出國報告（出國類別：會議）

出席「網際網路名稱與號碼指配機構」（ICANN）第 83 次會議報告書

服務機關	姓名 / 職稱
數位發展部	姜政男科長、曾文方司長（線上參加）、陳坤中高級分析師（線上參加）、葉信妤技正（線上參加）
外交部	曹伯晏二等秘書、蔣鴻名三等秘書
內政部警政署刑事警察局	黃禎慶股長、邱左傳巡官（線上參加）
法務部調查局	郭傳浩調查官（線上參加）
國家資通安全研究院	張元傑工程師（線上參加）
數位發展部資通安全署	莊璧華分析師、陳俊穎高級資安程式設計師、陳羿谷資安系統分析師、劉主強資安程式設計師（線上參加）
財團法人台灣網路資訊中心	黃勝雄董事長、余若凡執行長、丁綺萍副執行長、詹婷怡國際事務委員會主任委員、李曉陽組長、江進榮管理師、呂苗令管理師、湯序平管理師
財團法人中華民國國家資訊基本建設產業發展協進會	林郁敏資深經理
網中智庫股份有限公司	劉莘相董事長、賴俞帆專案經理、洪詩琳執行秘書

派赴國家：捷克 布拉格

會議期間：**114** 年 **6** 月 **9** 日至 **6** 月 **12** 日

報告日期：**114** 年 **8** 月 **1** 日

摘 要

一、 第 83 次網際網路名稱與號碼指配機構（ICANN）會議於今（2025）年 6 月 9 日至 12 日以結合線上參與與實體會議的混合模式舉行。

二、 本次 ICANN 會議為政策論壇（Policy Forum），議程共 4 天，議程安排主要著重於 ICANN 內部各社群議程、政策制定（PDP）工作小組會議，同時包含由技術社群主辦的 DN 技術研討會等。

三、 本次會議仍奉前行政院資通安全處指示擴大各部會參與 ICANN 事務，依照前行政院資通安全處指示各參團單位分工合作，分別參加政府諮詢委員會（GAC）、網路安全及穩定諮詢委員會（SSAC）、根伺服器系統諮詢委員會（RSSAC）相關會議，並參與 IP、DN 技術研討會。

四、 GAC 議程包括政策發展、註冊資料準確性、新一輪 New gTLD 申請計畫、DNS 濫用防制以及 ICP-2 文件修訂等議題。會議結束後，GAC 提出 ICANN83 公報。

目 次

壹、 目的

第 83 次網際網路名稱與號碼指配機構（Internet Corporation for Assigned Names and Numbers，ICANN）會議於本（2025）年 6 月 9 日至 12 日以結合線上參與及實體會議的混合模式舉行。

本次 ICANN 會議為政策論壇（Policy Forum），議程共 4 天，會議吸引來自 129 個國家和地區的參與者，共有 1,333 人實體與會，另有 569 人透過線上方式參與。實體參加者中，來自亞洲、澳大利亞及太平洋島嶼地區的有 208 人（15.6%），非洲地區 92 人（6.9%），拉丁美洲及加勒比海地區 87 人（6.5%），北美地區 353 人（26.5%），歐洲地區則有 593 人（44.5%）。

我國政府代表由數位發展部主政，與外交部共同實體出席，且協同國家資通安全研究院、資通安全署、刑事警察局、調查局等單位，以遠端方式參與。另有財團法人台灣網路資訊中心、財團法人中華民國國家資訊基本建設產業發展協進會，以及網中智庫股份有限公司共同組團與會。

政府代表主要參與政府諮詢委員會（Governmental Advisory Committee，GAC）會議，亦依照業管屬性參與網路安全及穩定諮詢委員會（Security and Stability Advisory Committee，SSAC）、根伺服器諮詢委員會（Root Server System Advisory Committee，RSSAC）等相關會議，以及各項 IP、DN 技術研討會。本次 ICANN 會議全部議程詳見附件 1，亦可由下述網址獲得：https://icann83.sched.com/。

其中 GAC 會議於 2025 年 6 月 9 日至 12 日召開，共有 80 個會員國與 9 個觀察員組織參與。會議中哀悼了前 GAC 資深成員 Nigel Hickson 的辭世，並表彰他對 ICANN 與網際網路治理的傑出貢獻。本次 GAC 討論包括 New gTLD 未來回合（Next Round of New gTLDs）、DNS 濫用、建立新地區網際路註冊管理機構準則（Criteria for Establishment of New Regional Internet Registries，ICP-2）以及域名註冊資料準確性等議題。會議結束後，GAC 提出 ICANN83 公報。

本報告將介紹 ICANN 組織最新現況，並說明本次參與 ICANN 年度大會各項議程、GAC、GNSO、SSAC、RSSAC 等重要議題及內容，最後就會議內容研提相關建議。

貳、 ICANN 簡介

ICANN 是全球性、非營利、共識導向的國際組織（International corporation），1998 年 10 月成立於美國加州，負責監督管理網際網路技術管理功能（Internet technical management functions）、通訊協定參數及通訊埠（Protocol Parameters and Port）之協調、域名系統（Domain Name System，DNS）之管理、IP[1]位址之分配暨指派，以及根伺服器系統（Root server system，RSS）之管理。

ICANN 強調由全球多方利害關係人（multistakeholder）參與（包括政府部門、私人企業、技術社群、個人使用者等）、以由下而上的共識機制為基礎，制定全球域名管理政策，以促進市場競爭機制，維護全球網際網路運作之穩定、可靠、多元及安全為主要使命。

一、 ICANN 組織架構

ICANN 下設有董事會（Board of Directors），基於網際網路由下而上的組織特性，為確保各界聲音與意見都能在網路社群會議中出現，董事會以多方利害關係團體共同組成。成員分別來自以下屬性團體：

1. 支援組織（Supporting Organization，SO）。
2. 諮詢委員會（Advisory Committee，AC）。
3. 網際網路工程任務小組（Internet Engineering Task Force，IETF）。
4. ICANN 組織職員（CEO/Staff）。
5. 提名委員會（Nominating Committee）遴選。

---

[1] 網際網路通信協定（Internet Protocol）容許電腦網路間透過實體鏈路（physical links）快速互相通信。IP 位址以數字表示，網際網路上電腦間的資訊傳輸及連結即藉 IP 位址達成，一般大眾係借用 DNS 以人性化名稱（human-friendly names）來辨識主機位址。

ICANN 多方利害關係人參與架構，可藉由 ICANN 董事會組成理解（如下圖 1）：

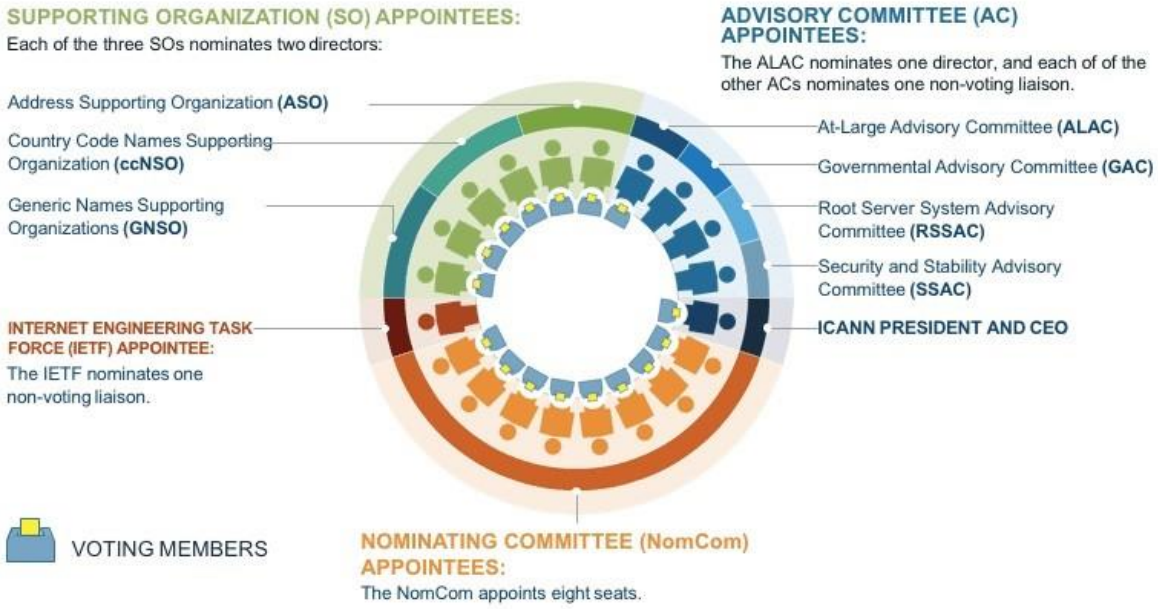

圖 1 ICANN 多方利害關係人參與架構圖

ICANN 大會每年召開三次，會議採取開放的參與模式，凡對網路治理有興趣之個人、團體皆可參加，並不侷限於 ICANN 會員。自 2016 年開始，會議模式調整為 A、B、C 三種類型：A 會議為年度第一次會議，會議型態與以往大會相同，但新增跨社群（Cross Community，CC）論壇；B 會議為年度第二次會議，亦稱為政策論壇（Policy Forum），會議主要任務在於 ICANN 內部各工作組織之溝通，以落實政策並促進討論；C 會議為年度第三次會議，會議除各支援組織及諮詢委員會既有議程外，亦增加熱門主題（High Interest Topics，HIT）論壇，以期吸引更多對域名相關議題有興趣的人士參與。與會人士可根據屬性團體性質，參加各利害關係團體討論，或選定感興趣之議題參與討論。

二、 ICANN 組成單位之功能

(一) ICANN 董事會

ICANN 於 2016 年 5 月 27 日通過新組織章程細則（Bylaw）。IANA 功能代管權正式轉移後，該組織章程於 2016 年 10 月 1 日正式生效。依據前揭組織章程，ICANN 董事會係由 16 位具投票權之董事組成，其中 8 位董事由提名委員會選出，位址支援組織（Address Supporting Organization，ASO）、通用名稱支援組織（Generic Names Supporting Organization，GNSO）、國碼名稱支援組織（Country Code Names Supporting Organization，ccNSO）各推舉 2 位，一般使用者諮詢委員會（At-Large Advisory Committee，ALAC）推舉 1 位，ICANN 組織執行長則為當然董事。

依慣例，董事之任期為 3 年，每年改選部分董事，故所有董事之任期交錯，隨時都有新舊董事參與會議討論及投票。

此外，4 位不具投票權之聯絡人則分別由根伺服器系統諮詢委員會（RSSAC）、網路安全及穩定諮詢委員會（SSAC）、網際網路工程任務小組（Internet Eegineering Task Force，IETF）及政府諮詢委員會（GAC）指派。

依據 ICANN 章程，董事會成員有 20 位：

1. **Tripti Sinha**，董事會主席（October 2018 – Annual General Meeting 2024）
2. **Chris Chapman**，董事會副主席（September 2022 - Annual General Meeting 2025）
3. **Catherine Adeya**，NomCom（October 2023 – Annual General Meeting 2026）
4. **Alan Barrett**，ASO（October 2021 - Annual General Meeting 2027）
5. **Maarten Botterman**，NomCom（November 2016 – Annual General Meeting 2025）
6. **Chris Buckridge**，GNSO（October 2023 – Annual General Meeting 2026）

7. **Becky Burr**，GNSO（November 2016 – Annual General Meeting 2025）

8. **Nico Caballero**，GAC 聯絡人（Since 2023）

9. **Sarah Deutsch**，NomCom（November 2017 – Annual General Meeting 2026）

10. **James Galvin**，SSAC 聯絡人（Since 2021）

11. **Wes Hardaker**，RSSAC 聯絡人（Since 2022）

12. **Byron Holland**，ccNSO（March 2025 - Annual General Meeting 2027）

13. **Christian Kaufmann**，ASO（September 2022 – Annual General Meeting 2025）

14. **David Lawrence**，IETF 聯絡人（Since 2024）

15. **Kurtis Lindqvist**，Executive Committee of the Board (BEC) Member

16. **Patricio Poblete**，ccNSO（October 2020 - Annual General Meeting 2026）

17. **Sajid Rahman**，NomCom（September 2022 - Annual General Meeting 2025）

18. **León Sánchez**，NomCom（November 2017 - Annual General Meeting 2026）

19. **Miriam Sapiro**，NomCom（November 2024 - Annual General Meeting 2027）

20. **Amitabh Singhal**，NomCom（November 2024 - Annual General Meeting 2027）

(二) ICANN 支援組織

目前 ICANN 下設有 3 個支援組織（SO），分別為 ASO、ccNSO、GNSO，各 SO 均有特定功能，為 ICANN 在各專責領域之主要政策建議來源及諮詢單位。簡介如下：

1. 位址支援組織（ASO）

ASO 負責向 ICANN 提出有關 IP 位址運作、指配及管理之政策性建言，其著重

於識別單一 Internet 上各種電腦之 IP 位址系統，如 210.69.99.253；ASO 係 ICANN 與各區域網際網路註冊管理機構（Regional Internet Registries，RIR）洽簽之 MoU 所設立之組織。目前按區域所設立之 RIR，分別有負責北美洲區域之 ARIN、歐洲區域之 RIPE NCC、拉丁美洲區域之 LACNIC、亞洲區域之 APNIC 及非洲區域之 AFRINIC。一般 RIR 的基本位址分配政策係依區域需要，並視未來一年內位址可能需求情形，來分配位址區塊（Address Block）。

2. 國碼名稱支援組織（ccNSO）

ccNSO 負責向 ICANN 提出有關 ccTLD（如：.us、.it、.tw、.jp 等）與 IDN ccTLD（如：「.台灣」、「.pф」（Russia））之政策性建言，ccNSO 係由 ccTLD 營運方組成，下設理事會（Council）管理相關政策制定流程，於羅馬會議期間（2004 年 3 月 1 日）正式成立。

3. 通用名稱支援組織（GNSO）

GNSO 負責向 ICANN 提出有關通用頂級域名之政策性建言，係由 gTLD 登記註冊管理機構、受理註冊機構、智慧財產權團體、商業團體、網路服務供應商團體、非營利組織團體及非營利使用者團體所組成，下設理事會（Council）管理相關政策制定程序。

(三) ICANN 諮詢委員會

諮詢委員會（AC）為正式諮詢團體，由來自網際網路社群（Community）的代表組成，各種不同社群的人員會依其利害團體性質參與相關諮詢委員會，並在委員會討論後，向 ICANN 提出政策建言。

ICANN 依組織章程設立不同諮詢委員會，諮詢委員會不代表 ICANN 行使職權，惟向 ICANN 董事會提出其研究報告及建言。

目前 ICANN 董事會設有 4 個諮詢委員會，簡介如下：

1. 政府諮詢委員會 （GAC）

GAC 由國家級政府（National Governments）、國際論壇承認之經濟體（Distinct Economies as recognized by International Fora）、多國政府組織（Multinational Governmental Organizations）及條約組織（Treaty Organizations）以會員代表或觀察員身分所組成，功能為向董事會表達政府與公眾事務單位之關切事項。

GAC 以會議方式討論政府之權益及關切議題，包含消費者權益、網際網路之運作對各國影響、各國政府或國際組織所關切之議題；GAC 不代表 ICANN 行使職權，惟向 ICANN 董事會提出其研究報告及建言。依據 ICANN 組織章程規定，董事會做決策時必須參考 GAC 建議。

2. 網路安全及穩定諮詢委員會（SSAC）

SSAC 負責就網域名稱及位址指配系統之安全及完整性向 ICANN 董事會提出建言，包括安全架構之擬定、與網際網路技術社群及重要 DNS 管理者/業者之溝通協調、風險分析評估、各項頂級域名之使用可能產生的系統問題等。

3. 根伺服器諮詢委員會（RSSAC）

RSSAC 負責向 ICANN 董事會提出有關網域名稱根伺服器運作之建言，包含主機硬體容量、作業系統、名稱伺服器軟體版本、網路連結、硬體環境、安全問題及系統效率、可靠度等。

4. 一般使用者諮詢委員會（ALAC）

ALAC 代表網際網路個人使用者向 ICANN 提出建言，其組成成員係來自網際網路之使用社群中，關切 ICANN 運作之人士。

參、過程

一、 會議過程：時間、地點、行程與議程

（一）時間：2025 年 6 月 9 日至 12 日

（二）地點：捷克 布拉格

（三）行程：

日期	行程
6 月 9 日	【GAC】開幕式 【GAC】GAC 能力建構：下一輪 New gTLD 申請人指南手冊 【RSSAC】中文根伺服器系統諮詢委員會工作坊 【RSSAC】ASO 與 RSSAC 會議 【ccNSO】Tech Day （2 場） 【ccNSO】DNSSEC 與安全工作坊（3 場） ICANN Community Discussion on the WSIS+20 Review
6 月 10 日	【GAC】GAC 與 GNSO 和 ALAC 雙邊會議 【GAC】GAC 策略規劃與營運會議和公報檢視 【SSAC】與 ALAC 會議 【GAC】DNS 濫用防制討論 【SSAC】SSAC 發表對於 DNS（域名系統）阻擋洞察新報告 【GNSO】RySG:BRG: DotBrand Use Cases/Key Insights for the Next Round
6 月 11 日	【GAC】討論 WHOIS 與註冊資料議題 【GAC】GAC 公報撰寫（2 場） 【GAC】討論 WHOIS 和註冊資料問題並與 ASO 會面 【GAC】探討網路安全與穩定

日期	行程
	【SSAC】工作會議
6 月 12 日	【GAC】GAC 公報撰寫（4 場） 【RSSAC】中文 根伺服器系統諮詢委員會

（四）會議議程：GAC 議程如附件 2，GAC 公報如附件 3。

二、 公共政策與重要議題

在 ICANN83 會議期間，GAC（政府諮詢委員會）與 ICANN 社群中的多個支援組織與諮詢委員會進行了廣泛的交流與合作，討論多項政策與運作相關議題。

首先，GAC 與 ICANN 董事會會晤，雙方就政策發展進度、域名註冊資料準確性、隱私與代理服務認證（Privacy and Proxy Services Accreditation）、社群利益揭露機制（Community Statements of Interest），以及第四次問責與透明度審查（ATRT4）的延期等議題展開討論。

接著，GAC 與 ALAC 進行會談，重點關注新一輪 New gTLD 計畫中的「申請人協助計畫」（ASP）以及 ICANN 諮詢機構在維護公共利益框架中的角色，雙方探討如何提升整體申請的公平性與可及性。

在與通用名稱支援組織（GNSO）理事會的會議中，GAC 聚焦於註冊資料準確性、DNS 濫用防制、註冊資料請求服務（RDRS），以及處理執法機關緊急資料揭露請求時的身分驗證問題，進一步交換政策實務上的看法。

此外，GAC 也與 ASO 會談，主要討論 ICP-2 文件修訂草案在社群諮詢期間所收到的意見回應、區域參與狀況，以及後續完成該治理文件的時間表與後續步驟。

與 SSAC 的交流則聚焦於域名註冊資料存取、自由與開放原始碼軟體的安全議題，以及 DNS 阻擋等技術性政策挑戰。

除聯席會議外，GAC 成員亦積極參與多場跨社群討論，包括關於 WSIS+20 審查進度的討論，以及針對 ICANN 實體會議策略（“How We Meet”）的社群規劃，展現 GAC 對跨部門、跨社群合作的高度重視與持續投入。

(一) ICANN 政策制定

在 GAC 與 ICANN 董事會的會議中，GAC 表達了對 ICANN 政策制定流程的關切，認為現行程式過於冗長，亟需改革，以更快速且具針對性地產出有效決策與落實成果。GAC 特別關切，在不大幅更動既有政策制定流程、且須與 ICANN 策略計畫一致的前提下，ICANN 董事會將如何推動提升政策制定效率的改革，並詢問 GAC 能否在其中扮演協助角色。

對此，ICANN 董事會回應指出，未來五年策略目標之一即為強化政策制定的靈活性與成效，具體作法之一是明確界定各項政策制定程式的範圍，藉此縮短進度。目前，GNSO 理事會已著手進行範圍更聚焦的政策制定計畫，並建議 GAC 予以支援與協助，以共同推動相關改進。

在會中，各方也提出具體建議與觀點。美國代表希望 ICANN 能採取更積極的措施，特別是針對政策制定流程（Policy Development Process，PDP）的管理與執行方法；瑞士則主張應在 PDP 程式中設定更清楚且具約束力的時程，以打破過往動輒需數年的決策慣例；ICANN 董事會則強調，其首要關切在於確保建議具備可行性，因若落實階段遇到困難，將導致實施審查小組（Implementation Review Team，IRT）及整體執行程式過度拖延，這與縮短 PDP 本身的進度同樣重要；而歐盟執行委員會則提醒 ICANN，應確保所納入的意見與觀點具有社群代表性，避免偏離多方參與的核心原則。

(二) GAC 領導團隊任期條款修訂（GOPE WG）

在本次會議中，GAC 根據《GAC 作業程序》（GAC Operating Principles，GAC OP）第 53 條，針對領導團隊任期條款進行修訂的投票表決。

針對是否同意修訂《GAC OP》，共計有 30 票贊成，無反對與棄權票。進一步針對具體修訂內容的投票結果則為 33 票贊成，無反對票，3 票棄權。

本次通過的修訂內容包括兩個主要部分：

1.調整領導職位的任期與連任次數，即《GAC OP》第 21 條的修訂，將主席任期定為兩年，可連任兩次，最長可任六年（2+2+2）；副主席任期亦為兩年，但僅能連任一次，最長可任四年（2+2）。

2. 明訂選舉時間為該選舉年度的第二次 ICANN 會議。

此修訂將對現任領導團隊任期造成直接影響，現任主席的任期將自 2027 年 3 月調整為 2026 年 10 月提前結束；下任主席的提名將於 2026 年 3 月展開，並於 2026 年 6 月完成選舉。至於副主席部分，現任副主席任期維持至 2026 年 3 月；下任副主席的提名將自 ICANN83 會議結束後至 2026 年 9 月 10 日截止，並將於 ICANN84 完成選舉。因選舉時程調整，下任副主席的首任任期將縮短至不足兩年（如圖 2）。

此外，埃及代表在會中提醒，未來有可能出現主席與五位副主席皆為新任人選的情況，建議工作小組提前討論應對機制。對此，GAC 支援團隊回應指出，未來三年內主席與副主席的任期仍將維持錯開的安排，並承諾會請 GOPE 工作小組留意並降低此潛在風險。

圖 2 GOPE 修正後對 GAC 領導層任期影響

(三) GAC 策略計畫

GAC 領導團隊計畫於近期向全體 GAC 成員提出下一年度的策略計畫草案，並

預計在 ICANN84 會議期間正式通過。該策略計畫旨在提升 GAC 在 ICANN 治理中的角色與整體運作效能。

該策略目標首先聚焦於 GAC 在 ICANN 治理中的定位，將致力於強化與 ICANN 董事會的互動，以及社群中的問責機制。同時，GAC 也期望能於 2026 年或 2027 年舉辦一場「政府高層會議」（High Level Governmental Meeting，HLGM），葡萄牙代表則提議，考量 ICANN88 將於 2027 年 3 月在里斯本舉行，屆時可同步召開 HLGM。

其次著重於提升 GAC 運作效率，特別關注新成員的能力建設與適應訓練。為此，GAC 正設計一份成員問卷，以蒐集目前運作中需改善的部分。目前，南美洲與阿拉伯地區均表達希望舉辦區域性的新成員培訓與能力建構活動。

次外，GAC 亦持續關注下一輪 New gTLD 計畫，特別是其安全性、穩定性與韌性等議題。GAC 荷蘭副主席 Marco Hogewoning 說明，該策略亦涵蓋 DNS 濫用防治相關工作。策略目標四則聚焦於 DNS 濫用議題，GAC 將規劃更多簡報與交流機會，以強化資訊傳遞與跨社群合作。在策略目標五方面，GAC 計畫加快與註冊資料相關工作的推動步伐，力求取得具體成果。

該策略目標亦包含了普遍適用性（Universal Acceptance）、新興技術發展對網路基礎設施的潛在衝擊及強化網路治理相關資訊的內部傳遞與成員溝通機制，確保 GAC 成員能掌握最新進展

會議最後總結，GAC 預定於 ICANN83 會議後公布下一年度的策略計畫草案，屆時將開放給 GAC 成員審議與提供意見，並力求於 ICANN84 會議期間正式批准該年度計畫。

(四) WSIS+20 討論

「ICANN 社群討論 WSIS 20 年成果審核（ICANN Community Discussion on the WSIS+20 Review）」會議在 ICANN 83 中，是以跨社群對話（Cross-Community

Interaction）的形式舉行。會議開放整體社群參與，討論與聯合國 WSIS+20 二十週年審核相關的合作與參與方式，屬於公共網路治理議題場次。

會上 ICANN 社群和其他的民間組織分享他們對於 WSIS+20 的主張或如何參與。例如：GNSO 報告其政策制定工作如何對映至 WSIS 行動主軸（Action Lines）；網際網路協會（Internet Society，ISOC）表示，將和 ICANN 共同發布報告 ，證明 IGF 的具體影響及其續存的必要性；技術社群多方利害關係人主義聯盟（Technical Community Coalition for Multistakeholderism，TCCM）強調其支持 IGF 永久運作，並將研擬具體立場；ICANN Org 重申 ICANN 的 WSIS 三大目標為：維護多方利害關係人模式、認可技術社群的獨特角色、延續 IGF 授權；英國政府表示他們關注數位落差、人權、網路阻擋等議題，並支持 IGF 永久授權。

最後，主持人總結表示，樂見其他 SOs 和 ACs 著手進行如同 GNSO 的 WSIS 行動主軸對映工作，並呼籲立即建置 WSIS+20 文件庫，以利社群於傳達訊息時能有完整論述。

(五) New gTLD 計畫進展

1. GAC 社群討論

(1) New gTLD 申請指南（AGB）

在「GAC Capacity Development Session – New gTLD Program Next Round Applicant Guidebook」會議中，ICANN 社群重點介紹了《申請人指南》（Applicant Guidebook，AGB）草案的內容與整體申請流程。會中指出， ICANN 董事會預計將於同（2025）年 12 月正式通過最終版本的《申請人指南（AGB）》，為 2026 年的申請作業鋪路。根據目前的時程，下一輪 New gTLD 申請作業預計於 2026 年 4 月開放，為期約 12 至 15 週，申請期間的確切安排仍需待 GNSO 理事會進一步確認。

會議並簡要說明瞭這次申請的關鍵流程與規範：首先，在申請資格與費用方面，僅法人、組織或政府機構具備申請資格，個人不得提出申請。申請人須提交完整文件，包含身份資訊、技術能力、財務狀況與域名使用計畫，並繳交基本申請費用每案 22.7 萬美元，若涉及額外審查或爭議處理，則可能產生附加費用。

在填寫申請內容時，申請人須透過系統填報其欲申請的主要字詞（string），同時可選填一組替代字詞（replacement），以備處理重複或爭議情況。接著進入初始審查階段，ICANN 會在約 56 個工作天內完成資料完整性確認。

接下來的公開日（Reveal Day）將揭示所有申請的字詞，申請人可在 14 天內決定是否改用替代字詞，此後即不得再變更申請內容。若同一字詞有多位申請人，ICANN 將透過抽籤排序決定處理順序，而非以先申請者優先。隨後，申請案將進入技術、營運能力、社群支援與法律風險等綜合審查流程。

此外，自公開日起 90 天內為異議與公眾評議期間，期間包括公眾意見徵詢平臺開放、GAC 預警（Early Warning）與 GAC 共識性建議等機制，提供多元意見與監督途徑。

最後，申請案若順利通過審查並完成所有異議程式，便可進入契約簽署與測試階段，與 ICANN 簽署註冊管理機構協議（Registry Agreement，RA），並完成系統測試程式後，即可進入正式授權（delegation）階段。

(2) 社群意見、異議與上訴

在 New gTLD 申請程序中，申請案若引發爭議，社群成員或相關利害關係人可依據具體證據與理由提出異議。異議的審理與流程管理將由獨立的第三方負責執行。若異議成立，相關申請字詞將被納入爭議集合中，或在申請人同意修正申請內容後，繼續後續審查流程。

除了正式異議機制外，系統亦設有「單複數衝突通知」功能，任何人均可在

提出充分證據的情況下，通報特定字詞之間可能存在的單複數混淆情形，作為ICANN 及第三方審查的參考依據。

表 1 對申請案提反對意見之方式及比較

	公眾評論平臺	GAC 預警	GAC 共識建議
提出時間	任何人得於字詞公開日後的 90 日內提交	GAC 成員得於字詞公開日後 90 日內提交	可隨時提出
申請人回應	意見回應非強制，但申請人得選擇回復。	回應意見，得選擇解決問題或撤銷申請	申請人需要在 21 天內進行回應
後續影響	意見不影響申請案，僅作為評估人員的參考	對申請人有警示作用，ICANN 亦可能視情節先暫停該申請案，俟申請者與 GAC 代表國協調後續行辦理	若董事會採納，可迫使申請人撤案或修改

(3) 字詞評估

在字詞評估階段，申請字詞須經過多重審查程式以確認其合法性與公共利益之符合程度。首先，涉及地理名稱的字詞受到嚴格限制。凡與《ISO3166-1》、《ISO3166-2》或聯合國 M49 所列之地理名稱相同者，申請人必須取得該地政府或相關社群出具的「支援」或「無異議」聲明，並經由「地理名稱專家小組」（Geographic Names Panel）進行審核與識別。

隨著下一輪 New gTLD 申請預計將導致網域名稱大幅增加，GAC 部分成員表達對 DNS 擴充可能導致垃圾郵件與濫用行為增加的擔憂。為確保 New gTLD 不對公共利益構成威脅，爰 GAC 開放有意願之 GAC 成員與 New gTLD 議題負

責小組（目前包含我國、瑞士、加拿大、哥倫比亞、荷蘭、萬國郵政聯盟等 6 成員之代表）合作，共同就下一輪 New gTLD 申請案進行早期檢視及討論，俾適時運用相關機制表達反對意見。

(4) 爭用處理

在處理爭用時，ICANN 明確禁止申請人間進行私下協商來解決字詞衝突，並建議透過提出「替代字詞」作為解決方案。然而，若替代字詞已被其他申請人提出，則該替代字詞亦不得再提出申請或納入爭議集合。

若遇到同一字詞由多位申請人申請，且皆聲稱代表某特定社群的情形時，ICANN 不會透過一般爭用與拍賣程式處理，而是交由獨立委員會進行「社群優先評估」（Community Priority Evaluation，CPE），以確認該字詞由何方社群代表最具優先性。

若爭用案最終需進入拍賣階段，將沿用 2012 年制度下的「次高價拍賣制」（second price auction）。為協助資源較弱的申請人，參與申請人協助計畫（ASP）者可獲得最高 35%的競標費用折扣，每件申請最多可折抵至 175 萬美元，藉此提高其競標的公平性與成功率。

會議中 GAC 之 APAC 代表提醒各方注意目前公眾評議期程，鼓勵亞太地區成員多參與並提出意見。同時也鼓勵 GAC 志工成員與 GAC 主題負責人合作，監控下一輪申請流程的時間表、里程碑。

(5) New gTLD 申請人支援計畫

在 GAC「New gTLD Program Next Round」相關會議中，成員針對第一輪申請人協助計畫（ASP）進行進度回顧與問題討論。該計畫預計於 2025 年 11 月 19 日截止，原訂目標為補助 45 件申請案。然而，截至 ICANN 83 會議期間，僅收到 4 件達最終階段的申請，其中 3 件來自亞太地區，1 件來自歐洲地區，申請數量

遠低於預期。

ICANN 已針對現有申請者進行問卷調查，深入瞭解其在申請過程中所面臨的實際困難，並為其媒合指導顧問，提供後續技術性與程序性的協助。

在與 GNSO 及 ALAC 的聯合會議中，各方進一步針對 ASP 的公平性問題展開討論。ALAC 指出，對於不熟悉 ICANN 制度與申請流程的潛在申請人，尤其是來自文化、法律制度差異顯著的地區，現行的 ASP 仍存在操作門檻與理解障礙，也反映在目前低落的申請量上。GAC 中的萬國郵政聯盟（UPU）亦呼籲應先分析造成申請數偏低的具體原因，包括制度設計、推廣效益及資源分配狀況，以確認哪些區域仍存在明顯支持需求，並避免資源過度集中於特定地區。

會議最後，GAC 呼籲 ICANN 應提供更細緻的統計資訊，特別是申請案的國別分布與申請類型（例如是否為非營利或商業性質），以利各國相關機構能就地協助推廣與提供適切支持資源，提升整體參與率與區域公平性。

2. SSAC 社群討論

在本次 SSAC 的 RIDE（Responsible Integration into the DNS Ecosystem，RIDE）工作小組會議中，與會者深入探討了 New gTLD 申請人指南（Applicant Guidebook，AGB）修訂中應關注的重點。

(1) 來自區塊鏈與 Web3 領域的名稱衝突風險

許多區塊鏈或 Web3 專案已經在其生態系中預先採用了類似頂級域名（Top-Level Domain，TLD）的格式，例如「.wallet」或「.crypto」，並已將這些名稱分配給大量用戶使用。

然而，若未來這些名稱在 DNS（網域名稱系統）中被正式核發給其他申請人，極有可能造成雙重名稱使用的情況，引發用戶混淆與潛在的安全風險。特別是在不同技術系統間缺乏一致性與協調機制的情況下，這類衝突可能導致服務誤導、資料

洩漏，甚至成為網路攻擊的漏洞。

與會者進一步指出，這些潛在衝突問題並不會透過既有的頂級域名申請流程中的傳統爭議解決機制（如拍賣程式或社群優先評估）自動顯現，因此更應該在政策設計階段就事先納入考量，以降低未來出現系統性風險的可能性。

(2) 社群優先評估（Community Priority Evaluation，CPE）制度的適用與限制

在會議中，與會者針對社群優先評估（Community Priority Evaluation，CPE）制度的適用範圍與其限制進行說明與討論。CPE 制度的設計原意，是用於處理「爭議組」（contention set）中的申請案，即當多個申請人競爭相同網域名稱字串時，藉由評估其中某一申請是否代表特定社群來決定優先權。

然而，若某一名稱僅有單一申請人提出申請，則 CPE 制度並不適用。即使該名稱在其他非 DNS 命名空間（例如區塊鏈系統）中已被廣泛使用，並擁有大量使用者，現行制度也無法據此阻止該申請案通過，這暴露出 CPE 在處理潛在名稱衝突上的制度性空缺。

因此，與會者建議未來應在 CPE 的評分標準中納入「潛在名稱衝突」的技術考量，具體而言，應評估該申請字串是否已在其他非 DNS 系統中被使用，且是否已有穩定的使用者基礎。如此一來，CPE 制度將能更全面地反映真實的命名環境，並有助於預防跨系統名稱衝突所帶來的風險。

3. ALAC 社群討論

「一般使用者第 1 場全體會議：為社群型頂級網域申請者剖析下一輪 New gTLD（At-Large Plenary 1: Unravelling The Next Round of New gTLDs for Community-Based Top-Level Domains Applicants）」由 ALAC 前主席 Cheryl Langdon-Orr 主持，會中由多位 ICANN 職員說明申請社群型 gTLD 時應留意的《申請人指南》（AGB）草案規範，重點內容包括：

(1) 社群型 TLD 申請：申請人必須證明自己和社群組織的關係。如果出現競爭，可選擇進行社群優先評估（Community Priority Evaluation，CPE），以爭取獲得優先資格。

(2) 社群優先評估（CPE）：為選擇性的爭用解決機制。主要評估社群建立情況、申請字串與社群的關聯性、註冊政策是否符合社群目的、社群機構是否予以書面支持。

(3) ASP 的拍賣競標抵免額（Bid Credits）：參考美國政府頻譜拍賣提供給中小型業者的優惠，競標抵免額訂為得標價 35%，但以 175 萬美元為上限（因 ASP 申請人年營收不得超過 500 萬美元），因此，若得標金額超過 500 萬，抵免比例可能逐步下降。

(4) 註冊管理機構協議（Registry Agreement，RA）之 4 種承諾條款：包括強制性公共利益承諾（Public Interest Commitments，PICs）、保障性公共利益承諾、註冊管理機構自願承諾（Registry Voluntary Commitments，RVCs）、社群註冊政策。

(5) 公眾意見、異議與上訴：包括申請案評論論壇（Application Comment Forum）、GAC 預警、GAC 共識建議、單複數（爭議）通知、異議與上訴。

(6) 費用與退款：基本申請評估費為 227,000 美元，符合 ASP 資格者獲 75~85%減免。退款方面，任何階段皆可撤回申請並退款，惟退款比例依時程而調降。此外，還有 CPE、地理名稱審查等條件性評估，以及參加拍賣、提出異議等特殊情況，皆會收取額外費用。

4. GNSO 社群討論

GNSO「註冊管理機構利害關係人團體（Registries Stakeholder Group，RySG）品牌註冊管理機構團體（Brand Registry Group，BRG）：品牌頂級網域名稱使用案例／下一輪的關鍵洞察」（GNSO: RySG:BRG: DotBrand Use Cases/Key Insights for the Next Round）會議中，首先，由多位 ICANN 職員介紹申請.Brand 應知曉的權利

保護機制：全球商標資料中心（Trademark Clearinghouse，TMCH）、統一快速暫停程序（Uniform Rapid Suspension，URS）、統一域名爭議解決政策（Uniform Domain-Name Dispute-Resolution Policy，UDRP）、商標授權後爭議解決程序（Trademark Post-Delegation Dispute Resolution Procedure，TM-PDDRP）；以及 AGB 草案中的相關規定。

後續則由通過 ICANN 認可的註冊管理機構服務提供商 LEMARIT 創辦人暨執行長 Martin Küchenthal 分享.Brand 案例。Küchenthal 表示，管理域名數量最多的國家，前 3 名依序為德國、法國、美國。而在 gTLD 當中，.Brand 具有市場行銷、IT 安全、節省成本等優勢。德國的.Brand 眾多，如：.aco（排水系統公司）、.schaeffler（機械與汽車零件製造商）、.dvag（保險公司）、.audi（汽車製造商）、.edeka（雜貨連鎖店）等。.Brand 的價值不在於擁有的域名數量，而是其「使用方式」。以.sky（衛星廣播公司）為例，creative.sky 用於展示該公司的創意內容。at.sky 用於內部員工查詢工作園區的資訊（如：bus.at.sky 查詢園區內的巴士時刻表、food.at.sky 查詢園區內的餐飲資訊）、skyzero.sky 用於宣傳該公司減少碳排放的承諾等。Küchenthal 並建議，如果有意申請 2026 年 4 月開放的 New gTLD，應於今年第 4 季做出申請決策，以免屆時作業時程不足而錯失申請。

5. 其他會議討論

「下一輪 New gTLD 計畫中的字串相似性審核（String Similarity Evaluation in the New gTLD Program: Next Round）」為 ICANN83 期間舉辦的專題討論會議，由 New gTLD 計畫團隊主導，聚焦於下一輪申請作業中「字串相似性評估機制」的現行規劃與未來調整方向。該會議是開放全體社群參與的政策議題場次，旨在促進多方討論並蒐集社群回饋，為後續申請人指南的完善提供參考依據。

本會議由 ICANN Org 的 IDN 及全球通用（Universal Acceptance，UA）計畫資深主任 Sarmad Hussain 主持，IDN 計畫主任 Pitinan Kooarmornpatana 等人報告。相

關重點彙整如下

(1) 評估的目的和範圍

SSE 旨在確保申請字串不會和既有 TLD 或保留名稱產生「視覺上」的混淆。評估範圍包含所申請 gTLD 主字串，及其所有的可分配異體字字串（allocatable variant strings，可申請），和阻擋異體字字串（不可申請）。這些字串將和所有其他的申請字串、既有 gTLD 和 ccTLD、已請求的 IDN ccTLD、仍在處理中的上一輪申請 gTLD、兩字元 ASCII、阻擋名稱（Blocked Names），進行比對；且須分析中、日、韓、阿拉伯、希伯來等 27 種文字（將新增馬爾地夫的 Thaana script）。

(2) 評估流程

當申請截止後，所有申請字串將從 TLD 應用管理系統（TLD Application Management System，TAMS）匯入 SSE 工具，以識別可能造成混淆的字串，並以均方值（mean square）計算得分，數值為 0~1，0 最相似，1 不相似；之後產出系統報告（專家亦可視情況建立客製化報告），以供專家做為人工審核的基礎資料，進而完成最終報告，且再回傳至 TAMS，TAMS 會將彼此「相似」的申請字串標記為「爭用」，和阻擋名稱「相似」的字串則標記為「拒絕」。

(六) 註冊資料請求服務（RDRS）

1. GAC 社群討論

(1) 註冊資料緊急請求

在「註冊資料緊急請求」議題中，GAC 與 GNSO 及 ALAC 的聯席會議討論指出，GNSO 理事會同意 GAC 的觀點，認為應在「快速政策制定流程」（Expedited Policy Development Process，EPDP）中持續討論有關資料請求回應時間的議題。尤其在執法機構的身份認證方面，GAC 轄下的「公共安全工作小組」（Public Safety Working Group，PSWG）正積極參與，並被視為社群最需要來自公部門協助的重

要項目之一。事實上，執法機構是否能順利通過認證，也會直接影響回應時間能否有效確定。

在 GAC 與 ICANN 董事會的會議中，GAC 進一步向董事會表達，希望能取得更多關於《受理註冊機構認證協議》（Registrar Accreditation Agreement，RAA）中對資料正確性要求的履約情況資訊，以便更深入了解當前執行情形。GAC 並詢問，在現行資料保護限制下，ICANN 董事會是否能建議公開更多相關資料。對此，董事會回應指出，依據 RAA，受理註冊機構確有驗證註冊資料的義務，ICANN 也具備審查其履行情形的權限。然而，自 2018 年起受到個資保護法規與隱私代理服務興起的影響，大量註冊資料不再公開，也限制了 ICANN 實質的審查能力。即使具備契約授權，也因資料取得困難及查覈成本效益問題，導致執行上受到挑戰。因此，ICANN 建議應思考除直接取得與查覈資料外，是否存在其他可行的替代方法。

會議最後討論出以下幾項結論：首先，PSWG 將執法機關身份認證及註冊資料揭露中的「緊急請求」事項列為工作重點。其次，GAC 敦促註冊資料政策施行審查小組（即政策實施監督機制）應儘速推動對於經認證的緊急請求，其回應時間的具體討論。最後，GAC 重申，鑒於此類緊急請求攸關重大公共安全利益，合理的回應時間應設為 24 小時內。然而，該立場目前在 ICANN 社群中尚未取得共識，GAC 因此呼籲 ICANN 的實施檢討團隊（Implementation Review Team，IRT）應積極提出相應草案，明確要求相關締約方（Contracted Party House，CPH）配合處理。

至 ICANN 82 會期我方與美國聯邦調查局（FBI）人員交流獲悉，執法機關緊急請求調閱網域名稱註冊資料，除以國際刑警組織（INTERPOL）會員作為身分認證機制外，另得透過 GAC 成員提供執法機關之電子郵件網域名稱等方式代替部分，經我方於本次會議再次向前揭人員詢問後，獲其回復相關身分認證資料已交予締約方卓處，俟身分認證機制確定後，將另行公布。

(2) 註冊資料正確性

在 GAC 與 GNSO 及 ALAC 的聯席會議中，GNSO 理事會明確表示將不會重啟先前的「資料正確性工作界定小組」（Accuracy Scoping Team）。取而代之的是，GNSO 理事會已於 ICANN82 會議結束後成立新的資料正確性工作小組，負責審視與整理社群所提出的意見。

該工作小組將優先處理社群內部對資料正確性議題已形成共識的部分，包括：註冊資料的正確性對網域名稱系統（DNS）的運作具有關鍵影響；正確性的定義應以現行的註冊機構認證協議與政策要求為基礎；在推動進一步行動前，必須蒐集更多資料並納入所有利益相關方的意見；此外，也應考慮在正確性議題上採取自發性且漸進式的推動方式。

除了上述優先處理項目外，資料正確性工作小組也列出了數項後續工作任務。首先，有研究指出若能在註冊流程早期（如註冊前、註冊當下或剛完成註冊後）進行資料正確性驗證，可有效減少約 70%的惡意註冊行為，這也成為潛在的行動方向。其次，工作小組將研析「註冊資料請求服務」（Registration Data Request Service，RDRS）紀錄中因資料不正確而導致網域名稱遭暫停的案例，以深入理解相關問題。最後，為提升整體資料正確性，工作小組亦將致力於對註冊人進行宣導，使其了解提供正確資料的重要性，同時強調這些資料將受到妥善保護。因有些註冊人可能出於隱私考量而故意提供不正確資訊，這點亦是未來需溝通的重點之一。

會議最後，GAC 表達期望能取得更多具體資訊以利後續討論，包括：GNSO 資料正確性工作小組的最終建議與未來的後續步驟、ICANN 如何確保締約方遵守合約中的正確性要求，以及各締約方對其資料正確性實務的相關說明。

2. SSAC 社群討論重點

SSAC 主席 Ram Mohan 在會議中說明 SSAC 對於網域名稱註冊資料存取議

題的基本立場。他強調，SSAC 的最終目標是確保所有通用頂級域名（gTLD）的註冊資料存取政策應具備明確性與穩健性，並能有效回應全球網路社群在防範各類安全威脅上的實際需求。

他指出，建立一套結構化且能迅速處理請求的資料存取系統至關重要。對於具有合法性且具緊急性的調閱需求，應設定明確而暢通的處理流程。同時，社群亦需共同釐清並形成共識，針對資料調閱的方式（how）、內容（what）與時機（when）等具體細節進行定義。

Ram Mohan 進一步表示，滿足合法資料存取需求與保障使用者個人隱私並非互相排斥的目標，兩者之間也不存在零和競爭關係。相反地，這是一項需要整體網路治理社群共同面對的挑戰，必須透過適當且平衡的方式加以處理，以同時維護資訊安全與個資保護的雙重目標。

(七) DNS 濫用

1. GAC 社群討論

(1) 處理 DNS 濫用漏洞

在 GAC 與 GNSO 及 ALAC 的聯席會議中，GNSO 理事會報告指出，已於今年 4 月重新召集 DNS 濫用工作小組，並計畫在六個月內確認需優先處理的 DNS 濫用漏洞。該小組的主要工作包括：全面評估 ICANN 社群中業界、締約方與其他成員對於 DNS 濫用的防治措施；重新檢視該小組在 2022 年提出的相關建議；分析契約修訂對 DNS 濫用防治與回應機制所可能帶來的影響；以及討論與 DNS 濫用相關的研究報告，以作為未來行動的依據。

會議結論指出，有關 DNS 濫用的狹義政策制定流程中涉及的潛在議題，已被 PSWG 列為優先處理項目之一。GAC 也強調，將持續探索多種因應方式，包括推動積極主動的實務作為、促進整個網際網路生態系統中的跨領域合作、對提供子網域

服務的註冊人提出更多要求，以及針對 DNS 濫用與網域註冊資料之間的關聯議題尋求進一步解方。

(2) GAC Discussion on DNS Abuse Mitigation

在本場次會議中，ICANN 理事會（ICANN Board）與安全與穩定諮詢委員會（SSAC）強調當前全球 DNS（Domain Name System，網域名稱系統）濫用日趨惡化，尤其是在惡意軟體傳播（Malware Propagation）、網路釣魚（Phishing）與指令控制伺服器（C2 Servers）等方面的濫用行為。SSAC 指出，部分註冊機構對於濫用事件的處置缺乏一致性，GAC 成員則關心其對用戶端信任之影響。

本場次一致呼籲 ICANN 強化與註冊商及註冊管理機構間的合作，訂定具約束力的「DNS 濫用響應框架（DNS Abuse Response Framework）」，並鼓勵建立公私協作平臺，提升濫用辨識與抑制效率。

2. SSAC 社群討論

(1) 緩解 DNS 濫用

ICANN Board 與 SSAC 強調當前全球網域名稱系統（DNS）濫用日趨惡化，尤其是在惡意軟體傳播（Malware Propagation）、網路釣魚（Phishing）與指令控制伺服器（C2 Servers）等方面的濫用行為。SSAC 指出，部分註冊機構對於濫用事件的處置缺乏一致性，GAC 成員則關心其對用戶端信任之影響。

另在 ICANN Board 與根伺服器系統諮詢委員會（RSSAC）的討論中，也有提到強化濫用通報標準化機制（Standardized Abuse Reporting）的迫切性，以及如何提升執法機關（Law Enforcement Agencies）適當介入的可行性。

依據 ICANN83 會議中討論，本場次結論一致呼籲 ICANN 強化與註冊商及註冊管理機構間的合作，訂定具約束力的「DNS 濫用響應框架（DNS Abuse Response Framework）」，並鼓勵建立公私協作平臺，提升濫用辨識與抑制效率。

(2) DNS 阻擋報告

SSAC 成員 Greg Aaron 與 Warren Kumari 共同闡述委員會關於 DNS 阻擋的更新報告，該項研究奠基於 12 年前的舊有文件，並加入嶄新觀察與技術發展。DNS 阻擋是透過技術，讓遞迴解析器（recursive resolver）刻意回傳不正確的答案，例如：當用戶查詢一個實際存在的網站時，解析器卻回傳「域名不存在」（NXDOMAIN），或將用戶重新導向其他非預期的網站。DNS 阻擋的常見應用，包括：

- 安全性：用於阻擋惡意軟體、釣魚網站，此類較無爭議。
- 內容控制：多半使用於圖書館阻擋成人網站，或企業內部網路限制員工造訪社群媒體。
- 具爭議性的應用：國家層級審查政治言論或其他敏感內容。

DNS 阻擋並非無法規避，使用者仍可輕易透過更換遞迴解析器（例如：改用 Google 的 8.8.8.8 或 Cloudflare 的 1.1.1.1 等公共 DNS 服務），或使用 VPN 繞過阻擋。在所有阻擋手段當中，「重新導向」是最危險的一種，因為此將訓練用戶習慣性忽略瀏覽器跳出的安全憑證警告，從而為真正的網路攻擊敞開大門，對使用者安全構成嚴重威脅。基此，SSAC 提出數項核心建議：

- 理解工具限制：任何考慮實施 DNS 阻擋的單位，都應充分認知其有效性的限制，以及潛在的連帶損害（collateral damage）。
- 制定清晰的政策：應明確定義阻擋的對象、方法，並建立審核與移除機制，將風險降至最低。
- 避免過度阻擋（Over-blocking）：阻擋應盡可能精準，避免影響無關的合法網站。
- 不應影響管轄範圍外的用戶。

- 絕對不要使用「重新導向」做為阻擋手段。

在問答環節，印度代表 Sushil 提出 DNS 註冊資料存取延宕超過 24 個月的疑慮，關切 GAC 與 SSAC 是否應發表聯合聲明，敦促 ICANN 董事會儘速訂定時間表。對此，SSAC 主席 Ram Mohan 表示 SSAC 成員普遍認為緊急請求著實應採取緊急處理，並對聯合行動持開放態度。荷蘭代表 Marco Hogewoning 亦認同該項觀點，並表示 GAC 會將此納入考量。

(八) 《ICP-2》進度更新

1. RSSAC 社群討論

在 RSSAC 與 ASO 的聯席會議中，ASO 向 RSSAC 說明其近期正在推動的重大工作—「ICP-2 框架」的制定進程。該框架旨在更新與強化對區域網際網路註冊管理機構（RIR）的整體治理架構，補足現行制度的不足，並因應時代變遷所帶來的新需求。

首先，ICP-2 在設計上強調完整的生命週期管理。不同於以往僅關注「成立新 RIR」的舊架構，新框架涵蓋了從 RIR 的誕生、運作階段所需的持續合規與責任要求，到最終可能的「終結（撤銷承認）」階段的全過程管理，使制度更加全面與健全。

其次，新框架導入了多項現代治理機制。這包括 2001 年尚不普遍的概念，如公司治理、反挾持（anti-capture）機制、審計義務以及「持續性規劃」（Continuity Planning）。這些設計目的在於確保即使某個 RIR 出現問題，也不會導致整體服務中斷，從而提升全球網路基礎架構的穩定性與韌性。

第三，ICP-2 亦特別強調權力與責任的明確劃分。草案試圖釐清 RIR、本地與全球社群、以及 ICANN 在整體治理中的角色與互動關係。其中，「ICANN 是否擁有對 RIR 的最終決定權」成為會議中最具爭議、也是討論最熱烈的議題之一，顯示該議題在社群內部具有高度敏感性與政策重要性。

會議最後，RSSAC 成員對 ASO 積極推動 ICP-2 框架表示支持，肯定其作為一項網際網路基礎建設工作的長遠意義。與會者也指出，「權力平衡」是 ICP-2 中最具挑戰性的議題之一，特別是在 RIR 承認與撤銷程序中，如何妥善處理 RIR 社群共識與 ICANN 權威間的界線，將是後續修訂的關鍵。

ASO 亦說明，社群對 ICP-2 草案的回應相當熱烈，尤其在治理權力分配方面反映出多元觀點。ASO 表示將審慎處理這些意見，並計畫在下一版草案中體現社群回饋。雙方同意未來將持續保持密切聯繫，並預告在預計於九月啟動的下一輪公眾意見徵詢中，ASO 將提供更多互動機會，並詳實說明其對各方意見的處理方式。

三、 其他議題

(一) ccNSO 相關會議

1. .TW DNSSEC update automation

台灣網路資訊中心的許乃文組長分享了.TW 網域在域名系統安全擴充的自動化更新實作與未來方向。目前，台灣網路資訊中心已建立與受理註冊機構之間的自動化作業流程，包括透過 EPP（Extensible Provisioning Protocol）將資料從受理註冊機構傳送至註冊資料庫，產生區域檔案後分發至所有授權名稱伺服器。

但當網域名稱使用第三方網域名稱系統服務供應商時，授權記錄（DS record）的更新仍需仰賴人工操作。由於第三方服務供應商無法直接存取受理註冊機構系統因此需經由手動處理導致流程繁瑣且易出現錯誤並增加設定失誤之風險。且多數受理註冊機構對相關機制亦不熟悉所以往往無法正確執行金鑰更換等操作。

據亞太網路資訊中心的統計，目前臺灣僅約 10%的域名系統查詢具備域名系統安全擴充驗證能力，主因在於本地多數網路服務供應商尚未於其遞迴伺服器中啟用驗證功能導致啟用率與使用率皆低的惡性循環。在所有.TW 網域中，實際啟用比例不到 0.5%，其中超過 10%出現驗證錯誤，顯示整體設定品質仍有待提升。

為降低操作風險並維持簡潔，台灣網路資訊中心目前僅支援子域授權記錄（CDS record），不支援 CDNSKEY 紀錄，也未採用 RFC 9615 中提出的 域名系統安全擴充委任啟用程序。雖然該程序雖提供額外驗證機制但需額外人為操作，與自動化目標不符。根據內部估算，若第三方網域名稱系統服務供應商全面支援 RFC 8078，.TW 網域中域名系統安全擴充的啟用率將有機會由 0.5% 提升至超過 20%。

2. EU Digital Identity Wallet

捷克註冊管理機構 CZ.NIC 介紹了歐盟執委會會推動的「歐洲數位身份錢包」（European Digital Identity Wallet）計畫。該計畫旨在建立一套歐盟統一的數位身份驗證機制，讓使用者可透過錢包應用程式進行線上或離線出示憑證與身分識別，包含駕照、學歷、醫療文件、旅遊資訊等。錢包將由各成員國政府核發，採開放標準並禁止追蹤使用者行為，目標在於降低對大型平臺如 Google Wallet 與 Apple Wallet 的依賴以推動歐洲數位自主權。

該計畫基於修訂後的歐盟電子身份認證規則（eIDAS），自 2024 年起各會員國需於兩年內發行合規錢包。歐洲數位身份錢包採去中心化身分架構（decentralized identity），與傳統聯邦式身分認證（federated identity）不同，透過裝置內部的錢包應用儲存並直接提供憑證給驗證端，不再透過身分提供者轉接。

講者亦提出進一步構想，將網域名稱擁有權以憑證形式儲存在錢包中使用戶可透過一鍵方式向第三方服務（如郵件主機或網站代管業者）驗證其擁有權，省去域名系統紀錄驗證的繁瑣程序。該構想需進一步定義資料格式與撤銷機制，目前正由中心成員組成的工作小組討論中。

3. DNSSEC Multi signer for PG

PCH(Packet Clearing House)分享了其協助.PG 網域部署域名系統安全擴充與多

簽署者(multi-signer)架構的實作經驗。過去.PG 並未啟用域名系統安全擴充，該團隊受託支援整體部署流程，包含簽章設定、金鑰管理、資料同步與測試驗證。

多簽署者架構允許多個註冊管理營運方(Registry Operator)共同簽署同一區域的域名系統安全擴充資料。為實現此目標，該團隊整合了 CDS(Child DS)與 CDNSKEY 紀錄機制，並針對系統在資料同步過程中的處理一致性進行測試。他們觀察在資料格式、順序、及重複性出現時，各系統是否能正確解析、保留或覆寫設定，並避免產生衝突或遺失。

講者表示，多簽署者模型在跨系統、自動化部署場景中具備重要意義，特別是在治理能力或資源有限的小型頂級域名中，能有效提升安全性與營運彈性。同時也指出目前不同註冊管理系統對於域名系統安全擴充資料的處理仍存在不一致情形，包含對無效參數的接受容忍度與更新策略差異，可能對域名系統安全擴充的整體部署穩定性構成風險。

講者呼籲社群應考慮建立針對多簽署者場景的更清晰技術規範，包含可延伸配置協議(EPP)與域名系統資料行為定義，以促進不同註冊管理機構間的相容性與可預測性。

4. ccTLD .UA with XoT

Hostmaster 介紹了在.UA 國碼頂級域名中部署域名系統安全擴充並引入 XoT 的實務經驗。XoT 全名為 DNS-over-TLS for zone transfers，是一種透過傳輸層安全性協議對區域資料傳輸進行加密的技術，可防止傳輸過程中資料遭竊聽或竄改。

在烏克蘭戰爭期間，Hostmaster 為強化.UA 網域的營運韌性，需將部分主名稱伺服器移轉至境外。由於傳統的 AXFR 協定以明文傳送資料，存在潛在風險，因此導入 XoT 以加密方式在主從伺服器間傳送區域資料。

講者說明了部署 XoT 的技術條件，包括支援傳輸控制協定和傳輸層安全性協議

的名稱伺服器軟體 (如 NSD、Knot 或 Unbound)、伺服器憑證與金鑰的管理方式，以及伺服器間的相互驗證程序。XoT 之實作難度相對低，可作為具成本效益的資料傳輸保護手段。

目前.UA 已將 XoT 納入正式營運流程，並與域名系統安全擴充併行使用，確保從資料生成到傳輸的每一環節均具備驗證與加密機制。Hostmaster 表示其他國碼頂級域名營運方亦可考慮將 XoT 納入備援與災難復原計畫，提升整體域名系統的韌性與信任性。

5. Blockchain Provider Mapping and Risk Analysis - Current and Upcoming Research

本分享介紹了一項針對區塊鏈基礎設施供應商的地理分布與風險評估研究，目標是建立可量化的觀測框架以分析不同區塊鏈平臺在營運層面所依賴的實體與網路基礎設施。該研究區分了四類關鍵角色，包括區塊生產者、基礎設施供應商、節點營運方與域名系統解析服務提供者，並透過 IP 掃描、BGP 分析與名稱查詢等方式進行資料收集與對應。

講者指出區塊鏈系統雖強調去中心化，實際上許多關鍵節點仍集中部署於特定雲端平臺，例如 Amazon、Hetzner 或 Alibaba Cloud，形成潛在的單點失效風險。此部分平臺節點依賴單一自治系統導致在面對技術或政治事件時可能導致網路異常。

研究同時檢視域名系統層級的潛在風險，發現部分節點仰賴共通的域名系統託管平臺或大型內容傳遞網路進行名稱解析與導向。一旦此類基礎設施遭遇攻擊或故障，整體區塊鏈網路可能出現存取中斷。

講者提到後續研究方向包含建立平臺營運風險的長期觀測資料集、將節點、域名系統與網路拓撲納入整合性風險評估模型與針對區塊鏈上與區塊鏈下基礎設施相依性提出韌性強化策略。講者表示後續將與社群、標準制定機構與營運者合作，提升去中心化系統的觀測能力與政策可行性。

(二) SSAC 相關會議

1. SSAL 與 ALAC 聯席會議

ALAC 與 SSAC 聯席會議中，ALAC 提到對於網域名稱系統（Domain Name System，DNS）的安全與保障問題，所提及之面向，包括 DNS 的獲取、防堵與遞回。政府機關或司法單位可能在一些情況下基於一些執法考量而防堵一些 DNS 管道。另也討論 DNS 應變方式，構建防火牆、VPN 等等部分，作為因應之道。SSAC 提及 DNS 現有生態之情形，包括 DNS 空間、涉及命名之規範制度、名稱衝突之應變作法等。

依據本次會議中討論 DNS 面對的現況與解方，盼能藉此提升網際網路使用環境的安全與制度，亦盼由各國產業界攜手合作，透過技術面持續加強維護包括 DNS 在內之網路安全措施。

2. SSAC 發表對於 DNS（域名系統）阻擋洞察新報告

「SSAC Presents: Insights from the New SSAC DNS Blocking Report」場次由 SSAC 報告其最新關於 DNS Blocking 的研究與洞見，內容涵蓋 DNS Blocking 的本質、實作方法、潛在影響及政策建議。

首先，與會者對 DNS Blocking 的定義進行說明。DNS Blocking 是一種技術手段，其主要目的在於阻止特定網際網路使用者存取某些網域名稱及其相關服務或內容。此技術通常被用來限制使用者對特定網頁內容的存取，但事實上，它對所有與該網域相關的服務也可能產生影響。值得注意的是，DNS Blocking 僅是控制存取的工具，並無法從網際網路上完全移除內容，其有效性也僅限於使用該 DNS 遞迴伺服器的使用者。

DNS Blocking 可被應用於多個層級，包括子域名、次級域名，甚至整個新興頂級域名（TLD）。在實際應用上，企業、學術機構或圖書館等常在其本地網路內部實

施 Blocking，以達到阻擋釣魚網站等資安目的。然而，當政府強制實施 DNS Blocking 時，特別是涉及跨國內容與註冊機構的情況，則更具爭議性，可能涉及言論審查與資訊自由的問題。

會中進一步介紹 DNS Blocking 的主要技術方式，通常由 DNS 遞迴解析器執行，常見的三種回應策略包括：（1）回傳 NXDOMAIN，表示查無此域名，是最標準且被廣泛採用的做法；（2）回傳其他 IP 位址，此方式可能導致 TLS 憑證錯誤與安全風險；（3）忽略查詢，雖然技術上可行，但使用者裝置仍可能透過其他解析器進行查詢，效果有限。

與會專家指出，DNS Blocking 並非無法繞過。使用者可以透過改用公共 DNS 解析器（如 Google DNS、Cloudflare DNS 或 Quad9）、使用 VPN、Tor 網路，甚至依靠 DNSSEC 驗證與加密 DNS 協定（如 DoT、DoH、DoQ）來避開限制，增加執行 Blocking 的技術挑戰。

討論也提及 DNS Blocking 所面臨的挑戰與潛在問題。首先，其有效性並非絕對，總有部分使用者能成功繞過。此外，因網際網路跨越地理與司法邊界，Blocking 行為常會影響到原本不在管轄範圍內的使用者，造成不必要的干擾。若 Blocking 措施操作層級過高，例如阻擋整個 TLD 或次級域名，也可能誤傷其他無關的服務與基礎設施，產生附帶損害。

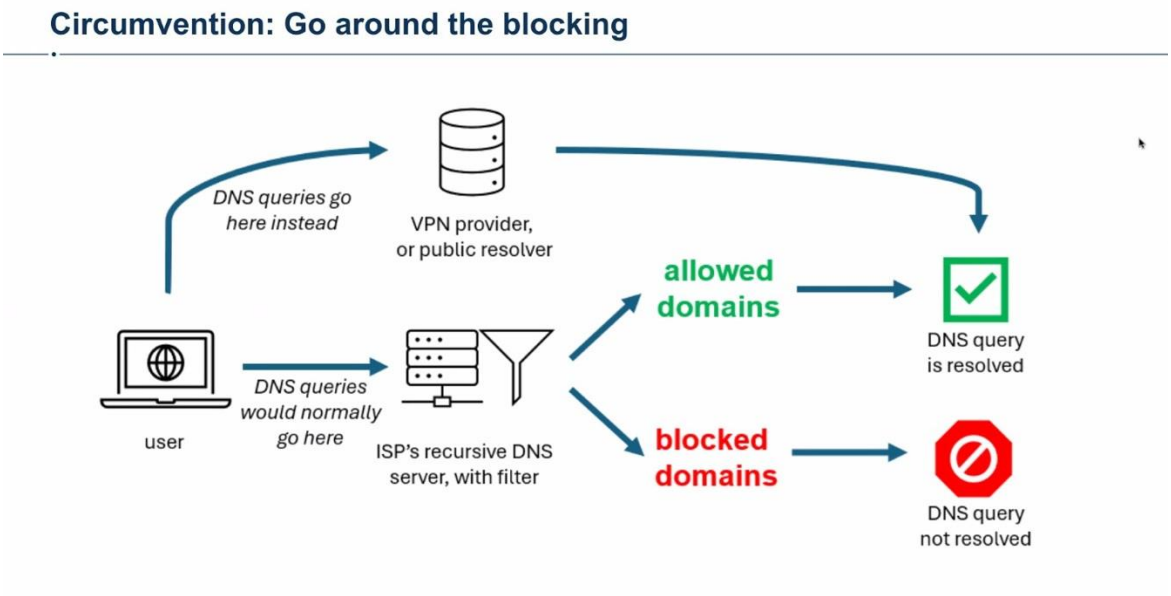

圖 3 規避 DNS Blocking 路徑示意圖

另一項風險在於缺乏透明度與披露機制。被阻擋的一方可能無從得知阻擋原因，特定政策如兒童性虐待內容的阻擋列表亦常因敏感性無法公開，增加社群疑慮。此外，用戶端可能將 Blocking 誤認為是網路故障，進一步削弱使用者信任。而技術實作上若將 DNS 查詢導向錯誤的 IP 位址，亦可能誘導使用者忽略安全警告，增加社會整體資安風險。此外，經由「史翠珊效應」（Streisand effect）也說明，阻擋某些內容反而可能激起更多公眾關注與反制行動。就法律與政策層面而言，跨境執法困難亦是一大挑戰。一國法院的阻擋命令未必在他國具執行力，容易引發司法管轄權衝突。

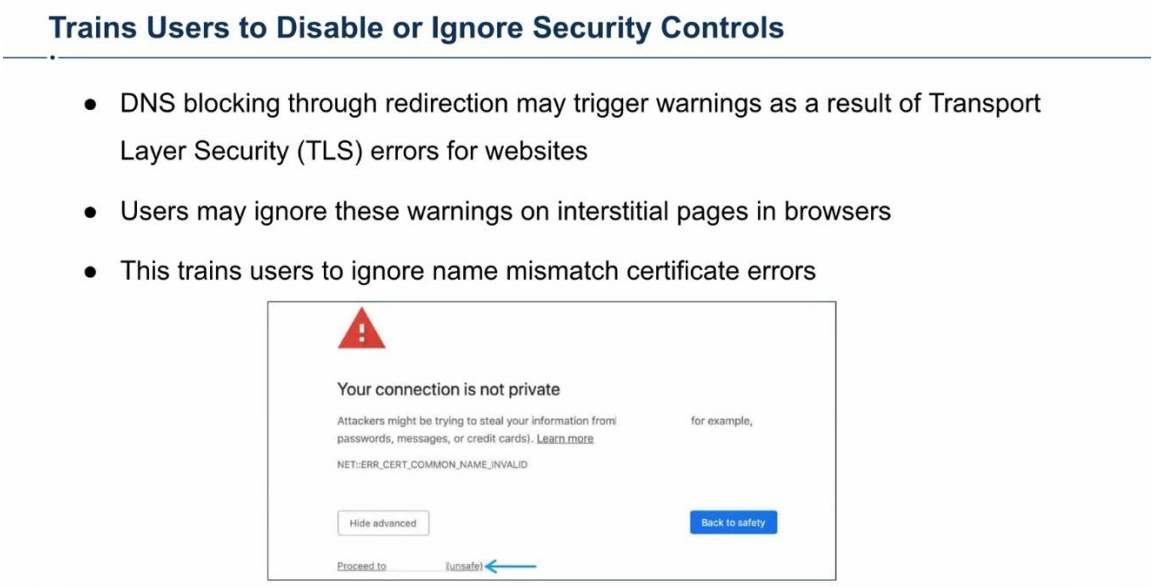

圖 4 DNS 重新導向之風險：降低使用者對安全憑證的警覺度

針對上述問題，SSAC 提出多項建議與結論。首先，任何實施 DNS Blocking 的實體應充分了解其技術原理、潛在風險與使用情境。實施者應訂定清楚政策與審查程式，避免因決策錯誤造成不當阻擋。Blocking 措施應力求精確，避免波及重要基礎設施與合法服務，並應限制在自身網路管轄範圍內實施。

在透明度方面，SSAC 建議遞迴解析器的運營商應考慮在回應中納入擴充錯誤碼(如 RFC 8914)，以向使用者說明阻擋的原因與背景，減少誤解與不滿。雖然 SSAC 不直接制定技術實作細節，但亦呼籲相關社群為政策制定者與技術實施者提供更具操作性的實務指南，以防止過度阻擋或錯誤應用。

最後，與會者強調需清楚區分 DNS Blocking 的合法應用與審查用途，並對執法單位與司法機關進行教育與對話，提升其對 DNS 技術限制與潛力的認識，確保未來阻擋命令的正確性與可執行性。整體而言，本場報告指出，DNS Blocking 雖可作為資安防護與內容控管的工具，但同時伴隨諸多技術、法律與治理層面的挑戰，其複雜性不容忽視。

3. 關於自由及開源軟體（FOSS）工作小組的更新

SSAC 成員 Maarten Aertsen 在會議中報告關於自由及開放原始碼軟體（Free and Open Source Software，FOSS）工作小組的最新進展，說明該委員會近期對 FOSS 進行的研究成果。他指出，全球網域名稱系統（DNS）基礎設施在很大程度上仰賴 FOSS，其中最具代表性的例子便是被廣泛採用的 BIND（Berkeley Internet Name Domain）軟體。

此次研究的主要目的有二：其一是提升整個 ICANN 社群，特別是政策制定者，對 FOSS 在 DNS 系統中關鍵角色的認識與重視，讓社群意識到全球網路運作的穩定性與安全性在很大程度上仰賴這些開放原始碼工具；其二則是釐清 FOSS 在開發模式與社群治理上的獨特性。Maarten Aertsen 強調，FOSS 有別於商業軟體，其開發與管理方式具有特殊的文化與結構。因此，政策制定者在討論與制定相關規範時，不應直接套用針對商業軟體所建立的假設與規範，以免產生誤解或誤導政策方向。

4. DNSSEC and Security Workshop

(1) DNSSEC, DANE & RPKI Deployments Around the World

此分享是關於全球域名系統安全擴充、DNS 的域名實體認證與資源公鑰基礎建設的部署現況與發展趨勢，呈現出這些網路安全機制在全球範圍內的成長態勢與未來可能面臨的挑戰。

關於域名系統安全擴充的全球部署情況，透過域名系統安全擴充部署地圖，詳細說明了不同國碼頂級域名在部署進度上的差異。他解釋了不同顏色所代表的狀態，從正在測試、已宣布計畫部署、部分部署到完整納入信任鏈的不同階段。整體來看，全球域名系統安全擴充部署呈現穩定增長的趨勢，雖離完全部屬仍存在挑戰，但各區域的進展已逐漸趨於成熟（詳見圖 5）。

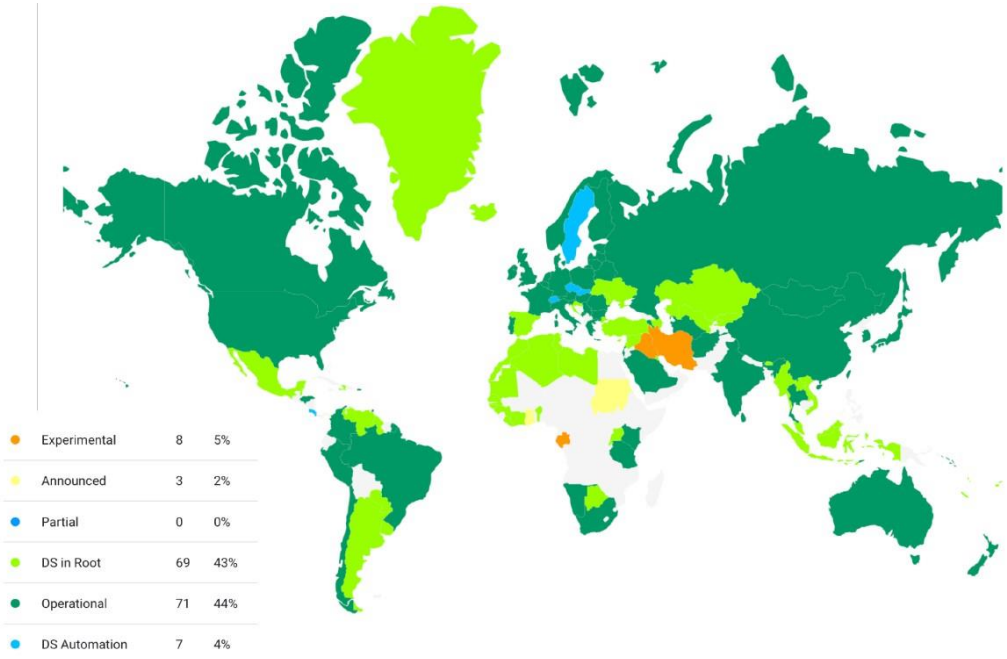

圖 5 全球域名系統安全擴充部署情形

在 DNS 的域名實體認證方面，講者指出其在電子郵件伺服器間使用傳輸層安全性協定進行加密連線的部署率持續增長，呈現穩上升的良好趨勢，顯示業界對於基於域名系統的加密認證機制的接受度提升。

整體而言，這場分享顯示全球在域名系統安全與網路路由安全方面的具體成就，並突顯出業界在域名系統安全擴充、DNS 的域名實體認證與資源公鑰基礎建設部署上的持續努力與未來的發展方向。

(2) DNSSEC protections are doing better than you'd think

域名系統安全擴充用於保護域名系統與網際網路協定地址的對應關係。但傳統的域名系統安全性評估主要著重在解析是否成功，而非關注域名系統安全擴充對自身協議中的物件（如金鑰、簽章等）保護是否有效。因此研究團隊提出了一

套新的評估框架以測量並分析域名系統安全擴充對域名系統物件之保護程度。透過這套框架他們發現過去十年間 域名系統安全擴充物件的保護狀況相當良好。

該研究進一步探討了安全協議的兩個核心面向，即「服務集」（service sets）與「保護」（protection）。服務集包含來源驗證（Origin Authentication）與完整性保證（Integrity Assurance），而保護集則關注這些安全機制在物件的整個生命週期內之有效性。如一個物件的名稱是否能在其存在的整個時間內保持可驗證狀態並持續受到監測與評估。

總結來說，這項研究表明域名系統安全擴充運行良好並提供了穩定的保護機制。此研究的方法學不僅能量化域名系統安全擴充物件的保護情形還可延伸應用至其他物件安全協議，透過不同的保護模型來評估其安全性。

(3) Some DNSSEC Measurements

此分享主要討論域名系統安全擴充的全球使用情形之研究，並分析其在實際應用中的影響。主要關注對象是終端使用者是否透過支援域名系統安全擴充驗證的遞迴解析器（Recursive Resolvers）進行查詢，而非個別解析器的行為或域名系統安全擴充簽署網域之完整普查。

根據 114 年的資料可看到各國在域名系統安全擴充驗證的採用情況有顯著變化。特別是非洲地區由於 Google 的公開域名系統解析器之普及，域名系統安全擴充的採用率有所提升。整體來說儘管全球的採用率有上升趨勢，但仍然只有約 30%的使用者開啟了這項技術。部分國家如羅馬尼亞、葡萄牙和挪威，甚至選擇關閉域名系統安全擴充驗證，這反映了對該技術應用的質疑。原因可能是該技術未能有效解決實際問題，且在很多情況下，服務中斷的風險被認為比域名系統安全擴充驗證所帶來的安全保障更為嚴重。

在檢視域名的使用情況時，雖然有大量的域名被註冊，但許多大型網路公司如 Google 或 TikTok 等實際並未啟用域名系統安全擴充來進行網域簽名。這顯示

儘管此技術在提升安全性方面有其潛力，但不被許多大型企業所接受，講者認為主要是因為其所帶來的實際效益難以衡量，且傳輸層安全性協定等其他技術已經在網路安全領域佔據了主導地位。

總結來說，儘管域名系統安全擴充在一些地區和國家取得了一定進展，但整體上其普及仍面臨挑戰，主要原因在於其部署難度高且效益不明與無法跟現有其他網路安全技術競爭。

(三) RSSAC 相關會議

本次 RSSAC 相關議程內容包含組織文件的修訂進度與例行月會的報告摘要。會議中成員針對文件內容與組織運作進行廣泛討論，並就外部協作與社群互動提出具體行動方向。

在 RSSAC 例行月會中，討論內容涵蓋內部治理、跨社群互動及國際議題追蹤三大面向。首先，RSSAC 針對成員活躍度標準進行調整，將評估基準由「歷史貢獻」轉為「近三年參與狀況」。目前已有 32 位不活躍成員被列入聯繫名單，並將給予六個月期限以恢復參與，否則將正式移除其成員資格。會議也決議未來即使與網際網路工程任務組（Internet Engineering Task Force，IETF）會議時間重疊，RSSAC 仍將照常舉行會議，並導入如 Lightning Talks 等新型互動形式，以提升 IETF 社群的參與度與技術交流。為此，亦已初步籌組非正式議程小組以負責相關規劃。

在外部合作與議題追蹤方面，RSSAC 持續關注 ICANN 社群中的關鍵討論。針對當責及透明度審核（Accountability and Transparency Review，ATRT）進度延宕引發的爭議，儘管 RSSAC 一貫對治理議題保持中立立場，但成員普遍認為審查機制本身具必要性，並強調未來應提升其有效性與執行合理性。另方面，RSSAC 亦指出部分外部參與者對根伺服器系統的理解仍有偏差，例如過度關注「延遲（latency）」問題，而忽略系統應具備的「韌性（resilience）」。

整體而言，本次會議不僅推動了 RSSAC 內部文件的更新工作，也積極規劃更

具效率的運作方式，並展現對外溝通的責任感與透明度，為後續發展奠定堅實基礎。

肆、 心得與建議

一、 申請人指南出爐，ICANN 展開全球推廣

ICANN 已於 2025 年 5 月 30 日公布完整版的新一輪 New gTLD 申請人指南（Applicant Guidebook，AGB）草案，並展開第 5 次（最後一次）公眾意見徵詢，同時也藉由本次 ICANN 83 會議的多個場次，分別向 ICANN 全體或各別社群介紹草案當中不同主題的規範重點。建議持續關注此項政策發展，以維護我國於國際網路關鍵資源的相關權益。

此外，自 2025 年初以來，ICANN 已在全球各地主辦或協辦逾 200 場推廣活動。鑒於新一輪 New gTLD 將於 2026 年 4 月正式開放申請，建議我國也應積極規劃推廣行動，向國內各機關團體、非營利組織、縣市政府、品牌企業及公益單位等介紹申請契機與挑戰，以及申請人支援計畫（ASP）等重點，協助相關單位評估是否參與這場國際網域名稱的申請盛事。

二、 強化跨部門合作，在 WHOIS 資料保護與公共利益間取得平衡

本次 GAC 會議聚焦於 WHOIS 資料保護、RDRS 系統實施、緊急請求處理機制與註冊資料準確性等核心議題，顯示出 ICANN 與 GAC 持續努力在公共利益與個人隱私保護之間取得平衡。建議未來應加速推動跨部門合作機制，提升執法機關取得註冊資料的效率，並建立透明、可持續的資料驗證制度，以強化整體網域名稱體系的安全性與信任度。

三、 WSIS+20：多方利害關係人模式面臨挑戰與回應

在 WSIS+20 審核方面，根據聯合國大會通過的 WSIS+20 進程，從 2025 年 5 月 30 日籌備會議起，至 2025 年 12 月 16~17 日聯合國大會高階會議止，將舉辦 4 次利害關係人協商，並產出 3 份關鍵文件。當中第一場（線上）協商會議已於 6 月 9 日和 10 日舉辦，包含 ICANN 在內的多個組織皆表明其維護多方利害關係人模式、支持 IGF 永久授權的立場。

聯合國並於 6 月 20 日發布第一份關鍵文件──《要素報告》（Elements paper），內容涵蓋數位經濟、數位落差、人權與倫理、網路治理、資料治理、AI 等領域共計 85 條。英國政府認為，報告內容引發網路治理倒退的疑慮，且未充分反映涵容及多方利害關係人方法；德國 Youth IGF 等國家型和區域型網路治理論壇（National and Regional Internet Governance Forums，NRIs）亦指出，報告於多方利害關係人方法和 IGF 角色等層面有所缺失，並發起聯署。我國可持續掌握並參與 ICANN 及社群的相關活動，間接參與 WSIS+20 進程。

四、 DNS 濫用防治

在全球網路資安威脅不斷擴大的情勢下，GAC 提出以多方協作方式對抗 DNS 濫用極具實務意義。建議我國在主管機關與註冊機構間建立快速通報與資料共享機制，並積極參與 ICANN 相關政策草案之討論，避免被邊緣化。

另外，SSAC 預計於 ICANN 84 正式發表「DNS 與開源軟體應用」，這次會議指出全球 DNS 的基礎設施已在極大程度上依賴開放原始碼軟體（FOSS），相信後續幾屆 ICANN 該議題會持續延伸。SSAC 也持續鼓勵技術社群及產業界多多參與，以強化 DNS 的安全性與可信度、確保新增的域名系統進行整合，減少 DNS 濫用。

五、 因應域名安全趨勢與政策挑戰，建議加強技術部署與合規準備

在本次 DNSSEC and Security Workshop 中，討論涵蓋多項與域名系統安全相關的重要議題，值得注意的是，美國政府近期發布一系列行政命令強化對關鍵基礎設施的安全管理，重點聚焦於供應鏈風險控管、加密通訊與身份驗證機制。政策明確要求提升技術透明度，並推動聯邦機構採用加密 DNS、電子郵件加密及後量子加密等措施。顯示政府部門對基礎網路安全架構的高度重視，也預示未來民間業者在合規層面將面臨更多技術與政策挑戰。

圖 6 我國代表團

伍、附件

1. ICANN 83 捷克布拉格會議議程
2. GAC ICANN 83 會議議程
3. GAC ICANN 83 會議公報