用領域，政府仍有需要在充分考量成本及效益的前提下，建構全新而適當的監管法規。

人工智慧監管發展最新趨勢

一、由道德層面逐步聚焦「可解釋性 AI」及「負責任 AI」

2018 年輪值 G7 集團主席的加拿大，開始倡議人工智慧全球監管合作。2019 年 5 月加拿大提議仿「政府間氣候變化專門委員會」（IPCC）成立「人工智慧專門委員會」（IPAI），同時發布「國際人工智慧小組宣言」（Declaration of the IPAI），揭櫫參與國家所應承諾及遵循的十款共同價值。在此同時，經濟合作與發展組織（OECD）著眼人工智慧監管問題，也在 2019 年 5 月發布「人工智慧建議書」（Artificial Intelligence Recommendation），提出了 5 項「人工智慧基本原則」，包括：（1）包容性成長、永續發展與福祉；（2）以人為本的價值觀和公平；（3）透明度及可解釋性；（4）穩健與安全；以及（5）問責機制。

隨著主要國家共通重視人工智慧帶來的挑戰，上述的人工智慧小組於 2020 年 6 月更名為「人工智慧全球夥伴聯盟」（Global Partnership on Artificial Intelligence, GPAI），並與 OECD 所作討論整合，正式架構於 OECD 之下。無論是 IPAI 闡述的共同價值或 OECD 提出基本原則，國際上針對人工智慧的治理，已由相對寬泛的道德層面，聚焦於諸如「可解釋性 AI」及「負責任 AI」等相對明確之議題。

二、主要國家開始思考人工智慧立法的必要

在人工智慧治理輪廓愈發明確下，各國更是積極思考以立法方式強化監理之合適性。歐盟執委會（European Commission）在 2018

年便已確定了歐洲人工智慧的發展願景，提出包括：（1）增加針對人工智慧的公私部門投資；（2）著眼社會發展預先作好準備；以及（3）確保適當的道德和法律框架等三大願景。為推動及落實上述願景，歐盟執委會成立「人工智慧高級專家小組」並在 2019 年 4 月發布「可信賴人工智慧道德指引」（Ethics Guidelines for Trustworthy AI），2020 年更進一步提出「人工智慧白皮書」（White Paper On Artificial Intelligence），表明歐盟將以「風險基礎管制模式」（risk-based approach）研訂人工智慧監管專法。

相對於歐盟表明制定監管立法勢在必行，美國則是以務實角度思考立法之必要。依據 Stanford 大學發布的 AI Index 2022 報告，全球主要國家通過的人工智慧立法，2016 年時僅有 1 件，2021 年全球則通過 18 件關聯立法；若以 2016 年至 2021 年累計通過的立法進行分析，美國更以 13 件立法居首。然而前揭 13 部立法大抵為部門立法或州法，隨著整合性聯邦立法倡議湧現，美國也持續討論如何在人工智慧發展與監管上取得衡平。

美國總統川普在 2019 年 2 月簽署行政命令啟動「美國 AI 倡議」（The American AI Initiative），美國 AI 倡議提出的六大目標中，包括應當制定必要的監管指南。白宮在 2020 年 11 月正式發布「人工智慧應用監管指南」（Guidance for Regulation of Artificial Intelligence Applications），提出美國聯邦機構在制定人工智慧應用立法時，應當納為考量的十項基本原則，包括「風險評估與管理」、「公平和非歧視」及「公開與透明」等重要要求。另一值得留意其後續發展的文件，則是白宮於 2022 年 10 月公布的「人工智慧權利法案藍圖」（Blueprint for an AI Bill of Rights），白宮提出：（1）建立安全有效的系統；（2）保護民眾免於演算法歧視；（3）維護資料隱私；（4）自動化系統運作之透明化；以及（5）保障退出權利在內等 5 項人工智慧應用監管基本原則，後續有無可能基此進一步發展為聯邦層

級的人工智慧監管專法，殊值持續關注。

三、歐盟已提出立於風險管制模式的全球首部「人工智慧監管專法」

歐盟執委會在「人工智慧白皮書」中表明將立於「風險管制」基礎，研商制定一體適用的人工智慧監管專法。經過廣泛討論與意見徵詢，歐盟執委會在 2021 年 4 月正式提出「人工智慧規則（草案）」（Artificial Intelligence Act），期藉由制定全球首部全面性監管立法，使歐洲達成其所揭示的「值得信賴的人工智慧之全球樞紐」此一重要目標。

草案將人工智慧應用系統具體區分為 4 個風險級別：（1）無法接受的風險（Unacceptable Risk）；（2）高風險（High Risk）；（3）有限風險（Limited Risk）；（4）最小風險（Minimal Risk），並根據風險級別的高低設定其受到的規範程度。若人工智慧技術與應用系統將導致「無法接受的風險」，依草案設計將完全禁止此等應用；被認定為「高風險」時，則應遵守草案所訂下之嚴格規範。

四、美國另以務實觀點推動「人工風險管理架構與管理標準」

美國向以務實立場思考人工智慧的發展與監管，美國國家標準暨技術研究院（NIST）為助益公、私部門有效管理人工智慧帶來的相關風險，於 2021 年 7 月宣示將研擬「人工智慧風險管理框架」（Artificial Intelligence Risk Management Framework, AI RMF），2021 年至 2022 年 NIST 陸續發布 AI RMF 草案與其修正版本。

AI RMF 表明如何識別、減輕及最小化涉及人工智慧技術的風險與潛在危害，將是各界開發可信賴人工智慧系統及其負責任使用上的重要步驟。在風險識別的基礎上，AI RMF 進一步建構人工智慧風險治理架構與管理標準，並提出以治理（Govern）、路徑（Map）、量測（Measure）及管理（Manage）為核心的風險管理架構設計。依據 NIST 公布資訊，NIST 預計在 2023 年上半度正式發

布 AI RMF 1.0 版本，從產業發展角度而言，AI RMF 更富實務操作可行性，其所生影響或將較監管立法更為深遠。

結語：人工智慧監管推動仍面臨嚴峻課題

當前主要國家咸認同人工智慧確有必要進行適當監管，然而人工智慧監管工作的推動卻也面臨數道難題，包括難以直接援引既有的監管經驗、監管創新動能落後於人工智慧技術創新，以及最為關鍵的「無法有效衡量人工智慧衍生風險」。而包括人工智慧在內，歷來著眼技術發展提出的監管立法，也往往面臨著：（1）如何跟上技術進步；（2）如何在促進技創新與保護基本權利和價值之間取得平衡；（3）監管方向係應順從社會多數共識抑或應反其道而行；以及（4）如何平衡手段的有效性與合法性等爭議。

David Collingridge 在 1980 年提出「科林格里奇困境（Collingridge Dilemma）理論」，其是指前瞻技術可能出現的負面影響，在技術發展前期往往難以預測，在無法獲得所生影響的必要資訊下，我們可以控制卻不知該控制什麼；當創新技術已在市場上佔有穩固地位，即使其所生影響隨著技術的發展而逐漸明朗，我們知道該控制什麼卻已陷入難以控制之困境。

就現況而言，各國已跨越早期以道德倫理層面為主的治理討論，逐步聚焦人工智慧的可解釋性與問責課題，近期更進而確定人工智慧監管的主要目的在於有效解決人工智慧系統衍生之相關風險。惟無論採取何種監管手法與所設定的監管強度為何，如何避免人工智慧監管推動落入「科林格里奇困境」，著實重要並值得國內各界深思。

群眾外包？「工人」智慧？

莊舒歆／東海大學資訊管理學系

https://blog.twnic.tw/2022/07/05/23580/

高品質數據

數據分析公司 Data Quality Solutions 總裁 Thomas C. Redman 表示「高品質的數據是能在操作、制定決策和規劃中符合預期。」[1]，也就是說高品質數據應具有精確、有效和完整等特性，使人類或人工智慧（Artificial Intelligence，AI）能夠從大數據中找出關聯，根據 DIKW 體系[2]，使數據（Data）轉變為智慧（Wisdom）。

機器學習（Machine Learning，ML）是人工智慧學習方式之一，著重訓練電腦從數據中學習並找出特徵。偶爾會聽到「垃圾進，垃圾出」（Garbage in, garbage out），是指蒐集的數據有問題，就會推論出錯的參數。在龐大的數據中，訓練 AI 模型若進入此種循環，要經過長時間才能慢慢剔除所謂的「垃圾」，需要耗費巨額成本和時間。

群眾外包

為了能訓練出精準的預測模型，歷史數據就必須符合高品質的標準。數據科學家會先進行數據清理工作，但那既無聊又耗時，且

[1] Thomas C. Redman (2004). Data: An Unfolding Quality Disaster. 檢自：http://www.estgv.ipv.pt/PaginasPessoais/jloureiro/ESI_AID2007_2008/fichas/TP06_anexo2.pdf (Jun. 17, 2022).

[2] Russell. L. Ackoff (1989). From Data to Wisdom. Journal of Applied Systems Analysis 16: 3-9. (Jun. 17, 2022).

團隊缺乏多樣性沒辦法完全找出並修正所有的錯誤數據，容易造成系統漏洞。技術公司 Narrative Science 在研究報告中指出[3]，有 59% 的公司將數據科學人才列為實現大數據技術的障礙。在美國，全職數據科學家的平均年薪為 12 萬美元，對企業來說是不小的負擔。

群眾外包的商機就此出現，企業提交工作到外包平臺上，僱用來自世界各地的員工完成任務，進而改進 AI 系統，平臺上會有各種工作，包含翻譯各種語言的文章、瀏覽大量照片找出有沒有圖片包含仇恨或歧視的內容等等。其中，最為出名的群眾外包平臺「亞馬遜土耳其機器人」（Amazon Mechanical Turk，MTurk），名稱取自 18 世紀發明的自動下棋裝置「土耳其機器人」，外型像是一個穿戴土耳其造型的假人，但其實內部是一個真的下棋大師，許多棋手都誤以為自己在與機器競爭。藏在內部的下棋大師是自動下棋裝置的重要齒輪；而看似自行運作與計算的 AI，背後也有許多努力工作的「工人們」被視為 AI 運作不可或缺的齒輪。

「工人」智慧

群眾外包工人與數據科學家團隊有甚麼差別？

與數據科學家相比他們**便宜**非常多，瀏覽 100 張圖片驗證有無不良內容，平均賺得 0.04 美元，任務開價的高低通常會直接影響接受任務者的多寡。工人們在**效率**表現上也較為出色，除了人數眾多的原因，工人為了賺得更多的工資會賣力完成任務。同為遠距工作，工人比企業員工效率快上許多，且企業平時也不需提供辦公室或硬體設施。

---

[3] Narrative Science. (2016). Outlook on Artificial Intelligence in the Enterprise 2016. 檢自：http://www.datascienceassn.org/sites/default/files/ Outlook% 20on% 20Artificial% 20Intelligence% 20in% 20the% 20Enterprise% 202016.pdf (Jun. 17, 2022).

對於能更快且降低成本的達成作業，企業絕對樂於委託。此外工人還能確保**高品質數據**，原因有以下四項：

1. 擁有多樣性

若只招募特定的群體來為目標受眾測試，容易出現偏見，企業透過使用來自不同國家的員工來測試或篩選數據，能夠更全面的發現錯誤數據。

2. 工作者數量多

工作者足夠多，除了代表有多樣性的特徵，同時也表示接受同一任務的人們所交出的數據量夠多，能夠有更少的誤差。此外，企業一定不只一項任務，有些人疲於做同一任務想更換工作時，有足夠多的人，才能使每項任務都有充足的工作者提供足夠多的數據。

3. 講求工人的品質

特別是講求某種能力的工作，接案的工人就必須不斷地接受測試，確保他們持續的符合執行任務的標準。以翻譯或錄製音訊來說，為了確保工作者對此種語言的熟練度，每隔一段時間就會經過嚴格的語言測試，由另一位同為外包平臺的工作者出題和驗證，測試內容也包含母語者會使用的慣用語或方言。以人工驗證方式確保工人品質，不斷循環達到更好的數據品質。

4. 機器學習

外包平臺會使用機器學習來監督工作者的行為，以同一類型任務過去的平均時間判斷，如果任務完成的過快可能代表工作者在任務上較急促不細心，而耗時太長可能意味他們曾分心或不能解決問題。機器學習還能發現工作者給出不一致的答案，運用演算法評估哪一種答案才是較為正確的，也就是一邊餵養數據一邊訓練 AI。

結語

群眾外包是一種全新的工作型態，能夠解決人工智慧缺乏高品質數據的問題，對企業來說是「性價比」非常高的完美團隊。

但轉念一想，這也促使大型企業將工作外包給勞動成本低的國家，使世界貧富差距擴大。很少人會為他們的權益發聲，甚至不知道他們的存在。工作時間長且不固定，使的工資低於最低時薪的狀況時有所聞，甚至平均每小時只有 2 美元。一位在 MTurk 工作的受訪者表示：「僱主比工作者擁有更大的權力，可以突然否定已提交的工作成果，但工作者卻沒有辦法採取任何行動」[4]。

群眾外包是推動人工智慧進步的好方法，但人類科技發展的同時，若輕忽勞動者穩定的收入和生活保障，演變成**科技進步**需伴隨**勞工生活品質退化**，後續的發展可能會造成更嚴重的社會問題，各國應開始省思並訂定相關政策，使各科技巨頭重視所有「工人」的付出。

[4] Jane Wakefield (2021). AI: Ghost workers demand to be seen and heard. BBC. 檢自：https://www.bbc.com/news/technology-56414491 (Jun. 17, 2022).

人工智慧的倫理課題

莊舒歆／東海大學資訊管理學系

https://blog.twnic.tw/2022/05/16/22994/

人工智慧的定義

「智慧」（Intelligence）一直沒有固定的標準和定義，各領域學者對於人工智慧（Artificial Intelligence，AI）的定義也有不同的見解，以下將從哲學與電腦科學觀點來粗淺地討論不同方面的定義。

一些哲學家認為物體含有意識和精神才能稱為智慧，現階段的 AI 並沒有心智可言，所以他們不認同「人工智慧」這個名稱，機器是否能思考的議題，哲學家分為二元論和唯物主義，前者認為智慧是要先擁有心靈，心靈是非物理物質；因此不能以純物理來解釋，後者認為頭腦可以用物理解釋，而動腦是包含智慧的行為；所以人工智慧是合理的產物。

電腦科學與人工智慧之父 Alan Turing 提出：「若有一台機器能夠與人對話而不被辨識出是機器的話，這台機器就有智慧。」這就是圖靈測試[1]（Turing Test），到了現今還沒有 AI 能夠完全達到標準。但隨著演算法與硬體設備的進步，AI 學者 Andreas Kaplan 則定義 AI 是「能從外部資料中學習並利用學習的知識，靈活達成特定目標和任務的能力」[2]。

---

1 A. M. Turing (1950). Computing machinery and intelligence. 檢自：https://www.csee.umbc.edu/courses/471/papers/turing.pdf

2 Andreas Kaplana, Michael Haenlein (2018). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of

上述來看，學術界各有見解，定義會不斷地改變。不管現階段我們如何解讀 AI 有沒有所謂的「智慧」，應先開始細想被稱為有「智慧」的 AI 犯錯時，它能揹負起倫理學上的責任嗎？

AI 的倫理

最常被討論的電車問題（Trolley problem），失控的列車在軌道上，有五個人被綁起來，另一條軌道上只有一個人被綁著，該保持原本的軌道碾壓過這五個人還是變換軌道壓另一個人？倫理學上這衍生了兩種倫理原則：

1. 效益主義：變換軌道撞上一個人而避開五個人，人會直覺認為這是追求多數人的利益。但 AI 思考的效益會包括許多因素，像是列車突然轉向會不會導致危險，或單獨在軌道上的那一人對社會的貢獻是否超越另五個人，AI 所參考的資訊和考慮的模式與人類不同，而 AI 判斷**價值**與**效益**的方式，人類的觀點能接受嗎？
2. 義務倫理學：不應外在的因素改變而造成傷害，後果不是選擇的考慮因素。如果不可以殺人是一種道德義務，那就算有五個人會死亡，也不能動手讓一個人犧牲。

AI 如何判斷應該如何做？人類在做選擇時就有不同的爭議，大多數人會選擇讓列車改道犧牲一個人，但如果那一個人是他們的親人或朋友，他們就會改變想法。除此之外還有責任的問題，當自駕車為閃避突然出現的路人而衝撞民宅，賠償責任是規於誰呢？是自駕車研發公司、車主、事發當下的乘客還是賣車的車商？這題可能是突然出現的路人要負責，但如果汽車被駭客入侵導致意

---

artificial intelligence. 檢自：https://www.sciencedirect.com/science/article/pii/S0007681318301393

外，誰要承擔？如果狀況變為閃避障礙物而造成他人傷亡，責任歸誰？

交通意外不能事先預料，訓練 AI 的過程中充滿人為的干預，AI 學習的是「多數人的行為模式」，但「多數人的行為模式」的數據來源是指眾人可能偏好的選擇結果，還是根據某些固定的決策模式（如義務論）決定 AI 要遵循的規範。杜克大學的 VincentConitzer 電腦科學教授等人提出一個想法[3]，讓 AI 學習博奕理論並提供大量倫理及心理學文獻。他們指出信任博弈（the trust game）是倫理選擇的一個普遍特徵，除了考慮行為造成的結果，還會考慮是否有公平、不感恩、不忠誠的表現。AI 能從過去選擇造成的影響來評價自己的行為，再透過學習大量文獻或許能讓 AI 找出最適當的倫理規則。

結語

倫理在人類判斷上就可以引發各種爭議，如果苛求 AI 需要搭載一個完美無缺的倫理系統讓眾人滿意是不可能的，頂多讓大多數人同意。我們說透過模擬人類心智來解決問題及決策能力的系統稱為人工智慧，重點是人類心智太過複雜，包含各種情緒、思想，有些人為大眾犧牲自己；有些人以自己利益為優先，不能說誰對誰錯，我們判斷他人的基準一向是他有無符合大眾利益，但套在自己身上時好像又是另一種標準。

或許我們該慶幸 AI 回應不包含情緒與態度，雖然這就表示它回應倫理情境的表現較差（沒有同理心等），但也表示它不會以自己為中心來做判斷的基準（先假設 AI 不像電影演的會攻佔人類），

[3] Vincent Conitzer, Walter Sinnott-Armstrong, Jana Schaich Borg, Yuan Deng, Max Kramer (2017). Moral Decision Making Frameworks for Artificial Intelligence. 檢自：https://users.cs.duke.edu/~conitzer/moralAAAI17.pdf

因為餵養 AI 訓練數據的人類會希望它符合大眾期待。所以 AI 是否從具體情境中學習如何做正確的倫理判斷，且經過不斷的自我調整及修正達到完美，在於選擇結果能否被人類接受。

AI 並不是用來取代、超越或必須比人類完美的存在，雖然道德概念充滿不確定性，但這不是反對或阻止 AI 發展的理由。過去石器時代以石頭作為代表性工具，青銅器時代以青銅為代表性；我們不會認為石頭、青銅要取代人類，未來人工智慧時代，也只是人類文化發展的一個階段，人們應當著重於討論相關議題，並積極思考該如何使用與活用這項「智慧」工具。

人工智慧對人權衝擊之評估

戴匡／東海大學資訊管理學系研究員

https://blog.twnic.tw/2022/02/24/21783/

人工智慧及人權爭議

聯合國人權事務高級專員 Michelle Bachelet 警告[1]，若未充分考慮**人工智慧**（Artificial Intelligence，AI）**科技**如何影響**人權**，可能將產生重大負面影響，她大力呼籲為 AI 設下人權規範。

根據 Bachelet 提出的一份新報告，特徵分析、自動化決策技術以及機器學習等技術可能大規模侵犯人權，若不為 AI 設下紅線，人們的隱私、健康、教育、自由遷徙、和平集會及結社，以及言論自由等人權可能將受衝擊。該報告指出，國家與企業經常急於整合 AI 應用程式，因此未能落實盡職調查責任，且許多受害者因政府單位濫用 AI 而遭不公平對待。舉例而言，社工或社會福利行政公務員使用具系統性偏誤的 AI 認證工具做出錯誤裁量，導致弱勢權益遭剝奪；或警方根據有缺陷的臉部識別軟體逮捕無罪人士。

該報告詳細介紹 AI 系統如何依賴大型資料集，且以多元、通常不透明的方式蒐集、共享、合成及分析個資。報告指出，用於通報及指導 AI 系統的資料不一定是適切的，許多資料有誤、過時、無關，甚至帶有人為歧視。報告強調，各國及相關行為者應嚴加審視 AI 工具的推論性、預測性及監控性，包括 AI 對人類行為模式的洞察。

---

[1] UN News. (2021). Urgent action needed over artificial intelligence risks to human rights. 檢自：https://news.un.org/en/story/2021/09/1099972 (Jan. 13, 2022).

AI 技術由人類建構、並被部署於具有根深蒂固歧視的系統與機構中，從刑事制度、住宅、工作場所到金融機構，既有社會偏見及歧視可說是無處不在[2]，因此，蒐集的資料很難避免人為偏見，以及因偏見導致的歧視性決策，其中社會邊緣群體可說是深受其害。例如：協助房東評估房客的 AI 系統仰賴於反映種族主義、性別歧視、身心障礙歧視等內在偏見的法庭紀錄與其他資料集，導致系統將部分有能力支付租金者認定為資格不符。

目前越來越多國家、國際組織與科技公司選擇使用以 AI 為本的生物辨識技術，這類技術可用於即時與遠距識別，儘管相當方便，卻可能造成政府或企業濫用所導致不當追蹤個人的後果。由於 AI 系統開發及維運所依賴的資料環境、演算法及模式的複雜性，以及政府與私營單位的刻意保密，大眾無法充分理解 AI 系統對人權及社會所造成的影響。Bachelet 呼籲，隨著人權風險愈高，針對 AI 的法律規範也應越愈趨嚴格。

此外，Bachelet 也呼籲[3]禁用未依國際人權法規範使用的 AI 應用程式，並點名去（2021）年爭議連連、由以色列監控企業 NSO Group 開發的 Pegasus 間諜軟體。根據去年夏天由公民實驗室（Citizen Lab）及國際特赦組織（Amnesty International）發布的調查報告[4]，許多人權紀錄不佳的國家（如：沙烏地阿拉伯及墨西哥）

---

2 Olga Akselrod (2021). How Artificial Intelligence Can Deepen Racial and Economic Inequities. ACLU. 檢自：https://www.aclu.org/news/privacy-technology/how-artificial-intelligence-can-deepen-racial-and-economic-inequities/ (Jan. 13, 2022).

3 Michelle Bachelet (2021). Committee on Legal Affairs and Human Rights, Parliamentary assembly Council of Europe Hearing on the implications of the Pegasus spyware. UN Human Rights Office of the High Commissioner. 檢自：https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27455&LangID=E (Jan. 14 , 2022).

4 Shoshanna Solomon (2021). Amnesty, research groups map out global reach of Israeli NSO Group's spyware. The Times of Israel.

利用 Pegasus 軟體監控國內維權人士、記者及政治人物手機，受害者達數千多名。隨著愈來愈多類似案件被揭露，NSO Group 成為全球頭條新聞，且廣受國際輿論批評，受 Pegasus 軟體監控之苦的受害者分布於 45 個國家，總人數達到數千人。

AI 浪潮無法擋，應促進大眾對 AI 技術的全面理解

世界經濟論壇（World Economic Forum，WEF）委託 Ipsos 市場研究公司，在 2021 年 11 至 12 月間針對 28 個國家的成年人對 AI 產品及服務的看法進行調查[5]。約莫三分之二接受調查者認為，AI 產品及服務將在未來 3 至 5 年內深刻改變日常生活，使生活更加輕鬆。然而，其中僅有一半相信 AI 技術利大於弊，且對 AI 產品及服務展現與其他企業相同的信任度，換言之，人們對於 AI 可能構成的衝擊也有所警惕。

此外，該調查亦指出，對 AI 理解程度愈高者，愈傾向對相關企業展現更多信任，值得一提的是，與高收入國家相比，屬於新興經濟體的國家公民認為其對 AI 有更多了解，他們在更加信任相關企業的同時，還能樂觀看待 AI 產品及服務對其生活構成的影響。

WEF 人工智慧與機器學習負責人 Kay Firth-Butterfield 表示，人們必須確切理解 AI 為何物、其運作方式及相關影響，未來國家與企業在運用這類技術時，必須將透明且值得信賴的 AI 技術列為優先項目。

檢自：https://www.timesofisrael.com/amnesty-research-groups-map-out-global-reach-of-israeli-nso-groups-spyware/ (Jan. 14, 2022).

5 Joe Myers (2021). 5 charts that show what people around the world think about AI. World Economic Forum. 檢自：https://www.weforum.org/agenda/2022/01/artificial-intelligence-ai-technology-trust-survey/(Jan. 14, 2022).

如何面對爭議：歐盟與大型科技公司正積極作為

釐清 AI 的人權爭議、發展透明且值得信賴的 AI 系統、促進大眾對 AI 技術及產品的理解，以及建立良好 AI 使用準則，應成為未來政府與企業發展 AI 的配套措施及政策。Bachelet 提出的報告即呼籲，在政府無法確保 AI 系統的精準度、不構成歧視、以及符合嚴格隱私及資料保護標準前，各國政府應立法禁止在公共場所中使用生物識別技術。此外，該文件還強調國家與企業應在開發及使用 AI 的層面上展現更高透明度。

目前嘗試為 AI 設下嚴謹規範的國際組織首推歐盟，去年 10 月，歐洲議會通過決議[6]，反對警方透過 AI 技術進行大規模監控，議員們擔憂 AI 演算法中的偏見，也同意須藉由人工監督與強大法令以防 AI 歧視，特別是在執法與過境時。該決議呼籲，為確保在使用 AI 技術時兼顧基本人權，應採用透明、可追溯且留存完整紀錄的演算法。此外，當局應盡可能使用開源軟體提升 AI 系統的透明度，並要求永久禁止在公共場所運用自動化識別系統，只能監控涉嫌參與犯罪的公民。

歐洲議會要求禁止使用私有的臉部識別資料庫（如：Clearview AI 系統[7]），以及根據行為資料的預測性警務。歐洲議員還希望能全面禁止試圖根據公民行為或人格特質進行評級的社會評分系統，並對使用生物資料進行遠端識別的系統提出擔憂，例如：使用自動識別技術、旨在核准旅客入境的智慧測謊系統 iBorderCtrl。

---

6 European Parliament. (2021). Use of artificial intelligence by the police: MEPs oppose mass surveillance. 檢自：https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance (Jan. 14 , 2022).

7 Clearview 為美國企業，專門提供人臉識別技術和服務，更多資料可參考官方網站：https://www.clearview.ai/

此外，包括 Google、Facebook 及 Microsoft 等大型科技公司與平臺，也開始探討 AI 的倫理問題[8]，例如：Google 旗下的 AI 研究公司 Deepmind 於 2017 年宣布成立專門研究小組，探討 AI 倫理問題；Facebook 在 2019 年初宣布資助德國慕尼黑工業大學，成立獨立的人工智慧倫理研究所，為用於社會及經濟的 AI 技術制定負責任道德準則；Microsoft 在內部成立 AI 倫理道德委員會，委員會由包括產品開發人員、研究員、法務及人力資源等不同背景的員工組成，共同針對 AI 技術可能涉及的各個層面訂定政策。

結語

AI 技術與人權之間的扞格仍將持續發酵，我國科技部於 2019 年發布的「人工智慧科研發展指引」[9]至今已過兩年，或許應重新評估當前 AI 技術發展更新準則。對民主國家而言，在追求 AI 技術的同時必不可忽略人權議題，我國應關注參考其他民主盟友之做法，並推出我國的相關規範或指引，供國內企業及政府單位依循參考。

---

[8] 科技報橘（2020）. AI 怎麼規範才叫有倫理？微軟推出 AI 教戰手冊，6 大準則逐步破解. 檢自：https://buzzorange.com/techorange/2020/02/11/microsoft-ai-ethics/ (Jan. 14 , 2022).

[9] 科技部（2020）. 科技部首度發布「人工智慧科研發展指引」. 天下雜誌. 檢自：https://www.cw.com.tw/article/5097901 (Jan. 14, 2022).

極端主義在網路中的擴散與防制

戴匡／東海大學資訊管理學系研究員

https://blog.twnic.tw/2022/01/06/21350/

極端主義在網路中的擴散：基本概念與相關案例

網路科技的興起加速資訊傳播，雖然網路用戶能獲取許多受用資訊，但不法人士也利用其便利傳遞不實資訊，其中恐怖主義或激進人士可使用網路促進極端主義（Extremism）與恐怖活動等行為，例如：利用網路宣傳招募新成員、透過網路在社會傳播恐懼訊息等，進而導致暴力犯罪，甚至衍伸出國安議題。

聯合國發布的《Update on the impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism》調查報告[1]將恐怖主義及暴力極端主義（countering violent extremism，CVE）列為後疫情時代的嚴峻網路議題[2]，紐西蘭國家廣播電臺（Radio New Zealand，RNZ）的報導[3]以伊斯蘭國為例，分析為何難以掃蕩網路中的極端敘事資訊，並點出即使恐怖主義面臨軍事上的失敗，但從未銷聲匿跡，其對於反西方的極端主義信徒仍具吸引

---

1 https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jun/cted_covid_paper_15june2021_1.pdf

2 調查結果：44%受訪者認為疫情增加其所在區域的恐怖主義威脅；69%受訪者認為因疫情之故，恐怖主義問題變得更加棘手；72%受訪者認為因疫情之故，暴力極端主義問題變得更加棘手；53%受訪者認為與疫情相關的社會經濟與政治影響將加劇未來恐怖主義及暴力極端主義之威脅。

3 Joe Burton (2021). LynnMall attack: Why Isis is harder to defeat online than on the battlefield RNZ. 檢自：https://www.rnz.co.nz/news/national/450806/lynnmall-attack-why-isis-is-harder-to-defeat-online-than-on-the-battlefield (Nov. 26, 2021).

力，並導致暴力恐攻事件[4]。儘管事件兇手可能未受到伊斯蘭國直接幫助，但案例中兇手之電腦設備存有伊斯蘭國相關內容，顯見其意識形態及行動受到該組織宣傳的世界觀所影響。此外，儘管多數國家皆有及於網路空間的反恐法案，但隨著 2021 年以美國為首的西方國家將外交政策重心從反恐轉移至印太戰略及防堵俄國，恐怖主義恐有再起之機。

社群媒體的流行也助長極端主義的發展，人們對社群媒體演算法引導用戶進入極端主義頁面的情況更加關注[5]，例如：2019 年 3 月發生的紐西蘭基督城槍擊案[6]；以及今年初美國大選後國會山莊暴動事件[7]都代表極右翼組織仍持續威脅各國治安，在網路中散播極端主義更是這些組織傳遞價值觀及引發暴力行為的有效手段。在國會山莊事件後，各大社群媒體平臺甚至停用美國前總統川普帳號，並下架有「川粉平臺」之稱的 Parler 社群平臺[8]，可見事態嚴重。

---

[4] 相關案例包括：一名伊斯蘭國擁護者於紐西蘭奧克蘭市郊區的超市發動恐怖攻擊；在美軍撤出阿富汗後，伊斯蘭國附隨組織 Isis-K 於喀布爾機場遂行恐怖攻擊並導致 13 名美軍和超過 150 名阿富汗公民死亡。

[5] RNZ. (2021). Plan for Christchurch Call to target social media algorithms welcomed. 檢自：https://www.rnz.co.nz/news/national/442557/plan-for-christchurch-call-to-target-social-media-algorithms-welcomed (Nov. 26, 2021).

[6] 吳玲臻、林欣蘋（2020）. 【即時】紐西蘭史上最大槍擊案判決出爐：廢死近 60 年來最重刑期。換日線. 檢自：https://crossing.cw.com.tw/article/13848 (Nov. 29 , 2021).

[7] 中央通訊社（2021）. 川普支持者直搗國會大廈 內部混亂場面曝光[影]. 檢自：https://www.cna.com.tw/news/firstnews/202101070051.aspx (Nov. 29, 2021).

[8] 潘柏翰、翁世航（2021）. 封殺激進川粉聯絡管道，社群平臺 Parler 遭科技巨頭下架、終止雲端服務。關鍵評論網. 檢自：https://www.thenewslens.com/article/145810 (Nov. 29, 2021).

如何遏止：以紐西蘭政府為例

在基督城槍擊案後，紐西蘭政府意識到既有法規不足以對抗網路上的極端主義，尚須透過相關政策與國際合作應對。總理 Jacinda Ardern 推動的「基督城呼籲」（Christchurch Call）行動[9]以反恐為目標，目前已獲許多國家及大型科技企業支持，且取得成效。該行動已針對全球網路反恐論壇（Global Internet Forum to Counter Terrorism，GIFCT）進行改革；創建一個擴及網路的危機應對協議，以在恐攻事件發生後進行有效合作；甚至促使公民社會更加積極投入反恐行列。

此外，紐西蘭還承諾加入《布達佩斯網路犯罪公約》（Budapest Convention on cyber crime）[10]，紐國將依約透過國際合作打擊網路上的暴力極端主義，並調查暗藏於社群媒體與暗網中的極端主義。紐國政府亦計畫建立一個專責處理暴力極端主義的機構，以催生相關研究及更有效的反恐政策。

演算法也是極端主義在網路中擴散的助力，受商業利益驅使，社群媒體平臺所使用的演算法會將受許多關注之貼文推送給更多用戶，演算法雖能為社群媒體平臺提高用戶數及廣告收益，但也造成具煽動性的貼文獲得更多關注的現實，從而導致極端主義的擴散。因此，Jacinda Ardern 呼籲科技平臺採用道德演算法遏止極端或惡意內容的發布。此外，若不即時進行政策調整或相關規管，極端主義透過網路擴散所導致的暴力事件可能將撕裂社會。舉例而言，紐西蘭一起超市恐攻案的兇手為當地的穆斯林，案發後，紐西蘭的穆斯林社群表達震驚，並擔憂這種恐怖暴力行徑將導致反穆斯

[9] RNZ. (2020). Christchurch terror attacks: Ardern and Macron hail success of Christchurch Call. 檢自 https://www.rnz.co.nz/news/political/416678/christchurch-terror-attacks-ardern-and-macron-hail-success-of-christchurch-call (Nov. 29, 2021).

[10] 公約內容可參考歐盟網站。

林情緒升高，只有團結不排外的社會方能協力對抗恐怖主義，而非將恐怖與極端主義怪罪於部分群體。

遏止極端主義於網路擴散的難題

儘管紐西蘭政府的作為極具參考價值，但預防恐怖攻擊實屬不易，其中關鍵是對自由網路的信念導致安全部門以反恐為由監控網路將衍生出人權爭議，且激進人士的信仰並非必然會轉化為具體行動。此外，安全部門難以全面監控激進人士，且若監控針對特定社群也會引發族群及意識形態爭議。因此，恣意打擊極端主義反而可能加劇分裂與仇恨，但若不採取作為又無法防制激進人士可能構成的公共危險，這使得網路上極端主義的管制淪為兩難議題。

儘管各國政府已開始推出平臺管制法規，科技巨頭也開始研發能識別恐怖分子及剔除極端敘事的演算法[11]，但極端主義仍暗潮洶湧的存於暗網或去中心化平臺中，且可透過加密科技隱匿行蹤，雖然這代表打擊網路上的極端主義已具初步成效，但極端意識形態仍將持續寄生於網路之中。

結語

有心人士透過網路散播極端主義已是備受重視的國際議題，其衍生出的暴力事件也已危及國安並構成規管難題，各國均積極著手相關策進作為，科技平臺也透過設計道德演算法來應對。未來可持續關注國際間的相關案件，以及各國政府與科技平臺的相關規管措施。

[11] 李蘇峻（2017）. 臉書開發新演算法 可辨識恐怖份子。新頭殼. 檢自：https://newtalk.tw/news/view/2017-02-17/81998 (Nov. 29 , 2021).

淺析數位威權主義

戴匡／東海大學資訊管理學系研究員

https://blog.twnic.tw/2021/11/25/20936/

數位威權主義：發展脈絡與興起

科技的興起導致人們生活多方受到監控審查，甚至在某些時刻受到社會信用體系之影響。科技的快速發展已超過政府立法速度，科技巨頭也因此日益強大，包括 Amazon、Apple、Google、Facebook 及 Microsoft 等企業已透過演算法滲透人們日常生活，因此，各國政府開始嘗試奪回主導權，頻頻以安全為由對社群媒體平臺及科技公司祭出法律措施及監管規範，進而控制網路資訊的種類及傳播[1]。

民眾普遍認為，每個網站都會以提供個人化服務（Personalized Service）為由追蹤點擊或任何形式的網路參與，儘管政府須處理科技巨頭透過演算法掌握大量個資之議題，但當各國政府開始監控企業，最大受害者仍可能是網路使用者。

一般而言，數位威權主義泛指國家政府對公民資訊進行不當控制或監視，雖有多種形式及規模，但在利用科技進行線上識別、監控及審查個人時最為明顯，部分國家甚至利用科技控制及形塑公民行為以擴大政治權威，閉路電視（Closed-Circuit Television，CCTV）、臉部辨識及 GPS 追蹤等監控技術已蓬勃發展，「用隱私換取方便」的概念已使監控數位世界成為一種日常。

COVID-19 疫情的大流行也助長數位威權主義之發展，部分政

[1] Neil C. Hughes (2021). The global rise of digital authoritarianism. Cybernews. 檢自：https://cybernews.com/editorial/the-global-rise-of-digital-authoritarianism/ (Oct. 22, 2021).

府開始審查異議言論並鼓勵用戶進行自我審查，甚至鼓勵公民透過 App 或專用電話舉報違規者，儘管政府能透過這些手段打擊與疫情有關的不實訊息，並因此挽救生命，但若這類監控措施在後疫情時代仍被延續，部分政府極有可能透過演算法利用個資控制公民，強迫公民以符合政府價值觀的方式進行社會互動，甚至透過制度移除不為政府所喜之內容，或揭露網路用戶在社群媒體及加密訊息 App 中的隱私。

數位威權主義已非獨裁國家特有現象

中國履次對國內科技企業推出監管措施，甚至限制 18 歲以下青少年每周使用線上遊戲時間不得超過 3 小時；印度推出一項新的數位法規，促使社群媒體、串流媒體及科技服務業者對用戶在平臺中發布或分享的內容負責；印尼政府在疫情期間利用政策措施，控制網路資訊的敘述及流動；非洲國家透過關閉網路、監控、對社群媒體提高稅率以進行控制，甚至公民因發布被視為反政府之貼文而遭逮捕；連號稱民主燈塔的美國，對工作場所施加監控的情況也日益增加，且可能在未來利用 AI 演算法發展「預測性警務」[2]。

助長數位威權主義的監控技術並非各國獨自發展，根據 2019 年世界貿易組織的資料[3]，中國是全球最大電信設備以及辦公與電信設備供應國，且傾向提供相關技術予威權國家，目前中國已向全世界出售監控技術，相關案例包括：2018 年辛巴威政府與中國 AI 新創企業 CloudWalk 簽署協議以部署國家級臉部辨識資料庫，該資

[2] Neil C. Hughes (2021). The global rise of digital authoritarianism. Cybernews. 檢自：https://cybernews.com/editorial/the-global-rise-of-digital-authoritarianism/ (Oct. 22, 2021).

[3] Ausma Bernot (2021). Digital authoritarianism not just a China problem. the interpreter. 檢自：https://www.lowyinstitute.org/the-interpreter/digital-authoritarianism-not-just-china-problem (Oct. 22, 2021).

料庫主要用於安全及執法目的，並可能擴展至其他公共計畫，中國 AI 研究人員將共享包含數百萬張辛巴威人臉照片的資料庫存取權限，這可能導致具價值之資料外洩[4]。政治上，監控技術貿易被包裝為外交策略或有效控制公共安全的手段，中國發起的大型外交行動「一帶一路計畫」（Belt and Road Initiative，BRI）也將監控技術視為外交資源，前面所提到的辛巴威就是其中之一。

出售監控技術非獨裁政府獨有作為，部分歐美企業也向中國出售監控技術，例如：美國企業甲骨文（Oracle）公司曾向中國公安部門出售具語言及行為分析功能的情報工具；2013 年宣布倒閉的加拿大電信及資料設備巨頭北電網路（Nortel Networks），在歇業前持續向中國公共及私營部門出售技術，使中國公安部門擁有更好的語音識別能力以攔截電話通訊，實現智慧影片監控、追蹤網路用戶並過濾網路內容。

今年，華盛頓郵報（Washington Post）、衛報（Guardian）、世界報（Le Monde）等全球數十家媒體共同發表調查報導[5]，揭露由以色列情報公司 NSO 集團所開發的 Pegasus 間諜軟體已對包含 189 位記者、85 位人權工作者、65 位企業高階管理者、阿拉伯王室成員、超過 600 位政治人物及外交情報官員進行監控，甚至法國總統 Emmanuel Macron 與南非總統 Cyril Ramaphosa 等國家元首也在監控名單之列。儘管以色列當局強調，出售監控技術僅出於防範與調查犯罪，以及打擊恐怖主義之目的，但調查結果顯見 NSO 集團客

[4] Lynsey Chutel (2018). China is exporting facial recognition software to Africa, expanding its vast database. QUARTZ AFRICA. 檢自：https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/ (Nov. 10, 2021).

[5] 科技新報（2021）. 飛馬間諜軟體醜聞，揭以色列科技外交黑暗面. 檢自：https://technews.tw/2021/07/22/nso-group-pegasus/ (Oct. 25, 2021).

戶的目的不僅於此，在東窗事發後[6]，美國總統 Joe Biden 的中東顧問 Brett McGurk 與以色列國防部高階官員 Zohar Palti 進行磋商；法國國防部長也就此事詢問以色列國防部長 Benny Gantz，可見監控技術可能進一步引發國際情勢緊張。

如何應對：開發全球監管架構以及適切新興技術規範

由於監控技術的發展已是全球性議題，因此須透過國際法或針對監控技術管制凝聚國際共識。今（2021）年 7 月，全球 148 個人權組織及 28 位專家聯合呼籲中止銷售、使用及轉讓監控技術[7]，而後，聯合國專家也發布公開信[8]表達相似立場，他們呼籲，在各國能依據國際人權法（International human rights law）推出保證監控技術符合國際人權標準的監管法規前，應停止出售及轉讓監控技術，並指出技術濫用可能導致包括侵犯言論自由、隱私權及媒體自由，並破壞民主價值、國際安全及國際合作等嚴重後果。

美國眾議員 Tom Malinowski 也在接受採訪[9]時提到，美國應透過立法及其他制裁制度強化出口管制；懲處遂行不當監控的企業或政府人員；甚至與以色列及歐洲國家在內的國際盟友訂定適切國際規範。

---

6 Drew Harwell and Shane Harris (2021). White House has spoken to Israeli officials about spyware concerns following Pegasus Project revelations. The Washington Post. 檢自：https://www.washingtonpost.com/technology/2021/07/29/pegasus-white-house-israel-concerns/ (Oct. 26, 2021).

7 Amnesty International. (2021). Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology. 檢自：https://www.amnesty.org/en/documents/doc10/4516/2021/en/ (Oct. 26, 2021).

8 https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379

9 科技新報（2021）. 飛馬間諜軟體醜聞，揭以色列科技外交黑暗面. 檢自：https://technews.tw/2021/07/22/nso-group-pegasus/ (Oct. 25, 2021).

在設計出符合人權價值的國際規範前，國家應設計符合民主價值與倫理的制度規範，其中以歐盟為代表。目前歐盟已發布防止AI技術遭濫用的AI人工智慧道德準則[10]；歐洲議會也通過一項禁止於公共場所使用自動化臉部辨識的非約束性決議[11]，決議指出使用AI人工智慧系統須尋求補救措施；部分議員也呼籲歐盟官員禁用私人臉部辨識資料庫、預測性警務及社會評分、社會信用系統，以及使用自動化辨識機制的邊境控管系統等數位威權主義工具[12]。

此外，歐盟執委會（European Commission，EC）今年4月提出的《人工智慧法案》（Artificial Intelligence Act）[13]也為人工智慧導入全面監管框架，禁止在公共場所使用遠端生物辨識技術（例如：臉部辨識），除非是用於處理恐怖主義或綁架之類的重大犯罪。

結語

數位威權主義的浪潮席捲而來，並對網路自由構成挑戰，且可能在後疫情時代持續發展，要抑制數位威權主義，須規範助長其發展的監控科技並推廣民主價值，首先從設計適切國內制度做起，進而達成國際影響力。

---

[10] 科技報橘（2019）. 一個「值得信賴AI」長什麼樣子？歐盟發佈7條人工智慧的道德準則. 檢自：https://buzzorange.com/techorange/2019/04/10/eu-guidelines-on-developing-ethical-ai/ (Oct. 26 , 2021).

[11] https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

[12] Almee Chanthadavong (2021). Amazon, Google, Microsoft and other tech giants establish Trusted Cloud Principles. ZD Net. 檢自：https://www.zdnet.com/article/amazon-google-microsoft-and-other-tech-giants-establish-trusted-cloud-principles/ (Oct. 15, 2021).

[13] https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

區塊鏈域名機制及潛力分析：以 Handshake 頂級域名為核心

林紘宇／奧果區塊（Argoblocks）首席顧問、加密貨幣律師

https://blog.twnic.tw/2022/11/14/24718/

網域名稱系統（DNS）是網際網路的電話簿，讓我們每天可以正常使用網路、訪問網站的重要系統。域名就是一串人類大腦可以記憶的一串字碼（如 Google.com）指向特定的伺服器 IP 位址，DNS 將網域名稱轉換為 IP 位址，以便瀏覽器能夠載入網站。

NFT（Non Fungible Token）熱潮帶來的數位資產概念，其實並非全所未有，實際上，域名，可以說就是最古早的 NFT，而且具有價值。

DNS 是一套重要、有效率的系統，每天讓數十億人輸入網址，並成功地將使用者導引到他們想要去的網站。而一直以來，始終有不同的團隊、專案、開源項目，希望打造一個 DNS 的「替代系統」（Alternative System），例如：Handle System, Onion System（洋蔥 Tor 系統），但不是失敗告終，就是停留在特定領域/測試使用階段，甚至有人開始認為，DNS 是一個近乎完美的系統，不需要改變，直到區塊鏈域名出現，再次攪亂一池春水。

ICANN 於 2022 年 4 月 27 日發布一份研究報告「Challenges with Alternative Name Systems」分析區塊鏈域名（Handshake, ENS）對當前域名系統造成的挑戰，其中 Handshake 這項 DNS 根伺服器 的「替代系統」（Alternative System）值得我們特別注意。

區塊鏈域名

因比特幣等加密貨幣技術，帶來了網路傳遞價值的 Web 3.0 新世界，人人擁有錢包，以及一串錢包位址（該錢包的公鑰），輸入錢包位址，就可以將加密貨幣傳送給對方。區塊鏈網域，帶來的全新的域名概念，簡單一句話解釋，就是將 IP 給寫到區塊鏈「鏈上」。

首先 IP 的概念被擴張了，除了 IP 位址外，你的錢包位址，一樣是人類難以記憶的，一樣可以透過域名來表彰。因此，區塊鏈域名，就是把 IP 位址、錢包位址寫在區塊鏈鏈上，並由區塊鏈公鏈運行、移轉的另類域名系統，其中目前贏面最大、也引起 ICANN 關注的有二種：ENS（Ethereum Name Service ），以及本文要特別介紹的 Handshake。

Handshake 引起我最多注意，並且讓我感到莫名興奮。我們知道，頂級域名（.com/.io/.tw）都不是一般人可以觸碰、擁有權利的，這就像是一個神秘、受少數企業、單位掌控的特殊市場。而 Handshake 要做的，就是讓頂級域名變成數位資產（廣義型態的 NFT），並且人人可以取得、使用、授權。

圖 1：Handshake 圖示

資料來源：https://learn.namebase.io/about-handshake/about-handshake

Handshake 的重要機制

Handshake 就像是比特幣網路，是一種分散式帳本、任何人可以加入成為節點的域名協議，每個節點都在進行驗證，並負責管理根域名檔案（roots file）。過去這個權限是由 ICANN 單一機構負責。（延伸：Handshake 協議）

白話文來說，Handshake 協議透過繞開 ICANN、替換由 ICANN 組織掌管的 DNS 根檔案（Roots File）系統，透過區塊鏈協議來運作根檔案（頂級域名）的管理。

這做到一件事：你可以申請任何名稱的頂級域名（Top Level Domain Name, TLD），不須經過 ICANN 組織審核、繳交 18 萬美元申請費，而是透過 Handshake 域名競標公開程序，來取得紀錄於 Handshake 區塊鏈帳本的頂級域名。

頂級域名可以源源不絕出現，舉例而言，目前 HNS 上熱門的頂級域名，都是一些很短、特定類別的「名詞」，像是「crypto/」、「wallet/」「P/」，從 Handshake 的邏輯，你可以看到：exchange.crypto/、your.wallet/、I.P 的網域出現，並且被使用於指向 IP 位址，及錢包位址。

Handshake 改變了什麼？

傳統的 DNS 網站解析流程，可以分成八大步驟：

1. 使用者在網頁瀏覽器（Browser）鍵入「com」，DNS 遞迴解析程式（解析程式，Recursive Resolver）接收。
2. 解析程式查詢 DNS 根伺服器（Root server）。
3. 根伺服器搜尋根檔案（root file）有關頂級網域（.com）的 IP 位址，並回應解析程式。
4. 解析程式向.com 頂級域名伺服器（TLD Nameserver）發出

請求。

5. 頂級域名伺服器使用.com 的 IP 位址進行回應。
6. 解析程式將查詢結果傳送到次級域名伺服器（Subdomain Nameserver）。
7. 接著「com」的 IP 位址從次級域名伺服器傳回該解析程式。
8. 解析程式傳送 IP 位址回應網頁瀏覽器。

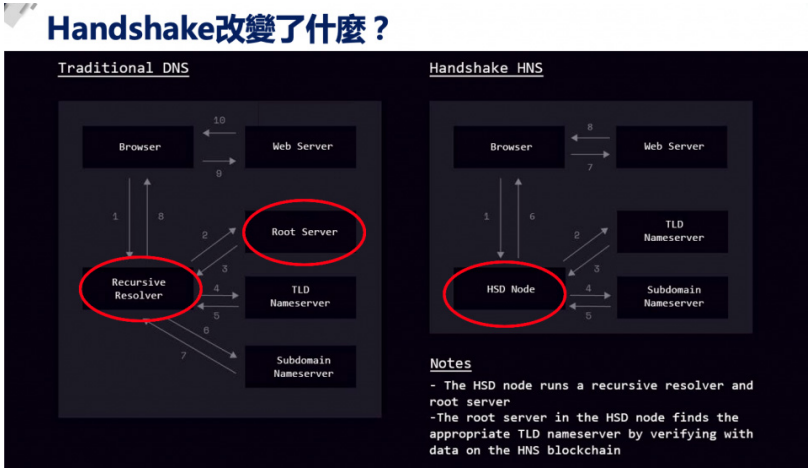


圖 2：Handshake HNS 與傳統 DNS 比較

資料來源：https://amentum.substack.com/p/the-handshake-browser-reference-client

Handshake 是一個類似比特幣的區塊鏈公鏈，但還是有其差異性，首先每一個 Handshake「節點」（HNS node）有兩項重要功能，改變了上述 DNS 八大步驟，並簡化為 6 步驟：

1. HNS node 具備解析程式（Recursive Resolver）及根伺服器（包括備份 Root file）的功能。因此，所有頂級域名的 IP 位址電話簿，將同步儲存備份於 HNS 的分散式帳本內，而瀏覽器只要透過 HNS node，可以直接接收頂級域名的 IP 位

址，取代上述步驟及 3.，其餘完全相同。

2. 換言之，對於整個 DNS 步驟而言，維持了 DNS 分層式訪問架構（先訪問 TLD Nameserver、再訪問 Subdomain Nameserver），只是 Root Server 由 Handshake 區塊鏈節點取代。

這樣的改變可能嗎？

答案是可能的。

我們知道，目前瀏覽器的設計是內建（解析程式，Recursive Resolver），域名的核心，是要讓瀏覽器可以解析到 IP 位址。因此，瀏覽器如果能夠解析到 Handshake 的域名（背後頂級域名的 IP 位址），那麼就可以按照既有 DNS 的流程，解析到網站。

現在有多種方式可以使用 Handshake 域名（詳細清單[1][1]），但 Handshake 網域仍不能直接使用在 Chrome 和 Safari 瀏覽器上，但已經有部分瀏覽器已原生支援 Handshake 域名（如 Puma Browser[2][2]），並直接瀏覽 Handshake 區塊鏈域名網站。據瞭解，市占率較具規模的 Opera 瀏覽器亦計畫於近期支援 Handshake 域名[3][3]。

從實際應用案例上，綜觀各大區塊鏈域名項目中，整體註冊量最高的也是 Handshake，Handshake 至 2020 年 3 月才正式上線，至今頂級域名的註冊數量已經突破 600 萬個，實際使用頂級域名（用於指向某 IP 位址）的數量，也突破 10 萬個。

---

1 https://learn.namebase.io/starting-from-zero/how-to-access-handshake-sites

2 https://www.pumabrowser.com/

3 https://blogs.opera.com/news/2021/12/opera-handshake-hns-partnership/

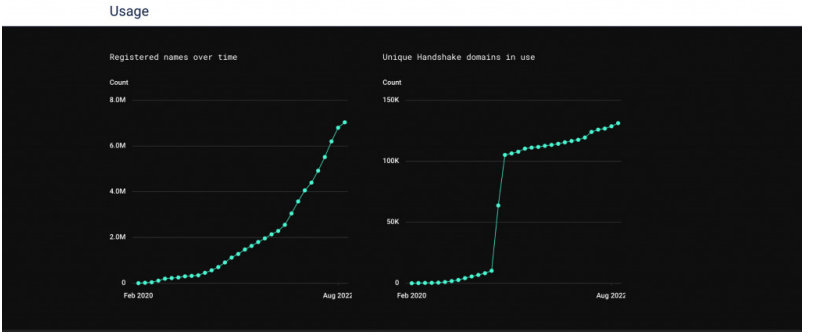


圖 3：使用 Handshake 數據圖

資料來源：https://www.namebase.io/stats

最後總結 Handshake 的兩大重點：

1. Handshake 目標並非取代 ICANN，而是希望開放、透明化頂級域名的註冊發放。
2. Handshake 可以融入 DNS 系統、並正在被快速採用中。

這也是為何，Handshake 值得我們特別注意。

量子電腦對未來科技的影響

吳宜庭／東海大學資訊管理學系

https://blog.twnic.tw/2022/05/02/22900/

「量子電腦」是什麼？

商業周刊其中一篇報導提過，台積電董事長劉德音認為：「若有一天，每個人的口袋都有一台量子電腦，我想 TSMC（台積電）一定不會缺席」，這句話影射了台積電在量子電腦的研發中勢必會佔有一席之地，並且認為量子電腦在未來可能會非常的普及。

在世界上第一部「電腦」是由美國人在 1946 年所發明的，隨著科技日漸進步，從以往我們所聽到的巨無霸電腦到現在的小型個人電腦，每個時代所演進的技術都是讓人非常驚嘆的。而至目前為止的電腦皆是採用馮紐曼式結構，其中的兩大建構電腦原則[1]：

1. 捨棄了十進制、改以二進制運算和儲存資料。
2. 要被執行的程式得先放在記憶體中、要執行時再去記憶體中抓出來。

而在馮紐曼式的電腦中，電腦被分為五大單元分別為：「控制單元」、「邏輯運算單元」、「記憶單元」、「輸入單元」（Input）和「輸出單元」（Output）。

而量子電腦卻不是如此，早在 1969 年量子電腦就已被提出，且由「基於量子力學的計算裝置」延伸而來，量子電腦擁有極快的運算速度，相較於傳統電腦的 0 與 1 位元（bit）的儲存，他可以有 0、1 或量子疊加為 0 和 1 的值，處理更多複雜的訊息。

---

[1] John Von Neumann (1993). First Draft of a Report on the EDVAC. 檢自：https://web.mit.edu/STS.035/www/PDFs/edvac.pdf (Apr. 07, 2022).

量子電腦的厲害之處

量子電腦以量子力學的疊加狀態及非局域糾纏為基礎，創造出一種處理資訊的全新觀點。量子電腦的特色即為：

- 量子疊加（quantum superposition）：有別於傳統物理態在某一特定時間上只具有一特定的狀態，量子態可以同時具有不同狀態。[2]
- 量子糾纏（quantum entanglement）：當多個量子系統進行交互作用，量子系統間可以進一步產生奇異的關連特性。[3]

而在量子計算中的最小儲存單位為量子位元（qubits），在計算能力上以「摩爾定律」（Moore's law）為例，積體電路上容納的電晶體數量，每隔兩年便會增長一倍，而量子的糾纏特性使量子電腦的計算能力以「雙指數成長」，即為 Google 量子人工智慧實驗室主任 Hartmut Neven 所提出的，又稱為「Neven Law」。[4]

量子電腦的應用領域非常的廣泛，從物理、化學、材料科學、人工智慧、金融科技等等，目前皆有各個專家在進行研究，微軟 CEO 納德拉曾提及：「量子運算的潛能在於原本需要花上好幾個世代才能處理的問題，在數小時或幾天內就能解決，比方說人工智慧、潔淨能源、全球暖化等。但是量子運算難題仍多，電腦也還在研發當中，仍有許多障礙。」[5]

---

[2] 李哲明、陳岳男（2011）. 簡單判別量子糾纏態.
檢自：http://research.ncku.edu.tw/re/articles/c../20110826/2.pdf (Apr. 07, 2022).

[3] 李哲明、陳岳男（2011）. 簡單判別量子糾纏態.
檢自：http://research.ncku.edu.tw/re/articles/c../20110826/2.pdf (Apr. 07, 2022).

[4] Kevin Hartnett (2019). A New Law to Describe Quantum Computing's Rise?
檢自：https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/ (Apr. 07, 2022).

[5] 黃亦筠（2017）. 量子電腦拚量產　解決全球暖化只要幾小時？
檢自：https://www.cw.com.tw/article/5086613 (Apr. 07, 2022).

量子電腦的挑戰

細緻的量子態十分容易受到振動或電磁場、熱擾動的干擾，所以在穩定量子態的維持需要在接近絕對零度的超低溫度操作。[6]目前主流的量子計算技術之一矽基（silicon-based）自旋量子已是可以利用且十分成熟的半導體技術，具有和現行電腦相容性，且被認為未來容易向上擴充，而吸引 Intel 和其他研究人員投入研發。[7]最後，為了使量子電腦真正發揮效能，專家們認為應該同步研發量子軟體以因應量子計算時的複雜與困難，若在未來需要大量使用時，運算的高複雜度勢必為人才培育帶來難題[8]。

結語

量子電腦的出現是科技的一個重大里程碑，量子運算有望解決地球上的某些最大挑戰：在環境、農業、健康、能源、氣候、材料科學等領域，以及我們尚未遇過的其他問題。雖然初期的應用只是在解決特定領域的特定問題，同時配合傳統電腦的操作為運算進行升級之用，若量子電腦一旦快速起飛，企業和國家就需準備如何因應這個新科技所帶來的利與害，並且需要為量子計算所帶來的破解資安威脅做好規劃與政策。

---

6 Jennifer ouellete. (2017). Nanofridge could keep quantum computers cool enough to calculate. 檢自：https://www.newscientist.com/article/2130210 -nanofridge-could-keep-quantum-computers-cool-enough-to-calculate/ (Apr. 07, 2022).

7 李建興（2017）. 低價量子電腦現曙光！普林斯頓大學矽基量子晶片實驗成功. 檢自：https://www.ithome.com.tw/news/119555 (Apr. 07, 2022).

8 Will Zeng, Blake Johnson, Robert Smith, Nick Rubin, Matt Reagor, Colm Ryan & Chad Rigetti. (2017). First quantum computers need smart software. 檢自：https://www.nature.com/articles/549149a (Apr. 07, 2022).

元宇宙中「個人隱私及數據」的法律隱憂

羅心妤／東海大學資訊管理學系

https://blog.twnic.tw/2022/06/16/23317/

元宇宙將如何蒐集數據?

參與元宇宙將涉及前所未有的數量和類型的個人資料。手機應用程式能夠了解個人在網路上移動或瀏覽的資訊，而元宇宙中，將能夠蒐集有關個人反應、運動甚至腦波模式等生理資訊，範圍從基本識別訊息至元宇宙中運動和活動的資訊，從而更深入地了解客戶的思維過程和行為。

參與元宇宙也將包括長時間的「登入」，這意味著將持續監控使用者的行為模式，使商品服務供應商能更「客製化」地為用戶提供服務。因此，在元宇宙中，用戶將不再需要通過打開手機並存取他們選擇的網頁或應用程式來主動提供個人資料。相反地，他們的資料將在進行虛擬生活時蒐集於後台。

歐盟與元宇宙相關的監管措施

元宇宙的機會伴隨著巨大的資料保護責任，最近的一些歐洲立法機構說明了監管機構在處理元宇宙問題時可能採取的方法。

1. 平臺到企業條例（Platform to Business Regulation，P2B Regulation）

元宇宙中電子商務領域將受制於歐洲的 P2B 條例，此條例涉及線上第三方服務，包括網路商店、社交媒體平臺和搜索引擎。其目的是透過「提高平臺的透明度和補救義務」，建立一個公平、可

預測、可持續和可信的線上商業環境。由於元宇宙中會有多種供應商在運營，此類的法規將非常重要。

《P2B 條例》對數位平臺供應商提出的要求如下：

- 明確描述平臺本身向消費者提供的商品或服務，以及其他供應商給予的任何差異化待遇。
- 不得在沒有明確理由的情況下終止供應商參與平臺，並在此後提供上訴權。
- 公開平臺對供應商商品和服務進行排名的參數。

2. 數位服務法（the Digital Services Act，DSA）

DSA 目的是提高用戶在網路環境中的透明度和安全性，並使創新的企業得以發展。雖然目前還只是一個提案，但它為數位平臺的服務和產品「導入責任和規則」，DSA 確認數位第三方服務提供者，對於內容審核、數據共用和使用以及監管的責任，避免對服務提供者施加不合理的處罰。

3. 數位市場法案（Digital Markets Act，DMA）

DMA 目的在解決平臺作為內部市場「資訊守門人」所產生的負面後果。根據歐盟委員會的說法，資訊守門人平臺受益於極端的規模經濟、網路效應，致使龐大的用戶依賴性、鎖定效應。這些特點將會大大破壞平臺服務的可競爭性，導致供應商和最終使用者受到不公平的待遇。在元宇宙內共享數據將是創建參與者旅程無縫銜接的關鍵方式，因而此法對於元宇宙設計有著巨大影響。

與元宇宙特別相關的是，資訊守門人必須：

- 避免將來自其核心平臺服務的個人數據與來其他服務的個人數據相結合，或在未經同意的情況下，將終端使用者登入其他服務以合併個人數據。
- 允許企業使用者向終端使用者推廣產品或服務並與之簽訂合同，允許終端使用者透過企業使用者在平臺上的應用程式

訪問、訂閱企業使用者的內容，無論終端使用者是否使用資訊守門人的核心平臺服務。

- 避免要求企業使用者使用、提供或相互協作身分識別的服務。

4. 歐盟人工智慧法規

元宇宙內的許多人類互動可能通過人工智慧來實現，該法規將禁止某些人工智慧實踐，並要求供應商和使用者遵守與高風險人工智慧系統有關的各種義務。特別是任何人工智慧解釋、操縱人類的反應、通過「深度造假」（Deepfake）模擬現實。如果人類與系統的互動是無縫的，並且是由人工智慧驅動，那麼在元宇宙內部，利害關係人應該遵守此類監管要求。

誰「負責」遵守適用的資料保護法？

為了實現可協作性，虛擬世界中一個實體蒐集的資料可能必須在不同的營運商甚至平臺之間無縫流動，軟體開發商和品牌將需要建立雙邊或多邊資料共享協議，以提高消費者體驗。因此，企業與平臺如何在實踐中實現合規性，引發了許多討論[1]：

1. 元宇宙是否會有一個主要管理機構負責收集所有個人資料並決定如何處理和共享這些個人資料？
2. 或是會有多個機構通過元宇宙收集個人資料，並各自確定自身利用目的？
3. 不同的機構應如何向使用者顯示各自的隱私聲明？
4. 還是機構應該聯合提供隱私聲明？
5. 如何以及何時徵求使用者的同意？

---

[1] The Metaverse: The evolution of a universal digital platform. 檢自：https://www.nortonrosefulbright.com/de-de/wissen/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform#section2 (May. 16, 2022).

6. 如果使用者在元宇宙中的個人資料被盜或濫用，誰來負責？
7. 哪些資料可以共享以及如何實施共享？

結語

雖然目前元宇宙的世界充滿未知及希望，但在個人隱私保護以及科技進步中取的平衡，一直是政府與開發者必須注重的必要條件。若共享數據是無縫旅程中的重要基礎，政府將是使用者在面對「元宇宙巨獸」的關鍵保障，因此在制定法規時，該如何與時俱進且明確地定義責任歸屬，以保護使用者的個人數據免受於不當處理，將會是需要戰戰兢兢面對的難題。

智慧城市發展與疑慮

吳幸芳／東海大學資訊管理學系

https://blog.twnic.tw/2022/03/07/22316/

何謂智慧城市

智慧城市的定義為利用資訊及通訊科技技術（information and communication technology，ICT）與數據分析的方式，創造、促進發展與解決城市的問題，以提升城市生活品質[1]。這意味著城市將擁有更智慧的交通運輸網路以及藉由智慧化技術擁有乾淨的水、空氣與土地，並且能維持更安全的治安，同時滿足人口高齡化需求。

智慧城市基本技術

智慧城市使用各種軟體程式、網際網路以及物聯網，以強化城市的管理。智慧城市的最終目的為居民提供智慧服務，提供更舒適的生活。

以下六大技術是將城市變成智慧城市的關鍵技術[2]：

1. 資訊及通訊科技技術（information and communication technology，ICT）[3]：智慧城市的一項重要元素是收集城市

---

1 TWI Ltd. (2018). What is a smart city?—Definition and examples. 檢自：https://www.twi-global.com/technical-knowledge/faqs/what-is-a-smart-city (Feb. 07, 2022).

2 Geospatial World (2019). Six technologies crucial for smart cities. 檢自：https://www.geospatialworld.net/blogs/six-technologies-crucial-for-smart-cities/(Feb. 07, 2022).

3 Allied Telesis (2022). ICT: The Fundamental Enabler for Smart Cities. 檢自：https://www.alliedtelesis.com/tw/en/blog/ict-fundamental-enabler-smart-

相關數據，因此需要使用能夠收集大量數據並加以詮釋與管理的 ICT 技術。藉由 ICT 在智慧城市中的應用，提高城市生活的品質、降低成本和資源的損耗。

2. 物聯網（Internet of Things，IoT）：隨著人工智慧與物聯網發展，硬體設備都可以增加聯網能力，透過資訊即時傳遞和處理，整合應用創造智慧加值服務。在智慧城市中，每台設備皆須互相連接，可互相交換資訊，進行智慧化判斷，進一步提升人們的生活品質。
3. 感測器（Sensors）：在智慧城市中無所不在的感測器是任何智慧系統中的重要組成成分，為了讓系統了解環境，配備感測器以從中收集所需資料相當重要。
4. 地理資訊技術（Geospatial Technology）：在智慧城市中，收集資訊的同時也須要對收集地點有精確的判定，地理資訊技術提供精確定位的需求，將地點收集成數據，以提供智慧判斷依據。
5. 人工智慧（Artificial Intelligence，AI）[4]：城市擁有大量的原始數據，AI 技術可辨別大量照片與影片，且可優化基礎設施、交通信號自動控制系統以及改善公共安全。
6. 區塊鏈（Blockchain）：區塊鏈技術保護數據資料的安全，與智慧城市結合後，可以整合所有城市服務，同時提高透明度與安全性。

智慧城市發展

2021 年 10 月瑞士洛桑管理學院（International Institute for

cities (Feb. 07, 2022).

[4] 名家廣場（2020）. 從人工智慧看全球智慧城市的應用趨勢. 檢自：https://view.ctee.com.tw/processing/14751.html (Feb. 07 2022).

Management Development, IMD）與新加坡科技設計大學（Singapore University of Technology and Design, SUTD）合作發布「2021 全球智慧城市指數（Smart City Index, SCI）[5]」，此 2021 年針對全球 118 座城市約 15000 名城市居民進行調查，重點聚焦於健康和安全方面的表現，亦包括在疫情發展下，科技如何解決工作環境等新項目，本篇專題文章將討論 2021 年 SCI 指數位居前兩名的城市，新加坡（第一名）與蘇黎世（第二名）。

新加坡：是世界上航運嶼位最繁忙的港口所在地，在過去幾年裡，新加坡政府實施新政策[6]，欲將新加坡打造成「花園中的城市」，綠色建築在新加坡已成為強制性的要求。在交通方面，新加坡政府通過車聯網（Vehicle to Everything, V2V）計畫[7]，若該計畫得以實現，到 2025 年，街道上所有汽車將為自動駕駛。正在籌劃的未來項目包含為無人機建立多條路線，以運送郵件等項目。

蘇黎世：是全球銀行和金融中心，被認為是瑞士的經濟和教育中心，也是歐洲最安全的居住地之一。蘇黎世政府實施一連串的戰略[8]，利用數位化轉型以改善環境，包括廢棄物循環管理以及保持城市安全、整合智慧電網與電動巴士取代柴油車等，共同努力打造一個可持續發展的城市。

---

5 IMD. (2020). Smart City index 2021. 檢自：https://imd.cld.bz/Smart-City-Index-2021 (Feb. 07, 2022).

6 Tania Alonso (2021). Success Story: The Transformation of Singapore into a Sustainable Garden City. 檢自：https://tomorrow.city/a/singapore-transformation-garden-city (Feb. 07, 2022).

7 We Build Value Digital Magazine. (2021). The future of sustainable mobility in Singapore. 檢自：https://www.webuildvalue.com/en/megatrends/singapore-smart-city.html (Feb. 07, 2022).

8 Murphy Morningstar (2021). About Smart Cities-Zurich. 檢自：https://www.aboutsmartcities.com/smart-city-zurich/ (Feb. 07, 2022).

智慧城市隱私權問題

雖然智慧城市有許多優勢，但智慧城市的發展會遇到像 Sidewalk Toronto 計畫[9]所出現的問題，該計畫之顧問因得知第三方公司有權取得收集到的個人資料內容，與當初承諾的去識別資料化相去甚遠，因而辭職，引起民眾恐慌。儘管該公司隨後有提出去識別化資訊方案，但因計畫中政府、其他公司皆有涉入，該公司無法要求每個人都須遵守。

為了打造智慧城市，生活中開始包圍著「看不見的科技」，感測器以及攝影機等設備可能架設在任何地點，不知不覺中感測器正默默地收集數據，人們也無法得知這些數據是如何被使用。因此有人會擔心政府取得過多的個人資訊，利用資訊以控制輿論，或公司取得資料後，讓商業利益極大化，這些問題都導致民眾對於智慧城市的反彈而失敗。

結語

智慧城市運用六大關鍵技術資訊技術來整合服務與系統，以提升資源運用效率與生活品質，六大關鍵技術包含：資訊及通訊科技技術、物聯網、感測器、地理資訊技術、人工智慧及區塊鏈，解決治安以及滿足人口高齡化的問題。2021 年之「全球智慧城市指數」由新加坡拿下第一，蘇黎世位居第二。智慧城市雖然有隱私權方面的問題，但不可否定的是各國政府和商業機構都積極發展，以支持可持續的智慧城市發展。

---

[9] Sidney Fussell (2018). The City of the Future Is a Data-Collection Machine. 檢自：https://www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551/ (Feb. 08, 2022).

網路世界中的媒體

吳宜庭／東海大學資訊管理學系

https://blog.twnic.tw/2022/07/13/23564/

「媒體」是什麼

日常生活中人們經常透過「大眾媒體」或「新聞媒體」來獲得知識，然後透過「傳播媒體」來傳遞這些訊息及知識，然而上述所提的大眾媒體、新聞媒體及傳播媒體皆統稱為「媒體」（media）。

「媒體」由拉丁字 medius 及 medium 而來，意指：「中間，中心，中介者，媒介」，亦有動態的媒介與傳遞之意。

由於資訊科技快速的發展，網際網路已成為眾多人獲取資訊的重要管道。運用電腦及應用程式，能在圖片上、影片上甚至多種多媒體的整合上呈現更多樣化的效果，藉由引起更多人的興趣並前往觀看，也因為資訊數位化，導致原本的大眾媒體與新聞媒體逐漸進行轉型，而傳播媒體可能也從舊有的報紙，電視、廣播或雜誌轉向至電腦或手機透過網路在各地傳播。

社群媒體 vs.傳統媒體

1. 傳統媒體：傳統大眾媒體傾向於使用線性概念化或面向源的定義，所呈現的資訊是單向的，沒有觀眾的回饋。[1]傳統媒體具有組織化體系及較高的專業素質，具有一定的公信力與

[1] Ade Kusuma & Adiasri Putri Purbantina & Citra Rani Angga Riswari & Ririn Puspita Tutiasri (2020). Is Online Media More Popular Than Traditional Media To Advertise a Brand in the Digital Age? (Jun. 11, 2022).

權威性。[2]與近幾年興起的網路媒體相比即時性與互動性較低，傳統媒體多以電視、報紙、廣播電台等方式，透過專業人員與設備藉由一對多的方式對大眾進行資訊的傳播。

2. 社群媒體：人們用來創作、分享、交流的虛擬社區與網路平臺，社群媒體備有讓使用者進行編輯與發布訊息的權利，並且可以自行集結成某種類型的群體，社群媒體上可以有多種不同的形式呈現，如：文字、圖片、音樂及影片，內容多以使用者的主觀方式呈現。[3]現今流行的社群媒體包含 Facebook、Instagram、Twitter、Snapchat、Pinterest 及 TikTok 等。

對於兩者間的差異，傳統媒體較針對區域性的訊息傳遞，而在社群媒體上，因為網路無邊界，所以世界各地的人皆可以透過網路在社群上傳遞訊息。傳統媒體在拍攝影片或撰寫文章上雖然可以立即製作，但是在傳播的過程上卻會因為需要印刷後發布或是透過機器轉播，而無法達到即時性，社群媒體則因為網路與通訊設備的進步，可以做到即錄即發布與隨寫隨上傳的效用。但傳統媒體的寫作內容風格與品質，會比社群媒體要客觀中立且更正式。

表 1：傳統媒體與社群媒體之比較

	傳統媒體	社群媒體
傳播管道	新聞、報紙、雜誌、廣播	Facebook、Instagram、Twitter、Snapchat、Pinterest、TikTok
傳播者	記者、報社、專業人士	社會大眾

[2] 陳國祥（2020）. 人人都是自媒體的時代，傳統媒體業該如何求新求變？檢自：https://bookzone.cwgv.com.tw/topic/17442(Jun. 11, 2022).

[3] Dewing, Michael (2010). Social Media: An Introduction. 檢自：https://bdp.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/InBriefs/PDF/2010-03-e.pdf(Jun. 11, 2022).

製作成本	高	低
寫作內容	具較嚴格的審核	自由
第三方公信力	高	低
即時性	低	高

社群媒體帶來的改變

1970 年瑞士研究員發出全世界第一封電子郵件，人們開始擁有網路上的「群組」，並開始討論各種話題，進而延伸發展到現今的社群，最知名的社群軟體 Facebook，最早為馬克·祖克柏（Mark Zuckerberg）在就讀學士時，在校內蒐集相片，並架設了「Facemash」網站吸引了許多訪客，雖在那時期網站遭受到關閉，但他也因此受到啟發，並在後續與幾名夥伴成立公司，推出了供大眾使用的 Facebook。在 2005 年 Youtube 問世，免費讓使用者上傳及分享影片，2006 年 Spotify 創立，使用者可以分享音樂撥放清單。[4]

根據 2016 年資策會產業情報研究所（Market Intelligence & Consulting Institute，MIC）對臺灣民眾的新媒體與網路社群行為研究顯示，在使用 Facebook 時有 60%的網友會因而減少瀏覽報紙、雜誌或電視新聞等傳統媒體的時間。[5]

在社群媒體使用的如此頻繁的情況下，同時也必須兼顧網路安全與資訊安全的問題。根據 2022 年的報導，在 2021 年期間社群媒體服務品牌遭受到釣魚攻擊的比例為最多，透過假冒各大知名品牌

[4] 孫耕悅（2020）. 社群媒體何時興起、從過去到現在的歷史、當前社會環境下的現況. 檢自：https://108104048.medium.com/social-media-d53a0b181074 (Jun. 11, 2022).

[5] 蔡美瑛（2016）. 傳統媒體如何因應新媒體發展的衝擊（一）：序言. 檢自：https://scitechvista.nat.gov.tw/Article/C000003/detail?ID=bcb3521e-5774-4a71-a283-27d40af25404 (Jun. 11, 2022).

來獲取受害者信任[6]。在 2021 年時，美國聯邦貿易委會員（Federal Trade Commission，FTC）發布消費者警訊，發現詐騙者透過網路社群媒體假冒知名人士的詐騙案不斷增加[7]。同年，歐盟消費者組織（The European Consumer Organisation，BEUC）對 TikTok 惡意利用年輕用戶的資料及權利提出投訴，因為其社群多次侵害歐盟消費者權利，也未保護兒童免受隱藏廣告及不當內容的侵害，雖然短短數年內，TikTok 已成為歐洲最受歡迎的社群媒體平臺，並擁有數百萬用戶，但 TikTok 的侵權行為卻一再辜負使用者。[8]

結語

網路的發展加上人們的創新，逐漸吸引眾多人使用社群媒體，透過社群在上面分享訊息與好友們互動或是從上面找尋所要的內容，甚至廣告商會在上面投放廣告獲取收益，不同類型社群平臺，已逐漸朝專業分眾社群發展，未來對於內容選讀及傳播的要求也會愈來愈高。而社群媒體的發展將現實與數位世界連結更緊密，並且可能會成為網路購物的主要管道，有四面八方的網路資訊自動找上門，交友也不受地域限制。[9]雖然社群媒體的發展日漸增長，但是在資訊安全這塊仍需持續加強，不論是修正條款或是加強政策，在社群上的使用者也須警惕自己在網路上的所作所為，因為所有的行徑皆會被記錄，並且不是能輕易被抹除的。

---

6 TWNIC. (2022). 2021 年假冒各大品牌的釣魚攻擊，以社群媒體為最頻繁的類型. 檢自：https://blog.twnic.tw/2022/03/23/22542/ (Jun. 11, 2022).

7 TWNIC. (2021). 詐騙者在社群媒體上假冒 Elon Musk 等知名人士，以多種詐騙手法，半年內詐得高達 8000 萬美元.
檢自：https://blog.twnic.tw/2021/05/27/18780/ (Jun. 11, 2022).

8 TWNIC. (2021). TikTok 被指控大規模侵犯歐洲用戶權利.
檢自：https://blog.twnic.tw/2021/03/16/17245/ (Jun. 11, 2022).

9 許凱玲（2011）. 10 個社群媒體的未來發展趨勢. 檢自：
https://www.bnext.com.tw/article/18898/BN-ARTICLE-18898 (Jun. 11, 2022).

該如何應對演算法偏見？

羅心妤／東海大學資訊管理學系

https://blog.twnic.tw/2022/04/11/22701/

為何會出現演算法偏見？

如今，人工智慧被嵌入在一個又一個的系統中，而人工智慧的偏見主要由以下兩個原因形成：

1. 認知偏差：源自於大腦試圖簡化處理有關人類的資訊而形成的無意識偏差，影響認知偏差的原因可能為：
   - 訓練的資料集中含有人類世界已存在的偏差
   - 設計者在不知不覺中將偏差類別引入算法模型
2. 數據的完整性不足：數據不完整可能不具有代表性，因此可能存在偏差。

演算法偏見的解決方法

自動決策並不是中立的決策，只要人類有偏見，演算法也會有偏見。消除偏見沒有快速的解決方案，但麥肯錫等顧問提出可參考的了「從業人員、商業人士和政策領導者需要考慮的六項人工智慧潛在解決方法」（Six potential ways forward for AI practitioners and business and policy leaders to consider）[1]：

1. 了解人工智慧可以幫助糾正偏見以及可能加劇偏見的領

[1] Tackling bias in artificial intelligence (and in humans). (2019). Jake Silberg and James Manyika. 檢自：https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans (Mar. 26, 2022).

域：組織將需要了解最新情況（例如：那些曾經有偏見的例子）以了解 AI 如何以及在何處可以提高公平性，以及 AI 系統在哪些方面遇到了困難。

2. 「建立流程」來測試和減輕系統中的偏見：技術工具可以突顯潛在的偏見來源，並揭示數據中影響最大的特徵；運營策略可以更有意識的抽樣來審計數據和模型以改進數據蒐集方式；流程和指標的透明度可以幫助觀察者了解相關權衡的步驟。
3. 對於人類決策中的潛在偏見進行事實分析：隨著人工智慧揭開更多關於人類決策的資訊，領導者可以考慮如何透過人工智慧找出長期被忽視的偏見來提供幫助。
4. 充分探討人類和機器如何最好地協同工作：考慮在什麼情況下，自動決策是可以接受的，以及什麼情況下人類應該持續參與。
5. 對「偏見研究」進行更多投資，為研究提供更多數據，並採用跨域方法：更多的進展將需要跨域的參與，包括倫理學家、社會科學家和最了解過程中每個應用領域的專家。
6. 加大人工智慧領域的多元化：一個多樣化的人工智慧社群將更有能力預測、發現和審查不公平的偏見，並能夠更好地與可能受偏見影響的社群接觸。

美國與歐盟政府的應對策略

1. 歐盟

2019 年歐盟議會發布《可信賴人工智慧倫理準則》（Ethics Guidelines for Trustworthy AI）[2]。共計七面向包括：應由人類監督

[2] Ethics Guidelines for Trustworthy AI. (2019). 檢自：https://www.aepd.es

AI、兼顧穩健與安全、重視隱私和資料治理、具有透明度及可追溯機制、確保多元和公平、尊重社會和環境福祉、建立完善的問責制度。

2021 年 4 月歐盟委員會發布了長達 108 頁的《關於制定人工智慧統一規則》（簡稱，《人工智慧法案》）[3]的提案，該法案以「安全」和「非歧視」為原則，根據 AI 可能對人的基本權利產生威脅劃分成三個等級：不可接受的風險、高風險、低風險。正如《通用數據保護條例》（GDPR）將個人數據按照敏感程度施以不同程度的保護義務並進行不同強度的監管。《人工智慧法案》的關注重點與 GDPR 高度相似，例如：年齡、種族、政治取向等可能成為社會中遭受歧視的因素，都被視為劃分風險的依據。

2. 美國

2022 年《演算法問責法案》[4]於 2022 年 2 月 3 日在美國眾議院提出，目標是提高自動化決策的透明度和公平性，並對要求相關公司要對偏見、有效性和其他因素進行影響評估。此法案為 2019 年《演算法問責法案》的更新版本，在專業性與細節有許多改進之處，包括：釐清涵蓋哪些類型的演算法及公司、確保將消費者影響放在評估首位，並提供如何建構報告的更多細節。該法案將授權聯邦貿易委員會（FTC，Federal Trade Commission）制定法規，要求其管轄範圍內的公司對高度敏感的自動決策系統進行影響評估。其內容包括：

/sites/default/files/2019-12/ai-ethics-guidelines.pdf (Mar.26 , 2022).

[3] Proposal for a Regulation of The European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. (2021). 檢自：https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (Mar.26, 2022).

[4] H. R. 6580: Algorithmic Accountability Act of 2022. (2022). Govtrack. 檢自：https://www.govtrack.us/congress/bills/117/hr6580/text (Mar.26 , 2022).

- 要求公司評估自動化關鍵決策的影響，包括已經自動化的決策流程
- 要求聯邦貿易委員會制定法規，為評估和報告提供結構化指南
- 要求公司向聯邦貿易委員會報告選定的評估資料
- 要求聯邦貿易委員會發布一份年度趨勢匿名匯總報告，並建立一個資料庫，消費者和宣導者可以在其中審查哪些關鍵決策已被公司利用人工智慧自動化。

結語

隨著人工智慧的應用變得無處不在，因演算法而形成偏見的可能性也隨之增加。此時，國際上重要的指引原則，體現民意對 AI 治理的期待。

人類正在創造有偏見的數據，而同時也在創造識別偏見的演算法來消除偏見。從上述資料中，可以歸納出解決演算法偏見的兩大主軸：如何積極地發現偏見、如何有效率地監督演算過程。因此，理解基礎數據中固有的偏見，並開發可解釋結果的決策系統，將是解決既有演算法偏見的潛力的關鍵。此外，政府應該立法明定如何處理文件評估、披露和糾正措施，並授權合格人員調查和糾正人工智慧系統中的偏見和安全漏洞。

新的革命：Web 3.0

莊舒歆／東海大學資訊管理學系

https://blog.twnic.tw/2022/04/27/22697/

網路的發展

網際網路的發展，從 Web 1.0 到現今 Web 3.0，是伴隨著人類的需求和使用而持續演進。以圖書館來譬喻可以貼切的形容網路世界，龐大的書籍數量就像網路世界的資訊和產品一般，人們可以輕易的探究、摸索和交易資訊與產品。

回顧過去，Web 1.0 只是單方的呈現內容，單純讓使用者接收，用戶就是搜索並瀏覽，就像去圖書館找書並且翻閱一樣。

到了 Web 2.0 時代，使用者不只是用眼睛瀏覽，可以到處留下自己走過的痕跡，能自行寫下內容並上傳到網頁上，就像圖書館讀者留言區，看書後提供自己的借書證（身分證明）讓管理員（第三方）核准，留下我們的筆記、心得在留言板；同樣地，在網路上我們寫上我們對於人、事、物的想法彼此分享，是一個開放的空間，但是相對的我們需要提供資料給予平臺才能做出行動。Web 2.0 具有互動性，由企業提供獨立、中心化的服務。

此時 Web 1.0 網站投餵資訊給用戶的時代過去了，Web 2.0 更注重於用戶交流和回饋的社交與評論網站。

來到聲量極大的 Web 3.0，其實 Web 3.0 概念早在 1998 年就被提出，最早期的推手是全球資訊網（World Wide Web, WWW）的發明者 Tim Berners-Lee，他提出語意網[1]（Semantic Web）的想法，

[1] Tim Berners-Lee, James Hendler and Ora Lassila (2001). The Semantic

認為新世代網際網路，電腦將用模擬人類的方式處理資料，所有數據都可以依據上下文、概念進行理解。約會網站 eHarmony 的研發高級主管 Gian Gonzaga 曾說：「網路可以開始回饋我們所不為人知的東西，Web 3.0 能學習並了解你是誰」[2]。2014 年，以太坊共同創辦人 Gavin Wood 重新提出 Web 3.0 的想法[3]。他指出，應該有一種不受審查、低門檻的基礎網路傳遞協議來取代目前的傳統網路技術，保護網路使用者的資訊與資金流動。不再像 Web 2.0 一樣，第三方科技巨頭有巨額利潤與壟斷權力。

理想中的 Web3.0，用戶每個人都身在圖書館內，沒有管理員，我們需要付出，幫忙維護、打掃環境，繼而取得我們想看的書籍，而不再需要透過管理員（第三方）。人們聚集圖書館內，一舉一動都會被觀察並學習，有時就會有熱情觀察你的小精靈（AI），推薦一本符合你閱讀喜好的書；Web 3.0 可以比作理解用戶並實現個性化的人工智慧助手，但這需要用戶提供大量且長久的數據，讓人工智慧了解你。

Web 3.0 爭議

密碼學家計算機安全研究人員 Moxie Marlinspike，同時也是 Signal 的創建人對於加密貨幣的世界有個疑惑[4]，人們所討論的區

Web. Scientific American. 檢自：https://web.archive.org/web/20171010210556/https://pdfs.semanticscholar.org/566c/1c6bd366b4c9e07fc37eb372771690d5ba31.pdf

2 Sara Martin (2011). The promise of Web 3.0. 檢自：https://www.apa.org/ monitor/2011/10/web

3 Tristan Winters (2014). WEB 3.0—A Chat with Ethereum's Gavin Wood. 檢自：https://bitcoinmagazine.com/business/web-3-0-chat-ethereums-gavin-wood-1398455401

4 Moxie Marlinspike (2022). My first impressions of web3. 檢自：https://moxie.org/2022/01/07/web3-first-impressions.html

塊鏈，只圍繞著與伺服器之間的信任模式。人們不會想自己建立伺服器，所以企業銷售能存取以太坊節點的 API 服務。然而，這些客戶端的 API 沒有任何方式來驗證區塊鏈是否真實存在，這又變成了一個中心化。

一般而言，NFT 不會把資料存放於區塊鏈上，因為成本太高，通常擁有者只會有一個指向內容的連結。Moxie 發現，在知名 NFT 平臺上，以數百萬、甚至千萬美元出售的 NFT 藝術品，其連結沒有使用加密技術。意味著只要能夠存取或駭進該機器、買下該網域名稱，任何人都能變更 NFT 的圖像以及名稱。

Moxie 還做了個實驗，在 NFT 交易平臺 OpenSea 上傳了圖片，後來因為不明理由遭到下架，他發現 NFT 作品消失在他的加密錢包中。原因是加密錢包使用了 OpenSea API 來顯示 NFT，所以當 OpenSea 移除了相關 NFT 之後，錢包內的 NFT 也跟著不見。但這本來不應該發生的，因為 Moxie 的 NFT 作品已經登記到以太坊的網路了。

上述的狀況顯露出 Web 3.0 行業的一個深層問題，標榜去中心化的區塊鏈應用，其實並沒有能力和區塊鏈進行直接關聯，反而使用的是幾家區塊鏈公司的 API。造成了明明知道自己的資產就在鏈上，但是加密貨幣客戶端卻無法顯示它存在的窘境。

Moxie 認為目前的 Web 3.0 不能將人們自中心化解放，也不認為它會改變人們與科技的關係，依舊需要仰賴中心化的分散式網路，他認為最值得思考的事情之一，是該如何避免其隱私能力低於目前的 Web 2.0。

除了 Moxie 外，Tesla 執行長 Elon Musk 也認為那只是個噱頭，曾說：「有誰看到 Web3 了嗎？我找不到」[5]。

---

[5] Twitter.com

結語

當人們以 Web 3.0 宣傳去中心化的時候，該思考的是：如果一個技術要最大化的被人使用，就必定會有中心化平臺的出現，因為只有平臺不斷的更新、改善，將產品做到簡單易用，才能吸引更多人使用。

單看區塊鏈行業，雖說去中心化，但實際仍是基於中心化（交易所）平臺；雖然去中心化的實現，在目前看來仍需更多的時間和技術去突破，但去中心化理念的確激發人類更多的想法，貨幣的去中心化產出了加密貨幣，網站的去中心化產出了 Web 3.0 概念。除此之外，我們還需要留意資安及隱私問題，網際網路的演進造就越來越龐大的網路群體以及巨大的網路經濟，Web 3.0 的實現需要更為安全的網路環境。

美國加密貨幣交易所 Coinbase 前技術長 Balaji Srinivasan 曾說：「Web 3.0 給予的是一種可能性，而不是保證」[6]。

目前的網際網路已可以滿足人們的需求，但從去中心化與個人隱私權益保護的立場來看，Web 3.0 有存在的價值，也是人類社會的未來式，期望 Web 3.0 能引領我們開啟下一場科技革命的大門。

[6] Balaji Srinivasan (2021). Web3 offers the possibility, not guarantee, of something better. 檢自：https://twitter.com/balajis/status/1473204021183668226?lang=zh-Hant

公私協力打擊域名濫用之司法解決架構倡議

蔡志宏／臺灣士林地方法院勞動庭庭長

https://blog.twnic.tw/2022/01/14/21408/

倡議背景說明

域名（domain name）是方便全球網路使用者近用網際網路所不可或缺的網路關鍵資源（Critical Internet Resources，CIR）。濫用域名將破壞公眾對於網際網路的信任，是違反全球網際網路社群公共利益的行為，應該予以有效打擊與遏止。為打擊遏止域名濫用而由各國法院對於違法使用域名進行沒收或扣押宣告時，如僅能由各國於其管轄權範圍內予以片面執行，將造成域名原本所具有網路空間單一識別功能之碎片化，終而影響單一全球網際網路（One World, One Internet）之終極理想。

為此，本文提出公私協力打擊域名濫用之司法解決架構倡議，旨在建立可供全球網際網路空間共同執行域名沒收或扣押裁判之標準要件及程序，以支持各國以司法程序打擊域名濫用，同時維繫全球網際網路空間運作之一致性。

倡議全文內容

有鑑於：打擊域名濫用是屬於與全球網路有關的公共政策議題，各國有權於其管轄範圍內，進行決策並依法落實執行，但各國依法執行其打擊域名濫用政策時，仍應儘量維持域名作為全球網路空間單一識別符號之功能，以維護全球網路社群之公共利益。

有鑑於：全球域名註冊管理機構（Registry）、受理註冊機構（Registrar）於適當且必要的情況下，如願自主協力執行各國法院關於沒收、扣押、禁制或暫時禁制使用特定域名之裁判，將有助於盡可能維護域名作為全球網路空間單一識別符號之公共利益。

有鑑於：各國於打擊域名濫用時，仍應注意維護域名註冊人應有之訴訟權益，並應合理行使其管轄權，對於自主協力執行關於域名裁判之域名註冊管理機構、受理註冊機構，應避免影響其既有之正當營運。

有鑑於：公私協力共同打擊域名之相關執行情形，應當公開透明，並接受全球網路社群的共同監督與問責。

我們共同認知並願共同致力如下：

第一條：（自主協力執行裁判之要件）

全球域名註冊管理機構、受理註冊機構在以下情況，願自主協力執行各國法院關於沒收、扣押、移轉、永久或暫時禁制使用特定域名之裁判：

- 作成裁判之法院屬於公正獨立之審判機構，其裁判之作成不受其他政府機關干涉；
- 該裁判係基於避免或遏止著作權、商標權遭受侵害、兒童色情之散布、詐欺資訊之傳遞或其他國際公認犯罪行為之繼續或擴大。
- 作成裁判之法院，其所在國家就該裁判之作成，應具備合於國際法之管轄權基礎。
- 關於沒收、移轉、永久或暫時禁制使用特定域名之裁判作成前已於適當時間按域名註冊人留存於 WHOIS 資料之聯絡方式通知，並給予表示意見之適當機會。
- 關於沒收、移轉、永久禁制使用特定域名之裁判，已提供域名註冊人至少一次不服裁判之救濟機會；關於扣押或暫時禁

制使用特定域名之裁判，應於裁判後之適當時間內（至遲不得超過 3 個月）提供域名註冊人正式接受審判之機會。

第二條：（自主協力執行裁判之方法及時限）

全球域名註冊管理機構、受理註冊機構為依前條自主協助執行各國法院裁判，願提供各國裁判執行機關及時有效之聯絡方式，並願於各國裁判執行機關提出協助執行裁判請求後 30 日內，依裁判意旨執行關於域名之裁判；如認受請求協助執行之裁判不合於前條所定之狀況者，亦願同上期間內，回覆請求協助之該裁判執行機關，並說明其理由。

第三條：（合於自主協力執行裁判要件之證明）

為便利全球域名註冊管理機構、受理註冊機構及時順利依第一條規定執行各國法院裁判，各國法院作成關於第一條之裁判時，宜於裁判內表明其作成已合於第一條所列情況；必要時，各國裁判執行機關，並願提供相關佐證資料參考。

第四條：（自主協助執行之相關費用及權益關係轉讓）

全球域名註冊管理機構、受理註冊機構為自主協力執行第一條所規定執行之各國法院裁判，得依事先公布之無歧視標準，收取相關必要合理費用；如經執行關於沒收或移轉域名之裁判，域名受讓人無論為公、私團體、機構或個人，均願按照沒收或移轉前之域名註冊協議，承擔域名註冊人之合約義務。

第五條：（自主協力執行之公開透明）

全球域名註冊管理機構、受理註冊機構願至少每年一次於網際網路上公布自主協力執行關於第一條所定各國裁判之情形。

倡議願景展望

經由本文倡議的提出，期待能夠藉此凝聚更多全球網際網路社

群的普遍共識，並使全球網際網路的使用與運營獲得更多全球公眾的信賴，從而提升全球網路治理更進一步接近理想與至善。

（本文倡議內容純屬筆者個人意見，並不代表 TWNIC 立場）

科技環境與永續發展

戴匡／東海大學資訊管理學系研究員

https://blog.twnic.tw/2022/02/08/21787/

資料中心普及與環境傷害

一篇刊載於《自然》（Nature）科學期刊中的研究指出[1]，資通訊產業很快就會占據全球總用電量 20%，其中約莫 3 成的用電需求將來自資料中心，換言之，該產業耗用自然資源的幅度未來只會繼續增加，不會減少。美超微電腦股份有限公司（Super Micro Computer，Supermicro）於 2020 年發布的《第三年度 Supermicro 資料中心暨環境報告》（The third annual Supermicro Data Centers & The Environment Report）[2]也點出，隨著資料中心的規模與效能日益增加，耗電量亦屢創新高。目前幾乎所有地區都對投資興建資料中心興致勃勃，各個組織正增加對伺服器、資料庫及其他資料中心基礎設施的投資，其中以亞太區擁有最多資料中心。由此可見，資料中心對環境構成的衝擊已是不得忽視的嚴正議題。

實務上，資料中心衍生的環保議題已受到環保團體的重視，例如：2021 年 12 月、荷蘭小鎮 Zeewolde 通過 Facebook 資料中心建設計畫[3]就遭受批評。根據目前預估，該中心每年將消耗 13 億 8 千

---

1 Nicola Jones (2018). How to stop data centers from gobbling up the world's electricity, Nature, vol. 561, No. 7722. 檢自：https://www.nature.com/articles/d41586-018-06610-y (Jan. 17 , 2022).

2 Supermicro (2020). The third annual Supermicro Data Centers & The Environment Report. 檢自：https://www.supermicro.com/zh_tw/white-paper/datacenter-report (Jan. 17 , 2022).

3 Nichola Daunton (2022). Could a new Facebook data centre throw the Netherland's

萬度電，且其消耗的能源相當於擁有 46 萬人口的城市，儘管 Facebook 母企業 Meta 一再強調將與利害關係者合作，將新興可再生能源引入電網，並保證中心僅使用再生能源營運，但仍遭國內環保團體無情砲火，他們擔憂荷蘭可能無法達成 2030 年的減碳目標。

根據資料中心基礎設施研究機構 Uptime Institute 調查[4]，大部分資料中心積極追蹤耗電量，因為電力是資料中心最大的營運成本，然而，由於用水及排碳並不在企業的商業考量中，多數資料中心營運商未衡量其電子垃圾處理計畫對用水量或排碳量之影響，根據相關統計，目前僅有一半的管理人員會追蹤用水量；約莫 33% 管理人員會監控排碳量或電子垃圾。

資料中心之所以如此不環保，很大原因是約 40%能源用於冷卻 IT 設備[5]。產業專家指出，在寒冷地區建立資料中心有助於減少碳排，然而，將所有資料中心遷移到寒帶國家顯得不切實際，且隨著越來越多國家要求在當地儲存公民資料，遷移資料中心的方案更是天方夜譚，此外，由危險化工製品製成的 IT 設備冷卻劑也構成另外汙染源。再者，由於能源供應是資料中心的關鍵業務[6]，因此各中心皆配備備用電池，而備用電池零件以及廢電池造成的毒害也都會影響環境，部分伺服器中心甚至使用汙染性較高的柴油燃料。

---

off its climate path? euronews.green. 檢自：https://www.euronews.com/green/2022/01/06/could-a-new-facebook-data-centre-throw-the-netherland-s-off-its-climate-path (Jan. 17 , 2022).

4 Rich Miller (2021). Uptime: Most Data Centers Still Not Tracking Environmental Impact. Data Center Frontier. 檢自：https://datacenterfrontier.com/uptime-most-data-centers-still-not-tracking-environmental-impact/ (Jan. 20, 2022).

5 Charlotte Trueman (2022). Why data centres are the new frontier in the fight against climate change. Computerworld. 檢自：https://www.computerworld.com/article/3431148/why-data-centres-are-the-new-frontier-in-the-fight-against-climate-change.html (Jan. 20, 2022).

6 能源成本占資料中心營運開銷的 70%至 80%。

加密貨幣挖礦也加劇全球暖化

除資料中心外，近年吸引大量投資人的加密貨幣浪潮也加劇全球暖化[7]。加密貨幣產業須投入大量運算技術進行驗證（俗稱挖礦），而這需要相當高效且耗能的電腦設備。隨著加密貨幣日益普遍，挖礦行動已從散戶轉變為大型礦場系統，當軟硬體設備愈先進，就愈有機會盡快算出答案、取得價值不斐的加密貨幣。這類系統通常包含數百萬臺高度專業的電腦設備，除成本高昂外，尚須大規模空間與足夠的冷卻能力，防止 24 小時運轉的設備過熱當機，也因此使加密貨幣體系成為耗電量極高的產業。

在所有加密貨幣中，比特幣更被點名已造成嚴重汙染，根據劍橋大學比特幣電力消耗指數（Bitcoin Electricity Consumption Index）[8]，比特幣每年消耗的電力超過馬來西亞或瑞典等國家一年的能源用量。此外，根據一項 2018 年發表於學術期刊《自然氣候變化》（Nature Climate Change）的研究[9]，因比特幣成長導致的碳排放相當可觀，最快將於 2033 年導致全球升溫攝氏 2 度。

有論者認為可用再生能源進行挖礦，但根據相關研究[10]，目前僅有 39%挖礦是運用再生能源，此外，即使在積極利用再生能源的美國，也有大量非環保礦場。例如：賓州一間名為 Stronghold 的比特幣挖礦公司收購燃煤發電廠 Scrubgrass 以進行比特幣挖礦，且案

---

7 Yahoo 新聞（2021）. 加密貨幣竟然加速全球暖化？比特幣「挖礦」年用電量竟超出阿根廷、荷蘭. 檢自：https://reurl.cc/KpQQZq (Jan. 21, 2022).

8 研究資料參考劍橋大學官方網站：https://ccaf.io/cbeci/index

9 Patrick J. Kiger (2021). Cryptocurrency Has a Huge Negative Impact on Climate Change. Howstuffworks. 檢自：https://science.howstuffworks.com/environmental/conservation/issues/cryptocurrency-climate-change-news.htm (Jan. 21, 2022).

10 Emma Newbery (2021). 4 Facts That Prove Bitcoin Is Still Disastrous for the Environment. the ascent. 檢自：https://www.fool.com/the-ascent/cryptocurrency/articles/4-facts-that-prove-bitcoin-is-still-disastrous-for-the-environment/ (Jan. 21, 2022).

例可不止這一樁。目前未見獎勵挖礦產業利用可再生能源的相關措施，因此為降低成本，產業通常選擇便宜好取得的能源來源。

各國也開始正視比特幣造成的環境衝擊，例如：瑞典政府因擔憂無法達成《巴黎協定》（Paris Agreement）設下的環境目標，呼籲歐盟明文禁止加密貨幣挖礦[11]，儘管針對加密貨幣產業徵稅，以及宣傳其對環境的影響也可產生些許效果，但由於加密貨幣產業的急速成長，上述方法並無法解決燃眉之急。

如何善用科技保護地球

資料中心與加密貨幣產業必然存續，因此緩解其環境衝擊已是重中之重。《歐洲資料中心能源效率行為準則》（The European Code of Conduct for Data Centre Energy Efficiency）計畫[12]就是一項很好的嘗試，該計畫為歐盟資料中心營運者提供應遵循的一般原則及實際行動，透過這些原則與行動，將可更經濟有效的利用能源。簽署方有義務遵守該準則及相關承諾，成效卓著者將有機會獲得《歐盟資料中心行為準則獎》（EU Data Centres Code of Conduct Awards）。

Amazon、Apple、Microsoft 及 Facebook 等科技巨頭對環境承諾也發揮領頭羊的作用，它們承諾在不久的將來完全使用可再生能源[13]。工程顧問公司 RED Engineering Design 執行長 Ian Whitfield

---

[11] Owen Hughes (2021). Cryptocurrency: Should Bitcoin mining be curbed in Europe? Swedish authorities say yes. ZD Net. 檢自：https://www.zdnet.com/article/cryptocurrency-should-bitcoin-mining-be-curbed-in-europe-swedish-authorities-say-yes/ (Jan. 21, 2022).

[12] 參考 ICT footprint eu 官方網站介紹：https://ictfootprint.eu/en/eu-code-conduct-data-centre-energy-efficiency-0

[13] Charlotte Trueman (2022). Why data centres are the new frontier in the fight against climate change. Computerworld. 檢自：https://www.computerworld.com/article/3431148/why-data-centres-are-the-new-frontier-in-the-fight-against-climate-change.html (Jan. 20, 2022).

建議，組織以「節能設計」的方式建設資料中心，同時採用最新建築技術並建立採購相關素材的整體供應鏈。透過在一開始即建立永續且高效的措施，並利用最新技術，企業可確保資料中心營運、維護、維修及翻新的品質；轉而使用更加環保的素材；同時透過更聰明且乾淨的方式使用能源及水資源。此外，部分企業還開始探索運用風力、水力或太陽能等可再生能源為資料中心供電，並透過技術優化及提升效能。最後，部分資料中心也已透過部署人工智慧（Artificial Intelligence，AI）[14]降低耗能，AI 可分析資料輸出、濕度、溫度及其他重要統計資料，找到能提高效率、降低成本及總能源消耗的方式。

加密貨幣產業也開始透過改變運算技術減少能源消耗，以緩解對環境造成的危害[15]。例如：加密貨幣平臺以太坊（Ethereum）打算改變過往讓用戶花錢買挖礦機或繳交鉅額電費的模式，未來客戶可直接花錢購買加密貨幣。以太坊創辦人 Vitalik Buterin 表示，此機制有顯著節能效果，可減少的耗能是過往的 100 倍。然而，除改善挖礦機制外，尚須透過國際合作對加密貨幣挖礦進行監管並制定相關指標[16]。

結語

無論是資料中心或是加密貨幣挖礦，其對環境造成的汙染已班

[14] Chris Gamble, Jim Gao (2018). Safety-first AI for autonomous data centre cooling and industrial control. DeepMind. 檢自：https://deepmind.com/blog/article/safety-first-ai-autonomous-data-centre-cooling-and-industrial-control (Jan. 21, 2022).

[15] Yahoo 新聞（2021）. 加密貨幣竟然加速全球暖化？比特幣「挖礦」年用電量竟超出阿根廷、荷蘭. 檢自：https://reurl.cc/KpQQZq (Jan. 21, 2022).

[16] André François McKenzie (2018). How can we reduce Bitcoin pollution? Yale Environment Review. 檢自：https://environment-review.yale.edu/how-can-we-reduce-bitcoin-pollution-0 (Jan. 21, 2022).

班可考，各國政府及相關產業已開始正視，並推出應對政策及措施，未來應持續關注國際間的相關進展。

正視網路與能源的問題

George Michaelson

https://blog.twnic.tw/2022/11/21/24971/

本 APNIC 文摘原標題為 Getting serious about the Internet and energy，由 George Michaelson 撰文。

2022 年 7 月於美國費城舉辦的 IETF 114，以瞭解當代網路的能源負擔及連帶影響為討論重心。APNIC 部落格過去亦有若干關於此議題的文章，包括本文作者 George Michaelson 的〈氣候變遷對資料服務的潛在影響〉（The potential impact of climate change on data services），以及客座作者 Tobias Fiebig 的〈世界末日的 13 個網際網路命題〉（13 propositions on an Internet for a burning world）。

IETF114 的運作與管理工作小組（Operations and Management Area Working Group，OPSAWG）場次中討論了 3 份草案，都與此議題直接相關。Toerless Eckert 在簡報其草案〈IETF 為能源做過什麼〉（What has the IETF ever done for energy?）時，簡介問題全貌與過去做法，Alex Clemm 則以〈綠色網路的管理營運〉（Management and Operations for Green Networking）為題，介紹 2 份草案。

這些草案當場都激起熱絡討論，有意見認為 IETF 應該「少管閒事」，僅關注涉及協定、加密和路由的能源負擔。其他意見則認為應採最大化方式，強烈展現 IETF 開發更好的指標和資料模型，揭露所有資料傳輸方式能源成本的決心。

此討論會後也在 IETF 的 mailing list 上繼續，網際網路架構委員會（Internet Architecture Board，IAB）宣布今（2022）年 12 月的 IETF115 期間，將舉辦半天工作坊，討論網路應用程式及系統的

環境衝擊。

Michaelson 認為，這現象表示 IETF 雖然還不一定同意問題範疇，但意識到了「如何改善網際網路的能源負擔？」在此領域已無疑具有一定重量。

RIPE NCC 在此議題上也一直有動作。今年 7 月在荷蘭舉辦的混亂電腦俱樂部（Chaos Computer Club，CCC）May Contain Hackers 2022 中，Vesna Manojlovic 演講以「極限」為脈絡，談為維護生物圈健全，應採取宏觀做法與社會互動。她也探討其他 LIMITS workshops 中談及的議題。同場會議中，Igor Nikolic 則以「可以會減緩氣候變遷」（~~May~~ Will Contain Climate Change）為題，討論在供應鏈受氣候變遷衝擊下，駭客將遇到的問題。

沒人應該假裝這個世界沒有正在付出極大的能源和永續成本，以壯大並持續營運網際網路。2013 年 IETF 中就出現相關草案的事實，證明網路維運社群早就意識到需要思考這個問題。從現在起，社群或許也願意投入更多人力，探索如何減少科技帶來的電力和冷卻能源負擔。

文章手段曾提及 Tobias Fiebig 在 APNIC 部落格撰寫的文章，那也是他在 APNIC54 專題演講的基礎。當天討論氣氛十分熱絡，Michaelson 也希望這能鼓勵 APNIC 社群投入此議題，共同為降低能源負擔及永續努力。

亞太地區仍有極大發展空間，APNIC 網際網路服務範圍也涵蓋全球大量人口。這些都會是維持全球網路永續必須正視的問題。

參考資料：

https://blog.apnic.net/2022/10/27/getting-serious-about-the-internet-and-energy/

數位韌性與科技倫理

Digital Resilience and Ethics of Technology

作　　者　財團法人台灣網路資訊中心

內容撰輯　E. Marie Brierley、Joy Chan、Andrew Cormack、Julia Evans、Geoff Huston、Alexander Kozlov、George Michaelson、Kathleen Moriarty、Moritz Müller、Shoko Nakai、Marcin Nawrocki、Dave Phelan、Seth Schoen、Raffaele Sommese、Terry Sweetser、Fred Templin、吳宜庭、吳幸芳、周冠汝、林昕璇、林紘宇、梁理旋、郭戎晉、陳曼茹、莊舒歆、潘育群、蔡志宏、謝國廉、羅心妤、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　黃勝雄

主　　編　丁綺萍

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 112 年 5 月

ISBN　9789860624762（epub）