111 年委託研究報告

「網路治理國際趨勢研析與人才培育」委託研究採購案

計畫委託機關：國家通訊傳播委員會

中華民國 111 年 12 月

111 年委託研究報告

PG11103-0281

「網路治理國際趨勢研析與人才培育」

委託研究採購案

受委託單位

財團法人中華民國國家資訊基本建設產業發展協進會

計畫主持人

梁理旋

共同主持人

林郁敏

研究人員

蔡佳淇、陳曼茹、楊馥瑄

本報告不必然代表國家通訊傳播委員會意見

中華民國 111 年 12 月

目 次

表 次 ..... **vi**

圖 次 ..... **vii**

提 要 ..... **ix**

第一章 計畫簡介 **1**

第一節 緣起與目標 1

第二節 計畫架構與內容 2

第三節 執行時程及進度 3

第四節 預期成果與績效指標 5

第二章 網路治理國際議題觀測 **6**

第一節 前言 6

第二節 區域網路註冊中心之國際會議 8

第三節 國際網路治理論壇 12

第四節 彙整分析 18

第三章 案例研析(1) 對俄斷網制裁的發展與影響 **21**

第一節 前言 21

第二節 對俄斷網制裁的政治訴求及相關回應 22

第三節 對俄斷網制裁的法令規定及實施狀況 26

第四節 美歐豁免電信網通制裁 30

第五節　對俄斷網制裁的影響 34
第六節　結論與建議 40
第四章　案例研析(2) 解讀《未來網際網路宣言》 49
第一節　前言 49
第二節　宣言內容重點 50
第三節　宣言夥伴和推動方式 55
第四節　近期相近和對立的國際倡議 59
第五節　宣言的政治意涵 62
第六節　對宣言的評論 65
第七節　結論與建議 70
第五章　案例研析(3)「公平分攤」網路成本的爭議 77
第一節　前言 77
第二節　韓國：「網路使用費」的爭議、訴訟和修法 78
第三節　歐盟：「公平分攤」的爭議和政策走向 83
第四節　美國：推動改革「普及服務基金」 90
第五節　專家綜合看法 95
第六節　結論與建議 98
第六章　大專校園講座辦理 108
第一節　執行概況 108
第二節　政治大學場次 110

第三節　東海大學場次 116
第四節　中正大學場次 122
第七章 人才培訓課程辦理 125
第一節　活動內容與辦法 125
第二節　學員招募與評選 132
第三節　課程摘要紀錄 139
第四節　圖文影音紀錄 154
第五節　實習意願調查及課後測驗 158
第六節　學員遴選及後續活動安排 166
第八章 課程影片製播 169
第一節　執行概況 169
第二節　2 小時視訊課程 170
第三節　精華短片 173
第四節　流量統計分析 176
第九章 國際會議 APrIGF 參與 182
第一節　會議簡介 182
第二節　會議重點摘要 184
第三節　心得與建議 194
第四節　會議剪影 195
第十章 結論與建議 196

第一節 案例研析 (1) 對俄斷網制裁的發展與影響 196
第二節 案例研析 (2) 解讀《未來網際網路宣言》 199
第三節 案例研析 (3)「公平分攤」網路成本的爭議 202
第四節 大專校園講座 205
第五節 人才培訓課程 206
第六節 課程影片製播 207
第七節 國際會議 APrIGF 參與 208
中英文對照表 209
附錄 213

附 錄

附錄一：大專校園講座簡報……...……...…214

附錄二：「2022 網路治理研習營」課程簡報（僅提供講師授權公開部分）...279

附錄三：優秀學員參與 APrIGF 2022 會議摘要報告……..…..333

附錄四：實習學員參與網路治理會議摘要報告……...…366

表 次

表 1-1 計畫時程表 3
表 1-2 計畫查核項目與履約期限 4
表 1-3 預期量化與質化成果 5
表 2-1 2022 年國際網路治理會議時程與主題 7
表 2-2 IGF 2022 討論議題和主題 14
表 2-3 2022 年國際網路治理會議討論議題 19
表 3-1 ICANN 和 RIPE 對烏克蘭政府斷網訴求的回應 23
表 6-1 大專校園講座活動辦理概況 108
表 7-1 課前自我預習教材 125
表 7-2 研習營課程表 126
表 7-3 研習營學員成果報告彙整表 152
表 7-4 實習學員分工表 167
表 8-1 課程影片製播總表 169
表 8-2 影片觀看次數與累積觀看時數彙整表 176
表 8-3 影片曝光次數與點閱率彙整表 179
表 9-1 APrIGF 2022 參與場次 183

圖 次

圖 1-1 計畫架構圖 2
圖 4-1 《未來網際網路宣言》夥伴（簽署國） 55
圖 5-1 全球 5G 滲透率（2021 年統計及 2025 年預測） 85
圖 5-2 全球 5G 可用性前 8 名地區 86
圖 6-1 校園講座活動海報（東海大學） 109
圖 6-2 政治大學線上講座畫面截圖 115
圖 6-3 東海大學講座照片 121
圖 6-4 中正大學講座照片 124
圖 7-1 研習營活動網站 132
圖 7-2 研習營學員組成概況 136
圖 7-3 研習營學員年齡分布 137
圖 7-4 研習營學員參與動機 137
圖 7-5 研習營學員最關心的網路政策議題 138
圖 7-6 《2021 年全球網路自由度報告》評比項目 140
圖 7-7 Webex 分組會議室示意圖 151
圖 7-8 研習營展架海報 154
圖 7-9 研習證明書 155
圖 7-10 參與人員名牌 155

圖 7-11 研習營活動紀錄 156
圖 7-12 研習營課程簡報資料與錄影檔 157
圖 7-13 課後測驗分數分布 159
圖 7-14 課後測驗作答結果 162
圖 7-15 研習營「課程內容」滿意度 163
圖 7-16 研習營學員課後自我評估 164
圖 7-17 其他建議調查結果 165
圖 7-18 實習學員線上交流會會議畫面 168
圖 8-1 Webex 錄影畫面布局 170
圖 8-2 課程影片視覺設計 171
圖 8-3 精華短片 1 示意圖 173
圖 8-4 精華短片 2 示意圖 174
圖 8-5 精華短片 3 示意圖 175
圖 8-6 影片觀看次數與累積觀看時數 178
圖 8-7 影片曝光次數與點閱率 180
圖 8-8 影片觀眾性別與年齡分布 181
圖 9-1 LACS（本地可存取的雲端服務）系統的外觀和裝置 191

提 要

關鍵詞：網路治理、未來網際網路宣言、地緣政治、公平分攤、人才培育

一、研究緣起

本計畫透過觀測國際網路治理關鍵議題及培育我國網路治理多元專業人才等方式，蓄積網路治理能量，促使未來關鍵議題增加國內多方社群對話機會，並同時透過參與相關國際會議，促進網路治理的國際交流與合作。

二、研究方法及過程

本計畫委託辦理工作項目分為：網路治理國際議題觀測及我國現況分析、網路治理校園講座及人才培育，以及國際網路治理交流 3 大項；並可再細分為：國際網路治理議題觀測、通傳政策案例研析、大專校園講座辦理、人才培訓課程辦理、課程影片製播、國際會議參與、配合提供計畫資料與成果等 7 個子項目。

本計畫如期完成契約（經契約變更）指定的履約項目，包括：

- 完成 3 個通傳政策案例研析，主題分別為：對俄斷網制裁的發展與影響、解讀《未來網際網路宣言》、「公平分攤」網路成本的爭議。
- 完成辦理大專校園講座，分別於政治大學（北部）、東海大學（中部）及中正大學（南部）舉辦，各場次時數皆達 2 小時，且出席人數超過 50 人。
- 完成辦理 7 小時的培訓課程，共計 21 人結業（通過課後測驗，且不含公務人員）；並選拔 1 位優秀學員於 9 月 12 日至 14 日參加 APrIGF 2022 新加坡會議；以及選拔並安排 4 位學員參與實習。

- 完成製作前項培訓課程約 2 小時 15 分鐘的課程影片，並從中剪輯出 3 支 5 分鐘以上的精華短片（精華短片皆附字幕、影片標題包含網路治理相關關鍵字）。4 支影片皆已上傳至網路，並提供影片點閱流量分析。（依 111 年 7 月 21 日通傳綜規決字第 11100373720 號函說明第六條內容，因應貴會需求變更，免除購買 YouTube 廣告執行，取消數位行銷工作項。）
- 完成 APrIGF 2022（新加坡）實地與會，並提供重要議題報告。
- 完成配合事項之提供 2 小時「網路人權與網路治理」演講簡報。

三、重要發現

(一) 案例研析 (1) 對俄斷網制裁的發展與影響

1. 國際普遍反對「全面性」斷網制裁，但對多方機制實施制裁無共識

從 ICANN（網際網路名稱與號碼指配機構）和 RIPE（歐洲 IP 網路資源協調中心）婉拒烏克蘭政府的斷網制裁政治訴求、公民團體聯合呼籲勿對俄羅斯斷網、美英兩國政府發布電信網通服務「通用許可」（General License）等，凸顯即使在強烈的挺烏反俄氛圍下，國際社會仍普遍反對對俄羅斯實施「全面性」的斷網制裁，以維護全球網路的正常運作，保障俄羅斯的人道通訊所需，以及避免助長普丁的資訊控制。至於部分專家聯合提出的「多方利害關係人實施網路制裁」，網路治理社群對此並無共識。

2. 歐美國家排除或豁免電信網通制裁，我國法規方向亦和國際一致

整體而言，除了受制裁或管制行業的實體和個人外，目前歐美各國沒有禁止對俄羅斯提供電信網通相關服務。我國亦加入制裁俄羅斯的國際行列，實施「輸往俄羅斯高科技貨品清單」（後來增加白俄羅斯），主要是針對電子等 8 大類產品出口俄羅斯進行管制，但一般民眾使用的電腦、電信和資訊安全類別產品，不在管制範圍內。此規範可謂和歐美國家排除或豁免電信網通制裁的法規方向一致。

3. 斷網制裁加上「數位孤立」，全球網路分裂危機更甚以往

由於多數國際資通訊大廠仍未恢復俄羅斯的業務或服務，加上普丁還以封鎖西方新聞媒體和社群平臺作為反制，進而形成雙向封鎖，因此，專家認為陷入「數位孤立」的俄羅斯將更積極推動網路主權，且更倚賴中國大陸的軟硬體；其他獨裁國家也會對俄羅斯的處境引以為鑑，為脫離全球網路做準備；而全球網路也因此更趨向分裂，可能形成依國界劃分、眾多無法互通的網路，甚至使用技術不相容的網路協議，或擁護不同的國際治理機構，以致全球網路互連的時代宣告終結。

(二) 案例研析 (2) 解讀《未來網際網路宣言》(DFI)

1. DFI 承諾廣受肯定，具有數位政策「定位」和改善施政的意義

專家認為，在當前數位威權主義興起和網路面臨分裂之際，重申「開放、自由、全球化、可互通、可靠和安全」的網路願景，有其時代意義，且 DFI 可為數位政策「定位」，避免推出偏離的政策措施。此外，DFI 還在美國內部發揮政策改善的具體價值，最近美國在促進隱私和確保國際資料流通等方面，已取得實質進展。

2. DFI 無約束力和實施機制，未來前景不明

儘管本計畫嘗試拼湊出 DFI 推動方式的模糊輪廓——如透過 TTC（美歐貿易和科技委員會）等多邊場合、國務院成立新的「網路空間暨數位政策局」等；且美國官員也認為DFI可形成的國際常規和公民社會監督力量，不容小覷。不過，DFI 不具法律約束力、缺乏實施機制、尚未和全球既有進程建立關聯性等問題，也引發外界對其未來發展的質疑。例如：美國智庫「外交關係協會」（CFR）指稱「未來也仍無法藉由 DFI 實現全球網路的烏托邦願景」。

3. DFI 制定程序違背多方承諾，如何重建多方社群信任亦是考驗

DFI 僅有政府單位參與，且沒有公開向公民社會徵求意見的方式制定，

違反其「強化多方利害關係人的網路治理」承諾及原則，也破壞多方方法的可信度，喪失非政府利害關係人的聯合支持，甚至可能讓威權政府加以仿效。後續如何重建多方社群對 DFI 的信任和支持，亦仍是一大考驗。

4. 民主和威權陣營對峙，全球網路治理更趨兩極化

目前 DFI 共有 61 個簽署國，美國也持續尋求願意落實 DFI 承諾，且沒有斷網或封閉平臺等不良紀錄的國家加入。而就在 DFI 發布後 2 個多月，中國大陸在北京成立「世界互聯網大會國際組織」（WICO），以強化在全球推動國家控制網路的理念，被視為是對 DFI 反擊。雖然這並非美中雙方陣營的首次網路治理理念之爭，例如 2020 年美國推出「乾淨網路」計畫後，中國大陸也提出《全球數據安全倡議》作為抵制。不過，此次更凸顯自由民主和數位威權兩個陣營的對峙，也讓全球網路治理更趨兩極化發展。

(三) 案例研析 (3) 「公平分攤」網路成本的爭議

1. 歐盟可能推出「公平分攤」網路成本規定，進而成為全球新標準

面對電信業者重提內容業者（CPs）應分攤網路建設成本的訴求，歐盟執委會已訂於 2023 年第一季正式商議此「公平分攤」政策議題。雖然目前無法確定商議後是否將提出法案，且面臨 CPs 和數十個公民團體的反對，指稱違反歐盟「網路中立」法規；還有專家們擔憂可能破壞全球數位常規、言論自由和流量產業發展等。不過，由於歐洲的 5G 佈署相對落後，可能衝擊 2030 年《歐洲數位十年》政策的兌現；加上近年歐盟的政策立場也轉向監管科技巨頭。因此，歐盟仍可能推出「公平分攤」網路建設成本的規定，《路透社》報導認為歐盟此次有機會為網路建設成本豎立全球新標準。

2. 韓案例凸顯中小型國若率先針對科技巨頭，恐影響對美政經關係

韓國於 2020 年 12 月率先全球，實施被稱為 Netflix law 的《電信事業法》部分修正條文，以便讓科技巨頭向韓國 ISPs 支付網路使用費。然因法規語意模糊，以致 Netflix 和 YouTube 迄今仍未付費，於是韓國國會議員繼

續提出相關修正草案，但也因此引來美國的政治回應。例如：美國對修法表達關切，致使一場法案公聽會從 4 月延宕至 9 月；美國將此問題列為 2022 年美韓的貿易障礙之一；美國 4 月底推動的《未來網際網路宣言》，韓國較各國延後近一個月才得以加入。此外，美國的商業組織還列出韓國可能違反的《韓美自由貿易協定》條款。由此也凸顯中小型國家如果率先推出不利於科技巨頭的政策，可能會影響對美國的政經關係。

四、主要建議事項

(一) 案例研析 (1) 對俄斷網制裁的發展與影響

1. 立即可行：研議建立多方機制，為重大網路事件奠定即時決策基礎

《麻省理工科技評論》（MIT Technology Review）指出，沒人能提出比現行多方方式更好的替代方案，來治理全球網路資源。因此，部分專家聯合提出的「多方利害關係人實施網路制裁」聲明，當中所建議的「建立多方機制作為因應重大或緊急網路事件的即時決策基礎」，可供通傳會和數位發展部參考。惟建立一個合適的多方機制，需先投入資源進行研議規劃，因為除了需掌握開放、平等、透明的參與原則；由下而上的運作過程；及共識決的決策方式等細節之外，還需因應常被詬病的效率低落等問題。而針對後者，或許至少先界定不同情境下將採行的不同機制。如重大但非緊急事件，採取真正的多方機制——從界定議題範圍、產出方案到決策執行；但緊急事件時，則回歸既有的行政程序，而多方僅扮演諮詢的角色。

2. 中長期：於 ICANN 推動 ccTLD 政策修改，避免.tw 因政治而遭移除

ICANN 表明無權撤銷俄羅斯的 ccTLD（國碼頂級域名），除了其成立宗旨並未被賦予實施網路制裁的權力之外，另一方面，根據 GAC（政府諮詢委員會）的《ccTLDs 授權與管理之原則和指南》，ccTLD 屬於各國的當地議題，且發生爭議時是訴諸各國的當地法規，ICANN 維持中立立場。而 ccTLD 主要又是參照 ISO 3166 國碼標準所制定，但隸屬聯合國組織的 ISO

（國際標準化組織）在 3166 國碼標準中，將我國標註為「中國大陸的一省」。由於我國無法排除中國大陸於 GAC 援用此標準要求移除.tw 的可能性，因此，儘管難度很高，但代表我國參與GAC之數位發展部仍可嘗試集結具有相似需求的其他國家，共同推動修改《ccTLDs 授權與管理之原則和指南》，藉由增加「尊重現狀、保護既有使用者權益」等條文（本計畫諮詢顧問曾更瑩律師之建議），降低.tw 因政治干預而遭移除的風險。

(二) 案例研析 (2) 解讀《未來網際網路宣言》

1. 立即可行：將 DFI 原則轉化為具體政策措施，以履行簽署國承諾

雖然 DFI 不具約束力，但為了維護自由開放的網路共同願景，身為簽署國的我國應履行承諾，也就是落實其 5 大類 23 個子項的關鍵原則。因此，首要之務是由數位發展部籌組多方利害關係人專家小組，逐項確認、解讀這些原則的文義重點，之後識別各項原則的主責部門及對應的業務，進而將 DFI 原則轉化為具體的政策措施，並加以推行。

2. 中長期：定期評估我國 DFI 履行情況，做為對內改善對外貢獻基礎

身為網路自由度於全球名列前茅的國家，我國可考慮提高標準，針對前述 DFI 的 5 大類 23 個子項的關鍵原則，由轄下包含民主網絡司的數位發展部委託公正第三方，定期評估我國 DFI 履行情況，進而做為改善國內相關施政，及貢獻國際社會的基礎。

(三) 案例研析 (3) 「公平分攤」網路成本的爭議

1. 立即可行：掌握「公平分攤」政策動向，以利國內政策順應國際潮流

國內電信業者亦關注網路建設成本分攤的國際政策趨勢，並曾呼籲開放它們向高流量的內容業者收取分潤費。故建議通傳會掌握國際「公平分攤」政策動向，以利國內相關政策能在第一時間順應國際潮流，尤其要密切追蹤可能為全球豎立新標準的歐盟政策方案（預計 2023 年 6 至 9 月期間

發布），並可留意歐盟和韓國如何回應違反「網路中立」原則的疑慮。此外，美國《公平資助法案》通過後，將評估內容業者資助美國普及服務基金的可行性，評估結果攸關內容業者是否應承擔網路普及服務責任的國際新趨勢，並可作為數位部管理我國「電信事業普及服務基金」的參考。

2. 中長期：普及連線概念已升級，我國數位平權計畫可參與 PNMA

美國《公平資助法案》（草案）和我國電信普及服務政策的最終目的，皆為確保寬頻網路普及化，進而縮減數位落差。不過，近年來普及連線（universal access）的概念已擴展至「有意義連網」（meaningful access）。所以，IGF 也於 2021 年成立「有意義連網政策網絡」（Policy Network on Meaningful Access, PNMA），期能從網路基礎設施、使用者的意願和能力、內容和網路環境的公平和多樣性等層面，找出成功案例、識別推動障礙，並提出政策建議，以協助各國落實數位平權，消弭數位落差。我國教育部自 2020 年起，實施為期四年的「邁向數位平權推動計畫」，整合包含通傳會（業務移撥數位部）等部會資源，建構人人享有數位平權且友善的數位環境。建議計畫主責和協辦部會派員參與 PNMA，和國際進行政策交流，並將最佳實踐引入國內，以促進我國實現數位平權的計畫目標。

(四) 大專校園講座辦理

近年因 COVID-19 疫情，老師已逐漸熟悉線上授課模式，且學生也適應線上課程。因此，建議未來在校園講座的規劃上，可放寬辦理形式，除了實體講座之外，亦可包含線上方式辦理，一方面保留計畫執行上的彈性，另一方面，線上講座不受區域性的限制，更可擴大講座辦理效益。

(五) 人才培訓課程辦理

本年度研習營再次因為疫情而從實體調整為線上活動，雖然學員普遍認為活動流程十分順暢，但亦有學員表示 1 日的研習課程太過緊湊，講師及學員沒有充分的時間進行問答及分組討論。建議未來可提高預算增加課

程時數，在實體搭配線上課程的混合方式下，增加授課天數，不僅能提供更具深度與廣度的教學，也讓學員能擁有更多時間消化學習內容，同時有更充裕的時間與講師交流，有助於提升培訓效益。

全球疫情逐漸好轉，國際網路治理會議得以重返實體，本計畫按照規劃補助 1 名優秀學員至新加坡參加 APrIGF 2022 會議。本屆優秀學員參與 APrIGF 非常主動且積極，亦回饋從參與實體會議中獲得許多新知獲益良多。建議仍可延續提供優秀學員出國參加國際會議之獎勵，以吸引更多人才報名參訓。

目前網路公司的實習機會競爭激烈且和網路治理無關，而公民團體或 NPOs 則無餘力可安排帶領實習生，以致難以媒合。建議 NCC 和數位部協調其所捐助成立或主管的 NPOs（如 TWNIC、TTC）提供實習機會。

（六） 課程影片製播

Youtube 平臺每日有數以萬計的影片上傳，網路治理主題影片對於大眾而言內容較為嚴肅，吸引力自然較低。若要追求較高的影片品質及推廣成效，在企劃影片內容、拍攝影片及選擇推廣通路時，相對必須投入較高的成本。建議未來若通傳會提高影片製播預算，可考量前 2 年計畫與知識型網紅合作拍攝相關影片的方式，借助網紅本身的高訂閱數以及號召力，應更能擴大推廣效果，亦可多加嘗試於 Youtube 以外的平臺進行宣傳，以增加能見度。

本項工作依據 RFP，主要是將課程影片剪輯為數位教材；然 RFP 又規定進行數位行銷（雖然後來取消）和流量分析等行銷推廣類影片的工作項目，而此類影片需要的是精心製作的內容和具相當流量的渠道。故建議釐清影片製播的目的，並調整相關的工作子項和所需的資源。

（七） 國際會議 APrIGF 參與

1. 立即可行：掌握《全球數位協議》因應網路問題之規畫，作為我國施政參考

聯合國訂於 2024 年通過《全球數位協議》(GDC)，以透過國際合作因應網路發展的挑戰。雖然我國無法簽署 GDC，但數位發展部仍應掌握其進展，及所規畫的網路問題因應方向和措施，以作為國內的施政參考，同時也尋求未來在國際合作實務上的臺灣參與機會。此外，由於聯合國秘書長之科技大使 Amandeep Singh Gill 於 APrIGF 承諾，會在聯合國的多邊程序中，採納多方利害關係人的觀點。因此，我國可透過網路治理國際會議的 GDC 相關場次，對 GDC 草案表達意見。

2. 立即可行：持續參與 APrIGF 進行國際政策交流，並將新資訊引進國內

我國數位發展部唐鳳部長應邀擔任「節能網路」議題的講者，分享臺灣以數位轉型推動減碳的作法；而同場次其他講者的主張，相信數發部亦會作為其施政參考。此外，本屆會議還有 ISOC 專家介紹「低軌衛星(LEOs)的機會與挑戰」。LEOs 亦是最近國內的熱門議題，數發部訂於 2022 年 11 月開放執照申請，明年或可於 APrIGF 申辦座談，進一步和其他國家探討相關政策。又日本專家於本次會議介紹新研發的 LACS(本地可存取的雲端服務)，可為受災地區、偏遠地區、開發中國家，甚至是活動慶典場合，立即提供通訊網路服務。LACS 即將量產上市，建議數發部取得詳細資料，並評估我國電信普及服務是否有採購需求。

Abstract

Through analyzing key policy issues in Internet governance, cultivating diversified professional talents of Taiwan and so on, this project aims to cumulate capacity of Internet governance, and promote multi-stakeholders dialogue of key policy issues in Taiwan. In the meantime, participating in related international forums were to enhance international policy exchange and mutual learning, and to ensure the digital strategy of Taiwan in line with international trends. In light of the above-mentioned tasks, conclusions and recommendations are proposed as follows:

1. Policy issues analysis: the development and impact of Internet disconnection sanction imposed on Russia

Rejections of ICANN and RIPE NCC on Ukraine's request to disable Russia's ccTLDs and IP addresses, the caution against taking Russians offline from civil society groups, and General Licenses issued by US and UK to exempt internet communications services for Russia, all underline the international community strongly support for sustaining global Internet interoperability and the essential humanitarian communication activities for Russian people even in the strong anti-Russian atmosphere globally. ICANN maintains its neutrality by not disabling Russia's ccTLD should be a positive news for Taiwan. However, according to *Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains*, ccTLDs are not only local issues of each country but also mainly referred to ISO 3166 (standard for country codes and codes for their subdivisions) in which Taiwan is marked as " Province of China". It is suggested to promote the revision of the above mentioned principles and guidelines to reduce the risk of ccTLD of Taiwan (.tw) being disabled by

political interference.

2. Policy issues analysis: decoding the Declaration for the Future of the Internet

In response to challenges of authoritarian governments' sponsored or condoned malicious behaviors, and making use of digital tools to repress freedom of expression and deny human rights, as well as online platforms' highly control over digital economy, possessing huge amounts of personal data and enabling the spread of illegal or harmful contents, the United States with more than 60 partners countries (including Taiwan) launched *the Declaration for the Future of the Internet (DFI)*, a commitment to advance an open, free, global, interoperable, reliable and secure Internet. The vision and commitment of DFI have been widely recognized, however, DFI is criticized for its' coming "top down" and signed exclusively by governments. In addition, China not only blamed the US inciting confrontation in cyberspace, but also established a new "World Internet Conference International Organization" to fight against DFI. Although DFI is not binding, in order to maintain a shared vision of a free and open Internet, we should fulfill our commitments and translate the principles of DFI into practical policy measures.

3. Policy issues analysis: the debate on the "fair share" of network costs

With the international internet traffic increasing enormously, especially as the six largest content providers account for over half of the global internet traffic alleged by telecoms providers, the battle to get Big Tech to "fair share" of network costs has raged in EU, South Korea, and the United States. The European Commission has set the agenda to launch the consultation on this issue in the first quarter of 2023 and may set a global standard on network costs. Netflix is in court fight with a local ISP and several amendments to *Telecommunications Business Act* has been introduced in the parliament in South

Korea. In the US Senate and House, The FAIR Contributions Act was introduced to study on the feasibility of funding the Universal Service Fund through contributions from content providers. Giving that telecom industry of Taiwan have called for profit sharing from content providers with high Internet traffic volume, the authority of Taiwan should stay on top of the above policy to ensure our digital strategy is in line with international trends.

4. Campus lectures in universities

Three campus lectures with the theme of "Internet Governance in the Age of Geopolitical Conflict" were held this year, and students showed their high interest in Internet governance issues by asking questions actively during QA. Giving that pandemics have made college lectures and students getting used to online education, it is suggested to have campus lectures either in physical or online forms so as to keep the flexibility of project execution and to make use of the boundless nature of the Internet to extend the publicity effect (by having students from different departments or universities to join the lectures).

5. Training courses

Twenty-one participants completed the full program of the training courses, including a distinguished one were awarded grants for onsite participation in APrIGF 2022 and four excellent participants were provided with internships. Increasing the budget for more courses arrangements (from one-day training to one and a half day or two-day and both in physical and online format) and rewards for traveling abroad to participate onsite are suggested so that participants would have more time for learning and experience sharing, and more talents would be attracted to sign up for the training courses. In addition, promoting Internet-related NPOs which are under governance by public sectors to provide internships is also recommended.

6. Video clips production and publication

Three video clips "edited from the video of the training courses" were produced and published online. There is no surprise that the audience are small with about 200 views of each video. Therefore, tailor-made videos for the public and to broadcast on appropriate online platform channels with sufficient budget are suggested.

7. International forums participation

The international forum participated this year is APrIGF 2022. According to the opening remark made by Amandeep Singh Gill, the United Nations Secretary-General's Envoy on Technology, an international initiative called the *Global Digital Compact (GDC)* will be adopted at the UN's Summit of the Future in 2024 to address Internet challenges such as fragmentation and harmful content. Although Taiwan cannot endorse GDC, we should still grasp its progress as a reference for digital policy, and seek opportunities for international cooperation in the future. In addition, there are several emerging issues like eco-Internet, LEO Satellite Constellations, and Locally Accessible Cloud Service (LACS) being discussed or addressed this year. According, it is suggested to participate APrIGF continually to enhance international policy exchange and introduce new knowledge and ideas to Taiwan.

第一章 計畫簡介

第一節 緣起與目標

一、計畫緣起

資通訊科技活絡發展，促進全球網際網路生態環境更為蓬勃，在全球各國所面對的網際網路治理議題面向亦更為多元複雜之情形下，如何作出合宜適切且穩定的網際網路治理政策，以構築開放、互通、安全與信任的網際網路基礎環境，成為各國積極討論與發展之目標。

國家通訊傳播委員會協同相關部會推動「數位國家・創新經濟發展方案」下階段方案，致力於加速國內數位轉型推動之際，應掌握國際先進國家對於各項網際網路治理政策的議題發展趨勢，俾利橋接先進國家具前瞻性之治理措施，進而蓄積我國網路與數位轉型政策治理能量。同時，為使我國具備網路治理相關人才，以因應數位轉型下的各項變遷，將藉由辦理網路治理人才培育課程，透過各式議題的探討，使相關人才具備參與網路治理政策討論的基礎知能，實踐多方利害關係人普遍參與，共同構思解決方案，以有效結合政府、公民社會與產業間的共同治理，營造我國良善之數位治理環境。

二、計畫目標

在數位轉型與數位經濟發展下所衍生出的多元議題，本計畫將透過觀測國際網路治理關鍵議題及培育我國網路治理多元專業人才等方式，蓄積網路治理能量，促使未來關鍵議題得增加國內多方社群對話機會，並同時透過跨國學習，促進網路治理的國際交流與合作。

第二節　計畫架構與內容

本計畫委託辦理工作項目分為：網路治理國際議題觀測及我國現況分析、網路治理校園講座及人才培育，以及國際網路治理交流 3 大項；並可再細分為：國際網路治理議題觀測、通傳政策案例研析、大專校園講座辦理、人才培訓課程辦理、課程影片製播與行銷及國際會議參與等 6 個子項目。計畫工作架構如下圖 1-1 所示。此外，本計畫亦將配合通傳會需求，於履約期間提供本案相關資料及分享計畫成果。



圖 1-1　計畫架構圖

第三節　執行時程及進度

本計畫執行時程為 111 年 3 月 18 日至 111 年 10 月 26 日止（自契約生效次工作日起，至提交完整期末報告等文件止），期間曾因應國內 COVID-19 疫情升溫，於 6 月 7 日依本案契約第十五條約定，向通傳會提出契約變更申請，將本案規劃之人才培訓課程「2022 網路治理研習營」及 1 場校園講座由實體活動變更為線上舉行。下表 1-1 為簽約後的計畫時程表，計畫查核項目與履約期限彙整如下表 1-2。

表 1-1 計畫時程表

	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月
(一)網路治理國際議題觀測及我國現況分析									
1. 網路治理國際議題觀測			RIPE 84 5/16~20	Euro DIG 6/20~22			APNIC 54 9/8~15 APrIGF 觀測報告	RIPE 85 10/24~28	IGF 11/28~ 12/2
2. 通傳政策案例研析		案例確認	案例 1	案例 2	案例確認	案例 3			
(二)校園講座及人才培育									
1. 大專校園講座辦理	安排聯繫	內容準備	場次 1 (5/12)		安排聯繫	內容準備	場次 2、3		
2. 人才培訓課程辦理	籌備招募	招生評選	5/7 開課	核發獎學金和補助	實習安排	實習	優秀學員 APrIGF 9/12~14		
3. 課程影片製播			課程影片		短片 1	短片 2	短片 3		
(三)國際網路治理交流									
1. 國際會議參與							APrIGF 9/12~14	出國報告	
專案管理（每月工作報告）									
報告與審查					期中報告	審查/修訂		期末報告	審查/修訂

表 1-2 計畫查核項目與履約期限

、	內容	履約期限
GRB 表	上網登錄基本資料（GRB 表）	契約生效次工作日起 3 工作日內
同意書	研究人員約定同意書	契約生效次工作日起 15 日內
期中報告（初稿）	初稿中文版本 12 份，包括： • 2 個案例研析 • 1 場次大專院校講座分享 • 1 場次專業培訓課程 • 2 小時視訊課程	契約生效次工作日 140 日內
期末報告（初稿）	初稿中文版本 12 份 （含電子檔）	契約生效次工作日起 220 日內
期末報告（修正）	依審查意見完成修正並送交	指定期限內
期末報告（定稿）	確認無誤後，提出完整報告 12 份，包括： • 計畫摘要中（約 3,000 字）、英文版（約 1,000 字） • 執行成果光碟片 1 式 2 份（含期中報告與期末報告、歷次本會審查或進度會議資料等電子檔案）	指定期限內

第四節　預期成果與績效指標

本計畫主要執行「網路治理國際議題觀測及我國現況分析」、「網路治理校園講座及人才培育」、「國際網路治理交流」等 3 大工作項目。預期成果依據政府研究資訊系統（GRB）之量化績效指標表，屬於「戊、非研究類成就」的人才培育、國際合作，與「己、其他效益（科技政策管理及其他）」類別。預期達成的質化與量化成果如下表 1-3 所示。

表 1-3　預期量化與質化成果

績效屬性		績效指標	量化成果	質化成果
非研究類成就 戊	人才培育	32.培育人才情形，含人數及內容	• 培訓課程人數≧20 • 培訓課程資料≧1 • 培訓課程影片≧4	提升我國網路治理知識能量，培育參與國內外網路治理的人才，並提供參與國際會議的機會
		33.研討會（學術活動）	• 大專校園講座場次≧3（每場人數≧50） • 大專校園講座簡報≧1	促進大專青年認識、關心、參與網路治理議題討論
	國際合作	43.人員互動	• 出席國際會議≧1	跨國分享並相互學習，展現網路治理的雙向實質國際交流，同時拓展國際人脈
		44.學術活動互動（研討會、專題討論…等）		
其他效益（科技政策管理及其他）己		56.決策依據	• 觀測全球治理議題≧1 • 分析通傳政策案例≧3	掌握全球網路治理方向與政策議題潮流，提供決策參考，協助我國網路治理發展符合國際趨勢

第二章 網路治理國際議題觀測

第一節 前言

本項議題觀測之對象，依據計畫委託辦理工作項目，包括聯合國網路治理論壇（Internet Governance Forum, IGF）、亞太區網路治理論壇（Asia Pacific Regional Internet Governance Forum, APrIGF）、亞太網路資訊中心（Asia Pacific Network Information Center, APNIC）國際會議，以及歐洲 IP 網路資源協調中心(Réseaux IP Européens Network Coordination Center, RIPE NCC）國際會議。此外，由於歐洲近年來致力成為制定網路規範的國際領導者，因此，本計畫將歐洲網路治理論壇（European Dialogue on Internet Governance, EuroDIG）也納入觀測。

上述會議依其性質，可分成兩大類：區域網路註冊中心（Regional Internet Registries, RIRs）國際會議，以及網路治理論壇。

APNIC 與 RIPE NCC 為全球五大 RIRs 的其中兩個，分別掌管亞太地區，以及歐洲、中東與部分中亞地區的 IP 位址及自治系統(Autonomous System, AS）號碼等關鍵網路資源（Critical Internet Resources, CIRs）；且是網路治理生態系統的重要技術社群。兩者皆是每年舉辦 2 次國際會議，無訂定大會主題的慣例，討論議題以 CIRs 的管理分配政策為主。

APrIGF、EuroDIG 及聯合國 IGF 分別為亞太地區、歐洲地區及全球型的網路治理論壇，共同特色為每年訂定不同的大會主題和議題類別，且座談（Workshops）場次皆採公開徵選方式評定，可呈現不同地區或全球的熱門議題。

本計畫執行期間所舉辦的上述國際會議，其時程與主題，如下表 2-1 所示。

表 2-1 2022 年國際網路治理會議時程與主題

屬性	會議名稱	日期與型式	大會主題與議題類別
RIR 國際會議	APNIC 54	9 月 8~15 日 混合式；新加坡	• 大會主題：無訂定大會主題的慣例 • 議題類別：主要討論各管轄區域範圍內關鍵網路資源的分配管理政策，以及其相關議題
	RIPE 84	5 月 16~20 日 混合式；柏林	
	RIPE 85	10 月 24~28 日 混合式；貝爾格勒(塞爾維亞)	
網路治理論壇	EuroDIG 2022	6 月 20~22 日 混合式；的里雅斯特 (義大利)	• 大會主題：航向正確的方向 • 議題類別：數位主權、法規和標準檢視、新興科技的展望和治理、混亂時代的網際網路（地緣政治）
	APrIGF 2022	9 月 12~14 日 混合式；新加坡	• 大會主題：以人為本：展望社群引領的包容性、永續性和可信賴的網路 • 議題類別：包容、永續、可信賴
	IGF 2022	11 月 28~12 月 2 日 混合式；阿的斯阿貝巴 (伊索比亞)	• 大會主題：為共享永續和共同未來打造強韌的網際網路 • 議題類別：人人上網及確保人權、避免網路分裂、資料治理與隱私保護、提升安全和課責、因應先進技術（包含 AI）

資料來源：本計畫彙整

第二節 區域網路註冊中心之國際會議

一、APNIC 54

APNIC 會議以會議形式(如：各種特別興趣小組 Special Interest Groups, SIG）或主題為名（如：IPv6）。APNIC 54 主要會議及其討論議題包括：

1. 國家級註冊管理機構（National Internet Registry, NIR）SIG 論壇
   RPKI(Resource Public Key Infrastructure，資源公鑰基礎建設)和 IPv6(第 6 版網際網路協定）佈署的案例研究、各 NIR 的 RPKI 和 IPv6 指派概況。

2. 合作 SIG 論壇
   網路治理的多方參與如何受到近期地緣政治衝突和國家法規的影響。

3. 路由安全 SIG 論壇
   紐澳 RPKI 進展、路由安全中 IPv6 擴展表頭（extension headers）、孟加拉的路由劫持。

4. 政策 SIG（又名開放政策會議）
   討論號碼資源的分配、回收、移轉，以及域名系統和 RPKI 等政策和服務，並通過「使用單一定義文檔，以確保 APNIC 政策文件用語的一致性」、「調整網路號碼資源政策文件的文字描述」兩項提案。

5. 技術場次
   Google 的網路互連、透過程式管理網路服務、如何防範新一代的網路威脅、識別和修復路由的安全漏洞、遠程互連的延遲影響。

6. 專題討論
   討論光纖網路的續用問題和解決方案。

7. IPv6 部署
   IPv6 性能和診斷指標、馬來西亞 IPv6 佈署經驗、Google 雲端的 IPv6 佈署、IPv4 / IPv6 雙重架構的基礎設施等。

8. APNIC - FIRST（Forum of Incident Response and Security Teams，資安事件應變小組論壇）安全會議

   演講：不丹的網路攻擊和安全措施、傳輸控制協議中間裝置反射（TCP Middlebox Reflection）攻擊的分析和緩解措施等。

二、RIPE 84 和 85

RIPE 會議以全體會議和各主題工作小組（如：DNS、IPv6）的會議為主。RIPE 84 和 85 的主要會議及其討論議題如下：

(一) RIPE 84

1. 反濫用

   DNS 反濫用工具、如何偵測和分類網路有害流量。

2. 域名系統（Domain Name System, DNS）

   QUIC（一種通用的網路傳輸協定）概述、DNS4EU（歐盟安全 DNS 平臺）研究。

3. 位址政策

   RIPE 社群的 IPv6 政策調查結果、建議刪除 RIPE 資料庫強制 IPv4 分配註冊的規定、討論 IP 位址碎片化問題。

4. IPv6

   全球佈署狀況、Windows 10 防火牆如何處理 IPv6、德國分享 IPv6 佈署。

5. IoT（Internet of Thing，物聯網）

   LwM2M（一種 IoTs 協議）的安全優勢、醫院使用的 IoTs 設備。

6. 路由

   路由劫持攻擊事件、Anycast（將資料傳送到最近位置的一種網路定址和路由的策略）經驗分享、路由除錯工具介紹、RPKI 驗證軟體介紹。

7. 網路連線

分享 25Gig 光纖到府（FTTH）服務的經驗、CDN（Content Delivery Network，內容傳遞網路）業者的規劃布局挑戰。

8. 合作

討論歐盟擬讓大型內容平臺分攤網路基礎設施費用的網路中立問題。

9. 開放原始碼

RIPE 開放 RPKI 原始碼、路由軟體 FRR（Free Range Routing）的發展。

10. 全體會議

烏克蘭的網路韌性、社群發起 Keep Ukraine Connected 行動、.ua 營運商如何因應網路和軍事攻擊[1]、使用歐盟電子身份識別系統（eIDAS）作為 ccTLD 註冊的驗證、探討 DNS 解析的存留時間（Time-To-Live, TTL）、邁向綠色的網路、DNS 快取毒害（DNS Cache Poisoning）攻擊的因應措施、在內容傳遞時切換網路的影響、2019 年路由洩漏事件的剖析。

(二) RIPE 85

1. 反濫用

反濫用培訓課程的籌備狀況、德國反濫用組織介紹。

2. 域名系統（Domain Name System, DNS）

透過 QUIC 評估 DNS 及其對網路效能的影響、域名伺服器不足的影響、加密 DNS 的量測。

3. 位址政策

檢視 IPv6 政策目標、討論 IPv4 暫時配置的最小數量、取消 RIPE 資料庫

1 這 3 場有關烏克蘭網路的演講，簡報檔和影片的網址如下：
https://ripe84.ripe.net/wp-content/uploads/presentations/23-ukraine-internet.emileaben.ripe84.pdf
https://ripe84.ripe.net/wp-content/uploads/presentations/12-KUC_Presi_final.pdf
https://ripe84.ripe.net/wp-content/uploads/presentations/39-UA-CCTLD-INFRA-RESILIENCY.pdf
https://ripe84.ripe.net/archives/video/738
https://ripe84.ripe.net/archives/video/739
https://ripe84.ripe.net/archives/video/753

強制登記可供 IPv4 配置的規定。

4. IPv6

佈署以 IPv6 為主的網路連線、不同 NAT64（IPv4 過渡到 IPv6 或 IPv4 和 IPv6 共存的一種機制）的使用比較。

5. IoT（Internet of Thing，物聯網）

可信賴 IoTs 裝置的社會和技術量測指標、IoTs 安全的產業挑戰和合作。

6. 路由

路由洩漏的影響、對 RPKI 驗證者的評論、路由註冊中心的資料分析。

7. 網路連線

歐洲網路交換中心（internet exchange point , IXP）概況更新、高容量乙太網路的重大技術改變。

8. 合作

路由安全的政策制訂者角色、歐盟科學前瞻小組（Scientific Foresight Unit）對網路分裂的研究、賽爾維亞的網路自由度。

9. 開放原始碼

歐盟《網路韌性法案》（The Cyber Resilience Act）草案的影響、管理 IXP 服務、如何偵測邊界閘道協定（Border Gateway Protocol, BGP）的前綴（prefix）遭到劫持。

10. 全體會議

路由安全共同協議規範（Mutually Agreed Norms for Routing Security, MANRS）的成果與挑戰、塞爾維亞的網路革命、IXP 的分散式阻斷服務（Distributed Denial of Service, DDoS）流量檢測、技術社群建立 MANRS/RPKI 行為準則的最佳範例和挑戰、透過 IXP 交換網路流量的不對襯性、近 10 年來全球 IPv6 的佈署和發展、GÉANT（歐洲學術研究網路）計畫的技術和服務發展、光纖網路和接取的最新發展。

第三節 國際網路治理論壇

一、APrIGF 2022

APrIGF 2022 大會主題為「以人為本：展望社群引領的包容性、永續性和可信賴的網路」，公開徵求座談提案時，所公布的議題類別為大會主題所列的「包容性」、「永續性」、「可信賴」，但由於議程表並未依慣例標示議題類別，因此，以下將座談（Workshop）和演講（Showcases，以個人或單位名義發表 30 分鐘演講）共計 25 場，改以 IGF 2022 的 5 個議題類別呈現。當中（S）代表 Showcases 的演講；未標示的為座談。

1. 人人上網及確保人權

   賦權網路治理新聲音、因應線上性別暴力、數位教育的包容性、ICT 工作對殘疾人士的包容性、促進永續的零工經濟、殘疾學生的數位可及性、以多方合作方式發展數位識讀、亞太地區的網路普及政策經驗、公民社會的數位韌性、強化殘疾者的網路治理聲量、打擊線上性別暴力經驗分享（S）、量測寬頻數據以加強基礎設施（S）、疫情後的數位人權優先順序、投資監控技術的風險評估和企業問責（S）。

2. 提升安全和問責

   醫療保健領域的網路攻擊問題、以在地雲端服務提升數位韌性（S）、低軌衛星和網路韌性（S）、兒少網路安全（S）、促進路由安全、打擊不實訊息和數位識讀、節能和環保網路的政策制定、社群媒體規範和選舉與民主、社群平臺的行為標準建議（S）。

3. 資料治理與隱私保護

   促進資料正義的東南亞觀點、因應網站的黑暗模式設計（dark patterns，如誘騙消費者訂閱服務、同意使用 cookies）。

4. 因應先進技術（包含 AI）

   無

5. 避免網路分裂

無

二、EuroDIG 2022

EuroDIG 2022 大會主題為「航向正確的方向」，討論主題分成「數位主權」、「法規和標準檢視」、「新科技的展望和治理」、「混亂時代的網際網路（地緣政治）」4 大類別，會議包含座談等型式共 17 場如下所列：

1. 數位主權

歐洲數位主權的願景和原則及行動、數位主權對網路基礎建設的影響、歐洲數位主權能否維護網路基礎建設的安全與開放、歐洲「資料門戶平臺」及「全球門戶」計畫如何促進歐洲數位主權。

2. 法規和標準檢視

歐洲政策和法規對於促進綠色數位轉型的有效性評估、協作開發標準如何支援歐洲的網路安全進程、從消保和人權角度探討歐盟新監管法規（如《數位服務法》、《數位市場法》、eID 提案等）、如何快速推動具影響力的網路安全標準、《布達佩斯公約》（Budapest Convention）增修條款等規範對網路空間的刑事司法國際合作的影響。

3. 新科技的展望和治理

如何規範 AI 和大數據的新進展、多方利害關係人模式能否因應快節奏的數位轉型、歐盟 eID 倡議對生活的影響、歐盟 eID 的跨境挑戰、在太空和陸地部署耐延遲網路（Delay-Tolerant Network, DTN）的意義。

4. 混亂時代的網際網路（地緣政治）

如何落實《未來網路宣言》（The Declaration for the Future of the Internet, DFI）原則、數位主權能否不造成網路分裂、疫情和地緣政治衝突時代的假訊息因應。

三、IGF 2022

IGF 2022 大會主題為「為共享永續和共同未來打造強韌的網際網路」，會議型式和場次眾多，以下僅彙整開放所有人提案申辦的「座談」（Workshop，簡稱 WS，共 79 場），以及限政府單位和國際組織申辦的「開放論壇」（Open Forum，簡稱 OF，共 45 場）的討論主題，並根據 IGF 的 5 個議題類別彙整如下表 2-2，且特別標示由政府申辦的「開放論壇」場次。

表 2-2 IGF 2022 討論議題和主題

議題類別	座談	開放論壇
1. 人人上網及確保人權	• 全球數位協議 (Global Digital Compact)的公民參與 • 社區網路 (Community Networks)的挑戰 • 促進有意義的連網 (Meaningful Access) • 普及連網的社群角色 • 災難或危機時期的網路連線 • 南方世界能力建構經驗學習 • 相互依賴網路的未來—與 Vint Cerf 對談 • 低軌衛星寬頻的全球治理 • 全球青年參與網路治理的機會 • 偏鄉社區網路和數位包容 • 運用無障礙技術的力量 • 於全球數位政策強化非洲的聲量 • 區域網路的資助機制 • 以合乎道德的方式運用健康數據 • 有意義連網的青年觀點 • 多方社群如何快速回應數位政策 • 如何落實《未來網際網路宣言》願景 • 南方世界對數位人權的觀點	• 賦權女性的網際網路 • 數位公共財憲章倡議 (The Digital Public Goods Charter) • 數位教育和女性的工作前景 • 非洲聯盟開放論壇 • 歐盟代表參與 IGF(歐洲議會) • 數位時代的地球永續計畫(德國政府) • 2023 年世界資訊社會高峰會 (World Summit on the Information Society, WSIS) • 線上參與的數位技能 • 巴西 ICT 性別與多元化議程 • 國家的普及服務與人權保護 • 非洲網路治理的社群參與 • 數位民主的支柱(瑞士政府) • 聯合國的技術和人權盡職調查 • 確保人人享有數位人權(西班牙政府)

議題類別	座談	開放論壇
	• 數位公民權對無國籍者的影響 • 《未來網際網路宣言》交流對話 • 緊急應變以人權為中心的科技 • 兼顧人權和網路安全 • 封網的挑戰和風險 • 建立數位身份證基礎設施的問責制	
2. 提升安全和課責	• 黑暗模式設計的消費者保護挑戰 • 網路安全架構的全球常規 • Z 世代的網路安全 • 協調網路安全法規 • 網路攻擊和電子證據 • 網路安全就業市場所需技能 • 保護雲端安全 • 安全網路空間的能力建構 • 加密是否為數位人權 • 改善網路安全的危害量測問題 • 間諜軟體產業與人權 • DNS 濫用問題的現在與未來 • 為兒童建立安全可信賴的數位世界 • 對抗不實訊息的散播 • 打擊線上性別暴力 • 因應青少年自製色情內容 • 通訊軟體的資料保護 • 平臺規範的南方世界觀點 • 規範或不規範數位平臺 • 平臺對記者線上安全的責任 • 南方世界有意義的平臺透明度	• 強化政府資安(阿根廷政府) • 強化多方合作以因應 DNS 濫用(英國政府) • 強化網路韌性以促進發展 • 推動網路安全標準(德國政府) • 弱化加密的表現形式 • 虛假訊息和多方利害關係人事實查核(日本政府) • 塑造公共利益的數位平臺 • 對抗仇恨言論 • 在不審查下打擊假訊息(拉脫維亞政府) • 歐盟數位轉型的方法 (歐盟執委會)

議題類別	座談	開放論壇
3. 資料治理與隱私保護	• 資料跨境流通的治理 • 資料隱私的南方世界觀點 • 個資隱私保護措施 • 建立可信賴資料流通的共同原則 • 資料安全整合的機會與風險 • 公開來源情報 (Open Source Intelligence, OSINT)的道德和法律界限 • 為公共安全分享跨境資料 • 保障隱私的數位基礎設施 • 電子化政府的個資保護 • 保護長者的資料安全和人權 • 兒童隱私和教育科技應用軟體	• 強化資料驅動經濟的國際合作 • 災害復原的資料治理 • AI 的隱私風險管理(義、加政府) • 促進資料跨境流通和可信賴的資料空間(日本政府) • 採用全面觀點的資料治理架構 • 非洲聯盟資料政策架構的實施 • 創造資料價值並避免掏金熱潮(歐盟執委會) • 促進資料驅動的非洲單一市場
4. 因應先進技術(包含 AI)	• 情緒運算(Affective Computing)的治理挑戰 • 促進可信賴的 AI • 非裔女性 AI 治理的挑戰 • 元宇宙模糊的法律條文 • 通用人工智慧(Artificial general intelligence, AGI)公平和安全的發展途徑 • 共建負責和永續的元宇宙 • 數位轉型和 AI 對正義的重要性 • 永續發展的全球 AI 治理 • 新興科技的擔保和認證 • 為南方世界制定 AI 基本規範 • 為南方世界設計 AI 道德框架 • AI 治理的教育轉型 • 如何實現資料正義	• 多方利害關係人的可信賴 AI 倡議(日本政府等) • 智慧社會的治理(中國大陸政府) • 技術標準制定和人權 • 危機時期的 AI 驅動內容治理 • Web 3.0 的治理合作 • 元宇宙時代的創意產業

議題類別	座談	開放論壇
	• 數位醫療的數位落差問題和隱私挑戰	
5. 避免網路分裂	• 網路治理的政府角色 • 南方世界的網路分裂和主權 • 在經濟制裁時代保護全球網路 • 不同的平臺規範是否為開放網路帶來風險 • 平衡數位主權和網路分裂 • 限制公民使用數位服務和數位種族隔離(Digital Apartheid)的合法性及人權問題 • 網路外交 2.0 • 網路標準的分裂 • 網路分裂和數位不信任	• 保護網路的開放和互連 • 網路分裂的原因和影響(加拿大政府等) • 確保單一識別碼的持續性 • 阿拉伯地區的數位和作 • 競爭如何有助於中小企業進入線上市場 • 網路關閉和限制(日本政府) • 實現網路共同願景(英國政府)

第四節 彙整分析

為能更清楚呈現本年度（2022）國際網路治理會議的討論議題趨勢，本計畫以 IGF 2022 的 5 大議題類別為基礎，並參考其內容說明，將當中範圍較廣的「人人上網及確保人權」，分成「普及與包容」、「人權和民主」2 類；以及「提升安全和課責」，分成「網路安全」、「內容治理」2 類；又考量 APNIC 和 RIPE 會議主要討論「關鍵網路資源」，應有其專屬類別。因此，總計本年度的討論議題可彙整為 8 大類別。本計畫進一步將前述的國際會議依此類別，進行重新歸類和次數統計，主要結果如下（詳表 2-3）：

- 關鍵網路資源：60 次
- 普及與包容：45 次
- 網路安全：35 次
- 人權和民主、內容治理、資料治理與隱私保護、因應先進技術、避免網路分裂：18~23 次（此 5 類的次數差異相對較小）

整體而言，由於各個 IGF 的議題類別，都是由其專家小組（由不同的利害關係人組成）依據當年度的議題發展情況重新擬定，因此，所彙整的 8 大議題類別可謂皆是本年度的討論重點。

當中因為聯合國 IGF 和 APrIGF 皆有許多開發中國家積極地提案申辦座談，所以，「普及與包容」議題被討論的次數通常都相對較高，但這並不代表已開發國家沒有此類問題。例如：本報告案例研析「公平分攤網路成本的爭議」（參見第五章），即是目前歐、美、韓等國熱烈討論的議題。

而「關鍵網路資源」，如前所述，為 APNIC 和 RIPE 的主要業務暨會議核心，統計次數自然容易名列前茅。本報告另一案例研析「對俄斷網制裁的發展與影響」（參見第三章），因為源自烏克蘭政府請求國際組織（包含 RIPE）撤銷俄羅斯的國碼頂級域名和 IP 位址使用權，因此，屬於此類議題，其影響層面還涉及「人權和民主」及「避免網路分裂」類別。還有一

個案例研析「解讀《未來網際網路宣言》」(參見第四章)，同樣屬於「人權和民主」及「避免網路分裂」類別，雖然並非討論次數較高的類別，但也是本年度的重點議題之一。

表 2-3 2022 年國際網路治理會議討論議題

議題類別	總次數	APNIC 54	RIPE 84 和 85	APrIGF 2022	EuroDIG 2022	IGF 2022
1.普及與包容	45	0	4	12	2	27
2.人權和民主	21	0	4	3	2	12
3.網路安全	35	3	6	5	3	18
4.內容治理	18	0	0	4	1	13
5.資料治理與隱私保護	23	0	0	2	2	19
6.因應先進技術	23	0	0	0	3	20
7.避免網路分裂	22	1	1	0	4	16
8.關鍵網路資源	60	14	46	0	0	0

資料來源：本計畫彙整

會議資料

- APNIC 54. Schedule. https://conference.apnic.net/54/program/schedule/#/day/1
- APrIGF 2022. Program Schedule. https://ap.rigf.asia/news/2022-program-schedule/
- APrIGF 2022. Overarching Theme. https://ap.rigf.asia/news/2022/aprigf-2022-overarching-theme-people-at-the-centre-envisioning-a-community-led-internet-that-is-inclusive-sustainable-and-trusted/
- EuroDIG 2022. Programme. https://www.eurodig.org/eurodig-2022/eurodig-2022-programme/
- IGF 2022. Programme. https://www.intgovforum.org/en/filedepot_download/249/22161
- IGF 2022. Themes: Descriptions. https://www.intgovforum.org/en/content/igf-2022-themes-descriptions
- RIPE 84. Meeting Plan. https://ripe84.ripe.net/programme/meeting-plan/

第三章 案例研析(1) 對俄斷網制裁的發展與影響

第一節 前言

烏克蘭政府於俄烏戰爭開戰不久，即致函 ICANN（Internet Corporation for Assigned Names and Numbers，網際網路名稱與號碼指配機構）和 RIPE NCC（Réseaux IP Européens Network Coordination Center，歐洲 IP 網路資源協調中心，以下簡稱 RIPE），提出撤銷俄羅斯的國碼頂級域名和 IP 位址使用權等制裁訴求。雖然訴求遭到婉拒，不過，部分網路公司和網路組織基於遵循歐美制裁法規等因素，切斷俄羅斯的網路連線／接取（access）。這些前所未見的斷網制裁政治訴求和法令規定，引發各界對關鍵網路資源治理、網路制裁等議題的討論，以及助長網路主權、催化全球網路分裂等疑慮。而後在公民團體的聯合呼籲下，美國白宮宣布，美國、歐盟和 G7（七大工業國家組織）的對俄制裁措施豁免電信網通領域。

俄烏戰爭涉及的網路治理議題不少，從網路三層架構[2]來看，在應用層（或稱經濟和社會層）有西方國家和俄羅斯皆封鎖對方的新聞媒體、莫斯科法院裁定 Facebook 為極端組織並將其封鎖等議題；在實體層（或稱基礎設施層）有全球首富馬斯克（Elon Musk）為烏克蘭提供 Starlink 低軌衛星網路、美國專家鑑於俄烏戰爭提醒臺灣海纜脆弱等議題。而本章所探討的斷網制裁之發展與影響，除了網路骨幹業者和交換中心的斷網案例涉及實體層，以及公民團體的信函等提及應用層的封鎖概況外，基本上以討論傳輸層（或稱邏輯層）的議題為主，以能更聚焦問題，避免治絲益棼。

[2] Jovan Kurbalija（2016）所著《網路治理導論》（An Introduction to Internet Governance）將網路分為三層架構，由上而下分別為：應用層、傳輸層、實體層。ICANN（2015）亦將數位治理分為三層，由上而下分別為：經濟和社會層、邏輯層、基礎設施層。基本上兩者只是名稱有異，各層內涵其實大致相同。

第二節 對俄斷網制裁的政治訴求及相關回應

一、烏克蘭政府的斷網政治訴求

烏克蘭副總理兼數位部長 Mykhailo Fedorov 分別於 2 月 28 日和 3 月 2 日，致函 ICANN（Fedorov, 2022a）和 RIPE（Fedorov, 2022b），指控俄羅斯的軍事行動違反多項國際法規、對全球帶來核武威脅，且其暴行之所以能得逞，是因為俄羅斯的宣傳機器不斷利用網路散播不實訊息、仇恨和暴力言論，以掩蓋戰爭真相，故而提出下列 4 項訴求以制裁俄羅斯：

- 撤銷俄羅斯的頂級網域.ru、.рф、.su；
- 協助撤銷上述網域的 SSL 安全憑證；
- 關閉俄羅斯境內 DNS (Domain Name System，網域名稱系統)；
- 撤銷俄羅斯 IPv4 和 IPv6 位址使用權。

上述.ru、.рф、.su 的正式名稱為國碼頂級域名（Country Code Top-level Domain, ccTLD）。.ru 為 Russia 的 2 字母代碼，.рф 為俄羅斯聯邦的俄文縮寫，.su 為 Soviet Union 的 2 字母代碼。

此外， 烏克蘭政府對俄羅斯斷網政治訴求的對象，還有國際 CDN（Content Delivery Network，內容傳遞網路）大廠。烏克蘭副總理 Fedorov 於致 Cloudflare 信函及其 Twitter 上表示「俄羅斯的坦克和導彈襲擊烏克蘭的幼兒園.....在全世界正透過制裁對抗侵略者之際……Cloudflare 不該仍然保護俄羅斯的網路資源」。烏克蘭裔的美國網路安全業者 SOC Prime 也敦促 Cloudflare 和 Akamai 等公司，停止於俄羅斯及白俄羅斯的網路服務，甚至認為美國政府應該禁止這些企業在俄羅斯的所有營運（Brodkin, 2022）。

二、政治訴求遭拒的原因

(一) ICANN 和 RIPE：無權斷網且須保持中立

不過，烏克蘭政府的斷網政治訴求，遭到 2 個國際組織婉拒。ICANN 於回函強調，其成立宗旨在於確保全球網路的正常運作，並無實施網路制裁的權力，且其角色為技術協調者，需保持中立並遠離政治。而 RIPE 亦提出相似說法，還特別保證烏克蘭會員的 IP 位址使用權益，不會因為戰爭時期無法付款或履行行政規定而喪失。ICANN 和 RIPE 的逐一婉拒說明，彙整如下表 3-1。

表 3-1 ICANN 和 RIPE 對烏克蘭政府斷網訴求的回應

烏克蘭政府的請求	ICANN 的回覆	RIPE 的回覆
1. 撤銷.ru、.рф、.su	任何片面阻斷 ccTLD，都會破壞大家對多方利害關係模式和維護全球網路互通政策的信任	與職責無關
2. 協助撤銷上述網域的 SSL 安全憑證	SSL 憑證由第三方運營商所頒發，ICANN 無法提供協助	與職責無關
3. 關閉俄羅斯境內 DNS	根伺服器系統是由眾多分佈在各地的節點所組成，且由獨立的運營商維運	雖然負責維運 K-root （全球有 13 組根伺服器，以字母 A 到 M 依序命名），但 DNS 必須保持中立
4. 撤銷俄羅斯的 IPv4 和 IPv6 位址使用權	未對 ICANN 提此訴求	無權採取此類行動，且不應將網路號碼資源作為政治手段，否則將破壞全球網路的穩定運作

資料來源：本計畫彙整

喬治亞理工學院教授暨「網路治理計畫」（Internet Governance Project）創辦人 Milton Mueller（2022）也表示，ICANN 成立的目的，正是讓全球網路基礎資源的管理遠離國家政府和地緣政治衝突。至於烏克蘭政府希望透過斷網以阻止俄羅斯不斷散播網路不實訊息，Mueller 指出，其實烏克蘭本來就可以在其認為有必要的情況下，阻斷特定的俄羅斯域名和 IP 位址，這正是網路「分散式」治理模式的優點，也就是每個網路運營商都可以自行決定要阻止或允許什麼網路連線。要求 ICANN 在全球範圍內禁用俄羅斯

的所有域名和 IP 位址，反而是不成比例的做法。

(二) Cloudflare 和 Akamai：為傳遞真相「不能斷網」

2 大 CDN 業者同樣婉拒烏克蘭政府的斷網政治訴求。Cloudflare 表示，該公司的偵測發現，俄羅斯連向國際媒體的流量大增，反映俄羅斯民眾希望看到外界的新聞，凸顯俄羅斯需要的是更多的網路接取而非切斷，一旦完全終止俄羅斯的網路服務，並不會對普丁政府造成什麼傷害，但卻會導致反普丁政權者陷於孤立無援之境（Prince, 2022）。Akamai（2022）也指出，在實踐保護其網路用戶（包含全球最大的新聞服務、社群平臺，及俄羅斯公民）並賦予他們能力的使命下，Akamai 決定繼續提供在俄羅斯的網路服務，以利各界向俄羅斯民眾傳遞重要且正確的訊息。

三、ICANN 評估.su 退場政策

雖然 ICANN 於烏克蘭政府的正式回函中，表明無權撤銷俄羅斯的 3 個 ccTLD，但其實 ICANN 目前正在評估 ccTLD 的退場政策，待定案後可望將當中的.su 移除。

根據 ICANN 之 GAC（Governmental Advisory Committee，政府諮詢委員會）《ccTLDs 授權與管理之原則和指南》，ccTLD 主要是參照 ISO（International Organization for Standardization，國際標準化組織）的 3166 國碼標準所制定（GAC, 2005）。而烏克蘭政府的請求，讓代表「蘇聯」的.su 早已不在 3166 國碼標準的問題（蘇聯於 1991 年解體），成為關注焦點，也就是.su 不再被視為具備 ccTLD 資格。

ICANN 表示，由 ccNSO（國碼域名支援組織，Country Code Names Supporting Organization）研擬的 ccTLD 退場政策係指「當國家不復存在等情況下，從根伺服器刪除 ccTLD 的流程」，且政策提案已經送交 ICANN 董事會進行評估。

不過，域名專業媒體 Domain Incite 指出，屆時要實施.su 退場，

ICANN 仍需解決新的政策能否溯及既有的 ccTLD，以及非 ccNSO 成員的.su 管理單位 ROSNIIROS 如何適用 ICANN 政策等難題。如果問題無解而允許.su 繼續存在，在.su 被視為不符合 ccTLD 資格，及具備刪除政策工具的情況下，ICANN 將陷於尷尬的處境（Murphy, 2022a）。

第三節 對俄斷網制裁的法令規定及實施狀況

一、 遵循歐盟 2022/350 號法規的網路骨幹業者

傳遞全球約 25% 網路流量的美國網路骨幹業者 Cogent Communications，於 3 月 4 日起對俄羅斯斷網。Cogent 表示，其遵循的是歐盟 2022/350 號法規（Council Regulation 2022/350）當中有關封鎖俄羅斯國營媒體 Russia Today（今日俄羅斯媒體集團，簡稱 RT），及旗下 Sputnik（俄羅斯衛星通訊社）的規定。不過，根據 Cogent 致俄羅斯客戶信函，Cogent 的制裁措施不只針對 RT，而是收回所有俄羅斯客戶的通訊埠（port）和 IP 位址（Greig, 2022）。

另一家網路骨幹業者 Lumen Technologies 亦史無前例地於 3 月 8 日起，中斷俄羅斯的所有網路服務，但沒有說明制裁法規的依據，僅表示該公司遵循所有的監管命令、制裁要求和相關限制（Lumen, 2022）。

此外，2 家業者也指出實施斷網還有安全考量，因為俄羅斯的安全風險上升，他們不能讓自家網路淪為俄羅斯政府攻擊西方國家的工具。

二、 遵循歐盟個人和實體制裁清單的網路組織

全球前五大網路交換中心之一的倫敦網路交換中心（London Internet Exchange, LINX）也於 3 月 11 日對俄羅斯斷網。LINX 表示，經考量烏克蘭情況，並遵循歐盟的個人和實體制裁清單（the list of the sanctioned individuals and entities），決定停止和清單上 2 家俄羅斯電信公司 Rostelecom 和 Megafon 的網路連線（Moss, 2022）。

前述婉拒烏克蘭政府「撤銷俄羅斯 IPv4 和 IPv6 位址使用權」政治訴求的 RIPE（2022），則是對上述清單上的所有被制裁者，停止或限制其權利。RIPE 表示，雖然頻繁更新的歐盟制裁法規目前沒有禁止他們對俄羅斯提供服務，但經洽荷蘭外交部（RIPE 總部位於荷蘭），確認法規將 IP 資源視

為必須凍結的經濟資源，因此，受制裁者將無法獲得新的 IP 或轉移既有 IP，惟已註冊使用的 IP 不會被取消。

三、 未指明特定制裁法規的其他網路業者

其他網路業者亦基於遵循制裁法規，而對俄羅斯斷網或暫停特定的服務。不過，他們並未說明究竟依據哪一項法規。前述婉拒烏克蘭政治訴求的 Cloudflare 表示，他們已經採取法遵行動，關閉制裁名單的付費網路服務和系統服務，以及終止和俄國金融機構、宣傳活動及支持烏克蘭 Donetsk 及 Luhansk 地區獨立政府有關的客戶服務。Akamai(2022)也指出，該公司遵守所有的制裁法規，並據此暫停在俄羅斯和白俄羅斯的銷售活動，以及終止兩國政府公營事業的客戶合約。

其他採取制裁措施的網路業者還包括：全球主要認證機構 Sectigo 停止對俄羅斯核發 SSL 安全憑證、域名註冊商 Namecheap 停止提供域名主機代管服務、CENTR（Council of European National Top-Level Domain Registries，歐洲國家頂級網域管理局）暫停俄羅斯的會員資格、全球最大域名註冊商 Godaddy 停止銷售.ru 域名等（Techstony,2022；Murphy, 2022b）。

四、 歐美制裁法規簡介

許多對俄羅斯斷網或暫停服務的網路業者沒有載明法規依據，或許原因正如 RIPE（2022）和 Cloudflare（2022）所述，「制裁法規頻繁地更新、數量前所未見、範圍空前廣泛」。

美國財經出版商道瓊公司亦指出，幾乎所有主要西方國家都加入制裁俄羅斯的行列，「制裁規模和法規更新速度是前所未見，要掌握其不斷變化的進展是巨大挑戰(需要律師團隊)」，企業也面臨巨大的法遵壓力(Dow Jones & Company, 2022）。

以美國的對俄制裁法規為例，大致可分成美國商務部工業與安全局

（Bureau of Industry and Security, BIS）主管的《出口管理條例》（Export Administration Regulations, EAR），和美國財政部外國資產控制辦公室(Office of Foreign Assets Control, OFAC)主管的《俄羅斯外國有害活動制裁條例》（Russian Harmful Foreign Activities Sanctions Regulations, RuHSR）。單是後者所涉及的法規即包括 5 份指令（Directive）、2 份指引（Guidance）、26 份通用授權（General License）、5 份總統行政命令（Executive Order），以及 2 份制裁清單等[3]。整體而言，這些法規規範其制裁對象為俄羅斯總統普丁、其親友、及支持其政權的重要人士；制裁範圍涵蓋能源、自然資源、金融服務、國防、航空、交通、科技等戰略領域的國有企業和關聯企業；制裁措施包括貿易限制、資產凍結、出口禁令、旅行禁令和其他懲罰性措施（U.S. Department of the Treasury, 2022; Dow Jones & Company, 2022）。

又如歐盟的法規，自 2 月下旬俄烏衝突爆發至 6 月初，歐盟對俄羅斯（及白俄羅斯）的制裁已實施至第六輪。歐盟的制裁法規是由歐洲理事會（European Council）通過，法規名稱如第六輪制裁為 Council Regulation (EU) 2022/879。總計此段期間所通過和實施的制裁俄羅斯規範包括 26 份規則（Regulation）、8 份實施條例（Implementing Regulation）及 34 份決議（Decision）。就內容屬性而言，則分成個人（和實體）制裁（如凍結資產、禁止旅行）、經濟制裁（包含金融、交通、能源、國防、原料和貨物等類別）、媒體限制（針對 5 家國營媒體）、外交措施（如停發官員和商務人士簽證）等大類（Corsoni-Husain,2022; European Council, 2022）。

此外，複雜又龐大的制裁法規該如何解讀及執行，也是一大問題。如前所述，RIPE 是特別詢問荷蘭政府後，才能確認「歐盟制裁法規沒有禁止對俄羅斯提供 IP，但將 IP 資源視為必須對受制裁者凍結的經濟資源」。又如 Cogent，它表明遵循的是歐盟有關封鎖俄羅斯國營媒體的規定，但執行上卻是中斷所有俄羅斯客戶的服務。

[3] 於 6 底查詢美國財政部網站（U.S. Department of the Treasury, 2022）。

五、俄羅斯的網路連線情況

至於上述網路業者或組織的斷網制裁措施所造成的影響，網路分析公司 Kentik 表示，Lumen 的俄羅斯客戶包含其國營電信公司 Rostelecom 和三大行動通訊公司 MTS、Megafon 和 VEON。雖然 Lumen 切斷俄羅斯的網路骨幹，會造成頻寬減少、網速變慢，也會對俄羅斯網路連線下游的哈薩克、烏茲別克、伊朗、亞塞拜然等地區的網路造成影響。不過，由於俄羅斯仍可連接其他的國際網路骨幹，因此，Lumen 的制裁措施不會導致整個俄羅斯斷網（Vaughan-Nichols, 2022）。

RIPE 則指出，雖然 Cogent 停止連接到俄羅斯的 8 個網絡(networks)，但是它和俄羅斯國營電信公司 Rostelecom 之間的互連點並沒有消失。而在網路交換方面，儘管俄羅斯網路通過 LINX 連接埠(port)的路徑明顯減少，但仍可透過重新路由，連到替代路徑，也就是另 2 個網路交換中心——AMS-IX（阿姆斯特丹）和 DE-CIX（法蘭克福）。整體而言，俄羅斯的網路連線雖然因為可用容量減少而有延遲情況，但由於網路具有高度的互連彈性，因此，和全球網路的連線沒有巨大變化，在網絡層面的斷網制裁影響有限（Aben, 2022）。

俄羅斯的電信業者也提出相近的回應。Rostelecom 表示，因為備有和其他國外機構交換流量的替代路徑，所以，俄羅斯的網路運作不會受到影響（Moss, 2022）。

第四節 美歐豁免電信網通制裁

一、美國許可電信網通服務

(一) 公民團體呼籲美國總統勿對俄斷網

有鑑於資通訊業者面臨強大的來自烏克蘭政府和遵循歐美制裁法規的對俄斷網壓力，包括 Access Now、ARTICLE 19、網際網路協會（Internet Society, ISOC）、維基媒體基金會等 40 多個公民團體，於 2022 年 3 月 10 日致函美國總統拜登，呼籲勿對俄羅斯斷網，以免孤立俄羅斯的反戰力量，迫使民眾只能接收官方訊息，進而助長普丁實現全面控制境內資訊的目標（Access Now, 2022a）。

此封信件所列舉的破壞俄羅斯連線全球網路的事件，除了烏克蘭政府對 ICANN（總部位於美國加州）的請求、網路骨幹業者 Cogent 和 Lumen（皆為美國業者）因為遵循美國制裁法規而停止對俄羅斯服務外，還提及美國主要的軟體業者和網路平臺及全球科技公司，也是因為遵循歐美制裁法規，暫停對俄羅斯銷售產品或服務。而普丁政府也因此採取更嚴格的網路限制措施，例如：禁止使用 Facebook 和 Twitter，並對一些外國媒體發出審查通知或威脅封鎖其服務。在此惡性循環下，將迫使俄羅斯的民運和反戰人士以及獨立媒體陷於孤立處境，民眾只能接收官方媒體訊息，進而助長普丁實現全面控制境內資訊的「主權網路」目標。

信件最後也敦促所有考慮對俄羅斯的網路連線採取限制措施者，應審慎考慮全面的影響性及可能的意外後果，且行事需具備針對性、開放性，並符合國際人權原則的合法性、正當性、必要性和比例原則。同時還呼籲美國財政部外國資產控制辦公室（OFAC）立即頒發「通用許可」（General License），允許對俄羅斯提供個人網路通訊所需的相關服務和軟硬體，以保護俄羅斯的資訊自由流動。

(二) 美國發布「通用許可」豁免電信網通服務

上述公民團體的勿對俄羅斯斷網聯合呼籲，獲得美國政府的迴響。美國白宮於4月6日表示，雖然美國、歐盟和G7持續擴大對俄羅斯的制裁措施，但「我們」也重申承諾，免除基本人道主義的相關活動，包含：食物和農產品的供應、藥品和醫療設備的獲取，以及有利資訊流通和網路接取進而向俄羅斯民眾提供外界觀點的「電信服務」；「美國和西方企業」可以繼續在俄羅斯提供這些業務（White House, 2022）。

美國財政部外國資產控制辦公室（OFAC, 2022）亦於次日發布《俄羅斯有害外國活動制裁條例》（RuHSR）NO.25「通用許可」（6月2日更新為General License NO. 25B），授權對俄羅斯提供電信和特定網路通訊交換相關的服務、軟硬體和技術。例如：即時通訊、視訊會議、通話、電子郵件、社群網路、相片共享、電影、文件、網路瀏覽、部落格、網站代管，及域名註冊服務。惟已遭制裁的特定俄羅斯金融機構、電視廣播媒體，及行政命令14066號或14068號禁止的項目除外[4]。

(三)學者亦肯定「通用許可」避免助長普丁的資訊控制

日本慶應義塾大學（Keio University）教授David J. Farber和資深研究員Dan Gillmor高度讚揚上述「通用許可」，認為這代表美國政府對切斷俄羅斯與全球網路連線的善意運動說「不」，因為「全面封鎖俄羅斯」的論述似乎贏得全球的公關戰，一旦被付諸實行，反而會助長普丁政權完成資訊隔絕和資訊控制的目標（Farber & Gillmor, 2022）。

當然，致拜登信函連署者之一的ISOC（2022）也表示樂見白宮、歐盟及G7豁免電信服務的共同承諾，認為此舉可以延緩全球網路分裂，維護網路的開放、互連、安全和可信賴。只是ISOC也強調，延緩並不代表網路分裂的威脅已經解除。相關問題將於本章第五節加以探討。

二、英國許可民用電信服務

[4] 行政命令14066號禁止進口和投資俄羅斯石油等能源。14068號禁止進出口和投資俄羅斯的海產、酒精、奢侈品。此處可能是指「通用許可」不含提供電信網通產品和服務給這些行業的業者。

(一) 公民團體呼籲英國政府勿對俄斷網

Access Now（2022b）、維基媒體基金會等 12 個公民團體，於 5 月 20 日致函英國政府，同樣提出勿對俄羅斯斷網的呼籲，且信件內容和致美國拜登總統也大致相近。不過，致函原由主要是擔心英國涉及網路連線的新制裁措施，可能影響英國業者和俄羅斯電信公司之間的業務，進而引發破壞俄羅斯網路連線的意外後果。

信函中還指出，資通訊廠商面臨越來越大的壓力，要求他們限制或阻止俄羅斯用戶的網路連線。而在模糊的法規下，科技公司紛紛撤回付費 Apps 和服務、停止整個俄羅斯業務，或限制對民間的服務。因此，希望英國政府參考美國做法，透過發布「通用許可」豁免網路連線相關的制裁措施，以免阻礙俄羅斯人民了解真相、孤立反戰人士、助長普丁實現全面控制境內資訊。

惟信函並未說明英國制裁新規的名稱或內容。本計畫經查詢，推測可能是指英國《俄羅斯(制裁)(脫歐)法案 2019》(簡稱 The Russia Regulations）於 4 月 29 日生效的第 9 號修正案[5]，當中新增社群媒體服務（包括影片分享平臺）、網路連線服務（包括固網和無線寬頻供應商）和 Apps 商店（包括智慧手機上的商店），必須採取合理措施，防止其英國用戶觸及（遭制裁）特定個人／實體所上傳的內容、提供的網站、開發的 Apps。

雖然此修正案是針對俄羅斯受制裁者所提供的網路內容或 Apps 進行限制，但英國 Hogan Lovells 律師事務所表示，為了遵守規定，相關業者需要實施強大的篩選機制，或主動採取網址或 DNS 封鎖等措施（Doussin & Malhi, 2022）。或許這種「強大的篩選機制」，即是公民團體所擔憂的「引發破壞俄羅斯網路連線的意外後果」。

(二) 英國發布「通用許可」豁免民用電信服務

[5] 制裁俄羅斯法規的英文全文為 The Russia (Sanctions) (EU Exit) Regulations 2019；修正案為 The Russia (Sanctions) (EU Exit) (Amendment) (No. 9) Regulations 2022。

英國財政部金融制裁執行辦公室（Office of Financial Sanctions Implementation, OFSI）依據 The Russia Regulations 第 64 條的「財政部許可」，於 5 月 30 日發布「通用許可」INT/2022/1875276，允許對俄羅斯提供民用電信服務和新聞媒體服務。此處「民用電信服務」係指英國《通訊傳播法》（Communications Act 2003）所定義的「以民眾使用為目的的電子通訊網絡（network）或服務」（OFSI, 2022）。

Access Now（2022c）也隨即對此「通用許可」表示肯定，指出英國政府聽取公民團體的呼籲，在制裁俄羅斯時兼顧保護該國的資訊自由流通（包含流入和流出），讓俄羅斯人民能夠繼續連線全球網路，並讓英國新聞媒體得以持續於俄羅斯營運，此舉有助於強化當地的民主和公民行動力量。

三、歐盟制裁排除民用電信網絡

有別於美英兩國是於公民團體聯合呼籲勿對俄羅斯斷網後，透過發布「通用許可」豁免對俄羅斯的電信網通服務制裁，歐盟的情況是原本制裁法規就無此項禁令。根據歐盟執委會持續更新的制裁法規常見問答集，制裁法規 Council Regulation（EU）No 833/2014 第 2 條第 4 款和第 2a 條第 4 款，排除（derogations）民用電信網絡（包含網路服務）制裁，惟須取得國家主管機關的授權才可以對俄羅斯出口。又《歐盟(軍商)兩用貨品條例》（EU Dual-Use Regulation）和先進技術項目的出口限制，也同樣排除民用電信網絡，但不含與俄羅斯國防、基礎工業、航空和太空工業相關的個人或實體（EC, 2022）。

第五節 對俄斷網制裁的影響

儘管烏克蘭政府的斷網制裁政治訴求遭 ICANN 和 RIPE 婉拒，且歐美國家也排除或豁免對俄羅斯實施電信網通制裁，不過，訴求的提出，以及網路業者和組織已採取的斷網措施，仍將對俄羅斯、其他獨裁國家，以及全球的網路發展，帶來深遠的影響。

一、對俄羅斯的影響

面對國際的斷網制裁，俄羅斯一度傳出訂於 3 月 11 日啟動本國網路 RuNet，雖然後來官方否認此消息，但是透過 RuNet 以監控或審查網路內容，進而全面實施網路主權，一直是普丁政府的目標，且為此籌謀已久。例如：於 2019 年通過且實施《主權網路法》（Sovereign Internet Law），賦予政府以國安為由，隨時切斷和全球網路連線的權力，同年還宣布 RuNet 和全球網路的斷線測試成功，惟外界對其宣稱測試成功多有存疑。德國外交關係委員會（德文簡稱 DGAP）的網路政策專家 Alena Epifanova 表示，俄羅斯迄今尚未備妥完全脫離全球網路，尤其目前整個俄羅斯經濟高度依賴全球網路，如果切斷連線，可能會導致經濟嚴重衰退（Meyer, 2022）。

ISOC 也持類似看法，指出俄羅斯一直想仿效中國大陸建立主權版的網路，但目前尚未成功，因為它的網路和 Internet 有諸多連接，不像中國大陸是連到中共控制的內容和服務。不過，ISOC 同時強調，歷經斷網制裁的俄羅斯，將會更努力尋求突破網路主權的困境（York, 2022）。

美國布魯金斯研究所（Brookings Institution）亦認為，歷經國際嚴厲制裁的俄羅斯，將會更積極推動網路（數位）主權。例如：普丁已成立新的「網路和科技主權委員會」，並任命前總統、現任國安會副主席 Dmitry Medvedev 為主委，以建立獨立自主的網路科技和經濟；另一方面，也封鎖西方媒體和平臺，並將 Facebook 和 Instagram 歸類為極端主義組織，以及將 YouTube 視為西方對俄羅斯發動資訊戰的工具。

不過，布魯金斯研究所並不看好俄羅斯的科技自主前景，因為它缺乏具競爭力的科技產業，加上西方科技公司大舉離境，當地科技人才也大量出走，未來俄羅斯只能更加依賴中國大陸的相關零組件、產品、技術和服務（例如華為的手機在俄銷售量暴增 3 倍），最終並淪為中國大陸網路主權倡議的追隨者（Wilde & Sherman, 2022）。

二、對其他獨裁國家的影響

對於俄羅斯遭到西方陣營斷網、停售數位產品、終止網路內容服務等制裁或抵制，加上俄羅斯也以封鎖西方新聞媒體和社群平臺作為反制，《麻省理工科技評論》（MIT Technology Review）形容俄羅斯淪為和伊朗一樣的「數位賤民國家」（Ball, 2022）；《政客》（Politico）雜誌指稱俄羅斯遭到「數位封鎖」（Stolton, 2022）；紐約時報亦描述俄羅斯陷入「數位孤立」（Satariano & Hopkins, 2022）。

愛爾蘭都柏林大學政治與國際關係學院研究員 Caitríona Heinl（2022）表示，雖然 ICANN 拒絕烏克蘭政府的請求，但俄羅斯陷入「數位孤立」，對其他的獨裁國家而言，猶如敲響一記警鐘，示警他們現在應該為未來可能發生的類似情況研擬因應戰略，即使短期內仍然無法和全球網路分離，但也應日益減少對全球網路生態系統的依賴，逐步實現科技和網路的自給自足，以便於未來發生危機之際，可以完全脫離全球網路。

上述觀點可從中國大陸學者的看法得到呼應。中國傳媒大學網絡空間全球治理研究中心主任徐培喜指出，「各國都要看到俄烏衝突對未來的預警，做好應對方案。在當前以美國為首的地緣政治操盤手眼中，『全球一網』的初始價值觀雖仍重要，但並非不可捨棄，當下針對俄羅斯的制裁圍堵和資訊戰有可能被完整複製到其他國家身上」（吳旭，2022）。

三、對全球網路發展的影響

(一) 捍衛網路資源治理原則

雖然烏克蘭政府的斷網政治訴求挑戰網路資源的「政治中立」治理原則，但 ICANN 和 RIPE 的婉拒訴求，也彰顯它們捍衛治理原則、維護全球網路正常運作的具體行動。美國喬治亞理工學院「網路治理計畫」創辦人 Milton Mueller（2022）教授表示，ICANN 成立的目的，正是讓全球網路基礎資源的管理遠離國家政府和地緣政治衝突。而烏克蘭政府的訴求，及部分人權團體要求將整個網路治理制度轉為對俄羅斯的憤怒，不但無法阻止俄羅斯的侵略惡行，還可能破壞全球網路治理機構的中立性和獨立性，並協助普丁實現操控俄羅斯資訊的目標。

《網路治理導論》（An Introduction to Internet Governance）作者 Jovan Kurbalija（2022）博士也指出，雖然從技術上而言，透過網路核心基礎設施可以切斷一個國家的網路連線，但自從網路創造以來，這種猶如數位核子選項的「數位緊急開關」（Digital Kill Switch）從未被用於對付任何國家，包括近年的伊拉克、阿富汗和利比亞危機。Kurbalija 強調，網路已成為當代主要的全球公共財，一個國家和網路的連線不該被切斷。

(二) 爭辯網路資源制裁原則

來自歐洲議會、歐美學研界和公民團體等單位的 36 位專家發表「多方利害關係人實施網路制裁」（Multistakeholder Imposition of Internet Sanctions）聯合聲明，主張在面對人道主義危機時，網路社群有責任訂定適當有效且經多方利害關係人（Multistakeholder，以下或簡稱為多方）決策的網路制裁措施，並提出下列網路基礎設施（主要指網路資源）的制裁原則，期能在捍衛社會道德的同時，將制裁的負面衝擊降到最低（Groothuis, et al., 2022）。

1. 切斷一國人民和網路連線的網路制裁，不符合比例原則且不適當，因為此舉阻礙人民獲取反戰的訊息，並迫使他們只能接收該國政府設定的訊息。

2. 網路制裁的有效性應根據目標進行評估，無效的制裁只會浪費精力

與意志力，且無法傳達團結和信念。

3. 網路制裁必須精確，應盡量減少意外後果或附帶損害的可能性，不符合比例或過度的制裁，也可能從根本上背離人民。

4. 軍事與宣傳機構及其資訊基礎設施，可以作為制裁的潛在目標。

5. 基於網路跨越國界的本質，及其採共識決的多方利害關係人治理架構，目前要在國家衝突時實施網路制裁並不容易。

6. 政府如果試圖於多方利害關係人決策流程外實施網路制裁，是不適當的，且易適得其反。

7. 網路治理社群在商議的過程中，可考量適當、有效且具體的制裁措施（建議參考網路營運商阻擋垃圾郵件和惡意軟體攻擊的措施，但採多方的機制——開放、透明、共識導向，以決定是否進行制裁，進而建立域名和 IP 位址制裁清單，讓願意共襄盛舉的組織採用。此機制亦可為未來重大緊急事件奠定即時決策的基礎）。

上述第一項原則主要描述不該切斷一國的網路連線，基本上和公民團體的聯合呼籲相同，也和網路資源治理原則所要維護的全球網路正常運作方向一致。然而，其他原則就和不少專家的看法有相當差異。

ISOC 執行長 Andrew Sullivan 表示，由於各方都有不同的利益及需求，所以，根本無法找到一個最有效的制裁方法。美國數位治理顧問公司 Digital Medusa 創辦人 Farzaneh Badii（2022）則指出，經濟制裁可以針對性地實施，但涉及網路的制裁很難不波及一般民眾，因為企業會為了避免違法而過度實施制裁，以致俄羅斯民眾也受斷網之苦；而針對軍事和宣傳機構的制裁根本無效，因為他們可以輕易轉換至民用網路和其他各式傳播管道；又制裁在本質上是國家政府的行為及外交政策的一種手段，「非國家行為者」的行動不是制裁制度，而是消費者抵制運動。

RIPE 顧問 Chris Buckridge 也擔憂由「非國家行為者」制定基於政治目

的網路制裁清單，不但破壞國際多邊制裁制度，還會引發各國政府介入網路運營商長期以來運作良好的自治機制[6]，進而危害整個網路的互連和韌性（Directions, 2022）。Access Now 法律顧問 Peter Micek 則認為，制裁清單的制定方式恐怕無法通過人權團體的標準，因為這需要耗費多年的設計和測試，才能建立完善、包容且開放的決策過程（Timberg, 2022）。

(三) 催化全球網路分裂

西方陣營的斷網制裁及所引發獨裁陣營將更積極追求網路主權，也帶來催化全球網路分裂的疑慮。以下先簡述專家對於當前全球網路是否已經分裂的不同看法。

- 主張全球網路已經分裂：美國矽谷思想家 Tim O'Reilly、歐洲網路治理論壇（EuroDIG）創辦人暨丹麥 Aarhus 大學榮譽教授 Wolfgang Kleinwächter 等人認為，中俄和美國的應用程式及網路服務皆屬不同生態系統、不同平臺間的封閉運作[7]，或是資料在地化和數位主權等國家立法，皆已打破網路互通的常規（Watanabe, 2022; Kleinwächter, 2022）。

- 主張全球網路尚未分裂：喬治亞理工學院教授 Milton Mueller 認為，不同國家在同一底層架構上使用不同平臺，並非網路分裂。唯有全球大量人口使用技術不相容的協議，或使用技術相容的協議但由不同的治理機構管理，才是真正的網路分裂（Ball, 2022）。

然而，不論當前全球網路是否已經分裂，俄烏戰爭都催化其發展趨勢。《麻省理工科技評論》和都柏林大學研究員 Caitríona Heinl 皆指出，雖然在戰爭前，中國大陸早已完成知名的「防火牆」網路——由中共完全控制內容和服務的主權網路；俄羅斯也藉由建立 RuNet 和《主權網路法》，提

[6] 意指網路運營商可以快速且有效地自行決定與誰交換流量。Buckridge 表示，網路的蓬勃發展證明這種自治機制的成效良好。

[7] 又稱圍牆花園（Walled Garden），如 Facebook 內容無法透過 Google 搜尋。

升官方管控網路基礎設施和內容審查的能力；且中俄雙方還聯手在 ITU（International Telecommunications Union，國際電信聯盟）推動新網路協議（New IP）計畫，以利政府可透過網路業者封鎖任何網站或 Apps。惟基於當前經濟利益和國家戰略等考量，即使是具備維運獨立網路能力的中國大陸，也仍然維持和全球網路的連線。不過，俄烏戰爭以來，西方陣營和俄羅斯的行動皆進一步深化全球網路治理的思維分歧，且激發獨裁國家更積極發展網路主權。因此，未來全球可能不再是單一網路，而是依國界劃分成許多無法互通的網路，甚至可能使用技術不相容的網路協議，或擁護不同的國際治理機構。而在複雜的政治利益結構糾結下，屆時的網路分裂恐將無法逆轉，全球網路互連的時代也將宣告終結（Ball, 2022; Heinl, 2022）。

第六節 結論與建議

一、結論

(一) 國際普遍反對「全面性」斷網制裁，但對多方機制實施制裁無共識

從 ICANN 和 RIPE 婉拒烏克蘭政府的斷網制裁政治訴求、40 多個公民團體聯合呼籲勿對俄羅斯斷網、美英兩國政府發布電信網通服務「通用許可」，以及專家學者對於網路資源治理得以維持政治中立的肯定，凸顯即使在強烈的挺烏反俄氛圍下，國際社會仍普遍反對對俄羅斯實施「全面性」的斷網制裁，以維護全球網路的正常運作，保障俄羅斯的人道通訊所需、獲取外界資訊，以及避免助長普丁的資訊控制。

至於部分專家聯合提出的「多方利害關係人實施網路制裁」，網路治理社群對此並無共識。反對方的理由如：網路制裁和經濟制裁不同，無法精準地不波及一般民眾；針對軍事和宣傳機構的制裁無效，因為可輕易轉換至民用網路和其他傳播管道；制裁的本質為國家政府的行為，而非其他利害關係人的消費者抵制運動；由「非國家行為者」制定基於政治目的的網路制裁清單，將破壞網路運營商的自治機制及全球網路的互連和韌性。

(二) 歐美國家排除或豁免電信網通制裁，我國法規方向亦和國際一致

不論是原本法規即排除民用電信網絡制裁的歐盟，或是在公民團體聯合呼籲後發布「通用許可」豁免電信網通相關制裁的美國和英國，整體而言，除了受制裁或管制行業的實體和個人外，目前歐美各國沒有禁止對俄羅斯提供電信網通相關服務。我國亦加入制裁俄羅斯的國際行列，於 4 月 6 日公告並實施「輸往俄羅斯高科技貨品清單」(5 月 6 日增加白俄羅斯)，主管機關為經濟部（2022)，內容主要是針對電子等 8 大類產品出口俄羅斯進行管制，但一般民眾使用的電腦、電信和資訊安全類別產品，不在管制範圍內。此規範可謂和歐美國家排除或豁免電信網通制裁的法規方向一致。

(三) 斷網制裁加上「數位孤立」，全球網路分裂危機更甚以往

雖然 ICANN 和 RIPE 維持俄羅斯關鍵網路資源的正常運作，且歐美和我國等也允許持續對俄提供電信網通服務，不過，多數國際資通訊大廠仍未恢復俄羅斯的業務或服務[8]。加上普丁還以封鎖西方新聞媒體和社群平臺作為反制，進而形成雙向封鎖。因此，專家認為陷入「數位孤立」的俄羅斯將更積極推動網路主權，且更倚賴中國大陸的軟硬體，甚至可能淪為其網路主權倡議的追隨者；其他獨裁國家也會對俄羅斯的處境引以為鑑，尋求數位自主，以為脫離全球網路做準備；而全球網路也因此更趨向分裂，可能形成依國界劃分、眾多無法互通的網路，甚至使用技術不相容的網路協議，或擁護不同的國際治理機構，以致全球網路互連的時代宣告終結。

二、建議事項

(一) 立即可行：研議建立多方機制，為重大網路事件奠定即時決策基礎

雖然由部分專家聯合提出的「多方利害關係人實施網路制裁」，因為制裁的本質是否屬其他利害關係人不宜涉入的國家政府行為等論點，而未能廣獲網路治理社群的支持，不過，這並不代表多方的方式或程序遭到否定，反而《麻省理工科技評論》還指出，沒人能提出比現行多方方式更好的替代方案來治理全球網路資源——儘管因為採取共識決而導致進展非常緩慢（Ball, 2022）。

為此，此份聯合聲明所建議的「建立多方機制作為因應重大或緊急網路事件的即時決策基礎」，仍可供通傳會和數位發展部參考。惟建立一個合適的多方機制需先投入資源進行研議規劃，因為除了需掌握開放、平等、透明的參與原則；由下而上的運作過程；及共識決的決策方式等細節之外，

[8] 本計畫於 7 月中旬查詢耶魯大學管理學院每日更新的全球跨國企業於俄羅斯營運狀況清單（Yale University, 2022），在其追蹤的 178 家資訊科技國際企業當中，大多是縮減、暫停業務(如我國的宏碁、華碩；美國的 Namecheap、Dell、Apple、Microsoft)，部分完全撤出俄羅斯市場(如美國 HP、GoDaddy)，只有 13 家維持原有的營運（包含我國微星科技）；而 61 家通訊服務國際廠商中，也只有 8 家維持原有的營運，其餘大多是縮減或暫停業務（如美國 Cogent、Lumen、Twitter、Meta、Alphabet）。

還需因應常被詬病的效率低落等問題（TWNIC, 2019）。而針對後者，或許至少先界定不同情境下將採行的不同機制。如重大但非緊急事件，採取真正的多方機制——從界定議題範圍、產出方案到決策執行；但緊急事件時，則回歸既有的行政程序，而多方僅扮演諮詢的角色。

此外，美國數位治理顧問 Farzaneh Badii（2022）也提醒，應避免多方機制被少數有權勢者控制。例如此份聯合聲明最後只有 4 成參與討論者簽署，另有高達 6 成未簽署，且不知他們是何許人也；加上 10 天內即從無到有火速完成所有作業，凸顯其運作和決策過程皆有問題，以致失去多方程序應帶來的不同思辨之優勢，且最終產出多項無效的建議。

(二) 中長期：於 ICANN 推動 ccTLD 政策修改，避免.tw 因政治而遭移除

ICANN 婉拒烏克蘭政府的斷網政治訴求，捍衛 ccTLD「政治中立」的治理原則，看似亦對我國有利，意即萬一中國大陸也要求撤銷我國.tw，ICANN 應會同樣基於中立立場而拒絕。然而，實際狀況恐非如此樂觀。

ICANN 表明無權撤銷俄羅斯的 ccTLD，除了其成立宗旨並未被賦予實施網路制裁的權力之外，另一方面，根據 GAC（政府諮詢委員會）的《ccTLDs 授權與管理之原則和指南》，ccTLD 屬於各國的當地議題，且發生爭議時是訴諸各國的當地法規，ICANN 維持中立立場。而 ccTLD 主要又是參照 ISO 3166 國碼標準所制定，但隸屬聯合國組織的 ISO 在 3166 國碼標準中，將我國標註為「中國大陸的一省」。

由於我國無法排除中國大陸於 GAC 援用此標準要求移除.tw 的可能性，因此，儘管難度很高，但代表我國參與 GAC 之數位發展部（原交通部和通傳會業務）仍可嘗試集結具有相似需求的其他國家，共同推動修改《ccTLDs 授權與管理之原則和指南》，藉由增加「尊重現狀、保護既有使用者權益」等條文（本計畫諮詢顧問曾更瑩律師之建議），降低.tw 因政治干預而遭移除的風險。

參考文獻

- 吳旭。(2022)。東西問丨徐培喜：互聯網為何成為俄烏衝突另一“戰場”？中新社，2022/3/13。https://www.chinanews.com.cn/gj/2022/03-13/9700491.shtml
- 經濟部 (2022)。公告「輸往俄羅斯高科技貨品清單」，擴大對俄出口管制。2022/4/6。https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=40&pid=740506&dl_DateRange=all&txt_SD=&txt_ED=&txt_Keyword=&pageindex=4&history=
- TWNIC (2019)。多方利害關係人網路治理模式。https://www.twnic.tw/mps/index.html
- Aben, E. (2022). How Is Russia Connected to the Wider Internet? CircleID, 2022/3/29. https://circleid.com/posts/20220329-how-is-russia-connected-to-the-wider-internet
- Access Now (2022a). Letter to U.S. government: Do not disrupt internet access in Russia or Belarus. 2022/3/10. https://www.accessnow.org/letter-us-government-internet-access-russia-belarus-ukraine/
- Access Now (2022b). Letter to U.K. government: Do not disrupt internet access in Russia or Belarus. 2022/5/20. https://www.accessnow.org/letter-to-uk-government-do-not-disrupt-internet-access-in-russia-or-belarus/
- Access Now (2022c). UK protects free flow of information amidst Russia sanctions. 2022/6/1. https://www.accessnow.org/uk-information-russia-sanctions/
- Akamai (2022). Actions Akamai Is Taking on Russia and Ukraine. 2022/3/7. https://www.akamai.com/blog/news/ukraine-statement
- Badii, F. (2022). How to multistakeholder wash Internet disconnection: On the multistakeholder Internet governance sanction regime. Digital Medusa, 2022/3/11. https://digitalmedusa.org/how-to-multistakeholder-wash-internet-disconnection-on-the-multistakeholder-internet-governance-sanction-regime/
- Ball, J. (2022). Russia is risking the creation of a “splinternet”—and it could be

irreversible. MIT Technology Review, 2022/3/17. https://www.technologyreview.com/2022/03/17/1047352/russia-splinternet-risk/

- Brodkin, J. (2022). Cloudflare refuses to pull out of Russia, says Putin would celebrate shutoff. Ars Technica, 2022/3/9. https://arstechnica.com/tech-policy/2022/03/cloudflare-wont-cut-off-russia-says-it-needs-more-internet-access-not-less/
- Corsoni-Husain, A. (2022). Update to EU Sanctions on Russia-Ukraine-Belarus. Harneys, 2022/6/3. https://www.harneys.com/our-blogs/regulatory/update-to-eu-sanctions-on-russia-ukraine-belarus-table/
- Directions (2022). Are Internet Sanctions a Good Idea? 2022/5/6. https://directionsblog.eu/are-internet-sanctions-a-good-idea/?fbclid=IwAR1M5Wh8j4Kn7zYGP35uOghF6DeYnWw8p1z2nxqFkJbKzmNYNp1kIZJ71i0
- Doussin, A. & Malhi, S. (2022). The UK introduces internet-related trade sanctions under the 2019 Russian Regulations. Hogan Lovells, 2022/5/6. https://www.engage.hoganlovells.com/knowledgeservices/news/the-uk-introduces-internet-related-trade-sanctions-under-the-2019-russian-regulations
- Dow Jones & Company (2022). Navigating the Breadth and Complexity of the Recent Russian Sanctions and What's Next? 2022/3/15. https://visit.dowjones.com/risk/webinar/russia-sanctions-amers/
- EC (2022). Commission Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014 . 2022/7/13 updated. https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/faqs-sanctions-russia-consolidated_en.pdf
- European Council (2022). EU sanctions in response to Russia's invasion of Ukraine. https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/
- Farber, D. J. & Gillmor, D. (2022). Cutting Russia off from the internet would be deeply problematic. Nikkei Asia, 2022/4/15. https://asia.nikkei.com/Opinion/Cutting-Russia-off-from-the-internet-would-be-dee

ply-problematic

- Fedorov, M. (2022a). Letter from the Vice Prime Minister of Ukraine to ICANN. 2022/2/28. https://eump.org/media/2022/Goran-Marby.pdf
- Fedorov, M. (2022b).Letter from the Vice Prime Minister of Ukraine to RIPE NCC. 2022/3/2. https://www.ripe.net/publications/news/announcements/request-from-ukrainian-government.pdf
- GAC (2005). Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains. https://gac.icann.org/principles-and-guidelines/principles-cctlds.pdf
- Greig, J. (2022). Internet service provider Cogent cutting off access to Russian customers. ZDNet, 2022/3/5. https://www.zdnet.com/home-and-office/networking/internet-service-provider-cogent-cutting-off-access-to-russian-customers/
- Groothuis, B. et al. (2022). Multistakeholder Imposition of Internet Sanctions. 2022/3/10. https://www.pch.net/resources/Papers/Multistakeholder-Imposition-of-Internet-Sanctions.pdf
- Holen, H. P. (2022). Response from Managing Director of the RIPE NCC. https://www.ripe.net/publications/news/announcements/response_to_ua_gov_-_10march.pdf
- ICANN (2015). Three Layers of Digital Governance Infographic. https://www.icann.org/news/multimedia/1563
- ISOC (2022). US, EU, and G7 Commitment Will Slow the Splinternet, But More Work Needed. 2022/4/14. https://www.internetsociety.org/blog/2022/04/us-eu-and-g7-commitment-will-slow-the-splinternet-but-more-work-needed/
- Kleinwächter, W. (2022). World Economic Forum Davos 2022: War in Ukraine, Metaverse und Splinternet. 2022/5/30. https://circleid.com/posts/20220530-world-economic-forum-davos-2022-war-in-ukr

aine-metaverse-und-splinternet

- Kurbalija, J.(2016). An Introduction to Internet Governance. https://www.diplomacy.edu/wp-content/uploads/2021/12/AnIntroductiontoIG_7th-edition.pdf
- Kurbalija, J. (2022). The Ukraine crisis may shape the future of the internet. DiploFoundation, 2022/04/15. https://www.diplomacy.edu/blog/the-ukraine-crisis-future-of-internet/
- Lumen. (2022). Lumen's Readiness to Meet Global Events. https://news.lumen.com/RussiaUkraine
- Marby, G. (2022). The Response Letter of ICANN to Ukraine's Request to Disable Russia's ccTLDs. https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf
- Meyer, D. (2022). Russia's denying that it's about to cut itself off from the global internet, but it's acting a lot like it. Fortune, 2022/3/7. https://fortune.com/2022/03/07/russia-runet-disconnect-ukraine-dns-chernenko-letter/
- Moss, S. (2022). London Internet Exchange disconnects Megafon and Rostelecom. DCD, 2022/3/14. https://www.datacenterdynamics.com/en/news/london-internet-exchange-disconnects-megafon-and-rostelecom/?fbclid=IwAR0aunEHrvdDjskL0M6UmYXvxlerlop6odBRUB4Qvy3ZZCOL4_ss_E28sL0
- Mueller, M. (2022). ICANN, Ukraine and Leveraging Internet Identifiers. CircleID, 2022/3/1. https://circleid.com/posts/20220301-icann-ukraine-and-leveraging-internet-identifiers
- Murphy, K. (2022a). Soviet Union "no longer considered eligible for a ccTLD", ICANN chair confirms. Domain Incite. 2022/3/11. https://domainincite.com/27636-soviet-union-no-longer-considered-eligible-for-a-cctld-icann-chair-confirms
- Murphy, K. (2022b). GoDaddy stops selling .ru domains, commits money to support Ukraine. Domain Incite, 2022/3/3.

https://domainincite.com/27602-godaddy-stops-selling-ru-domains-commits-money-to-support-ukraine

- OFAC (2022) Russian Harmful Foreign Activities Sanctions Regulations 31 CFR part 587, General License NO. 25B. 2022/6/2. https://home.treasury.gov/system/files/126/russia_gl25b.pdf
- OFSI (2022). General Licence INT/2022/1875276. 2022/5/30. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1079707/30.05.2022_INT20221875276_Telecoms_and_News_General_Licence_Publication_notice.pdf
- Prince, M. (2022). Steps we've taken around Cloudflare's services in Ukraine, Belarus, and Russia. The Cloudflare Blog, 2022/3/7. https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/
- RIPE NCC (2022). The RIPE NCC and Ukraine/Russia. Last updated: 12 April 2022. https://www.ripe.net/participate/member-support/the-ripe-ncc-and-ukraine-russia
- Satariano, A. & Hopkins, V. (2022). Russia, Blocked From the Global Internet, Plunges Into Digital Isolation. The New York Times, 2022/3/7. https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html
- Stolton, S. (2022). Ukraine minister pleads to expand 'digital blockade' on Russia. Politico, 2022/3/29. https://www.politico.eu/article/ukraine-digital-transformation-mykhailo-fedorov-russia-blockade/
- Techstony (2022). Digital War: What Sanctions Were Imposed on Russia by Internet Companies From the USA. 2022/3/5. https://techstony.com/digital-war-what-sanctions-were-imposed-on-russia-by-internet-companies-from-the-usa/
- Timberg, C. (2022). Internet experts suggest ways to selectively block Russian military and propaganda sites. The Washington Post, 2022/3/10. https://www.washingtonpost.com/technology/2022/03/10/internet-russia-sanctions-proposal/

- U.S. Department of the Treasury (2022). Russian Harmful Foreign Activities Sanctions. https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/russian-harmful-foreign-activities-sanctions
- Vaughan-Nichols, S. (2022). Breaking Russia's internet backbone. ZDNet, 2022/3/10. https://www.zdnet.com/article/breaking-russias-internet-backbone/
- Watanabe, N. (2022). National 'splinternets' already here, Web pioneer O'Reilly says. Nikkei Asia, 2022/4/19. https://asia.nikkei.com/Editor-s-Picks/Interview/National-splinternets-already-here-Web-pioneer-O-Reilly-says
- White House (2022). FACT SHEET: United States, G7 and EU Impose Severe and Immediate Costs on Russia. 2022/4/6. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/
- Wilde, G. & Sh erman, J. (2022). Putin’s internet plan: Dependency with a veneer of sovereignty. Brookings Institution, 2022/5/11. https://www.brookings.edu/techstream/putins-internet-plan-dependency-with-a-veneer-of-sovereignty/
- Yale University (2022). Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain. Retrieved July, 5, 2022. https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain
- York, D. (2022). What Is the Splinternet? And Why You Should Be Paying Attention. ISOC, 2022/3/23. https://www.internetsociety.org/blog/2022/03/what-is-the-splinternet-and-why-you-should-be-paying-attention/
- Zhu, L. (2022) A Revisit of the Domain Name System After Russia’s Invasion of Ukraine. Congressional Research Service, 2022/3/23. https://crsreports.congress.gov/product/pdf/IN/IN11898/2

第四章 案例研析(2) 解讀《未來網際網路宣言》

第一節 前言

美國政府於 2022 年 4 月 28 日在白宮召開《未來網際網路宣言》（The Declaration for the Future of the Internet, DFI）發布會，共有美、英、日、澳、歐盟、烏克蘭和我國等 61 個政府簽署，承諾將促進一個開放、自由、全球化、可互通、可靠和安全的網際網路，以因應威權政府支持及縱容網路惡意行為、運用數位工具壓制言論自由、侵害人權；以及線上平臺高度掌控數位經濟、持有巨量個資隱私、助長散播非法及有害線上內容等挑戰（U.S. Department of State, 2022）。

白宮官員表示，中俄等威權主義國家試圖創造分裂的網路，且共同成為網路政策危險新模式的領導者，所以，DFI 正是要挽救網路免於分裂，確保世界一個網路的願景。後續美國也將持續尋求更多志同道合的國家加入 DFI，並樂於和相關的公民團體及非營利組織建立夥伴關係（White House, 2022）。

DFI 公開發布後，其願景和承諾廣獲各界肯定，不過，在制定程序和實施機制等層面，卻引發諸多質疑。而中國大陸除了嚴厲抨擊 DFI 是美方陣營煽動網路空間對抗的最新例證外，還成立新的「世界互聯網大會『國際組織』」加以反擊（新華網，2022b）。

我國是由時任行政院政務委員唐鳳應邀代表線上出席白宮的發布會，並簽署 DFI。身為應當履行承諾的簽署國，我國需對 DFI 有相當程度的了解。為此，本章首先簡介 DFI 的內文重點、當前簽署情況和推動方式，以及近期相近和對立的國際倡議，接著探討 DFI 的政治意涵及各界對於 DFI 的評論，最後並提出我國相關建議以供政策參考。

第二節 宣言內容重點

一、重申網路的承諾

網路的宏偉承諾源自其開放的「網路的網路」（network of networks）設計，以提供所有人一個互連的通訊系統；且網路單一識別碼系統的安全穩定運作，自始即以多方利害關係人的方式管理，以避免網路分裂。然而，過去二十年來，此願景出現嚴峻的挑戰，包括：

(一) 來自威權政府的挑戰

數位工具日益被用於壓制言論自由，及否定其他人權和基本自由。國家支持或縱容的惡意行為持續上升，包括散播假訊息和勒索軟體等網路犯罪行為，不但影響關鍵基礎設施的安全與韌性，也對重要的公私財產構成風險。許多國家還建立網路圍牆、採取封網等技術措施，並以違反國際人權的方式，限制取得新聞、資訊與服務。部分政府更單獨或透過私部門，試圖濫用網路治理及相關流程的開放性，以推進其封閉的願景。

(二) 來自線上平臺的挑戰

曾是去中心化的網路經濟已變得高度集中，許多人擔憂其隱私和個資安全。線上平臺增加非法或有害內容的傳播，這些內容可能威脅個人安全，並助長極端化和暴力。假訊息和外國惡意活動被用來製造社會分裂和衝突，且破壞對人權及民主制度的尊重和保護。

二、我們的願景

我們相信應透過未來網路的共同願景，迎向這些挑戰。簽署夥伴承諾維護「開放、自由、全球化、可互通、可靠和安全」的未來網路，以確保網路能夠強化民主原則、人權和基本自由，促進公平競爭的數位經濟。網路應以單一、去中心化的「網路的網路」方式運作，但又全球可及；並應

透過多方利害關係人方式，由政府和相關機關，攜手學術界、公民社會、民間部門、技術社群等共同治理。此外，數位科技也應用於促進社會具備以下的特質：

- 保護及促進所有人的人權、基本自由及福祉。
- 透過提升網路的普及性、可負擔性，及個人使用網路的技能，讓所有人皆能無所不在地連網。
- 個人及企業可以相信所使用數位科技的安全性及保密性，且其隱私受到保護。
- 任何規模的企業均可在公平競爭的生態系統中，進行創新、競爭並憑其優勢蓬勃發展。
- 基礎設施應以安全、可互通、可靠與永續的方式設計。
- 科技應被用於促進多元主義、言論自由、永續發展、共融的經濟成長，並對抗全球氣候變遷。

三、推動願景的原則

宣言夥伴將採取下列關鍵原則（分成 5 大類共 23 個子項），透過現有的多邊和多方利害關係人論壇，在全球推廣這些原則，並將原則轉化為具體的政策和行動，同時也尊重各自司法管轄權範圍內的監管自主權，及各自遵守相關國內法和國際法的義務。這些原則不具有法律約束力，但應作為公共政策制定者，以及民眾、企業和公民團體的參考。

(一) 保護人權和基本自由

- 國內相關機構執行權力時，無論線上或線下，皆應尊重包括《世界人權宣言》（Universal Declaration of Human Rights）所載的人權，以及尊重法治、正當性目的、不恣意武斷、有效監督及透明性。

- 促進線上安全並持續加強打擊線上暴力，包括基於性別與性暴力的行為，以及兒童性剝削；讓網路成為對所有人都安全的地方，尤其是女性、兒童、青少年。
- 促進人人安全且平等地使用網路，消弭基於性別、種族、膚色、族群、國家或社會出身、遺傳特徵、語言、宗教或信仰、政治或其他意見、原住民身分、財產、出生、身心障礙、年齡、性別認同或取向等歧視。
- 重申政府、主管機關和線上平臺等數位服務，於採取減少線上非法及有害內容與活動的行動時，會符合國際人權法規的承諾，包括言論自由權，並鼓勵多元意見及多元主義，讓民眾免於言論審查、騷擾或恐嚇的恐懼。
- 保護及尊重數位生態系統內的人權與基本自由，並遵照國際人權法規，對侵犯和踐踏人權的行為，提供有意義的救濟措施。
- 避免網路或演算法工具及技術，被誤用或濫用於不符合國際人權原則的監聽、壓迫與鎮壓，包括開發社會評分卡，或其他的國內社會控制、證實犯罪前的拘留與逮捕等機制。

(二) 推動單一全球網路

- 避免政府全面或部分強制關閉網路，或限制網路連線（接取）。
- 避免封鎖或限制取得網路合法的內容、服務及 Apps，以符合包括國際人權法在內相關法律所適用的網路中立（Net Neutrality）原則。
- 基於我們共享的民主、開放和關懷等價值觀，以信任致力實現資料自由流通所帶來的益處。
- 促進在研究、創新和標準制定方面的合作，鼓勵透過國際論壇分享安全威脅的相關資訊，並重申我們對網路空間採取負責任國家行為框架的承諾。

(三) 推動包容和可負擔的網路連線

- 推動個人和企業可負擔、具包容性及可信賴的網路連線，並努力消弭全球數位落差，以確保全體人類能從數位轉型中受益。
- 支持數位識讀、技能取得及發展，使個人能夠克服數位落差，安全地使用網路，實現數位經濟的經濟與社會潛能。
- 強化網路上不同文化，以及多語內容、資訊和新聞的呈現，此舉應有助於多元化的公共論述、促進更廣大的社會與數位包容、強化因應虛假訊息及錯誤訊息的韌性，以及擴大民主進程的參與。

(四) 促進對數位生態系統的信任

- 共同合作打擊網路犯罪，包括運用網路的傳統犯罪，並嚇阻惡意網路活動。
- 確保政府及相關單位依照法律規定使用個人資料，且相關作為符合國際人權法規。
- 保護個人隱私、個人資料、電子通訊的機密性，及個人電子終端設備上的資訊，並符合保護公共安全和適用的國內和國際法規。
- 推動消費者保護，尤其是弱勢消費者，避免他們遭到網路詐騙、其他網路上的不公平行為，以及購買網路上危險與不安全的商品。
- 推廣及使用值得信賴的網路基礎設施與服務供應商，所依據的風險評估應包含技術和非技術因素，以確保網路安全。
- 避免透過網路破壞選舉的基礎結構、選情和政治進程，包括透過訊息操弄活動。
- 支持以規則為基礎的全球數位經濟，以強化線上市場的貿易、競爭和公平，使公司和企業能以其優勢進行競爭。
- 透過合作以發揮科技對抗氣候變遷及保護環境的最大效果，同時儘

可能減少網路和數位科技的環境足跡。

(五) 強化多方利害關係人的網路治理

- 保護和強化網路治理的多方利害關係人系統，包括主要技術協定和其他相關標準及協定的開發、部署與管理。
- 避免破壞攸關網路一般可用性及完整性的技術基礎設施。

第三節　宣言夥伴和推動方式

一、宣言夥伴

DFI 以「夥伴」稱呼「簽署者」或「簽署國」。4 月 28 日發布會所公布的「夥伴」共計 61 個，除了歐盟之外，其餘包含美、英、日、澳、烏克蘭和我國在內的 60 個，皆為國家政府（如下圖 4-1）。此外，正如美國國務院表示，DFI 會持續開放給願意承諾且實施其願景和原則的「政府」或「相關當局」加入（U.S. Department of State, 2022），因此，韓國於 5 月 21 日美國總統拜登在首爾與韓國總統尹錫悅舉行峰會時加入 DFI（Kim, 2022）。總計截至本報告撰寫期間，DFI 共有 62 個「夥伴」。



資料來源：European Commission

圖 4-1 《未來網際網路宣言》夥伴（簽署國）

美國喬治亞理工學院「網路治理計畫」創辦人 Milton Mueller（2022）教授表示，DFI 基本上是「跨大西洋的倡議」，亞洲、拉丁美洲、加勒比海和非洲只有少數國家簽署，且中東、南亞和東南亞國家是大規模缺席。美

國布魯金斯研究所（Brookings Institution）也指出，簽署國主要是歐盟的 27 個成員國，且 G20 或 OECD 的民主國家中，智利、墨西哥、挪威和南非等國均未加入（Kerry, 2022）。

我國是由時任行政院政務委員唐鳳（2022）代表簽署 DFI。她於會後透過臉書表示，如何營造與維護促進民主和社會經濟發展，以及保障所有人權益的網路環境，不僅是 DFI 成員國的共同願景，也是臺灣能夠有所貢獻的議題。外交部（2022）也指出，我國政府始終堅持「寬頻是基本人權」，並認為對所有人完全開放且不受控管的言論環境，是讓數位民主開花結果的土壤。因此，臺灣積極與美國等理念相近國家合作，推動 DFI 願景。

至於為何韓國沒有一開始就加入 DFI，《外交家》（The Diplomat）雜誌認為，可能和韓國電信業者 SK Broadband 及美國串流影音業者 Netflix 的分攤網路流量驟增成本費訴訟有關，且韓國也推動《電信事業法》（Telecommunications Business Act）修法，擬強制大型內容業者支付網路使用費。但韓國後來得以加入 DFI，顯示兩國領導人原則上同意在近期內解決此項紛爭（Kim, 2022）。

二、推動方式

有關 DFI 的推動方式，除了 DFI 文中提及「透過現有的多邊和多方利害關係人論壇在全球推廣」外，美國官方尚未就此提出完整的說明，這也是 DFI 遭負面評價的其一主因（詳本章第六節）。本計畫僅就 4 月 28 日白宮記者會的問答（White House, 2022）、美國國務卿 Blinken（2022）6 月 7 日的媒體訪談，以及 DFI 的主要推手——白宮科技與競爭政策特別助理 Tim Wu，和國安會國際經濟與競爭力主任 Peter Harrell 於 6 月 22 日布魯金斯研究所（Brookings Institution, 2022）座談會上的言談，彙整出美國截至目前 DFI 的如下推動方式，在方向上除了爭取更多的國際合作及支持外，美國也要以身作則，進行落實 DFI 願景的相關措施。

(一) 對外推動方式

1. 透過現有多邊和多方論壇推廣 DFI 原則

Tim Wu 等美國白宮官員提及的多邊場合或組織如下，有些並附舉例說明。至於 DFI 所指的多方利害關係人論壇，則仍尚未著墨。

- 美歐貿易和科技委員會（U.S.-EU Trade and Technology Council, TTC）：例如討論如何共同因應俄羅斯在全球散播對烏開戰的假訊息；及會後聯合聲明重申擁護 DFI 願景，並將其原則付諸實踐。
- 印太經濟框架（Indo-Pacific Economic Framework, IPEF）：無說明。
- 網路自由聯盟（Freedom Online Coalition, FOC）：FOC 價值觀和 DFI 相近，且美國將於 2023 年擔任 FOC 輪值主席，可望共同推動 DFI。
- 國際電信聯盟（International Telecommunication Union, ITU）：負責國際通訊技術事務的聯合國 ITU，對於科技如何被使用扮演要角。美國將努力爭取其候選人 Doreen Bogdan-Martin 贏得 9 月份 ITU 秘書長選舉，進而於未來合作推動 DFI。
- G7 和其他聯合國組織：美國將 DFI 視為可以在其他場合中發揮作用的平臺，例如作為 G7 聯合聲明的基礎協議，以及和聯合國機構合作的基礎。

其實 DFI 文末也列舉擬合作的多邊場合或組織，除上述外，還有 G20（二十國集團）、經濟合作暨發展組織（Organisation for Economic Cooperation and Development, OECD）、世界貿易組織（World Trade Organization, WTO），以及屬於多方論壇的 ICANN 和 IGF；並樂於和公民團體及非營利組織建立夥伴關係。惟除了點名外，就無任何訊息了。

2. 其他既有援助機制

- 資訊共享：持續透過美國國土安全部和轄下網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）的機制，共享網路安全和維運資訊。

- 提供工具和技術：持續透美國國務院和轄下美國國際開發總署（United States Agency for International Development, USAID）的計畫，為各地獨立媒體和非營利組織提供反審查的工具和技術。

(二) 美國國內相關措施

1. 成立「網路空間暨數位政策局」

美國國務院於 4 月初新成立「網路空間暨數位政策局」（Bureau of Cyberspace and Digital Policy，簡稱 CDP 局），該局特別設有「數位自由」部門，以確保科技用於促進自由和民主。CDP 局將由參議院確認的無任所大使領導，後續將透過外交層面推動 DFI，並提出具體措施。

2. 強化美國的隱私保護

美國總統拜登在 3 月的國情咨文中即表示，要強化美國的隱私保護，且隱私保護也是 DFI 的承諾，因此，拜登政府樂見美國兩黨對於推動隱私法案有所進展（參眾兩院已聯合發布《美國資料隱私和保護法》草案[9]）。

3. 推動寬頻基礎建設

拜登政府斥資 650 億美元興建的寬頻基礎設施，已經開始進行。另據《美國之音》報導，白宮還努力和網路業者協商，以確保美國家庭的每月上網費不超過 30 美元。此外，美國商務部國家電信暨資訊管理局(National Telecommunications and Information Administration, NTIA）於 5 月份也宣布啟動 450 億美元的「全民網路」（Internet for All）計畫，以為所有美國人提供負擔得起的高速網路（孫承，2022）。

[9] 美國參眾兩院於 6 月 3 日聯合發布《美國資料隱私和保護法》（the American Data Privacy and Protection Act, ADPPA）草案，這是首個獲得兩黨和兩院支持的國家隱私草案，且 7 月已有更新版本（Edelman, 2022）。

第四節 近期相近和對立的國際倡議

一、相近的國際倡議

(一) 歐洲數位十年之數位權利和原則宣言

歐盟執委會（European Commission, EC）於 DFI 相關新聞稿指出，**DFI** 符合歐盟強力支持的權利和原則，並**以《歐洲數位十年之數位權利和原則宣言》**（European Declaration on Digital Rights and Principles for the Digital Decade）**為基礎**。此份宣言（草案）是 EC 於 2022 年 1 月 26 日提出，草案目前仍在審理討論中。EC 表示，宣言一旦獲得歐洲議會和歐盟理事會的聯合簽署，宣言所制定的數位轉型方法將使歐盟成為國際舞臺的領導者（EC, 2022a；2022b）。

宣言旨在推動數位轉型的歐洲方式——以人為中心、以歐洲價值觀為基礎，並造福所有的個人和企業。EC 指出，此宣言將指引歐盟推動包容、繁榮和永續的社會，以及歐盟和成員國的數位政策和法規，還可作為數位科技公司的指南。而後歐盟的行動、工作、和全球夥伴的互動，都將展現宣言中如下所列的 **6 大數位權利和原則**。

- **將人民及其權利置於數位轉型的中心**
  數位科技應保護人民的權利，支持民主，並確保所有參與者負責任和安全地行事。歐盟將在全世界推廣這些價值觀。

- **支持團結和包容**
  數位科技應該團結而不是分裂人民。每個人都應該能夠獲取網路連線、數位技能、數位公共服務，以及公平的工作條件。

- **確保線上自由選擇權**
  人民應該有權在網路上做出自己的知情選擇，包含自由選擇所使用的數位服務。此外，也要確保演算法和人工智慧使用時的透明度，

且是在充分尊重基本人權的情況下使用。

- **促進數位公共領域的參與**

  支持數位科技的開發和最佳使用，以激勵公民參與民主進程，並持續維護線上基本權利，尤其是言論和資訊自由。

- **提高個人的安全、保障和賦權**

  每個人都應該能夠獲取安全、可靠和保護隱私的數位技術、產品和服務；應該打擊網路攻擊和資料外洩等網路犯罪，以保護所有人的利益不受侵害。

- **促進永續的數位未來**

  數位設備應支持永續性和綠色轉型。數位產品和服務的設計、生產和處置方式，應減少對環境和社會的影響。人民也需了解他們的設備對環境和能源消耗的影響。

《政客》(Politico)雜誌指出，雖然這些原則大多重複歐盟近年來已經在做的事情，也就是將人權和歐洲價值觀置於網路治理政策或法規的核心，但隨著華盛頓和北京對國際標準組織和外交機構（如聯合國）的影響力越來越大，歐盟期盼藉此宣言提高在國際數位治理相關談判的話語權，甚至是嘗試將歐洲的網路治理方法轉變為全球標準。此外，此宣言還能對內向歐洲公民宣導其線上權利，因為EC調查發現，40%的歐洲公民不知道他們擁有言論自由、線上隱私等網路權利（Scott & Kayali, 2022）。

二、 對立的國際倡議

(一) 中俄聯合聲明

中、俄兩國元首於2022年2月4日在北京舉行會談，並於出席北京冬季奧運開幕典禮後，發表《中華人民共和國和俄羅斯聯邦關於新時代國際關係和全球可持續發展的聯合聲明》，聲明中包含下列網路治理主張：

雙方支持打造國際化的互聯網治理體系，認為各國平等享有互聯網

治理權，主權國家有權管控和保障本國網絡安全，任何企圖限制國家網絡主權的行為不可接受，應促進國際電信聯盟在解決有關問題上發揮更加積極的作用（新華網，2022a）。

布魯金斯研究所認為，此聯合聲明和 DFI 形成明顯對比。兩國所擁護的，是以安全和控制為重點的網路主權，且「本國網絡」代表支持全球網路的分裂，並為了「保障安全」而推廣國家防火牆。此外，「國際化」和 ITU 意味讓政府控制網路，而不是由跨行業和跨國界的網路技術系統，以去中心化的方式治理網路（Kerry, 2022）。

(二) 中國成立網路國際組織

中國大陸 7 月 12 日在北京成立「世界互聯網大會國際組織」（World Internet Conference organization, WICO），以推動國際社會建構「網絡空間命運共同體」，並承擔化解國際社會分歧、凝聚共識等「新歷史使命」。中國大陸國家主席習近平的祝賀信函指出，這是「深化網絡空間國際交流合作的重要舉措……網絡空間未來應由世界各國共同開創。中國願同國際社會一道……推動構建更加公平合理、開放包容、安全穩定……的網絡空間」（新華網，2022b；人民網，2022）。

根據新華網（2022b）報導，WICO 已有來自約 20 國的近百個網路相關的機構、組織、企業及個人加入，成為 WICO 的創始會員，當中包括知名的企業龍頭、具代表性的產業組織，以及對網路發展有卓越貢獻的知名人士等。不過，中國大陸官方和媒體並沒有公布上述創始會員名單，以及 WICO 的組織章程。

《政客》報導指出，北京在此刻將一個自家於 2014 年起主辦的「年度會議」（世界互聯網大會），轉變成一個致力於推動全球網路發展和治理的「常設國際組織」，是對 DFI 的反擊，並顯示北京正增強力道以改變全球網路的規則和標準，強化在全球推動國家控制網路的理念。而儘管「世界互聯網大會」已經風光不再，但從中國大陸日益擴大在聯合國主要機構的影響力來看，美方陣營對於 WICO 的發展應該保持警戒（Kine, 2022）。

第五節 宣言的政治意涵

一、對抗中俄數位威權和網路分裂

雖然 DFI 的全文並未點名任何國家，不過，出現獨裁政府、分裂網路、社會評分卡等措詞，其劍指中俄已是昭然若揭。此外，美國白宮官員於 DFI 發布會前的背景說明會上，更是直指中俄兩國。官員表示，中俄等威權主義國家試圖創造分裂的網路，俄羅斯等國壓制言論自由、審查新聞網站、干預選舉、散播假訊息，並剝奪其公民的人權；俄羅斯還和中國大陸等審查最嚴格的國家，共同成為網路政策危險新模式的領導者。而 DFI 正是要挽救網路免於分裂，扭轉分裂的趨勢，確保世界一個網路的願景（White House, 2022; Kerry, 2022; Bose, 2022）。

白宮國安會國際經濟與競爭力主任 Peter Harrell 於布魯金斯研究所的座談會上也指出，世界各國的專制政府正在相互學習，加強推動他們所認為的網路模式。相對的，全球民主不論是網路空間或實體世界皆處於衰退，俄烏戰爭更是凸顯民主受到嚴峻挑戰。因此，我們應該積極反對並遏止來自中俄且已散播到許多國家的數位威權主義模式，這正是 DFI 的價值和工作要項（Brookings Institution, 2022）。

二、警告或拉攏搖擺不定的國家

不過，《經濟學人》（The Economist, 2022）認為，DFI 的目標並不是中俄兩大強權，因為他們根本不在乎 DFI 的內容為何。DFI 的真正目的，在於「警告」其他想仿效中俄獨裁方式的國家。

布魯金斯研究所研究員 Alex Engler（2022）也主張 DFI 並非劍指中俄。他表示，拜登政府深知中俄不會理會 DFI，所以，試圖影響和「拉攏」搖擺不定的民主國家，才是 DFI 的真正目標。如簽署國當中的哥倫比亞、尼日共和國、匈牙利、以色列等（甚至包括美國本身），都曾有可疑的網路越

界行為，但它們是為了維護民主而持續奮鬥，而不是如中俄般的系統性數位威權主義。在此情況下，如果 DFI 的其他夥伴能夠相互支持，這些簽署國才不會傾向數位威權主義。正如美國國家安全顧問蘇利文（Jake Sullivan）在白宮發布會上強調，DFI 是「關於我們支持什麼願景……是關於簽署者的行為……而不是世界上的其他地方」。

三、堅定民主國家的信念

美國美利堅大學科技法律計畫主任 Ya’ara Barnoon（2022）指出，DFI 有助於堅定民主國家的信念，為數位政策「定位」。她表示，世界各地的獨裁政權正以合法的網路安全和假訊息等疑慮為藉口，通過危害公民隱私、核心公民權利和政治權利的法規。另一方面，民主國家也正在努力解決有害內容和網路安全等問題，此時若沒有指導性的原則，政策鐘擺就容易產生偏離，例如連美國前總統川普都曾建議關閉網路，以因應恐怖分子的線上招募活動。由此凸顯當面臨嚴峻的網路挑戰時，即使是網路自由開放的支持者，也會迷失在開放系統和封閉系統的拉鋸戰中。因此，DFI 的原則有助於在這些權衡中，做出正確的抉擇。

四、展現美國重回國際舞臺

《政客》報導認為，DFI 是拜登政府對於美國重回國際舞臺和重拾國際領導力的展現（Scott, 2022）。布魯金斯研究所研究員 Alex Engler（2022）也指出，有別於美國前兩屆總統的外交政策（歐巴馬時期的加強與中俄關係、川普時期的「美國優先」），DFI 顯示拜登政府對於引領國際網路民主發展有濃厚興趣。

不過，嚴格來說，DFI 雖然由美國發起，但內文並非完全由美國主導。綜合多位網路治理專家的說法，原本白宮擬於 2021 年 12 月所主辦的首屆全球民主峰會上，宣布成立「未來網際網路『聯盟』」，但消息一出即引發各界質疑，因為「聯盟」的訴求重點似乎只在於成員國之間的互利互惠，

以及前總統川普時期的「乾淨網路計畫」，卻沒有強調網路發展的自由、人權、民主等重要價值觀。因此，美國取消原定的發布計畫，改為和其他政府進行協商（Mueller, 2022；Kleinwächter, 2022；Mok, 2022）。

而經協商轉變成的 DFI，也反映各國的不同利益，如加上「尊重各自司法管轄權範圍內的監管自主權」等文字，而且如前所述，歐盟執委會於 DFI 相關新聞稿指出，DFI 是以《歐洲數位十年之數位權利和原則宣言》（草案）為基礎。這就是為什麼 2 位白宮官員 Tim Wu 和 Peter Harrell 皆強調，DFI 是國際外交的共同努力，是由核心盟友共同完成（Brookings Institution, 2022）。

第六節 對宣言的評論

一、獲肯定之處

(一) 從承諾、原則到簽署國皆獲肯定

DFI 承諾的願景及其原則廣獲各界肯定。如美利堅大學網路治理實驗室研究員 Fiona Alexander（2022）指出，一個基於開放、包容、人權和民主的網路願景，是非常值得追求和讚揚的目標。數位人權組織 Access Now（2022）也表示認同宣言的避免封網、建構包容性的數位能力等原則。

歐洲網路治理論壇（EuroDIG）創辦人暨丹麥 Aarhus 大學榮譽教授 Wolfgang Kleinwächter（2022）則稱許 DFI 能夠正視來自西方民主國家的平臺挑戰，以及支持關鍵網路資源管理的中立性等原則。此外，美國喬治亞理工學院「網路治理計畫」創辦人 Milton Mueller（2022）教授表示樂見簽署國抵制日益增長的數位威權主義。

而讚揚簽署國的，還有維基媒體基金會副總裁 Rebecca MacKinnon（2022）。她指出，雖然許多民主國家也未完全善盡保護網路自由之責，但和威權國家的最大區別在於「我們可以為此在網路上自由且無虞地批評政府」。因此，簽署 DFI 的政府值得肯定，他們讓公民社會有具體機會督促其信守承諾，所以，「接下來我們有很多工作」。

(二) 內容雖為老調重彈但符合當前需求

Kleinwächter（2022）教授表示，雖然 DFI 的願景和原則在過去的國際議程都曾出現，例如：2005 年聯合國資訊社會世界高峰會（World Summit on the Information Society, WSIS）的《突尼斯議程》（Tunis Agenda）、2014 年在巴西聖保羅通過的《網路世界多方利害關係人聲明》（NETmundial Multistakeholder Statement），但是這些原則卻被日漸忽視。所以，在當前數位威權主義興起和網路面臨分裂之際，重申這些原則有其時代意義。

Barnoon（2022）主任也指出，雖然宣言的語言令人覺得熟悉，但全球的網路情境已經發生變化，尤其在面臨嚴峻的網路挑戰時，即使是民主國家也可能推出偏離的政策，而 DFI 所強調的原則，正是因應這些棘手治理問題不可或缺的基本價值。因此，DFI 完全符合當前需求。

(三) 位階雖降但更具包容性和建設性

Mueller（2022）和 Kleinwächter（2022）兩位教授皆認為，雖然此倡議從「聯盟」降級為「宣言」，會導致效果弱化，但由於網路代表一種普及的基礎設施，如果採用具有排他性、且易造成地緣政治分裂的「聯盟」，反而會有所矛盾。因此，基於民主價值觀的「宣言」，其實是更具建設性和包容性的作法，只要是認同或支持 DFI 價值觀者，都有機會加入，不會邊緣化或排斥任何人。

(四) 有助於改善施政

Barnoon(2022)主任認為，DFI 已經展現其具體價值，如近幾個月來，美國在改善隱私（參眾兩院已聯合發布《美國資料隱私和保護法》草案）和確保國際資料流通（美國和歐盟已就新的《跨大西洋資料隱私框架》Trans-Atlantic Data Privacy Framework 達成協議）等方面，都取得實質進展。此外，如前述 MacKinnon（2022）副總裁指出「公民社會有具體機會督促政府信守承諾」，顯示部分公民團體將以 DFI 作為監督政府施政的依據，進而可望發揮改善施政的正面效益。

二、遭質疑之處

(一) DFI 制定程序違背其多方方式的承諾

「強化多方利害關係人的網路治理」是 DFI 的承諾及五大推動原則之一，因此，其制定程序沒有採取多方方式，引發諸多抨擊。Access Now（2022）甚至指其為黑箱作業，不但制定者不詳，也沒有公開向公民社會徵求意見，以致 DFI 缺乏非政府利害關係人的聯合支持，喪失原本可望帶

來有意義變革的機會。

Alexander（2022）研究員指出，美國率先採取多方方式治理網路，促成當今全球網路和數位經濟的蓬勃發展，是一項突破性的成就，這應該讓美國更有理由繼續沿用。然而，DFI 的制定程序卻是不透明、封閉的、僅限政府參與，顯然違背 DFI 的承諾與原則，不但引發拜登政府的誠信問題、美國喪失引領網路決策方式的機會，而且也會讓威權政府加以仿效。

Kleinwächter（2022）教授亦表示，DFI 以「由上而下」及僅有政府單位參與的方式制定，是一大弱點，也和 DFI 的承諾自相矛盾，且破壞多方方法的可信度。他強調，以多方方式制定全球網路宣言並非不可行，而是已有成功案例，如 2014 年的《網路世界多方利害關係人聲明》，就是由全球數百名的多方利害關係人參與起草和簽署，並發揮具體影響力，促成 2016 年 IANA（Internet Assigned Numbers Authority，網路號碼分配機構）監管權從美國商務部移轉至 ICANN 的多方社群。

(二) 加入 DFI 的資格和方式不明

Kleinwächter（2022）教授指出，雖然 DFI 已有超過 60 個政府簽署，且載「樂與相關的社會公民團體建立夥伴關係」，但是政府如何加入 DFI、需具備什麼資格，又其他非政府關係人將如何參與 DFI，都無相關訊息。

ISOC 前政策策略與發展主任 Konstantinos Komaitis（2022）也對 DFI 簽署國的資格提出質疑。他表示，如果 DFI 信守其捍衛網路民主的承諾，就應該拒絕英國的簽署，因為英國《網路安全法》（Online Safety Bill）是最不民主的法規之一。不過，Mueller（2022）教授對此有不同看法。他指出，雖然認同 Komaitis 對英國法規的評價，但就 DFI 而言，一個國際外交宣言不能也無法基於一國的特定政策，就判斷其是否具備加入的資格。

白宮官員 Harrelly 對於簽署國的資格問題，也有所回應。他表示，DFI 希望擁有一個既具包容性又能鼓勵提高民主標準的成員資格，後續會持續尋求願意落實 DFI 承諾，且沒有斷網或封閉平臺等不良紀錄的國家加入

（Brookings Institution, 2022）。

(三) 沒有約束力和執行動力

Access Now（2022）認為，不具法律約束力的 DFI，最終只會淪為空談，正如國際間既有的許多全球性原則和聲明一樣，皆無實質進展。美國重要智庫——外交關係協會（Council on Foreign Relations, CFR）也指出，現今的網路更不自由、更分裂、更不安全，凸顯開放、可靠和安全的全球網路烏托邦願景尚未實現，且未來也不太可能藉由 DFI 實現，因為沒有約束力的承諾，無法阻止或扭轉已經邁向分裂的網路發展趨勢（Segal, Goldstein & Schmemann, 2022）。

不過，美國官員認為，DFI 可形成的國際常規和公民社會監督的力量，不容小覷。Tim Wu 表示，任何法律都會因為某個原因而被違反，所以，DFI 是透過價值觀認同，尋求更多志同道合的國家加入，進而發揮國際常規的力量來因應挑戰，而不是基於害怕受到違規懲罰的約束力，才去推動 DFI。Harrell 和 Blinken 也指出，民間部門、公民社會和非政府組織，都是推動 DFI 的要員，當大家監督、要求各自政府履行 DFI 承諾時，就會形成強大的執行力量（Brookings Institution, 2022; Blinken, 2022）。

(四) 和既有的全球進程沒有關聯性

如前述 Access Now（2022）指出，國際間已有許多毫無實質進展的全球性原則和聲明，因此，它進而認為 DFI 是個多餘的國際倡議，甚至還會佔用國際政策論辯的有限資源，從而降低其有效性。

Kleinwächter（2022）教授也表示，雖然 DFI 文末提到，希望為既有的國際進程如聯合國、IGF、OECD、WTO、ICANN 和 FOC 等做出貢獻，但卻完全沒有說明將如何進行，及 DFI 和這些進程的關係是替代方案或相互競爭。尤其 IGF 目前已依據聯合國秘書長 Antonio Guterres 於 2021 年發布的《數位合作藍圖》（Roadmap on Digital Cooperation）進行改革，Guterres 還推動於 2023 年簽署《全球數位協議》(Global Digital Compact），且 2025

年 WSIS 也將召開成立 20 年的檢視大會……。如果 DFI 未能與這些網路治理生態系統的既有進程建立聯繫，不排除發生 Access Now 所擔憂的情況。

三、 中國大陸的嚴厲抨擊

DFI 所要遏止的數位威權主義最具代表性國家之一的中國大陸，自然對 DFI 提出嚴厲抨擊，並將炮火集中在 DFI 的動機及其原則。

中國大陸外交部（2022）表示，DFI 就是美國及其盟友以意識形態分裂網路、煽動網路空間對抗、破壞國際規則的最新例證，且有下列罪證：

- DFI 聲稱致力於全球性、可互操作的網路；但卻以基於意識形態的「家法幫規」取代聯合國等多邊平臺，破壞全球性網路治理原則。
- DFI 聲稱不應濫用數位科技進行非法監控；但美國多年來卻對全球進行大規模監控，嚴重損害全球網路用戶隱私，踐踏國際人權原則。
- DFI 聲稱應避免使用網路進行訊息操弄，破壞他國選舉；但美國多年來卻不斷散播假訊息，肆意干涉他國內政，甚至顛覆其政權。
- DFI 聲稱企業皆可在公平競爭的生態系統中發展；但美國卻濫用國安為由，打壓他國企業，並乘機推行自己不成熟的系統。
- DFI 聲稱各國政府應避免影響網路連線；但美國卻率先將網路空間作為新戰場，進行網路軍事力量的「前沿部署」，危害他國的關鍵基礎設施安全。
- DFI 宣揚挑選安全供應商的「非技術因素」，是為其不得人心的「乾淨網路」計畫改頭換面，企圖搞封閉排他的小圈子。

中國大陸外交部最後還呼籲回歸聯合國的多邊平臺，共同制定尊重各方利益的網路治理國際規則，建立真正的多邊、民主、透明的全球網路治理體系。

第七節 結論與建議

一、結論

(一) DFI 承諾廣受肯定，具有數位政策「定位」和改善施政的意義

雖然 DFI 所承諾「開放、自由、全球化、可互通、可靠和安全」的網路願景，在過去的國際議程都曾出現，但專家認為，在當前數位威權主義興起和網路面臨分裂之際，重申這些承諾有其時代意義，尤其在面臨嚴峻的網路挑戰時，DFI 可為數位政策「定位」，避免推出偏離的政策措施。此外，DFI 還在美國內部發揮政策改善的具體價值，美國學者表示，最近美國在促進隱私（公布《美國資料隱私和保護法》草案）和確保國際資料流通（和歐盟達成《跨大西洋資料隱私框架》協議）等方面，已取得實質進展。

(二) DFI 無約束力和實施機制，未來前景不明

儘管本計畫嘗試拼湊出 DFI 推動方式的模糊輪廓——如透過 TTC（美歐貿易和科技委員會）等多邊場合、國務院成立新的「網路空間暨數位政策局」等；且有公民團體表示將促使政府信守 DFI 承諾；又美國官員也認為 DFI 可形成的國際常規和公民社會監督力量，不容小覷。不過，DFI 不具法律約束力、缺乏實施機制、尚未和全球既有進程建立關聯性等問題，也引發不少對其未來發展的質疑。例如：美國智庫「外交關係協會」(CFR）指稱「未來也仍無法藉由 DFI 實現全球網路的烏托邦願景」、公民團體 Access Now 認為「DFI 最終只會淪為空談，甚至佔用國際政策論辯的有限資源」。

(三) DFI 制定程序違背多方承諾，如何重建多方社群信任亦是考驗

DFI 以「由上而下」、僅有政府單位參與，且沒有公開向公民社會徵求意見的方式制定，違反其「強化多方利害關係人的網路治理」承諾及原則，

不但引發拜登政府的誠信問題，也破壞多方方法的可信度，喪失非政府利害關係人的聯合支持，甚至可能反而讓威權政府加以仿效。後續如何重建多方社群對 DFI 的信任和支持，亦仍是一大考驗。

(四) 民主和威權陣營對峙，全球網路治理更趨兩極化

目前 DFI 共有 61 個簽署國（加上歐盟則有 62 個簽署者），美國也持續尋求願意落實 DFI 承諾，且沒有斷網或封閉平臺等不良紀錄的國家加入。而就在 DFI 發布後的 2 個多月，中國大陸在北京成立「世界互聯網大會國際組織」（WICO），將一個已經舉辦 8 年的「國際會議」，升級為「常設國際組織」，以強化在全球推動國家控制網路的理念，被視為是對 DFI 的反擊。中共官媒聲稱，WICO 已有來自近 20 國的上百個網路相關機構、組織、企業及個人加入。雖然這並非美中雙方陣營的首次網路治理理念之爭，例如 2020 年美國推出「乾淨網路」計畫後，中國大陸也提出《全球數據安全倡議》作為抵制。不過，就 DFI 和 WICO 的目標來看，此次更凸顯自由民主和數位威權兩個陣營的對峙，也讓全球網路治理更趨兩極化的發展。

二、建議事項

(一) 立即可行：將 DFI 原則轉化為具體政策措施，以履行簽署國承諾

雖然 DFI 不具約束力，但為了維護自由開放的網路共同願景，身為簽署國的我國應履行承諾，也就是落實其 5 大類 23 個子項的關鍵原則。因此，首要之務是由數位發展部籌組多方利害關係人專家小組，逐項確認、解讀這些原則的文義重點，之後識別各項原則的主責部門及對應的業務，進而將 DFI 原則轉化為具體的政策措施，並加以推行。

以 DFI 第 5 大類「強化多方利害關係人的網路治理」的第一項原則「保護和強化網路治理的多方利害關係人系統，包括主要技術協定和其他相關標準及協定的開發、部署與管理」為例，可能是指維護 IETF（Internet Engineering Task Force，網際網路工程任務組）和 IANA 的多方運作方式。

又其第二項原則「避免破壞攸關網路一般可用性及完整性的技術基礎設施」，可能是指維護 ICANN 掌管全球關鍵網路資源，避免將治理權移轉到由國家政府控制的 ITU。這 2 項原則應為數位發展部資源管理司（原通傳會射頻與資源管理處）的國際交流合作相關業務。至於如何在參與這些國際組織時，維護其多方運作方式，則需由該處（司）進一步研議。

(二) 中長期：定期評估我國 DFI 履行情況，做為對內改善對外貢獻基礎

身為網路自由度於全球名列前茅的國家 [10]，我國可考慮提高標準，針對前述 DFI 的 5 大類 23 個子項的關鍵原則，由轄下包含民主網絡司的數位發展部委託公正第三方，定期評估我國 DFI 履行情況，進而做為改善國內相關施政，及貢獻國際社會的基礎。

例如 DFI 第 1 大類「保護人權與基本自由」的其一原則為「……採取減少線上非法及有害內容的行動時，會符合……言論自由權，並鼓勵多元意見及多元主義，讓民眾免於言論審查、騷擾或恐嚇的恐懼」，如經評估認定期間內有「查水表」事件，數位發展部可基於履行 DFI 簽署國承諾，請執法單位予以改善。又如第 3 大類「推動包容和可負擔的網路連線」當中的「推動個人和企業可負擔、具包容性及可信賴的網路連線……」原則，如經評估認定已高度落實，則可將通傳會基礎設施與資通安全處（移撥數位發展部韌性建設司）所推動的數位基礎建設及縮短偏鄉數位落差相關計畫，透過國際會議或交流訪問等場合，提供他國參考，貢獻國際社會。

[10] 根據 Freedom House《2021 網路自由度報告》，我國網路自由度全球第五，亞太第一。

參考文獻

- 人民網 (2022)。習近平向世界互聯網大會國際組織成立致賀信。2022/7/13。http://politics.people.com.cn/BIG5/n1/2022/0713/c1024-32473476.html
- 中國大陸外交部(2022)。外交部發言人關於美國發布《互聯網未來宣言》的答問。https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/jksxwlb_674635/202205/t20220505_10681658.shtml
- 外交部 (2022)。我國簽署美國政府發起的「未來網際網路宣言」。2022/4/29。https://www.mofa.gov.tw/News_Content.aspx?n=95&s=97761
- 唐鳳 (2022)。Facebook, 2022/4/29。https://www.facebook.com/digitalminister.tw/posts/pfbid038B5h1U8nHuwHNdEDbTrUjXtrqCiVq8X8XCSvWtei9SXUtzMdbg615PffhSEHNUvl
- 孫承 (2022)。美中網絡空間治理模式和理念之爭漸趨白熱化。美國之音(VOA)，2022/7/24。https://www.voacantonese.com/a/china-internet/6671629.html
- 新華網 (2022a)。中華人民共和國和俄羅斯聯邦關於新時代國際關係和全球可持續發展的聯合聲明。2022/2/4。http://www.news.cn/2022-02/04/c_1128331320.htm
- 新華網 (2022b)。世界互聯網大會國際組織在北京成立。2022/7/13。http://www.xinhuanet.com/tech/20220713/d30531213905496eb744534876007cf6/c.html
- Access Now. (2022). Empty promises? Declaration for Future of the Internet is nice on paper. 2022/4/28. https://www.accessnow.org/declaration-for-future-internet/
- Alexander, F. & Redl, D. (2022). Governments only: The public doesn't get a say in the internet's future. The Hill, 2022/5/7. https://thehill.com/opinion/technology/3479885-governments-only-the-public-doesnt-get-a-say-in-the-internets-future/
- Barnoon, Y. (2022). America's sorely needed internet declaration is far from redundant. The Hill, 2022/5/12.

https://thehill.com/opinion/technology/3485925-americas-sorely-needed-internet-declaration-is-far-from-redundant/

- Blinken, A. (2022). Secretary Antony J. Blinken With Maria Ressa on Digital Diplomacy and Human Rights Online. U.S. Department of State, 2022/6/7. https://www.state.gov/secretary-antony-j-blinken-with-maria-ressa-on-digital-diplomacy-and-human-rights-online/
- Bose, N. (2022). U.S. joins 55 nations to set new global rules for the internet. Reuters, 2022/4/29. https://www.reuters.com/technology/us-joins-55-nations-set-new-global-rules-internet-2022-04-28/
- Brookings Institution (2022). Webinar: The democratic future of the internet. 2022/6/22. https://www.brookings.edu/events/the-democratic-future-of-the-internet/
- EC (2022). Declaration for the Future of the Internet（FactSheet）. 2022/4/28. https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet-factsheet
- EC (2022a). EU and international partners put forward a Declaration for the Future of the Internet. 2022/4/28. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2695
- EC (2022b). European Digital Rights and Principles. 2022/5/4 updated. https://digital-strategy.ec.europa.eu/en/policies/digital-principles
- Edelman,G. (2022). Don't Look Now, but Congress Might Pass an Actually Good Privacy Bill. Wired, 2022/7/21. https://www.wired.com/story/american-data-privacy-protection-act-adppa/
- Freedom House (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech
- Kerry, C. F. (2022). Battle lines for the future of the internet. Brookings Institution, 2022/5/11. https://www.brookings.edu/blog/techtank/2022/05/11/battle-lines-for-the-future-of-the-internet/

- Kim, S. (2022). What the South Korea-US Summit Had to Say About Internet Policy. The Diplomat, 2022/6/7. https://thediplomat.com/2022/06/what-the-south-korea-us-summit-had-to-say-about-internet-policy/
- Kine, P. (2022). China launches new bid for internet dominance. Politico China Watcher, 2022/7/21. https://www.politico.com/newsletters/politico-china-watcher/2022/07/21/china-launches-new-bid-for-internet-dominance-00047037
- Kleinwächter, W. (2022). How to Save the "Past" in the "Future of the Internet": Principles, Procedures and Problems of the Washington Declaration. CircleID, 2022/5/7. https://circleid.com/posts/20220507-how-to-save-the-past-in-the-future-of-the-internet-principles-the-washington-declaration
- Komaitis, K. (2022). https://twitter.com/kkomaitis/status/1520039256093306881?s=20&t=DJ1m56_LYhmXbEyagrxebQ
- MacKinnon , R. (2022). https://twitter.com/rmack/status/1519652732164059136
- Mok, C. (2022). Taiwan can be East Asia's New Internet and Data Hub. Friedrich Naumann Foundation for Freedom,2022/5/3. https://www.freiheit.org/taiwan/taiwan-can-be-east-asias-new-internet-and-data-hub
- Mueller, M (2022). The Declaration for the Future of the Internet. IGP, 2022/4/29. https://www.internetgovernance.org/2022/04/29/the-declaration-for-the-future-of-the-internet/
- Scott, M. & Kayali, L. (2022). Europe pitches tech 'principles' to rule the internet. POLITICO, 2022/1/26. https://www.politico.eu/article/europe-tech-principles-internet-rules-digital-rights/
- Scott, M. (2022). WASHINGTON'S VISION FOR THE FUTURE OF THE INTERNET. Politico, 2022/4/28. https://www.politico.eu/newsletter/digital-bridge/trade-and-tech-council-again-washingtons-declaration-margrethe-vestager/

- Segal, A., Goldstein, G. & Schmemann, A. (2022). Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. Council on Foreign Relations, 2022/7/12. https://www.cfr.org/report/confronting-reality-in-cyberspace
- The Economist (2022). The war in Ukraine is spurring transatlantic co-operation in tech. 2022/5/14. https://www.economist.com/international/2022/05/14/the-war-in-ukraine-is-spurring-transatlantic-co-operation-in-tech
- U.S. Department of State (2022). Declaration for the Future of the Internet. 2022/4/28. https://www.state.gov/declaration-for-the-future-of-the-internet
- White House (2022). Background Press Call by Senior Administration Officials on the Declaration for the Future of the Internet. 2022/4/28. https://www.whitehouse.gov/briefing-room/press-briefings/2022/04/28/background-press-call-by-senior-administration-officials-on-the-declaration-for-the-future-of-the-internet/

第五章 案例研析(3)「公平分攤」網路成本的爭議

第一節 前言

歐盟執委會（European Commission, EC）副主席兼數位執委 Margrethe Vestager 於 2022 年 9 月 28 日在布魯塞爾和美國聯邦通訊委員會（Federal Communications Commission, FCC）委員 Brendan Carr 會面，針對內容供應商（Content Providers, CPs）是否應和網路服務供應商（Internet Service Providers, ISPs）「公平分攤」（fair share）網路建設成本，交換意見。雖然兩人的談話內容不得而知，但 Carr（2022a）當日在其 Linkedin 貼出下文：

> 美國和歐洲的網路建設融資模式自 1990 年的撥接上網時代以來，一直沒有改變，而現在是大西洋兩岸更新方法的時候了——讓科技巨頭開始貢獻於「公平分攤」。

上述「大西洋兩岸更新方法」指的是，歐盟訂於 2023 年第一季正式商議「公平分攤」訴求；以及美國擬立法授權 FCC 研議 CPs 資助「普及服務基金」（Universal Service Fund, USF）的可行性。無獨有偶，此議題也在韓國延燒，甚至爭論更為激烈——CPs 和 ISPs 的對簿公堂，且政策發展更加迅速——國會已有多項旨在要求 CPs 向 ISPs 支付網路費的提案正在審議。

其實分攤寬頻網路建設成本的倡議，並非新鮮事，而是至少已經爭論十年的老議題。然而，老調之所以在現今重彈，且同時引發歐、美、亞國家的政策發展行動，當中原委值得關注國際網路政策趨勢的我國進一步了解。惟此議題涉及層面廣泛且複雜（否則不會爭論十年還無解），且各國的發展情況也有所差異，因此，本章僅是拋磚引玉，首先各別介紹韓國、歐盟和美國在此議題的近期不同驅動事件和發展面向，以及相關利害關係人的立場或論點，接續再彙整不同專家對於「公平分攤」政策的綜合看法，最後並提出我國相關政策建議以供參考。

第二節 韓國：「網路使用費」的爭議、訴訟和修法

一、Netflix 和 SKB 的網路費訴訟

由於 Netflix 的網路流量大幅增加，韓國主要 ISPs 之一的 SK Broadband（SKB），於 2019 年 11 月請求韓國國家通訊傳播委員會（Korea Communications Commission, KCC）調解它和 Netflix 的網路使用費問題。SKB 主張 Netflix 應該為網路的維護付費，但 Netflix 並沒有等待 KCC 的調解結果，而是於 2020 年 4 月直接對 SKB 提起訴訟，要求法院確認 Netflix 沒有義務向 SKB 付費。

根據《外交家》雜誌報導，Netflix 和韓國其他 ISPs 都達成協議，主要是和 Netflix 建立獨家的內容合作夥伴關係，或是透過 Netflix 提供自家開發的快取（Cache）伺服器等方式（稱為 Netflix Open Connect 計畫），來緩解流量。不過，SKB 拒絕此項提議，並堅持要求補償費（Kim, 2021）。

經過開庭審理，首爾中央地方法院於 2021 年 6 月裁定 Netflix 敗訴，應支付「合理的」補償費，至於金額則由兩家公司自行協商。SKB 希望 Netflix 支付每年約 2,300 萬美元（約新臺幣 7.25 億元）的補償費共 3 年，但 Netflix 認為此裁決是將 ISPs 的責任移轉給 CPs，因而於 7 月提出上訴。

適逢 Netflix 於同年 9 月中旬上線的原創韓劇《魷魚遊戲》掀起追劇熱潮，SKB 立即趁勢反告 Netflix，要求就「魷魚遊戲」帶來的額外網路流量及維護成本提供賠償。SKB 表示，受到該劇和數部韓國熱門影集爆紅的影響，9 月份處理的 Netflix 流量較 2018 年 5 月增加 24 倍。

目前首爾高等法院持續審理 Netflix 的上訴案。整體而言，雙方的主要主張如下（Lee, 2021；Yoon, 2022a）：

(一) SKB 的主張

- Netflix 的網路流量從 2018 年的每秒 50GB 增至 2021 年的 1,200 GB，

額外的網路流量使得網路維護成本攀升。

- 其他國際 CPs，如 Amazon、Apple 與 Facebook，皆已支付網路使用費，唯獨 Netflix 和 YouTube 從未付費（參見本節第二大項）。

(二) Netflix 的主張

- 網路流量的遞送以免費為原則，SKB 的費用是在其履行和終端用戶的合約時產生的，且他們已向 SKB 支付上網費。而今再向 Netflix 收費，形同雙向收費，破壞「網路中立」（Net Neutrality）原則。
- 自 Netflix 於 2016 年進入韓國市場以來，對當地的內容投資已超過 10 億美元（約新臺幣 315 億元），並為韓國創造 1.6 萬個工作機會。
- 支付網路使用費將造成不公平、反競爭的環境，ISPs 任意收費將使 Netflix 難以負擔，進而可能影響韓國消費者的權益。此外，其他國家的 ISPs 也可能效仿韓國的收費制度。
- Netflix 已免費提供快取伺服器等設備和方式（Netflix Open Connect 計畫），來緩解流量。

二、多數 CPs 已向 ISPs 付費

上述 SKB 指稱「其他國際 CPs 皆已付費」，是因為根據 2020 年 12 月生效的韓國《電信事業法》（Telecommunications Business Act, TBA）部分修正條文，每日平均吸引超過 100 萬用戶，並佔韓國網路流量 1% 以上的所有 CPs（法規用字為「附加價值電信服務供應商」，Value-added Telecom Service Providers，簡稱 VSPs），有義務為其用戶提供「穩定的」服務，否則最高可處折合 18,000 美元（約新臺幣 57 萬元）罰鍰（Kim & Chang, 2020）。

這項修法也被稱為 Netflix law，原本旨在解決 Netflix 和 SKB 的網路使用費爭議，並讓所有大型 CPs 付費。但由於「穩定的」電信服務在語意上

模糊不清，因此，Netflix 和 YouTube 皆拒絕向 ISPs 付費（Yoon, 2022a）。

根據韓國科學技術資訊通信部（Ministry of Science and ICT）資料，符合上述法規門檻的 CPs 共計 5 家，依韓國網路流量佔比的順序，分別為 Google/ Alphabet（27.1%）、Netflix（7.2%）、Meta（3.5%）3 家美國業者，以及 Naver（2.1%）、Kakao（1.2%）2 家韓國業者（Yoon, 2022b）。綜合韓國媒體報導，這 5 大 CPs 中，除了 Netflix 和持有 YouTube 的 Alphabet(Google 母公司）外，其他美國和韓國業者皆已向 ISPs 付費。

三、國會推動《電信事業法》相關修正案

由於 Netflix law 沒有發揮預期作用，韓國國會議員於是持續推動《電信事業法》相關修正案，目前已有 7 個修正案提交國會。以《網路使用費法案》(Net Usage Fee Act) 為例，其重點在於規定業者須揭露合約的細節，如履約期限、定價資訊等。又如《防止搭便車法案》(Free Ride Prevention Act)，重點則為禁止不合理或歧視性（意指不付網路使用費）的合約條件，及禁止對合約條款採取不解釋或不實解釋等（Yoon, 2022；Lee, 2022）。

《網路使用費法案》已於 9 月 20 日召開公聽會。有議員表示，網路使用費的爭議凸顯市場失靈，需由政府出面解決；但也有議員擔心，立法會使政府過度干預民間的合約關係，尤其有些資訊揭露所要求的是企業的機密資料；然而，也有議員反駁指出，合約的秘密性質會導致雙方發生糾紛，因為兩造都不確定是否支付或收取正確的金額。另有議員從產業角度表示，韓國探討此問題受到 ISPs 主導，應該也要考量內容產業的發展，避免失去韓國內容在全球的傳播力。內容產業代表也指出，內容產業在韓國經濟扮演要角，過去 5 年韓國內容產業的營業額每年平均成長 4.9%，出口的年平均成長率更達 18.7%。因此，呼籲國會推動讓網路生態系統共同發展的法案，而非只是讓特定企業受惠的法案（Lee, 2022；Anand, 2022）。

四、修法可能引發韓美貿易問題

其實上述的《網路使用費法案》公聽會原定於 4 月舉辦，但在美國政府表達關切（指稱法案對美國公司有歧視性）後，延宕 5 個月才恢復審議。此外，美國《2022 年各國貿易障礙評估報告》（2022 National Trade Estimate Report On Foreign Trade Barriers）也將收取網路使用費問題，列為美韓的貿易障礙之一（Kim,2022）。又美國商務部於 9 月下旬表示，美韓經貿部長近期亦針網路使用費的立法交換意見，雙方重申雙邊經貿關係的重要性，但也暗示了緊張局勢（Shin, 2022）。

會員包含美國科技巨頭的電腦與通訊產業協會（Computer & Communications Industry Association, CCIA）亦指出，韓國推動的相關立法違反《韓美自由貿易協定》（Korea-United States Free Trade Agreement, KORUS）的下列義務，以及《未來網際網路宣言》（參見第四章）維護自由和開放網路的承諾（Mchale, 2022）。

- 第 14.2 條「接取和使用」：韓國應確保所有美國服務供應商都能以合理和非歧視性的條款及條件，接取和使用任何公共電信網路或服務。
- 第 14.5 條「確保競爭」：韓國應採取或維持適當措施，以防止供應商參與或繼續反競爭行為。
- 第 15.7 條「開放網路原則」。

五、YouTube 和民間團體反對立法

YouTube 亞太區執行副總裁 Gautam Anand（2022）於《網路使用費法案》公聽會後，當日即在 YouTube 韓國官方部落格發文，此為他今年(2022)第二度對法案提出回應（第一次於 4 月份）。兩次回應的重點可歸納如下，當中還包括鼓勵創作者參加民間發起的反對立法連署活動。

- 主張 ISPs 的收費不合理

CPs 已經支付高額費用將內容傳遞到韓國 ISPs 的網路上，甚至 Google 在過去十年來還在亞太地區斥資 22 億美元建設網路基礎設施，且用戶也已經向 ISPs 支付上網費。因此，此項收費是不公平的，且為雙向收費，只是讓 ISPs 獲利，卻增加 CPs 額外負擔，世界各國皆無類似的立法。

- 表明立法將影響在韓投資

一旦法案通過，將增加 YouTube 巨大的額外成本，迫使 YouTube 改變在韓國的營運方式，恐怕難以持續投資韓國的創作者生態系統。因此，立法猶如懲罰 CPs 和韓國創作者。而韓國創作者們也都擔憂，立法將破壞他們多年來的努力成果。

- 呼籲創作者參加反對立法的連署活動

韓國非營利組織 OpenNet（2022）發起反對立法的連署活動，請創作者們參加連署，以表達對此項法案的疑慮和反對（OpenNet 發起「保護網路、保持網路中立、反對網路費法案」簽名活動，並指此法案將阻礙公眾免費使用網路交流空間、回到過去昂貴的國際通話費時代、韓國將無法誕生第二個享譽國際的 BTS 防彈少年團）。

- 強調 YouTube 對韓國的經濟貢獻

YouTube 提供韓語服務 14 年來，促進 K-Pop 聞名於世，韓國 YouTube 頻道超過 35% 的觀看時間來自國外，這些發展也回饋到韓國的經濟。2021 年 YouTube 的創作生態系統為韓國 GDP（國內生產毛額）貢獻超過 2 兆韓元（約新臺幣 448 億元），並支持 8.6 萬個全職工作。

而 YouTube 的主張也引來韓國政府部門的關切。有官員表示，韓國 CPs 已支付相當的費用，但外國業者卻拒絕付費，形成國內外業者之間不合理的逆向歧視（reverse discrimination）；且法律所要求的公平付費，竟會導致 YouTube 將損害轉嫁給 YouTuber，此論點實在令人難以理解；甚至它還將 YouTuber 作為人質，對抗公眾輿論。因此，將向 Anand 或 YouTube 其他人員進行詢問（Ahn, 2022）。

第三節 歐盟：「公平分攤」的爭議和政策走向

一、電信商呼籲規定科技巨頭「公平分攤」

歐洲電信商及其產業協會 ETNO（European Telecommunications Network Operators' Association，歐洲電信網路營運商協會）長期遊說 CPs 分攤網路費的訴求，最著名的是 2012 年於國際電信聯盟（International Telecommunication Union, ITU）的國際電信世界大會（the World Conference on International Telecommunications, WCIT）上，提出相同概念的「發送方付費」（Sending Party Pays，或 Sender Pays）原則，但此提案被當時多數歐美國家認為不公平且不必要，最終未能通過（EDRi, 2022）。

而近來這些業者及其組織之所以又積極重推舊案，歐洲政策研究中心（Center for European Policy Analysis, CEPA）資深研究員 Fiona Alexander 等人認為，一方面是因為電信業者需要資金投資 5G 建設（2012 年時是投資 4G 建設）；另一方面則是科技巨頭的聲譽不如十年前，且近年歐盟的政策立場也轉向監管科技巨頭（Alexander, 2022；Mitaksh, 2022）。以下以今年（2022）歐洲電信商和 ETNO 發起的 2 次倡議行動為例。

(一) 4 大電信 CEO 呼籲制定「公平分攤」法規

歐洲 4 家主要電信公司 Telefónica、Deutsche Telekom、Vodafone 和 Orange 的執行長，於 2 月發表聯合公開信，聲稱電信業者為了因應每年 50% 的網路流量高速成長，已經投入巨資升級網路基礎設施，但也陷於無力為繼之境，尤其現今 7 成以上的流量來自少數內容業者的串流影音、遊戲和社群媒體，所以，應該以符合比例原則的方式，分攤網路基礎設施的費用。然而，ISPs 無法和巨頭平臺談判公平的條款，因為它們擁有強大的市場地位、不對稱的議價能力，加上競爭環境也缺乏公平性。

信中並指出，國際間對此議題已有變化跡象，韓國和美國皆討論相關立法，故而呼籲歐盟制定法規，實現其所承諾的「所有從數位化轉型中受

益的市場參與者，都承擔他們的社會責任，並為公共財、服務和基礎設施的成本，做出公平和符合比例的貢獻」[11]，否則歐洲的網路建設將落後於世界各國，且無法實現 2030 年《歐洲數位十年》的政策目標（Telekom, 2022）。

(二) ETNO 建議規範科技巨頭的議價義務

會員涵蓋歐洲主要電信業者的 ETNO 於 5 月發布《歐洲網路生態系統：科技巨頭與電信運營商之間更公平平衡的社會經濟效益》（Europe’s Internet Ecosystem: Socioeconomic Benefits of a Fairer Balance Between Tech Giants and Telecom Operators）研究報告，指出歐洲電信業者過去 10 年來已在網路建設投資超過 5,000 億歐元（約新臺幣 15.5 兆），反觀產生歐洲 55%以上網路流量的 6 大科技巨頭（Meta、Alphabet、Apple、Amazon、Microsoft 和 Netflix），對於歐洲的網路發展卻無財務貢獻。此種不公平削弱電信業者的財力，進而延宕歐洲 5G 的推出，建議歐盟明確規範科技巨頭須和 ISPs 議價的義務，協助創造公平談判的基礎。

報告並強調，此項政策將可為歐洲帶來社會經濟效益，如果以科技巨頭每年對網路成本貢獻 200 億歐元（約新臺幣 6,181 億）計算，至 2025 年將可為歐洲增加 720 億歐元（約新臺幣 2.2 兆）GDP、創造 84 萬個就業機會，以及減少網路基礎設施 28%的能源消耗（ETNO, 2022）。

二、歐盟執委會將研議「公平分攤」

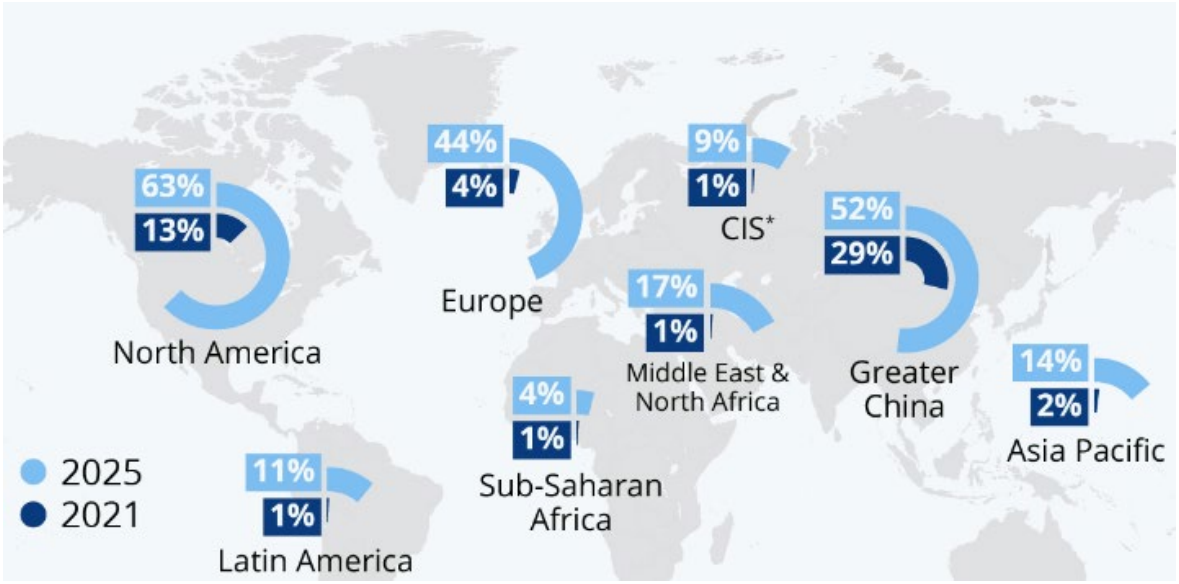
就在 ETNO 於 5 月發布上述研究報告後，歐盟執委會（EC）的 2 位相關業務最高主管旋即回應 ISPs 的主張。EC 副主席兼數位執委 Margrethe Vestager 表示，網路的「公平貢獻」（fair contribution）是 EC 應該關注的重點議題，因為有些參與者創造巨大流量，卻沒有為網路連線貢獻投資（Chee, 2022）；EC 內部市場執委 Thierry Breton 更直接指出，EC 將於年底前發布提案，因為 ISPs 沒有從網路維護中獲得投資回報，應重新安排網

[11] 摘自《歐洲數位十年之數位權利和原則宣言》草案之其一承諾，相關內容可參考本報告第四章第四節之 (一)，及第七節之二建議事項(二)。

路的公平報酬（Bertuzzi, 2022）。

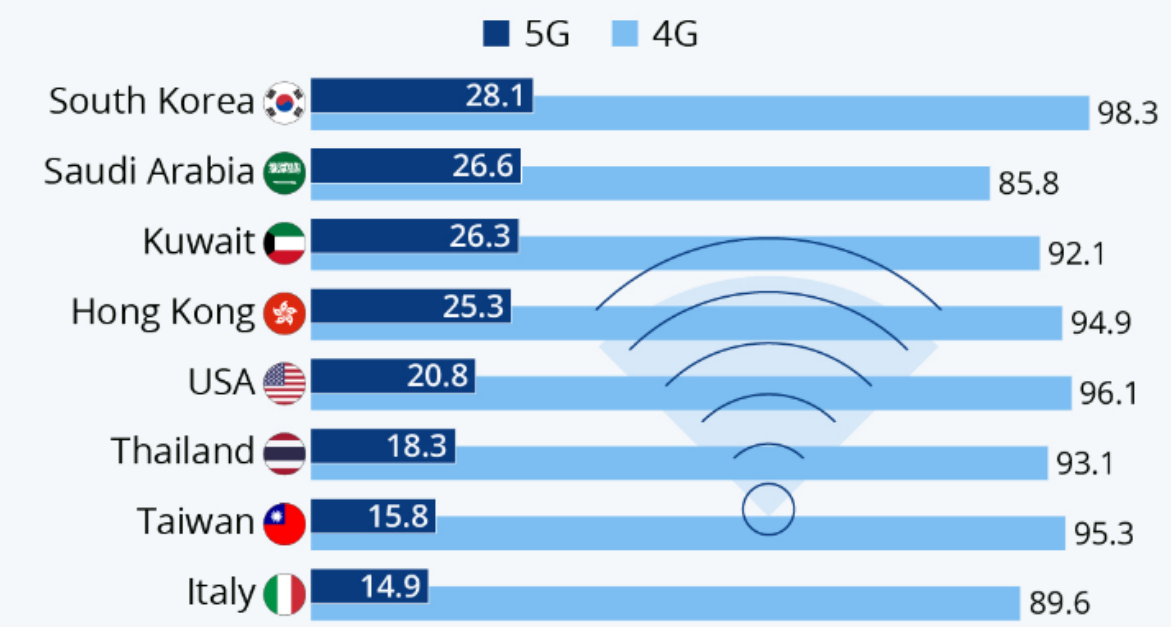
Breton 所謂的提案，或許是指《連網基礎設施法案》（Connectivity Infrastructure Act, CIA）。根據《政客》（Politico）雜誌 6 月底訪問不具名 EC 官員的報導，為了改善歐洲失敗的 5G 佈署（全球概況如下圖 5-1 和 5-2），且回應電信業者的擔憂，EC 規劃於秋季提出 CIA，內容包括強制某些線上平臺為 5G 建設成本貢獻，但尚不清楚是否會要求平臺巨頭直接承擔更廣泛網路基礎設施成本的義務。CIA 的其他部分則是將一些既有規範，如《寬頻成本降低指令》（Broadband Cost Reduction Directive, BCRD）、《國家寬頻援助指南》（Broadband State Aid Guidelines），於修訂後納入（Stolton, 2022）。

不過，Breton 於 9 月更新進度，表示 EC 將於 2023 年第一季針對科技巨頭是否應「公平分攤」電信業者的網路成本，進行研議諮商，預計約需 5、6 個月，之後就會提案。同月，他談論歐洲的元宇宙（metaverse）計畫時，再度提及基礎設施問題，指出新的虛擬世界將對連網基礎設施帶來更大的需求壓力，但其佈署成本增加而投資回報卻呈停滯。所以，EC 將對其願景和商業模式進行全面反思和諮詢（Rosemain & Chee, 2022; Breton, 2022）。



資料來源：GSMA, Statista (2022)

圖 5-1 全球 5G 滲透率（2021 年統計及 2025 年預測）



資料來源：Open Signal, Statista (2021)

圖 5-2 全球 5G 可用性前 8 名地區

三、歐盟成員國持不同立場

(一) 荷德等 7 國呼籲 EC 審慎決策

荷蘭、德國、丹麥、愛沙尼亞、芬蘭、愛爾蘭、瑞典七個歐盟國家，於 7 月連署致函 EC，呼籲不要草率決策「公平分攤」提案，因為高容量網路的發展及 CPs 和 ISPs 之間的關係，是攸關當前網路運作方式的複雜問題，此項政策改變除了需和各成員國的政府交流，以考慮所有相關的觀點和專業知識外，還需讓所有利益相關者從各個方面仔細審查，並進行公開透明的諮詢和辯論。此外，歐盟電子通訊傳播監管機構（Body of European Regulators for Electronic Communications, BEREC）已就此問題進行研究，建議等待 BEREC 於 2023 年公布評估結果（Bertuzzi, 2022）。

(二) 法義等 3 國呼籲 EC 立法「公平分攤」

法國、義大利、西班牙三國則是聯合呼籲 EC 透過立法要求大型科技公司為歐盟的電信基礎設施提供部分資金。根據《路透社》8 月的獨家報導，

這三國政府在聯合文件中表示，6 大 CPs 佔網路流量的 55%，增加歐洲 ISPs 的成本，但它們已於 5G 網路和光纖到府等項目投資巨額。因此，呼籲 EC 為「公平分攤」立法，確保所有的市場參與者都為數位基礎設施成本作出貢獻，同時也兼顧依據「網路中立」規則保障用戶之間的公平性（Pollina & Fonte, 2022）。

四、內容業者強調已投資基礎設施

會員包含美國科技巨頭的電腦與通訊產業協會（CCIA）針對 ETNO 再次大舉推動網路費議題，表示 ETNO 仍然抱持過去的錯誤觀念，認為 ISPs 的投資短缺是由仰賴高速和高品質網路的服務所造成的。但研究顯示，單是 2014 年至 2017 年期間，CPs 對網路基礎設施的投資就超過數千億美元。CCIA（2022）強調，儘管歐洲長期以來致力於「網路中立」，但現在電信業者似乎想從終端用戶和 CPs 獲取雙重報酬。

CCIA 所指的研究是 Google 委託顧問公司 Analysys Mason 於 2018 發布的「線上服務供應商投資基礎建設」（Infrastructure Investment by Online Service Providers）報告。報告指出，為了因應線上內容和雲端服務的爆炸式成長，並縮短這些服務和終端用戶的距離，CPs 對網路基礎設施的投資已超過 3 千億美元，當中 9 成以上資金是用於興建超大規模的資料中心，其餘則投資陸地和海底光纖電纜，以及 CDN（Content Delivery Networks，內容傳遞網路）等項目。

Google 歐洲地區業務主管 Matt Brittin 也強調，「公平分攤」提議忽略 Google 在歐洲投資基礎建設的事實，例如：興建連接美歐地區的海纜、在歐洲增建資料中心及快取節點（cache node）等，單是 2021 年的投資金額就超過 230 億歐元，以降低歐洲地區網路傳輸的流量壓力。他並表示，「公平分攤」還會破壞歐盟的「網路中立」，並損及消費者權益（FT Live, 2022）。

五、公民團體擔憂破壞「網路中立」

來自 17 國的 34 個公民團體如歐洲數位權利組織（European Digital Rights）、歐洲公民自由聯盟（Civil Liberties Union for Europe）、電子前哨基金會（Electronic Frontier Foundation）等，於 6 月聯合致函 EC，表示「公平分攤」政策將會破壞且違反歐盟「網路中立」法規，形同美國川普政府時期廢止保護網路中立（可參考本章第四節第五項）。其信函重點包括（EDRi, 2022）：

- 網路佈署成本大降，現今更無理由改變政策立場

ITU 已於 2012 年拒絕電信產業的「發送方付費」提案。而今由於網路技術的進步，佈署和營運網路基礎設施的成本已大幅下降，因此，更加沒有理由改變政策立場以滿足電信產業的利益，卻犧牲自由開放的網路。

- CPs 已投資基礎設施，且帶動終端用戶需求成長

大型 CPs 已在內容傳遞網路（CDN）和必要的網路基礎設施上，投入可觀的金額；且正如前 EC 執委 Neelie Kroes 所述，CPs 的成功帶動歐洲終端用戶購買更多高速的寬頻服務，EC 應該強化此良性循環，而不是破壞。

- 歐盟「網路中立」法規保障用戶的自由使用

巨大的流量是來自歐洲終端用戶的需求，是用戶要求 CPs 傳送資料封包到歐洲，他們已經向 ISPs 付費；且歐盟的「網路中立」法規保障用戶自由使用寬頻服務，無論是用於 Netflix、YouTube，或是歐洲當地的小型網站或服務。ISPs 的主張只是想以相同的服務獲得兩次報酬。

- 各國仿效歐盟，將導致全球網路分裂

一旦歐盟立法，其他國家可能會仿效歐盟模式，屆時端到端（end-to-end）和全球公平競爭的原則將不復存在，全球的網路傳輸會因為需要透過官僚程序，逐一協商每個網路的接取條款，而變成分裂的網路。

六、歐盟「網路中立」法規

歐盟「網路中立」規則訂於 2015 年的 Regulation (EU) 2015/2120 第 3 條（Article 3）保護開放網路的接取，又被稱為開放網路法規（Open Internet Regulation），主要規定如下的 ISPs 義務和終端用戶權利（EU, 2015）：

- ISPs 提供網路接取服務時，應平等對待所有流量，禁止歧視、限制或干擾，不論這些流量是來自發送者或接收者、造訪或發布的內容、使用或提供的應用程式或服務，或使用何種終端設備。
- 終端用戶有權利自由選擇想要造訪和發布的訊息及內容、想要使用和提供的應用程式和服務，以及想要使用的終端設備，不論終端用戶或提供商位在何處，或訊息、內容、應用程式或服務來自哪裡，又要傳送至何處。

第四節 美國：推動改革「普及服務基金」

一、國會推動《公平資助法案》

有鑑於新冠肺炎疫情期間凸顯消弭數位落差的重要性與必要性，美國參議院兩黨議員於 2021 年 7 月提出《公平資助法案》（FAIR Contributions Act，全名為 Funding Affordable Internet with Reliable Contributions Act），並於 2022 年 5 月獲得「商務、科學和交通委員會」通過（Congress, 2022a）。另一方面，共和黨眾議員也於 2022 年 7 月將此案提交眾議院，目前待「能源暨商務委員會」審議（Congress, 2022b）。

《公平資助法案》旨在要求聯邦通訊委員會（FCC）針對邊緣提供商（edge providers，指線上內容或服務的提供商，後續統一用語為 content providers，簡稱 CPs）資助「普及服務基金」（USF）的可行性，進行研究並報告。法案內容非常簡短，沒有相關背景說明，主要是規範研究報告的內容，例如：須仔細分析資助企業和服務的類型及規模、USF 現有經費來源機制和替代方案之間的公平性問題、改變 USF 現有經費來自「消費者電信帳單」的影響性，以及 UFS 的永續性及如何確保其支付的一致性和可預測性等項目。

提案參議員之一的 Shelley Moore Capito（2021）表示，網路基礎設施的建設成本昂貴，大型科技公司長期從中獲利，但卻沒有適當協助寬頻網路的投資。而隨著通訊方式從電話轉向網路平臺，現在應開始研究大型科技公司如何幫助縮減數位落差，並確保真正的普及服務。

提案的眾議員 Markwayne Mullin（2022）也指出，Netflix 等串流媒體佔鄉村寬頻網路流量的 75%，並獲得可觀的收入，但他們並沒有支付傳遞服務的成本，這些費用是由消費者、ISPs 和聯邦政府承擔。因此，此法案可讓我們更加了解串流媒體應如何協助消弭數位落差。

二、FCC：改變既有機制需國會授權

對於國會推動《公平資助法案》（草案），被指定進行 CPs 資助 USF 可行性研究的 FCC，於 8 月發布的《普及服務基金展望報告》（Report on the Future of the Universal Service Fund）中，雖然沒有直接表明其政策立場，但已指出向所有寬頻業者收費的不可行，因為該費用會轉嫁給消費者，進而影響網路服務的可負擔性。

報告還指出，FCC 是否有職權可以評估大型科技公司的營收，非常不明確，因此，建議國會提供其改變 USF 籌資方法和稅基所需的立法工具，以減輕消費者的財務負擔，為需要付費的實體提供確定性，並維持 USF 及相關計畫的長期維運（FCC, 2022）。

FCC 委員 Brendan Carr（2022b）除了樂見《公平資助法案》（草案）和 FCC 的報告，凸顯要求大型科技公司公平貢獻的想法已日益獲得認同之外，也對 USF 的概況提供補充說明。

Carr 表示，USF 用於資助鄉村、學校、圖書館、醫院和生命線（Lifeline）等計畫的網路服務，每年 90 億美元的基金，是 FCC 眾多縮減數位落差計畫的唯一經費來源，但籌資機制（對傳統電話費的每月帳單課稅）卻陷入死胡同。這種機制在撥接上網的 1990 年代有其意義，然而傳統電話費的收入已從 2000 年的每年約 800 億美元，大幅降為現今的不到 300 億美元，以致消費者支付（貢獻）的比例從 2001 年的 6%，躍升為今日的 30%；且 FCC 的研究發現，如果放任不管，此比例將在 4 年內達到 75%。因此，USF 需要大型科技公司的公平貢獻，而 FCC 也需要國會授予額外的權力，以開始評估大型科技公司的營收。

三、民間對改革 USF 的看法

(一) 支持改革 USF 和「公平資助」

電信產業自是站在支持的一方。美國電信協會（US Telecom Association）表示，USF 創立於早期年代，而今大多數的網路流量是來自少數不向 USF 捐獻的 CPs，因此，國會探索「公平資助」義務是正確的，同時也讚賞 FCC 籲請國會授權其擴大 USF 稅基，將科技巨頭也納入其中（Dano, 2022）。

支持者還至少包括數十個來自少數族裔、婦女權益、公民權利和人權領域的民間團體。例如：數位進步學會（The Digital Progress Institute）呼籲，將資助的負擔從消費者轉移到從普及服務獲利的企業身上；自由國度基金會（The Free State Foundation）認為，只要大型科技公司沒有「公平資助」，普及服務就缺乏中立性；網路創新聯盟（Internet Innovation Alliance）表示，讓獲利的內容業者資助USF，將可大幅提高USF的永續性（Layton, 2022）。

此外，也有創投業者指出，去年全球六大網路公司 Meta、Alphabet、Apple、Amazon、Microsoft 和 Netflix 佔全球網路流量 56%以上，首度超越其他所有網路公司的總和，引發電信業關注。而隨著元宇宙及其資料密集型應用程式的到來，大型科技公司的流量佔比只會增加，進而帶動其收益。因此，現在該是拯救 USF、讓科技巨頭付費的時刻了（Weinberg, 2022）。

(二) 反對改革 USF 和「公平資助」

會員包含科技巨頭的商業組織，如電腦與通訊產業協會（CCIA）和網路及競爭網絡協會（Internet and Competitive Networks Association, INCOMPAS）自然是反對改革 USF 和「公平資助」。CCIA 表示，消費者已支付網路接取費，且使用額外頻寬的公司不論是提供搜尋或串流影音等服務，也已向 ISPs 支付額外費用，況且這些內容服務還幫助 ISPs 創造銷售接取服務的需求。INCOMPAS 則指出，美國家庭正在為飛漲的油價和物價奮鬥，他們最不需要的，就是網路服務被加徵新稅（Gold & McGill, 2022）。

也有產業分析師認為，要求科技巨頭付費反而不合理，因為如果沒有內容，終端用戶就沒有高容量頻寬的需求，依此邏輯，反而 ISPs 應向科技巨頭支付接取內容的費用（Dano, 2022）。

四、Netflix 曾向美國 ISPs 付費

其實 Netflix 有一段時期曾向美國 ISPs 支付網路接取費。2014 年期間 Netflix 的「紙牌屋」（House of Cards）等熱門影集引發收視熱潮，卻也因此導致網速太慢，許多客戶退訂。因此，Netflix 不情願地和 Comcast 簽訂 7 年合約，以確保 Comcast 提供高速網路服務（原本 Netflix 是透過第三方連到 Comcast 網路，簽約後改為直接連線）。由於付費後，Netflix 影片的傳輸速度飆升，於是 Netflix 又和 AT&T、Verizon、時代華納有線電視等其他美國 ISPs 達成類似的交易。不過，Netflix 也指責 ISPs 採取勒索策略，並呼籲 FCC 禁止此類收費行為（Goldman, 2014）。

雖然 Netflix 向美國 ISPs 付費的相關細節不得而知，且近幾年美國的「網路中立」法規也歷經實施又撤銷（參見下段內容），不過，Netflix 曾於 2021 年表示，已經沒有向 Comcast 付費，並且是透過和全球數千家 ISPs 的密切合作（指 Netflix 免費提供自家開發的快取伺服器等方式，又稱為 Netflix Open Connect 計畫），來緩解網路擁塞及降低傳輸成本（Lee, 2021）。

五、美國「網路中立」法規

雖然《公平資助法案》（草案）或改革 USF 的討論，皆未見提及「網路中立」問題，而且也不清楚上述 Netflix 對美國 ISPs 的付費情況是否受到美國「網路中立」法規的實施及撤銷的影響。不過，由於此詞彙和法規皆首見於美國，因此，以下仍提供相關簡介。

「網路中立」一詞源自美國哥倫比亞大學法學院教授 Tim Wu（現任白宮科技與競爭政策特別助理）於 2003 年一篇探討當時寬頻業者採取歧視性措施的論文。根據美國全國州議會聯合會（National Conference of State Legislatures, NCSL）資料，「網路中立」係指網路上的所有資料流量應受平等對待，禁止 ISPs 逕自封鎖、減慢或加速所傳送的線上內容。而美國「網路中立」法規則可追溯至 2005 年，主要歷程如下（FCC, 2015；NCSL, 2022；

Nakutavičiūtė, 2022）：

- 2005 年 FCC 提出「網路中立」政策宣言，保護消費者自由接取合法內容、自由選擇應用程式與服務等權益。
- 2010 年 FCC 公布《開放網路命令》（Open Internet Order），首度將「網路中立」原則入法，也就是禁止封鎖、禁止歧視（不合理的差別待遇），以及透明度義務（須公開網路管理等政策）。
- 2015 年 FCC 將寬頻服務歸類為美國《電信法》（The Telecommunications Act）第二章（Title II）的公用事業（common carrier），並修正《開放網路命令》，除了原有的「網路中立」原則外，還加上禁止提供付費優先服務（快車道服務）、禁止不合理的干擾等規定。
- 2017 年底川普執政下的 FCC 正式廢除《開放網路命令》，並於 2018 年改為實施《恢復網路自由命令》（Restoring Internet Freedom Order），將寬頻服務恢復為《電信法》第一章（Title I）的資訊服務（information service），且主管機關改為美國聯邦貿易委員會（Federal Trade Commission, FTC）。此舉引發美國各州反彈並提起訴訟。
- 2019 年法院裁定各州可以自行制定 ISPs 的規範，FCC 不得干涉。美國加州、新澤西州、俄勒岡州等 7 州陸續通過「網路中立」立法。
- 2021 年有 16 個州推動「網路中立」立法。同年 7 月，拜登總統發布行政命令，呼籲 FCC 撤銷川普時期所改變的網路服務分類。

第五節　專家綜合看法

一、反而促 CPs 成為全面性的霸權

APNIC（亞太網路資訊中心）首席科學家 Geoff Huston（2022）表示，雖然就技術層面而言，即使 CPs 無法和 ISPs 達成直接接取的付費協議時，仍可透過外部互連（external peer）或轉接網路（transit network）來提供服務，但 ISPs 會故意讓這些流量阻塞，使其內容服務品質嚴重下降。如此也陷入需耗時解決的「網路中立」之爭，CPs 可能會為了能夠持續提供服務而不得不付費。

Huston 指出，在此環境下，只有大型 CPs 能夠生存，進而一方面成為內容巨獸；另一方面，則成為攸關 ISPs 獲利的關鍵客戶。長此以往，內容巨獸將能夠直接接管 ISPs，對關鍵基礎設施握有更大的控制權。屆時我們可能沒有工具，甚至不知道該如何應對這種全面性霸權所帶來的後果。

Huston 強調，以上看法並非無謂猜測。近十年來，海底電纜的格局已經產生全面性變化。現今多數新的海纜計畫以及洲際海纜的連接，皆由最大的 CPs（意指 Google）承擔，例如：跨大西洋海纜容量 80% 以上即由 CPs 掌控，單一的電信財團無法取得足夠資金來完成海纜計畫，CPs 在海纜的主導地位已經形成壟斷，它不再是海纜的客戶，而是自己的傳輸提供者。此外，在最後一哩（the last mile）的接取市場方面，多年來 Google 持續試水溫，推出 Wi-Fi 上網服務。未來如果 Google 對接取市場興趣增加，推出受消費者歡迎的低價、高品質上網服務，屆時監管機關恐怕也沒有理由加以阻止。

二、破壞全球數位常規且導致網路品質下降

網際網路協會（ISOC）政策和宣傳資深經理 Adrian Wan（2022）表示，網路的基本結構，是由眾多獨立網路相互連接所形成的一個共享系統。這

些自願性的網路互連安排，形成全球的常規，讓 ISPs 得以優化連線來滿足客戶需求，另也造就一個高效、強韌、持續創新的全球網路。然而，韓國和歐洲正在推動或討論的付費機制，一旦通過將引發其他國家仿效，進而造成全球數位常規的分裂，破壞全球數位生態系統。

Wan 並指出，目前韓國的數個提案都是從強制 CPs 和 ISPs 簽訂合約的角度切入（歐洲電信業者的建議也類似——由歐盟明確規範科技巨頭須和 ISPs 議價的義務）。然而，ISOC 的網路影響性評估發現，韓國於 2020 年底實施的 CPs 支付網路費（5 大 CPs 已有 3 家向 ISPs 付費）等措施，已對韓國的數位生態系統造成不必要的成本和瓶頸。例如：流量傳輸效率和網路連接結構的韌性皆降低、資料傳輸成本卻升高，進而導致用戶的服務品質下降。而推動中的修正案通過後，將會需要更多的網路安排才能遵循強制性的互連結算方案，上述問題也將因此更加惡化。

三、破壞「網路中立」、言論自由和流量產業發展

美國史丹佛大學法律學院網路政策中心研究員 Joan Barata（2022）認為，推動中的法規擬強制 CPs 和 ISPs 協商財務貢獻，以換取連線至終端用戶的措施，將會帶來下列負面影響：

- 違反「網路中立」最基本的平等對待原則。
- 造成新進和小型業者的市場進入障礙，進而導致各自市場皆由最強大的參與者全面統治，除了引發歧視或濫用市場支配地位的問題外，還會直接影響終端用戶自由選擇多樣化和多元化的內容、服務和應用程式的權力。
- 網路流量的「正常」、「過度」、「濫用」沒有衡量標準，法案形同懲罰雲端、AI、大數據等流量密集型產業，可能嚴重破壞數位轉型的發展。

Barata 強調，要兼顧網路的公平使用和基礎設施的投資，監管機關需要

超越特定產業利益和壓力的解決方案，且應該拒絕會破壞網路成功基礎的自由開放網路和「網路中立」理念，或危及言論自由和多元化民主原則的解決方案。

四、公平成本需進行商業研究

丹麥 Aalborg University 研究員暨 Strand Consult 顧問公司副總裁 Roslyn Layton 博士表示，不成比例的流量大增的確會增加 ISPs 的成本，尤其對鄉村地區的寬頻而言，中間一哩才是關鍵，業者必須以更多的設備、軟體、人力和能源，才能提供服務。南非 University of South Africa 教授 Petrus Potgieter 也補充指出，寬頻接取和傳統電信一樣，都是資本密集型產業，但不同之處在於寬頻接取需要隨著產品性質的發展而一再投資。例如：靜態網站的偶爾加載和電子郵件的發送，所需的連接設備就和線上遊戲及串流影音不同（Layton & Potgieter, 2022）。

Layton 進一步表示，公平成本和其回收是一個全球性問題。儘管學術界和監管機構長期研究寬頻資金短缺的問題，但意外的是他們沒有從企業和商業的角度進行研究。現今使用的寬頻訂閱模式是在 email 為關鍵應用的時代，也就是串流影音出現之前所訂定，但商業模式並沒有隨著技術的發展而演進。其實定價的靈活性和中間一哩的定價，對於縮小數位落差的政策更加重要。因此，樂見美國國會推動的《公平資助法案》將責成 FCC 進行必要的研究；而歐洲的 ISPs 也需要提出更系統性和可信的證據，來證明其公平成本回收的論點。

Layton 並對 Netflix 宣稱其 Open Connect 方案可以減緩流量，表達不同看法。他認為，該方案反而增加流量、成本和能源，因為 Netflix 提供的裝置大部分時間都處於閒置狀態，且不能用於其他非 Netflix 內容。然而，鮮少有運營商敢勇於挑戰 Netflix 的這項論點。

第六節 結論與建議

一、 結論

(一) 歐盟可能推出「公平分攤」網路成本規定，進而成為全球新標準

面對電信業者重提內容業者（CPs）應分攤網路建設成本的訴求，歐盟執委會已訂於 2023 年第一季正式商議此「公平分攤」政策議題。雖然目前無法確定商議後是否將提出法案，又如果提案是否和原先研擬的《連網基礎設施法案》（CIA）相關。另一方面，此訴求也面臨 CPs 和數十個公民團體的反對，指稱違反歐盟「網路中立」法規；而且專家們亦提出破壞全球數位常規、言論自由和流量產業發展等疑慮。不過，由於歐洲的 5G 佈署相對落後，可能衝擊 2030 年《歐洲數位十年》政策的兌現；加上近年歐盟的政策立場也轉向監管科技巨頭。因此，歐盟仍可能推出「公平分攤」網路建設成本的規定，《路透社》報導甚至認為歐盟此次有機會為網路建設成本豎立全球新標準。至於「網路中立」問題，有電信商表示不必擔憂，因為他們並不會限制網路流量，目標只是確保科技巨頭為飆升的網路成本作出貢獻，而小公司根本不必支付任何費用（Chee & Mukherjee, 2022）。

(二) 韓案例凸顯中小型國若率先針對科技巨頭，恐影響對美政經關係

韓國於 2020 年 12 月率先全球，實施被稱為 Netflix law 的《電信事業法》部分修正條文，藉由賦予大型 CPs 提供「穩定服務」的義務，讓科技巨頭向韓國 ISPs 支付網路使用費。然因「穩定服務」語意模糊，以致 Netflix 和 YouTube 迄今仍未付費，於是韓國國會議員陸續再提出相關修正草案，目前已有 7 案送至國會。韓國此項政策發展也成為歐洲電信業者津津樂道的案例，但卻引來美國的政治回應。相關事件如：美國直接對修法表達關切，致使一場法案公聽會從 4 月延宕至 9 月才召開；美國將此問題列為 2022 年美韓的貿易障礙之一；美國商務部於 9 月份雙方經貿會議暗示此問題造成緊張局勢；美國 4 月底推動的《未來網際網路宣言》韓國較各國延

後近一個月才得以加入（參見本報告第四章第三節）。此外，美國的電腦與通訊產業協會（CCIA）還列出韓國可能違反《韓美自由貿易協定》當中的數項條款。由此也凸顯中小型國家如果率先推出不利於科技巨頭的政策，美國勢必會有所回應，並可能影響雙方的政經關係。

二、 建議事項

(一) 立即可行：掌握「公平分攤」政策動向，以利國內政策順應國際潮流

國內電信業者亦相當關注國際間涉及網路建設成本分攤的議題。例如：2017 年美國廢除「網路中立」法規、2021 年韓國判決 Netflix 應該合理補償寬頻業者 SKB 之際，國內的電信三雄和台灣電信產業發展協會都曾呼籲，讓電信業者可以向高流量的內容業者收取分潤費（江明晏，2021）。因此，建議通傳會掌握國際「公平分攤」政策議題的動向和進展，以利國內相關政策能在第一時間順應國際潮流。

當中，尤其要密切追蹤可能為全球豎立新標準的歐盟政策。依據歐盟執委會的時程規劃，其政策諮商將於 2023 年第一季啟動，預計 6 至 9 月期間發布政策方案。而在政策明朗化之前，歐盟電子通訊傳播監管機構（BEREC）訂於 3 月到 6 月發布的評估報告，亦值得關注。BEREC 副主席 Konstantinos Masselos 於 9 月底表示，當前充斥各種訊息，有賴蒐集大量資料並進行仔細研究（包括 ISPs 網路互連的實際狀況），才能得出具體結論。因此，此份報告可能有助於釐清各方立場和各種意見的合理性（FT Lives, 2022）。

此外，「公平分攤」的政策方向在歐盟和韓國皆被指稱違反「網路中立」原則。因此，亦可留意歐盟和韓國如何回應此項疑慮，以釐清「網路中立」的意涵或是否有新的解讀。至於美國《公平資助法案》，雖然立法進展難以預測，且美國「普及服務基金」的用途和籌資機制和我國有所差

異[12]，但一旦法案通過後，FCC 須於 180 天內完成可行性評估報告，屆時評估結果將攸關內容業者是否應承擔網路普及服務責任的國際新趨勢，並可作為數位部管理我國「電信事業普及服務基金」的參考。

(二) 中長期：普及連線概念已升級，我數位平權計畫可參與 PNMA

美國《公平資助法案》（草案）的最終目的，是希望科技巨頭能夠資助普及服務基金（USF），以確保美國寬頻網路真正普及化，進而縮減數位落差。同樣地，我國電信普及服務亦是透過積極建設通信基礎設施，以消弭數位落差。不過，根據 IGF（2021, 2022）資料，普及連線（universal access）的概念已隨著時間演變，從 1990 年代的步行距離內付費電話的可用性、2000 年代中期的廣泛寬頻網路的可用性，到近年來已擴展至「有意義連網」（meaningful access），因為許多例證顯示，有些地區即使有網路覆蓋，人們也不使用。為此，IGF 於 2021 年成立「有意義連網政策網絡」（Policy Network on Meaningful Access, PNMA），期能透過專家工作小組的引領和全球多方利害關係人的討論，從網路基礎設施、使用者的意願和能力、內容和網路環境的公平和多樣性等層面，找出成功案例、識別推動障礙，並提出政策建議，以協助各國落實數位平權，消弭數位落差。

我國教育部自 2020 年起，實施為期四年的「邁向數位平權推動計畫」，整合包含通傳會（業務移撥數位部）等部會資源，建構人人享有數位平權且友善的數位環境。建議計畫主責和協辦部會派員參與 PNMA，和國際進行政策交流，並將最佳實踐引入國內，以促進我國實現數位平權計畫目標。

12 例如：美國「普及服務基金」還須用於資助醫院和生命線（Lifeline）的網路服務，我國「電信事業普及服務基金」的網路服務補助範圍則不含此等項目；又美國的經費來源是向民眾的傳統電話費帳單課稅，我國則是由年營業額達特定門檻的電信業者（如 109 年度為新臺幣 1 億元以上），依其營收規模分攤該年度的普及服務支出。

參考文獻

- 江明晏 (2021)。魷魚遊戲讓韓國電信怒了？台電信協會也盼爭取分潤。中央社，2021/10/5。https://www.cna.com.tw/news/afe/202110050243.aspx
- 林上祚 (2019)。前瞻砸 8 億推「村村有寬頻」，偏鄉民眾不買單，NCC 決從 5 大公共場所下手。風傳媒，2019/1/30。https://www.storm.mg/article/891669
- Ahn, S. J. (2022). Google clearly dominates the Korean ecosystem… The 'public opinion of YouTube' has also excelled. iNews24, 2022/9/23. https://www.newsdirectory3.com/google-clearly-dominates-the-korean-ecosystem-the-public-opinion-of-youtube-has-also-excelled-it 돋보기/
- Alexander, F. (2022). What's Old is New Again: Is Retrograde Telecom Policy Returning to Europe? CEPA, 2022/5/12. https://cepa.org/article/whats-old-is-new-again-is-retrograde-telecom-policy-returning-to-europe/
- Anand, G. (2022). 망 이용료에 대한 국회 토론회 내용을 공유드립니다. YouTube 한국 블로그, 2022/9/20. https://youtube-kr.googleblog.com/2022/09/blog-post.html
  한국 크리에이터 커뮤니티에 전하는 망 이용 관련 법안에 대한 업데이트. 2022/4/20. https://youtube-kr.googleblog.com/2022/04/blog-post.html
- Analysys Mason (2018). Infrastructure investment by online service providers. 2018/12/5. https://www.analysysmason.com/consulting-redirect/reports/online-service-providers-internet-infrastructure-dec2018/
- Barata, J. (2022). The Re-Emergence of the Net Neutrality Debate in Europe. Verfassungsblog, 2022/8/5. https://verfassungsblog.de/net-neutrality-eu/
- Bertuzzi, L. (2022). Seven EU countries warn the Commission against hasty decisions on 'fair share'. EURACTIV, 2022/7/20. https://www.euractiv.com/section/digital/news/seven-eu-countries-warn-the-commission-against-hasty-decisions-on-fair-share/
- Breton, T. (2022). People, technologies & infrastructure – Europe's plan to thrive in

the metaverse. Linkedin, 2022/9/14. https://www.linkedin.com/pulse/people-technologies-infrastructure-europes-plan-thrive-thierry-breton/

- Capito, S. M. (2021). Capito, Colleagues Introduce Bill to Explore Collecting USF Contributions from Big Tech. 2021/7/22. https://www.capito.senate.gov/news/press-releases/capito-colleagues-introduce-bill-to-explore-collecting-usf-contributions-from-big-tech
- Carr, B. (2022a). Brendan Carr's Post. Linkedin. 2022/9/28. https://www.linkedin.com/posts/brendan-carr-0030b126_the-us-and-europe-have-models-for-funding-activity-6980279427137953792-UVh-
- Carr, B. (2022b). Statement of Commissioner Brendan Carr. 2022/8/18. https://www.fcc.gov/document/fcc-reports-congress-future-universal-service-fund
- CCIA (2022). EU Telcos' Demand for Network Traffic Payments is Fundamentally Flawed. 2022/5/2. https://www.ccianet.org/2022/05/eu-telcos-demand-for-network-traffic-payments-is-fundamentally-flawed/
- Chee, F. Y. (2022). EU's Vestager assessing if tech giants should share telecoms network costs. Reuters, 2022/5/2. https://www.reuters.com/business/media-telecom/eus-vestager-assessing-if-tech-giants-should-share-telecoms-network-costs-2022-05-02/
- Chee, F. Y. & Mukherjee, S. (2022). Analysis: European telcos set to win fight with Big Tech, could set global agenda. Reuter, 2022/10/3. https://www.reuters.com/business/media-telecom/european-telcos-set-win-fight-with-big-tech-could-set-global-agenda-2022-09-30/
- Congress (2022a). S.2427 - FAIR Contributions Act. https://www.congress.gov/bill/117th-congress/senate-bill/2427?q=%7B%22search%22%3A%22s.+2427%22%7D
- Congress (2022b). H.R.8575 - FAIR Contributions Act. https://www.congress.gov/bill/117th-congress/house-bill/8575?s=1&r=4
- Dano, M. (2022). Here's why the telecom industry is taking aim at Big Tech.

2021/12/22. Light Reading. https://www.lightreading.com/optical-ip/heres-why-the-telecom-industry-is-taking-aim-at-big-tech/d/d-id/774280

- EDRi (2022). The European Commission threatens to undermine the core values of the free and open internet. 2022/6/9. https://edri.org/our-work/the-european-commission-threatens-to-undermine-the-core-values-of-the-free-and-open-internet/
- ETNO (2022). Europe's Internet ecosystem: A 72bn boost to GDP and 840k new jobs are within reach if gaps in network costs are tackled. 2022/5/2. https://etno.eu/news/all-news/8-news/735-eu-internet-ecosystem.html
- EU (2015). Regulation (EU) 2015/2120. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&from=en#d1e445-1-1
- FCC (2015). Open Internet Order. https://www.fcc.gov/document/fcc-releases-open-internet-order
- FCC (2022). Report on the Future of the Universal Service Fund. 2022/8/15. https://www.fcc.gov/document/fcc-reports-congress-future-universal-service-fund
- FT Live (2022). Keynote Panel: The Future of the EU Internet ecosystem – How should all digital actors contribute to a gigabit future?2022/9/26. https://techandpoliticsforum.live.ft.com/agenda/session/938789
- Gold, A. & McGill, M. H. (2022). New push to make Big Tech pay more for bandwidth. Axios, 2022/5/11. https://www.axios.com/2022/05/11/big-tech-pay-for-bandwidth-eu-south-korea
- Goldman, D. (2014). Slow Comcast speeds were costing Netflix customers. CNN, 2014/8/29. https://money.cnn.com/2014/08/29/technology/netflix-comcast/index.html
- Huston, G. (2022). From "Network Neutrality" to "Sender Pays", the Principles Remain Much the Same. CircleID, 2022/9/12. https://circleid.com/posts/20220912-from-network-neutrality-to-sender-pays-the-principles-remain-much-the-same

- IGF (2021). Universal access and meaningful connectivity. https://www.intgovforum.org/en/content/universal-access-and-meaningful-connectivity
- IGF (2022). Policy Network on Meaningful Access (PNMA). https://intgovforum.org/en/content/policy-network-on-meaningful-access-pnma
- Kim & Chang (2020). New Requirement and Enhanced Obligations for Value-Added Telecommunications Service Providers to Secure Means for Stability of Service. 2020/9.28. https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=22016
- Kim, S. (2021). Netflix and SK Broadband Battle Over Who Pays in South Korea. The Diplomat, 2021/8/6. https://thediplomat.com/2021/08/netflix-and-sk-broadband-battle-over-who-pays-in-south-korea/
- Kim, S. (2022). What the South Korea-US Summit Had to Say About Internet Policy. The Diplomat, 2022/6/7. https://thediplomat.com/2022/06/what-the-south-korea-us-summit-had-to-say-about-internet-policy/
- Layton, R. (2022). The Growing Global Movement For Fair Cost Recovery On Broadband Networks. Forbes, 2022/5/12. https://www.forbes.com/sites/roslynlayton/2022/05/12/the-growing-global-movement-for-fair-cost-recovery-on-broadband-networks/
- Layton, R. & Potgieter, P. (2022). A global movement for broadband fair cost recovery is underway. Strand Consult , 2022/8/10. https://strandconsult.dk/why-do-you-have-such-a-big-interest-in-the-way-companies-charge-for-traffic-on-the-internet-and-what-you-call-fair-cost-recovery-ceo-john-strand-talks-with-internet-policy-experts-r/
- Lee, J. (2021). S.Korea broadband firm sues Netflix after traffic surge from 'Squid Game'. Reuters, 2021/10/13. https://www.reuters.com/business/media-telecom/skorea-broadband-firm-sues-netflix-after-traffic-surge-squid-game-2021-10-01/

- Lee, W. (2022). Network-fee payment dispute draws mixed responses from South Korean lawmakers. MLex, 2022/9/21. https://mlexmarketinsight.com/news/insight/network-fee-payment-dispute-draws-mixed-responses-from-south-korean-lawmakers
- Mchale, J. (2022). New Korean legislation undermines Internet norms and raises broad trade concerns. The Disruptive Competition Project (DisCo), 2022/9/19. https://www.project-disco.org/21st-century-trade/091922-new-korean-legislation-undermines-internet-norms-and-raises-broad-trade-concerns/#.Yy97JnZBzIU
- Mitaksh (2022). European Union's Proposal To Get Big Tech To Pay Interconnection Fee Threatens Net Neutrality. MediaNama, 2022/8/23. https://www.medianama.com/2022/08/223-european-union-proposal-big-tech-telcos-net-neutrality/
- Mullin, M. (2022). Mullin Introduces Fair Contributions Act to Improve Rural Broadband Access. OKW News, 2022/8/1. https://okwnews.com/news/whatzup/whatzup-politics/mullin-introduces-fair-contributions-act-to-improve-rural-broadband-access
- Nakutavičiūtė, J. (2022). What is net neutrality: its history and importance. NordVPN, 2022/4/26. https://nordvpn.com/blog/what-is-net-neutrality/
- NCSL (2022). Net Neutrality 2021 Legislation. 2022/5/4. https://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-2021-legislation.aspx
- OpenNet (2022). [서명운동] 인터넷을 지킵시다! 망중립성을 지킵시다! 우리는 '망이용료' 법안에 반대합니다. https://docs.google.com/forms/d/e/1FAIpQLScVtXUb_26yWstm74mfmO9RiKFpm9Ut311q4kVn1kopY-acuw/viewform
- Pollina, E. &, Fonte, G. (2022). Exclusive: Big Tech should share Europe network costs, France, Italy and Spain say. Reuters, 2022/8/2. https://www.reuters.com/business/media-telecom/exclusive-france-italy-spain-call-tech-firms-pay-telecoms-networks-2022-08-01/
- Rosemain, M. & Chee, F. U. (2022) EU to consult on making Big Tech contribute

to telco network costs. Reuters, 2022/9/9. https://www.reuters.com/technology/eu-consult-big-tech-contribution-telco-networks-by-end-q1-2023-2022-09-09/

- Shin, H. (2022). S.Korea's Yoon asks Biden to resolve concerns over EV subsidy rules. Reuters, 2022/9/22. https://www.reuters.com/technology/us-skorea-exchange-frank-views-vehicle-credits-network-fees-2022-09-22/
- Stolton, S. (2022). EU executive eyes Big Tech's money to save 5G. Politico, 2022/6/27. https://www.politico.eu/article/commission-present-connectivity-infrastructure-act-eu/
- Telekom (2022). United appeal of the four major European telecommunications companies. 2022/2/14. https://www.telekom.com/en/company/details/united-appeal-of-the-four-major-european-telecommunications-companies-646166#2
- Wan, A. (2022). South Korea's 'Sender Pays' Policy Is a Threat to the Internet. The Diplomat, 2022/8/3. https://thediplomat.com/2022/08/south-koreas-sender-pays-policy-is-a-threat-to-the-internet/
- Weinberg, M. (2022) Saving the Universal Service Fund: Time for big tech to pay up. The Hill, 2022/8/25. https://thehill.com/opinion/congress-blog/3616131-saving-the-universal-service-fund-time-for-big-tech-to-pay-up/
- Yoon, H. S. (2022). Public Hearing Today on the Network Usage Fee Law… Will 2R of 'Big Tech Regulations' Begin? Korea Post English, 2022/9/19. https://korea.postsen.com/trends/amp/73628
- Yoon, S. Y. (2022a). [NEWS IN FOCUS] In Korea vs. tech giants, Goliath is winning. Korea JoongAng Daily, 2022/5/1. https://koreajoongangdaily.joins.com/2022/05/01/business/tech/Google-law-Netflix-law-inapp-payment/20220501070008988.html

- Yoon, S. Y. (2022b). Google, Netflix and Meta on the annual 'Netflix law' list. Korea JoongAng Daily, 2022/2/3. https://koreajoongangdaily.joins.com/2022/02/03/business/tech/telecommunication-service-Google-Netflix/20220203190110529.html

第六章 大專校園講座辦理

第一節 執行概況

本計畫依據委託辦理工作項目規定，規劃於我國大專院校辦理分享網路治理發展與國際趨勢實體講座至少 3 場次、各 2 小時、且出席人數需達 50 人以上（參閱表 6-1）。藉以讓更多大專青年對網路治理產生興趣，並了解網路治理發展與當前國際趨勢，進而願意關心並參與網路治理的議題討論。宣講場合則配合大專院校教師或校方人員安排於特定課程，或全系所的固定集會活動進行，出席者涵蓋全校師生。

本計畫已完成辦理北中南部各一場次的講座，惟受到 COVID-19 疫情影響，5 月 12 日的政治大學講座辦理方式從實體調整為線上；其餘兩場次，除維持實體辦理及保留「對俄斷網制裁」內容外，也請講者增加「未來網際網路宣言」相關資訊。

表 6-1 大專校園講座活動辦理概況

時間	學校	系所 / 課程	講題/講者	人數
5 月 12 日 15:00~17:00	北部 政治大學	傳播學院／ 「傳播法規與倫理」課程	黃勝雄 NII 董事長 TWNIC 執行長 ／ 地緣政治衝突 時代的網路治理	58 人
9 月 29 日 14:10~16:10	中部 東海大學	資訊管理系暨研究所／ 專題演講		77 人
10 月 5 日 14:00~16:00	南部 中正大學	傳播學系-電信傳播研究所／ C-Club 傳播專題演講		51 人

為了讓更多學校師生獲知活動訊息，執行團隊配合學校需求提供活動海報（參閱圖 6-1）讓系所進行公告，利於活動的宣傳，吸引更多校內師生參加。



圖 6-1 校園講座活動海報（東海大學）

第二節 政治大學場次

一、活動訊息

- 時間：111 年 5 月 12 日（四）15:00～17:00
- 系所：政治大學 傳播學院
- 課程名稱：傳播法規與倫理
- 辦理方式：線上課程（使用 Microsoft Teams 視訊系統）
- 人數：58 人
- 講題：地緣政治衝突時代的網路治理
- 講者：黃勝雄 執行長／財團法人台灣網路資訊中心

二、演講內容摘要

(一) 網路治理的發展與關注焦點

網路治理發展的軌跡濫觴於 1960～70 年代美國軍方進行的科學研究計畫，隨著網路技術的成熟及應用方式的改變，網路治理已經從單純的軍事研究，轉變成多方利害關係人共同針對網路相關議題進行探討與協調。到了 2010 年後，網路治理不只是針對人類世界的需求，隨著物聯網、AI 技術以及大數據的蓬勃發展，這些可連上網路的物件（如穿戴裝置等）都將納入網路治理的探討範圍之內，如今的網路已經發展為跨物種的網路世界。

網路治理的關注焦點與網路技術的發展息息相關。在過去數十年的發展重點為基礎建設的擴散與普及，網路技術的逐漸成熟以及商業模式的大量應用，使得網際網路具有高度的包容性。近十年來的發展主軸則強調技術創新，例如 Facebook、Instagram 等業者提供了許多創新的服務與應用。

未來十年的發展重點為建構網路政策法規與治理框架，過去數十年來關於網路治理的發展過程十分緩慢，相關法律、規範成效不彰，導致問題未能從根本解決，因此未來網路治理的發展重心將著重於打造一個具有穩定性、安全性的一個全球性網路治理架構。

(二) 網路空間的規範

根據芝加哥學院 Lawrance Lessig 所提出的理論，網路空間是由 4 個驅動力所規範，包含：法律、他律或利害關係人訂定的共識、技術標準，以及市場。過去數十年，大多是由技術標準引領法律的制定，但 2018 年歐盟的 GDPR 施行後，訂定了技術標準必須符合法律的相關要求。

講者以網路中介者（Internet intermediaries）的責任為例，說明網路空間的規範如何實行。所謂網路中介者即為電信業者、註冊管理機構、平台業者和搜索引擎等中間人，僅負責提供網路資訊的傳遞，而不介入內容的編輯與修訂。例如電信業者需要遵守當地電信管理法的規定，且須依循網路中立原則，使網路的使用得以普及且不得有差別待遇。而平台業者除了須遵守當地法律規定(例如美國通訊端正法 Communications Decency Act)，也普遍遵守由多方利害關係人訂定馬尼拉中介者責任原則（Manila Principles on Intermediary Liability），該原則並非國際法無強制效力，但多數國家及業者願意遵守該原則，形成一種普遍的自律規範。

(三) 網路犯罪追查不易

根據我國警政署的網路犯罪頂級域名統計資料，僅有 4.1%的域名屬於.tw，亦即高達 95.9%的網路犯罪案件難以追查。網際網路具有多層斷鏈的特性，即伺服器 IP、域名註冊人，以及攻擊發動者，三方可能位在不同的法律管轄範圍，加深了犯罪偵查的困難度。

法律與管轄權具有地理限制，但網路具備「跨境」的特性，目前國際間的解決方案包括：司法互助，特色是緩慢且複雜；布達佩斯協定，同樣緩慢且複雜，擴充性也不足；最後一項是法律合作，但不僅透明度不足，

證據的採納性也有疑慮，此外也可能因為國家之間對於法律認定的不同而產生法律衝突。

講者接著介紹 TWNIC 整合國內 ISP 建構的 DNS RPZ（Response Policy Zone）機制，各家 ISP 的 DNS 可與 TWNIC 串接，透過法院判決、扣押命令，或是行政處分來啟動 RPZ。一旦 RPZ 寫入黑名單，全臺灣的解析系統皆會進行屏蔽。

(四) 經濟制裁與網路治理

經濟制裁在國際衝突事件中是常見的抵制手段，透過限制經濟資源的移轉達到制裁效果。制裁的種類可分為針對個別國家之制裁以及針對性的制裁，如恐怖主義份子、人口販運或特定人士、團體等。經濟制裁具有強制的法律效力，違反制裁可能面臨數百萬美元的罰鍰及相關刑責，因此被視為是非常有效的抵制手段。

2022 年 2 月底俄烏戰爭爆發後，烏克蘭政府正式向 ICANN 提出要求對俄羅斯實施制裁，停止俄國頂級域名 .ru、.pф 及.su 解析，並要求關閉位於俄國的 DNS 根伺服器。烏克蘭政府亦要求歐洲 IP 位址管理機構 RIPE NCC 取消其核發給俄國所有 IPv4 與 IPv6 位址的使用權。

對此，ICANN 與 RIPE NCC 均回應本身為中立機構，並無權力涉入戰爭，後續不會停止提供相關服務，亦不會刪除俄羅斯頂級國碼網域名稱。雖然 ICANN 與 RIPE NCC 拒絕烏克蘭的請求，但在可行的權限範圍內仍採取相關措施制裁俄羅斯，如 RIPE NCC 凍結俄羅斯主要電信公司之 IP 位址。

俄烏戰爭的爆發，促使三十多位 ICANN 現任前任董事及網路主導者共同發表「網路治理制裁原則」，內容包含切斷國家與網路連結的制裁行為不符合比例原則、將軍事與宣傳機構基礎設施視為網路制裁目標、建立有效網域名稱與 IP 位址制裁清單，並將其列入限制接取的目標、以及建立具有正當性的多方利害關係人審議程序等。當未來再度發生戰爭時，希冀

透過網路治理制裁原則能夠建立一具有正當性的審議程序，為網路治理制裁奠定基礎。

(五) 俄烏戰爭對網路世界的衝擊與影響

俄烏戰爭的爆發對於網路世界產生了改變。例如.UA 烏克蘭頂級國碼域名的重新配置，分別交由美國、法國、奧地利及波蘭來代管，使得烏克蘭的域名伺服器不被戰爭所影響；經濟制裁導致俄羅斯無法更新憑證，使得俄羅斯數位發展部發展自己的憑證及瀏覽器，並可能讓俄羅斯進一步使用獨立網路；Starlink 星鏈支援烏克蘭作戰，使得戰爭型態有所改變。而星鏈低成本、不易被干擾的特性未來也可能替代全球定位系統 GPS。

(六) 未來臺灣的數位發展建議

過去臺灣關注的數位發展主要為基礎設施，講者建議未來可多加關注太空以及海纜相關領域。俄烏戰爭爆發後，許多媒體評論以及外國智庫均認為中國大陸如對臺發動攻擊，必先透過攻擊海纜以切斷臺灣與世界的聯繫，進而提升攻擊成功的機率。

臺灣雖地處亞太地區海纜重要節點，但受周邊海域地形影響，導致海纜容易因為地震或洋流影響而斷裂，亞太區海纜迫切需要技術可行備援方案。對此，臺灣日前已提出「臺灣光纜通道計畫」透過在臺灣境內設置「陸纜」，以作為海纜斷裂時的備援方案，提升海纜的韌性，該計畫也能為臺灣帶來相關的政策效益。

過往政府對於網路基礎設施的發展較少介入，通常使其以自由放任的市場機制來發展，不過一旦基礎設施的發展無利可圖，將導致業者不願投入資源。講者建議政府此時應該積極介入競爭不足的區域，且建置相關公共設施、降低市場限制以鼓勵相關業者投資。

問與答

提問一：請黃執行長再詳細說明在演講中提到的「經濟可行性」？

回覆一：在訂定技術標準以及偵查網路犯罪時應考量「經濟可行性」的因素。在發表新的技術標準時，IETF 會確保其提供的程式碼是否夠在現行的系統內正常運作，且不會耗盡系統資源，符合經濟可行性方得予以通過。

講者接著以假冒銀行騙取重要個資的釣魚網站為例，說明網路犯罪的追查如依循刑事法進行追查，需經過冗長的偵查與審查過程，若是該犯罪網站 IP 位址註冊於國外，則耗費更多時間進行跨國訴訟，顯然不符合經濟可行性原則。TWNIC 與調查局、金管會合作成立三方快速通報管道，一旦調查局得知有國外金融釣魚網站，會立即通報金管會及 TWNIC，在三方互相確認後，TWNIC 即會停止解析該網站，以避免更多無辜民眾受害。停止解析釣魚網站雖非法院正式判決且無強制效力，但降低民眾受害擴散的效果立竿見影，顯然較經由法院判決來得快速有效，具有較高的經濟可行性。

三、活動剪影

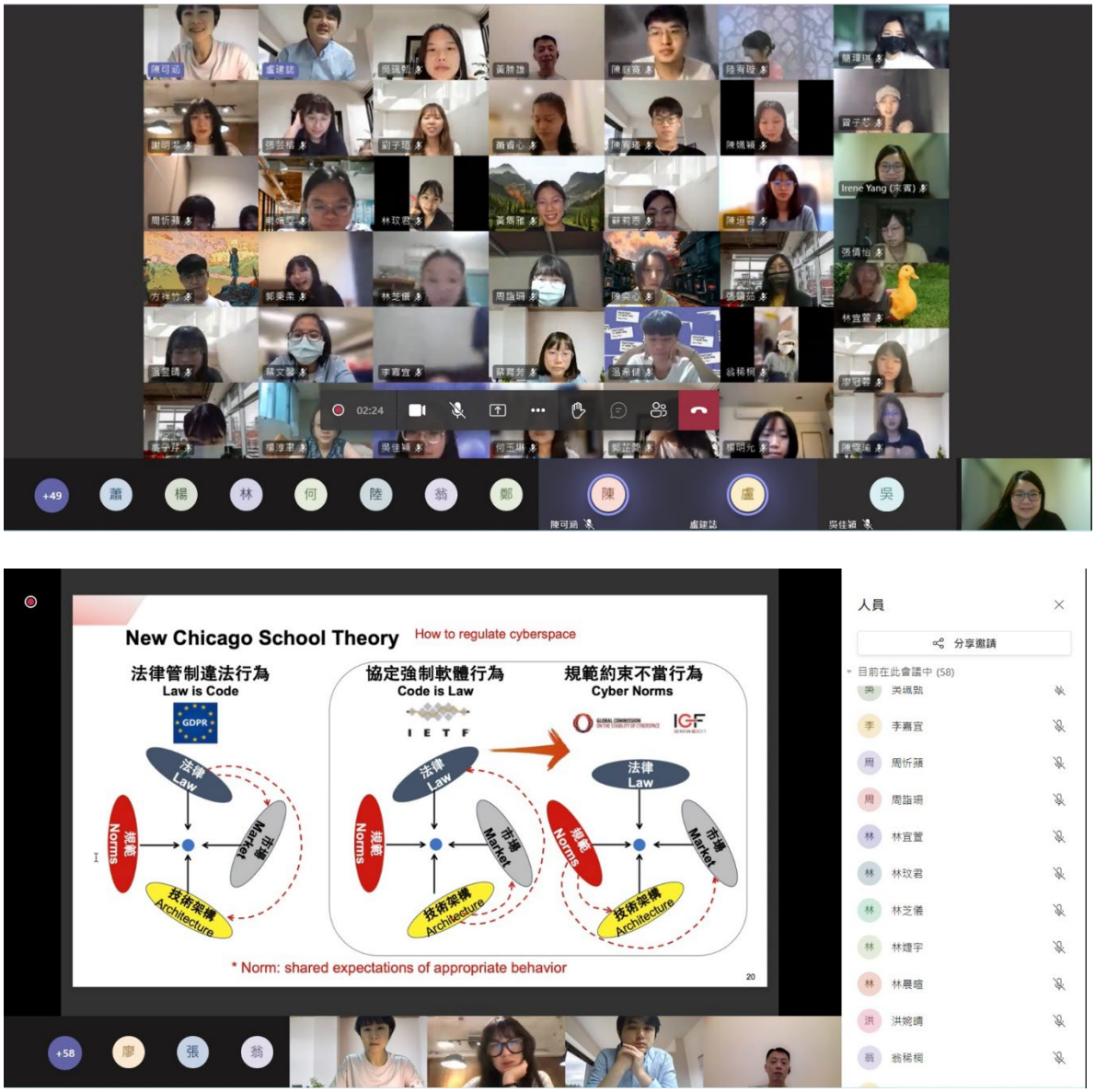


圖 6-2 政治大學線上講座畫面截圖

第三節 東海大學場次

一、活動訊息

- 時間：111 年 9 月 29 日（四）14:10～16:10
- 系所：東海大學 資訊管理系暨研究所
- 課程名稱：專題演講
- 地點：管理學院 M201 教室
- 人數：77 人
- 講題：地緣政治衝突時代的網路治理
- 講者：黃勝雄 執行長／財團法人台灣網路資訊中心

二、演講內容摘要

(一) 資訊安全的風險概念

黃執行長首先說明資訊安全的風險可分為「非系統性風險」以及「系統性風險」，非系統性風險僅對私人企業或單位造成影響，而系統性風險則會對整個網路世界造成危害，影響力更為深遠。

講者進一步將「非系統性風險」比喻為船隻、「系統性風險」比喻為海洋，說明私人企業就如同一艘船，若願意投入成本改善資訊安全，例如導入資訊安全系統、辦理資安教育訓練或採取相關資安措施，就彷彿是提升船隻的裝備及安全性，使得私人企業能夠逐漸茁壯成大船，能夠更加安穩地行駛於大海之中，同時也間接提升了企業的資產價值。而系統性風險就如同海洋，若稍有風浪，即對海上行駛的所有船隻（私人企業）造成影響，若從網路治理的角度思考，網路治理的目的即在降低海上的風浪，讓所有船隻可以安穩行駛。我們可透過多方利害關係人的治理，持續改善通

訊協定或相關法律、政策或教育等多個面向，讓整理網路安全更加穩定。

(二) 網路犯罪追查不易

根據我國警政署的網路犯罪頂級域名統計資料，僅有 4.1%的域名屬於.tw，亦即高達 95.9%的網路犯罪案件難以追查。網路攻擊的組成可分為伺服器 IP、域名註冊人，以及攻擊發動者，三方可能位在不同的法律管轄範圍，加深了犯罪偵查的困難度。

法律與管轄權具有地理限制，但網路具備「跨境」的特性，目前國際間的解決方案包括：司法互助，特色是緩慢且複雜；布達佩斯協定，同樣緩慢且複雜，擴充性也不足；最後一項是法律合作，但不僅透明度不足，證據的採納性也有疑慮，此外也可能因為國家之間對於法律認定的不同而產生法律衝突。

講者接著介紹台灣資訊網路中心（TWNIC）整合國內 ISP 建構的 DNS RPZ（Response Policy Zone）機制，各家 ISP 的 DNS 可與 TWNIC 串接，透過法院判決、扣押命令，或是行政處分來啟動 RPZ。一旦 RPZ 寫入黑名單，全臺灣的解析系統皆會進行屏蔽。此外，TWNIC 今年亦和 Dot Asia 簽署互助協議，針對發生於.tw 或.asia 的網路犯罪，雙方可互相通報不當內容，啟動迅速下架機制。

(三) 降低網路攻擊的手段

但凡連接網路的任何設備或資訊系統，無論投入多少成本防護，皆有可能遭到有心人士的入侵，且目前多數網路攻擊案件通常具有跨境的特性，受限於不同國家的法律管轄範圍，因此大部分的網路攻擊者至今仍逍遙法外，不必承擔法律責任。在如今資訊發達的時代，發起網路攻擊並非難事，基本上無須耗費太多成本即可能讓受害者蒙受巨大損失，自身也能獲取高額利益，直接助長網路攻擊發生的機率。

黃執行長以經濟學的角度分析，他認為提高網路攻擊的成本，降低網路攻擊所帶來的預期利益，便可減少網路攻擊事件。以私人密碼長度設定

為例，8 位數的大小寫字元僅需 22 分鐘即可被破解，但若使用者願意花費一點心思，將密碼長度增加為 11 字元（包含大小寫英文及數字），其被破解的時間將大幅增加為 41 年。對於使用者而言，多加背誦 3 字元也許難度不高，但對於攻擊者來說卻需要花費 41 年來破解，完全不符預期效益，如此便可降低攻擊者的企圖。

(四) 網路空間的規範與共識

根據芝加哥學院 Lawrance Lessig 所提出的理論，網路空間是由 4 個驅動力所規範，包含：法律、他律（Norms）或利害關係人訂定的共識、技術標準，以及市場。過去數十年，大多是由技術標準引領法律的制定，但 2018 年歐盟的 GDPR 施行後，訂定了技術標準必須符合法律的相關要求。不過，現行的網路世界仍以他律為主要規範，他律雖無強制法律效力，但在網路世界的所有利害關係人大多願意遵守相關共識以及技術標準。

現行網路空間存在許多熱門議題，包含 DNS 安全、網路犯罪、網路戰爭等，針對這些網路議題衍生出許多相關規範或共識，可從深度（Depth）、廣度（Breadth）以及合規性（Compliance）三個構面，來分析多方利害關係人對於相關議題之共識。深度層面即為規範是否具有標準一致性；廣度層面為評估多方利害關係人是否願意接受或加入該規範；合規性層面則是評估多方利害關係人是否願意完全遵守。

黃執行長接著以美國提出的《未來網際網路宣言》（The Declaration for the Future of the Internet, DFI）為例來分析，以深度層面而言，DFI 制定了一套完整的原則供加入簽署國遵守；在廣度層面來看，DFI 簽署國僅有 61 個，遠不及世界國家總數的半數，稍嫌不足；以合規性層面來說，簽署的國家皆承諾自願遵守 DFI 相關原則，合規性相對較高。

(五) 以使用者為目標的網路攻擊

黃執行長指出，目前的網路攻擊有大約 50%是以使用者為主要目標。很多網路攻擊源自於使用者習慣不佳，如密碼設定過於簡單、電腦未設置

登入密碼等弱點，讓入侵者有機可乘。講者進一步以國內知名半導體公司以及美國大型石油公司 Colonial Pipeline 為例說明，駭客經常使用「供應鏈攻擊」，透過駭侵企業員工或第三方合作夥伴取得權限後，進而存取企業內部網站進行綁架，並向受害企業要求高額贖金以取回系統控制權，造成企業偌大損失。若被駭對象為國家基礎設施，其造成的影響將更加嚴重。

網路攻擊未必需要規畫一套精良的攻擊手段才能成功，有時僅是因為個人或企業忽略了一個簡單的資安措施，而讓攻擊者抓到得以入侵的弱點，講者比喻就彷彿停車時忘記將摩托車鑰匙拔起，增加竊賊直接將摩托車騎走的機率。黃執行長也呼籲網路的使用者都應具備基本的資安意識，才不會讓有心人士趁虛而入。

(六) 未來戰爭型態將有所改變

俄烏戰爭爆發後，許多媒體評論以及外國智庫均認為中國大陸如對臺發動攻擊，必先透過攻擊海纜以切斷臺灣與世界的聯繫，進而提升攻擊成功的機率，更有報導指出若臺灣不幸失守，基於國安考量，美軍將會登陸摧毀臺灣的基礎設施，以免軍事機密被傳送至中國大陸，由此可知臺海發生戰爭，海底纜線存留的機率微乎其微，即便不被敵國攻擊，也會被以美軍保護國家機密的名義進行斷線措施。

在現行海洋法公約規範中，切斷海纜並非軍事攻擊行為，也就是說攻擊海纜可被視為合法的軍事目標，攻擊海纜議題成為灰色地帶。假設未來中國大陸真的攻擊臺灣海纜，囿於戰爭法不將攻擊海纜視為軍事攻擊，因此臺灣不得將其攻擊海纜行為視為發動軍事攻擊的理由。

(七) 制裁與網路治理

2022 年 2 月底俄烏戰爭爆發後，烏克蘭政府正式向 ICANN 提出要求對俄羅斯實施制裁，停止俄國頂級域名.ru、.pф 及.su 解析，並要求關閉位於俄國的 DNS 根伺服器。烏克蘭政府亦要求歐洲 IP 位址管理機構 RIPE NCC 取消其核發給俄國所有 IPv4 與 IPv6 位址的使用權。

對此，ICANN 與 RIPE NCC 均回應本身為中立機構，並無權力涉入戰爭，後續不會停止提供相關服務，亦不會刪除俄羅斯頂級國碼網域名稱。雖然 ICANN 與 RIPE NCC 拒絕烏克蘭的請求，但在可行的權限範圍內仍採取相關措施制裁俄羅斯，如 RIPE NCC 因遵守歐盟制裁令凍結俄羅斯主要電信公司之 IP 位址。

俄烏戰爭的爆發，促使三十多位 ICANN 現任前任董事及網路主導者共同發表「網路治理制裁原則」，內容包含將軍事與宣傳機構基礎設施視為網路制裁目標、建立有效網域名稱與 IP 位址制裁清單，並將其列入限制接取的目標、以及建立具有正當性的多方利害關係人審議程序等。當未來再度發生戰爭時，希冀透過網路治理制裁原則能夠建立一具有正當性的審議程序，為網路治理制裁奠定基礎。

然而，如此仍可能引發其他潛在問題，比如國家為避免自己遭受他國的經濟制裁，自行研發新的網域系統或網路空間，如此將會產生網路分裂的問題。講者表示，經濟制裁手段已不再只是凍結銀行帳戶，凍結網域名稱與 IP 位置已然成為新戰場，而網路制裁的權力落在少數利害關係人手上，判決上的偏頗也是另一項隱憂。

(八) 結語

全球地緣政治衝突頻傳，也漸漸影響了網路治理的面貌。針對地緣政治衝突所帶來的衝擊，黃執行長提出了 3 個值得注意的重點，第一是提升網路韌性，研擬關鍵基礎設施之相關應變措施，特別是針對戰爭時期應有不同的管理措施；其次為資料備援的重要性，在戰時緊急狀態如何合理的調動資源是至關重要的；最後是網路分裂議題，目前層出不窮的國際衝突讓網路面臨被分裂的危機，如何維護網路世界的穩定與安全，是所有網路世界的公民需要共同努力的目標。

問與答

提問 1：近期熱門的柬埔寨詐騙事件，我們該如何應對？

回覆 1：柬埔寨詐騙人員以及相關網站大多分布於境外，跨國的網路犯罪因涉及境外司法管轄權的問題，追查相當困難，即便得以進入司法審查階段，也是非常曠日廢時。網路詐騙的樣態日新月異、千變萬化，僅靠政府及相關單位的把關無法全面防堵，因此，最根本的防治方法為提升自身的資安意識，看到不合理的工作招募、來路不明的網站或廣告切勿隨意點擊也勿輕易採信。

提問 2：中、俄多年來宣稱要脫離現行網路世界，建置另一獨立網路空間，是否有可能實現？

回覆 2：現行網路世界並無強制所有國家必須連上網路，就以經濟效益角度而言，現行網路世界所帶來的經濟效益十分龐大，若是中國大陸、俄國等國家完全脫離，極可能喪失極大的經濟利益，也因此目前仍不太容易發生網路分裂，意圖實行網路分裂的國家必須考量政治與經濟的因素。

三、活動剪影



圖 6-3 東海大學講座照片

第四節 中正大學場次

一、活動訊息

- 時間：111 年 10 月 5 日（三）14:00～16:00
- 系所：中正大學 電訊傳播研究所
- 課程名稱：CC Club 專題演講
- 地點：社會科學院 R227 教室
- 人數：51 人
- 講題：地緣政治衝突時代的網路治理
- 講者：黃勝雄 執行長／財團法人台灣網路資訊中心

二、演講內容摘要

本場次演講內容與東海大學場次雷同，以下僅記錄問與答的部分。

提問 1：目前科技巨頭所提供的服務與人民的生活息息相關，這些科技巨頭所制定的規範是否將成為未來網路空間的共同規範？

回覆 1：現行網路空間確實有受到科技巨頭規範影響的趨勢，用戶在使用相關服務時都必須同意相關條款，這是無可避免的契約行為。先前提到 Lawrance Lessig 的網路空間規範中，「市場」也是一個網路空間規範的驅動力，科技巨頭在擁有廣大用戶之後取得主要市場，其巨大的影響力必然會逐漸改變網路空間規範，這是網路規範形成的自然過程，且市場的自由競爭也無法單靠政府進行介入。

提問 2：若未來職場想進入數位或是科技產業，老師會建議如何培養自身的技術與能力，增加進入業界的機會？

回覆 2：從就業的角度，資訊科技的人才需求會越來越少，而其他延伸出來的工作（如治理）的人才需求會越來越多，跨領域的能力會越來越重要，舉例來說，政府與大型科技公司的資訊部門需要同時懂一點技術與法律的人才，因為雙方都需要這樣的人才進行相互溝通。

提問 3：VPN 真的如廣告所言的安全嗎？

回覆 3：以資訊技術的角度來說，開發者投入大量資本研發出來的東西是很安全的，但我們無法控制安全資訊技術以外的控制措施、法律要件、監管機制，也就是說，我們無從得知他們是否有自己使用那些資料，或是否有真的保護我們所交出的那些資料，才是真正的潛在風險。

提問 4：網路發展多年，但使用者規範仍無法達到法律的層次，目前相關網路的法律多還停留以經濟層面去管制大型科技企業，請問未來會不會如傳播科技的相關法規，回到國家層級以法律去規範網路市場或使用？

回覆 4：我個人認為有點困難，傳播領域的規範是以限制物理性的方式去限制產業發展，可以維持較長的時間，但網路發展的速度太快，管制無法透過物理層次去進行限制，比如封鎖一個侵權網站就會出現 100 個新的網站，另外，法律須得到社會共識才得以產生，速度也遠遠追不上科技的快速發展，更不用說網路的基礎建設（如海底纜線）十分脆弱，而且還有許多漏洞。

三、活動剪影



圖 6-4 中正大學講座照片

第七章 人才培訓課程辦理

第一節 活動內容與辦法

一、活動簡介

為什麼烏克蘭政府提出「將俄羅斯從全球網路『消失』」的訴求，沒有獲得國際廣泛支持？歐美國家接連針對網路平臺祭出法規措施，能否有效打擊網路違法內容及促進數位市場公平競爭？又為什麼全球的網路自由度會呈現持續下滑，而各國和臺灣的情況又是如何？如果您關心這些問題，歡迎報名「2022 網路治理研習營」免費課程活動，除了將帶您探討當前重要的網路政策議題外，結業學員還可獲頒獎學金，並有機會參加國際會議。

- 名稱：2022 網路治理研習營
- 時間：111 年 5 月 7 日（星期六）
- 地點：Webex 線上會議室

二、課程簡介

本年度研習營課程包含 3 小時的課前自我預習（參閱表 7-1），以及 1 日（7 小時）線上互動式課程（參閱表 7-2）。上課方式有課堂講習暨問答，以及分組演練；課程主題涵蓋：網路人權、網路內容與平臺、網路治理準則探討以及網路安全。課程最末，也邀請到先前表現優異的結訓學員韋詠祥（陽明交通大學資工系學生），與學員分享其實際參與網路治理之經驗。

表 7-1 課前自我預習教材

5/7（五）前	課前預習
1. 影片	• 網路基礎建設（吳國維理事長，臺灣網路治理論壇）

	• 內容亂象誰負責？（曾更瑩合夥律師，理律法律事務所）
2. 文章	• What is Internet governance? (The Digital Watch of the Geneva Internet Platform) • Critical internet resources (The Digital Watch of the Geneva Internet Platform) • Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains • 網路治理：展望 2022（TWNIC Blog 摘譯）

表 7-2 研習營課程表

時間	課程		講者 / 主持人
08:45 - 09:00	線上報到		
09:00 - 09:50	專題講習	數位人權：全球網路自由度及政策趨勢	NII 產業發展協進會 陳文生顧問
10:00 - 10:50	案例探討	平臺規範的時代來臨了？	理律法律事務所 曾更瑩合夥律師
11:00 - 12:00	專題探討	GAC 對 ccTLD 的準則及綱領 （針對預習 QA，無講習）	TWIGF 吳國維理事長
12:00 - 13:00	午休		
13:00 - 13:50	專題講習	網路安全：從烏俄戰爭看安全議題	TWNIC 黃勝雄執行長
14:00 - 15:30	分組演練	議題討論／角色扮演 (分組：人權、平臺規範、安全)	講者帶領學員演練
15:40 - 16:20		小組成果報告	學員推派代表
16:20 - 17:00	結業式	經驗分享、課後測驗、結業手續	

三、講師簡介

講師	經歷與專長
 陳文生 顧問 NII 產業發展協進會	**經歷** • 臺灣網路治理論壇（TWIGF）常務監事（現任） • NII 產業發展協進會執行長 • 哈瑪星科技公司總經理 • 中國科技大學資訊學院院長 • 臺灣網路資訊中心董事兼執行長 • 國立高雄第一科技大學資管系主任、所長/電算中心主任/圖書館館長/教務長 • 教育部電算中心高級管理師、高級分析師、副主任 • 行政院資通安全稽核委員 • IEET 評鑑委員、教育部科大／技術學院評鑑委員 • 經濟部科專計畫、SBIR 等政府計畫評審委員 • 行政院工程會政府採購評審委員 **專長** • 網路規劃與管理 • 資通安全管理 • 資訊系統與管理 • 網路治理公共政策
 吳國維 董事 NII 產業發展協進會	**經歷** • 亞太區網路治理論壇（APrIGF）多方利害關係人指導委員會委員（現任） • 臺灣網路治理論壇（TWIGF）理事長（現任） • 中華電信股份有限公司董事 • NII 產業發展協進會執行長 • ICANN 董事 **專長**

講師	經歷與專長
	• 網路治理 • 網路關鍵資源管理政策 • 資訊安全管理 • 組織領導管理 • 國際事務推動及參與
 曾更瑩 合夥律師 理律法律事務所	**經歷** • 國家發展委員會個人資料保護法諮詢顧問（現任） • 台灣網路資訊中心（TWNIC）國際事務委員會委員（現任） • 臺灣網路治理論壇（TWIGF）常務理事（現任） • 台北市消費者電子商務協會監事、法規委員會委員（現任） • 台灣網路與電子商務產業發展協會監事（現任） **專長** • 電信、電子商務 • 網路法律、OTT • 金融科技、共享經濟、電子支付 • 個資及隱私權保護
 黃勝雄 執行長	**經歷** • NII 產業發展協進會 董事長（現任） • 亞太網路資訊中心（APNIC）董事（現任） • 亞太網路治理論壇（APrIGF）多方利害關係人指導委員會委員（現任） • 臺灣網路治理論壇（TWIGF）理事（現任） • 國際發展合作基金會諮詢委員（現任） • 行政院資通安全稽核委員（現任）

講師	經歷與專長
台灣網路資訊中心（TWNIC）	• 台灣高等檢察署電腦犯罪防治中心諮詢委員（現任） • 電信事業普及服務基金管理委員會委員（現任） • 亞洲（.asia）頂級網域註冊管理局諮詢委員 • ICANN Root Zone 中文標識生成委員會副主席 **專長** • 網際網路通信技術 • 資訊治理 • 政策規劃 • 關鍵網路資源 • 國際事務推動及參與

四、報名資格與方式

(一) 報名資格

開放具備以下條件的大專青年及社會各界人士（政府部門、企業、學研單位、公民團體等）報名：

- 對網路公共政策有興趣，且
- 樂於參與網路政策議題討論，且
- 具備一定英文程度(課程資料含有英文內容,且鼓勵參與國際會議)

(二) 報名時間

自 111 年 3 月 23 日起，至 111 年 4 月 10 日截止（臺灣時間）。

(三) 報名方式

本次活動一律透過活動網站線上報名，報名時須完整填寫報名表，報

名表內容包含以下問題：

- 姓名、年齡、單位職稱、聯絡資訊等基本資料。
- 為什麼想參加本研習營？
- 如何得知本研習營訊息？
- 最關心什麼網路政策議題？
- 曾參加哪些網路政策議題相關事務或活動？
- 除了以上提供的資訊，使用 200 字以內的文字簡短介紹自己。

五、評選與錄取

(一) 評選標準

主辦單位組成評選小組針對報名者的申請動機、對網路議題的關切度、相關事務或活動參與經驗及熱忱、英文程度等項目，進行綜合評估。

(二) 錄取名額

本研習營預計招收 20 名學員。

(三) 結果公布與通知

評選結果於 111 年 4 月 18 日於本研習營網站公布，並以電子郵件個別通知錄取學員。

惟我國 COVID-19 疫情自 4 月開始升溫，雖疫情指揮中心未將全國疫情警戒調整為三級，但每日確診人數逐日攀升，為維護全體學員及講師的健康，以及全力配合政府防疫措施，經與通傳會討論後，決議將本研習營由實體調整為線上課程，並於以電子郵件信件通知錄取學員。

六、學員義務

(一) 活動前夕

繳交「出席保證書」：為避免浪費學習資源，錄取學員須於 111 年 4 月 22 日前完成填寫「線上出席調查表」，調查表中需一併上傳「出席保證書」，先回傳者可優先選取分組組別。逾期未完成填寫者，視同放棄錄取資格，由候補名單遞補。

完成 3～4 小時的課前自我預習：錄取學員須於 111 年 5 月 7 日前完成指定的預習課程。

(二) 研習營期間

全程出席，積極參與討論，並遵守主辦單位訂定之活動規範。

七、學員獎勵

全程參與課程且通過課後測驗者，可獲得：

1. 結業證書乙紙（公務人員可獲得學習時數 7 小時認證）。
2. 結業獎學金新臺幣$ 1,000 元（不含公務人員）。
3. 參加優秀學員遴選：優秀學員可獲得全額差旅補助參與國際相關會議（以 1 名為限；視新冠肺炎疫情和國際會議舉辦情況而定）

八、實習安排

針對有意願的結業學員，安排實習機會。預計實習時數約 12 小時，名額以 3 人為限，並提供每人新臺幣 2 千元的實習津貼。

實習項目（包含但不限於）：

- 協助蒐集和彙整網路治理議題資料
- 參與國內外網路治理相關會議（實體／線上）並提供會議記錄
- 彙整中英文資料

第二節 學員招募與評選

一、活動網站

本年度研習營活動網站網址為 https://www.igcamp.tw/，共有：首頁、最新消息、活動內容、活動辦法、評選公告、學習資源等 7 個項目選單，網站首頁如圖 7-1 所示。



圖 7-1 研習營活動網站

二、活動宣傳

本年度研習營的活動宣傳方式，除了請通傳會協助透過公文系統發文至業務相關部會之外，亦請教育部協助轉文至全國大專院校，其他的宣傳管道如下：

- 臺灣網路治理論壇（TWIGF）Facebook 社團發文



- 設計電子報



為什麼烏克蘭政府提出「將俄羅斯從全球網路『消失』」的訴求，沒有獲得國際廣泛支持？歐美國家接連針對網路平臺祭出法規措施，能否有效打擊網路違法內容及促進數位市場公平競爭？又為什麼全球的網路自由度會呈現持續下滑，而各國和臺灣的情況又是如何？如果您關心這些問題，歡迎報名「2022網路治理研習營」免費課程活動，除了將帶您探討當前重要的網路政策議題外，結業學員還可獲頒獎學金，並有機會參加國際會議！

名額有限，報名從速！更多活動詳情，請至活動網站查詢。

活動資訊
時間：2022年5月7日（六）08:40~17:00
地點：IEAT 會議中心9樓 902教室

報名時間
即日起至2022年4月10日（日）23:59 截止

錄取公告
2022年4月18日（一）於本活動網站公布，並以email個別通知錄取學員。

立即免費報名

igcamp@nii.org.tw | https://www.igcamp.tw/

© Copyright 2022 網路治理研習營 All Rights Reserved

- 網路治理觀測站（https://igwatch.tw/）



三、報名與評選

本次研習營報名期間共收到 55 份報名表，執行單位首先針對報名表填寫之完整性進行初步審查，篩選標準包括：各項欄位是否均已填寫，以及內容是否有明顯的答非所問之情形等，初步篩選之結果，55 筆報名資料均符合資格，並於 4 月 12 日提請委員審查。

本次評選作業由本計畫之計畫主持人及協同主持人，以及 3 位外部專家組成，共同針對報名者的申請動機、對網路議題關切度、相關事務或活動參與經驗及熱忱、英文程度等項目進行綜合評估。

評選方式係採個別評分及評選會議討論兩階段進行，最後依據 5 位審查委員之共識，選出 26 位正取學員及 13 位備取學員。

四、學員組成概況

經執行單位通知聯繫正、備取學員後，共計 31 人繳交出席保證書聲明將出席研習活動，學員的組成概況可參考圖 7-2，以大專院校為最多，共有 22 位參加（71%），其他組成分別為：1 位來自公民團體（3%）、2 位來自學研單位（6%）、2 位來自民間企業（7%）以及 4 位任職於政府部門（13%）。

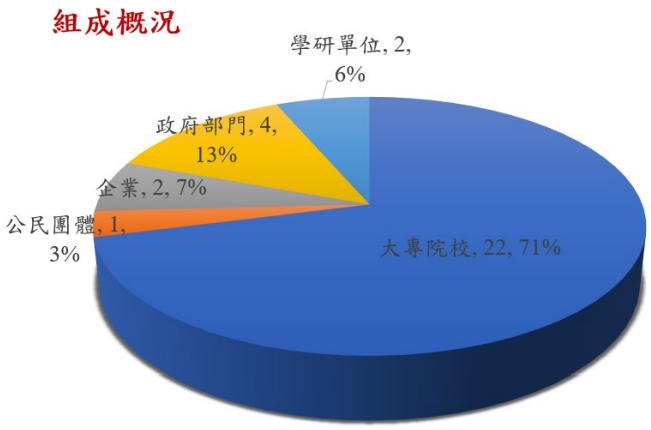


圖 7-2 研習營學員組成概況

若從參加者的年齡分布來看（參閱圖 7-3），以 20～29 歲為最多，共有 18 位參加（58%），其他年齡層分別為：19 歲及以下 1 位（3%）、30～39 歲 6 位（19%）、40～49 歲 4 位（13%）、50 歲及以上 2 位（7%）。

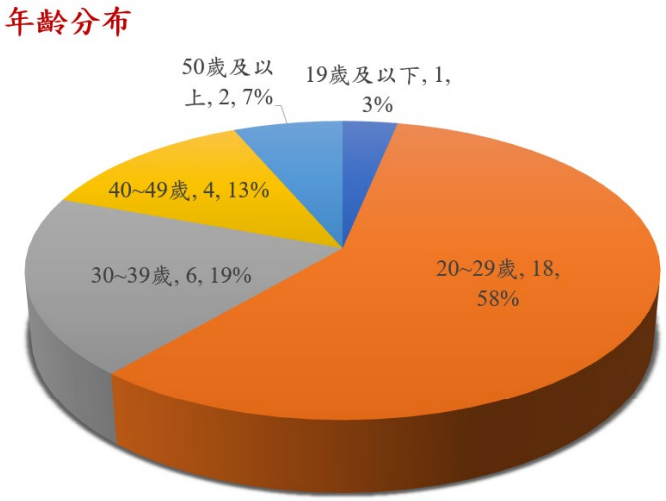


圖 7-3 研習營學員年齡分布

在參與動機方面（參閱圖 7-4），近半數學員均是因為對網路治理議題有興趣 13 位（42%），其他的動機分別為：與工作或學業相關 8 位（26%）以及想參與網路政策議題討論 10 位（32%）。

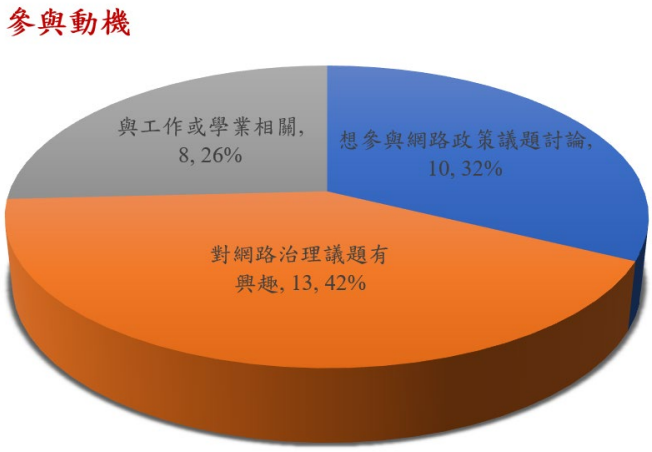


圖 7-4 研習營學員參與動機

執行單位亦參考 IGF 2022 議題徵求類別，以及本次研習營規劃之課程內容，針對學員最關心的網路政策議題進行調查（參閱圖 7-5）。將近半數

學員最關心網路安全議題（14 位，45%），其他由高至低依序為：數位經濟（5 位，16%）、網路人權（4 位，13%）、新興科技（4 位，13%）、內容與平臺（3 位，10%），以及數位包容（1 位，3%）。

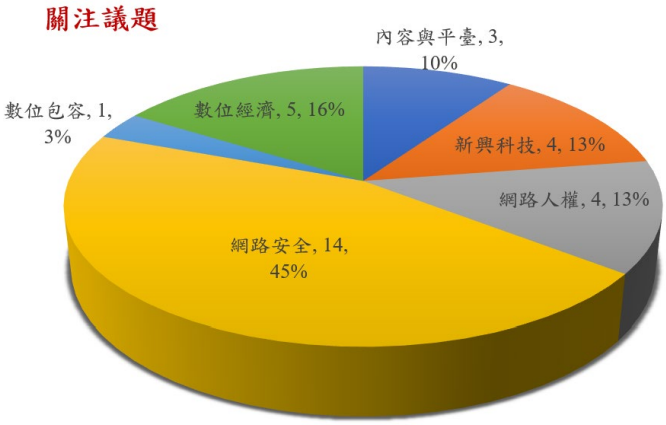


圖 7-5 研習營學員最關心的網路政策議題

第三節 課程摘要紀錄

一、專題講習

(一) 數位人權：全球網路自由度及政策趨勢

講者：陳文生／NII 產業發展協進會 顧問

1. 前言

美國發起的《未來網路宣言》在 2022 年 4 月 28 日舉辦線上發布會，全世界有 61 個國家參加，我國由時任行政院數位政委唐鳳代表簽署。宣言的內容包括：保護所有人的人權和基本自由、推動訊息自由流通的全球網路、推動包容性且可負擔的連線，讓所有人從數位經濟獲益、加強對全球數位生態系統的信任，包含透過保護隱私及保護和強化以多方利害關係人模式（multistakeholder）來治理網路共 5 大承諾。

2. 人權與數位人權

實體世界中，人民是受到憲法的保障，在我國憲法第二章中，規範許多人民權利及義務。目前聯合國的九大核心人權公約裡面，臺灣也已經通過施行法之公約，包括了「公民與政治權利國際公約」、「經濟社會文化權利國際公約」、「消除對婦女一切形式歧視公約」、「兒童權利公約」及「身心障礙者權利公約」。

OCF（Open Culture Foundation）是 APC （Association for Progressive Communications，進步通訊協會）的會員之一，其制定的網際網路憲章（Association for Progressive Communications），以七個大主題定義了網際網路中各種關於人的權利：包含人人都能上網；言論和結社自由；獲取知識；共享學習和創造—自由和開源軟體和技術開發；隱私、監控和加密；治理網路；權利的認識、保護和實現。

另外，澳洲的研究機構 Digital Rights Watch 及國際網路人權組織

（Access Now）也都對數位人權做長期的研究並提出相關重點主題。

3. 全球網路自由度

由 Freedom House 所提出的《2021 年全球網路自由度報告》中顯示，全球自由度連續 11 年下滑，美國連續 5 年排名下滑，而中國則持續 7 年都墊底。本評比共有 3 大類 21 子項共 100 分（詳圖 7-6），評比全球 70 個國家。臺灣在評比後獲得 80 分，全世界排名第五、亞洲排名第一。

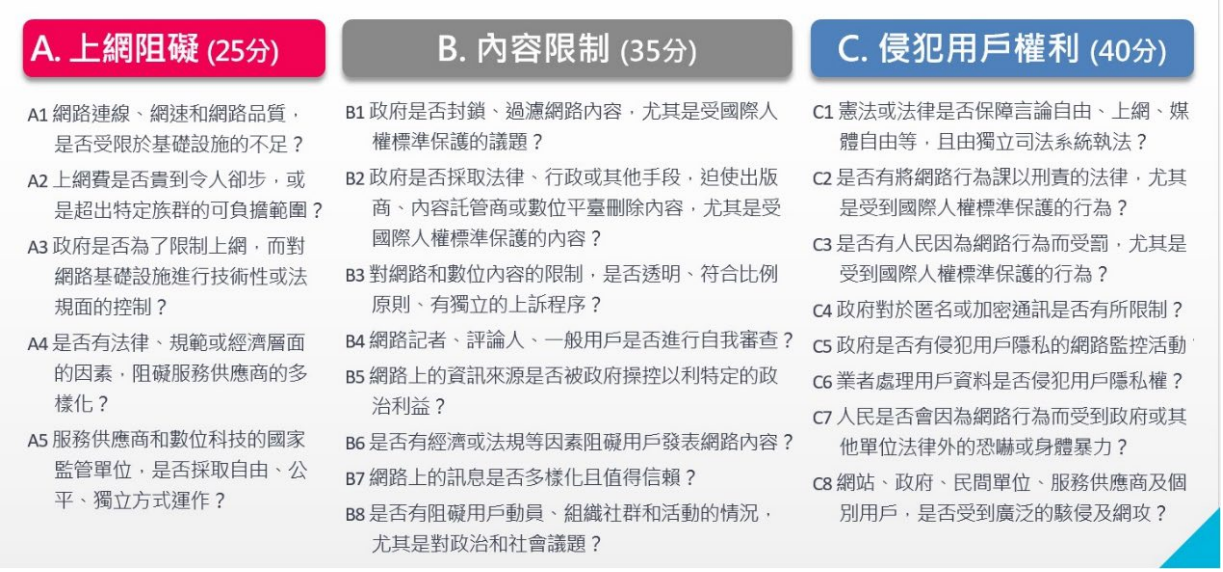


圖 7-6 《2021 年全球網路自由度報告》評比項目

4. 全球相關政策趨勢

早期的網路規範由美國主導，但自由放任方式衍生各種網路濫用問題，於是各國政府開始監管數位領域，有 48 國推出新規監管科技公司，當中有 24 國已經開始針對平臺內容監管、38 國做到資料監管，另外有 21 國對於競爭秩序做監管。

在平臺內容監管方面，民主國家精心設計的內容法規主要是加強透明度與問責制，希望可減輕線上危害。而在威權國家，平臺內容監控可能會遭到獨裁者濫用，用在打壓人民對政治、社會和宗教的不同訴求。

資料監控方面，為方便政府擴大監控的法規或措施，採取的作法包括了資料在地化、禁止私人通訊採用加密、把個資交給幾乎不受監督的執法

單位、以模糊的國安為由索取個資以及對資料跨境傳輸施加繁重的許可要求等，38 國實施資料在地化、破壞加密，也因此擴大了人民對於政府監控的疑慮。而在21個擬捍衛市場競爭秩序的國家中，也可能因為各個國家對於政策不同目的，讓競爭秩序監控淪為專制政權的工具。

對於網路監管，除了中國的數位威權主義及美國的傳統自由主義外，歐盟提出第三種方式，如數位服務法草案、數位市場法草案為科技產業制訂積極的規則；臺灣則有「網際網路視聽服務法」草案（簡稱 OTT TV 專法）、美國「平臺問責制和消費者透明度法」草案等，都是希望能透過多方利害關係人的討論得出共識，討論出著重透明度和正當程序的規範，讓網路監管能朝著正向發展。

5. 我國網路自由度和相關政策

臺灣在「A.上網阻礙」的 5 項指標中有 4 項滿分，凸顯出臺灣網路普及率很高、沒有顯著數位落差、有獨立監管單位，且資費民眾可負擔也可自由選擇 ISP。但也有需要改善的地方，像是供應商多樣化項目因被視為電信市場由特定業者主導，另外，雖有電信和廣播的獨立監管單位「通傳會」，但民眾對其獨立性還是有所疑慮。

「B.內容限制」的 8 項指標中，臺灣則獲得 5 項滿分，代表沒有網路封鎖和審查、言論自由、訊息多樣化。待改善的問題包括網路內容責任的法律，如社會維護法等，可能會導致民眾自我審查言論；臺灣兩大政黨和中共皆於臺灣的網路空間進行政治影響力的假訊息操弄也是需注意及改善的地方。

「C.侵犯用戶權利」的 8 項指標中臺灣沒有獲得滿分的項目，但報告中指出我國憲法有保障言論自由且有獨立的司法系統。這項指標有很多需要改善的問題，包括多項法律將網路行為定論為犯罪，且有受罰案例、未經法院核准的通訊監察，及索取通聯紀錄的案件增加、「科技偵查法」草案提高執法單位的監控能力，有侵犯人權的疑慮等。

根據國際媒體的報導，臺灣的網路自由度排名超越德、美等民主國家，是不錯的成績。網路自由需全民共同捍衛，網路治理也需要大家共同參與，我們如何在數位領域裡，適當和負責任地將數位人權理念推廣至全球各地，俾讓更多人享有數位人權。我們每一個人都有責任成為一個良好的數位公民，共同打造一個更理想的數位世界。

(二) 俄烏戰爭對網路治理規則的影響

講者：黃勝雄／台灣網路資訊中心 執行長

1. 網路治理的發展軌跡

網路治理的發展軌跡共分為五個階段，第一階段為軍事發展階段，網際網路的起源始於 1960 年代美國軍方的科學研究，網際網路僅作為軍事用途；第二階段為學術研究階段，1970～1990 年代產出了大量的技術標準如 TCP/IP（傳輸控制通訊協定／網際網絡通訊協定），而此階段的網際網路能夠快速發展，是因為 TCP/IP 技術標準訂定時須提供可執行的開源程式碼以供審核，一旦新技術標準發表，就能讓所有網路相關社群及終端設備取得程式碼，得以快速適用最新標準；第三階段為商業發展階段（1990～2000 年代），Tim Berners-Lee 所開發的 World Wide Web 大量發展，而全球資訊網協會（World Wide Web Consortium，W3C）也訂定網頁的相關技術標準，使得瀏覽器具有更強的共通性。第四階段為大量媒介階段（2000～2010 年代），網路治理在此階段之前僅是一個概念，隨著 ICANN、IGF 等國際組織的相繼成立，讓網路治理走向體制化、具體化、具有強制力的運作機制；最後一個階段為所有人及所有物件階段（2010～2020 年代），網路治理不只是針對人類世界的需求，隨著物聯網、AI 技術以及大數據的蓬勃發展，這些可連上網路的物件（如穿戴裝置等）都將納入網路治理的探討範圍之內。

2. 網路空間領域的組成

網際網路具有三大特性，分別為基於點對端點原則（end-to-end）的技

術架構；包含通訊協定、網域名稱以及網路號碼近乎無數量限制的資源；在本國法、國際法之上的程式碼規範、自律、及他律的混合型態法規。

講者接著說明網路空間領域主要是由網域名稱系統（Domain Name System，DNS）所主導，其中包含 IP 位址、網域名稱以及根伺服器。 IP 位址包含 IPv4 以及 IPv6，而 IPv6 的數量幾乎無上限，可視為無限的網路資源；網域名稱主要包含通用頂級網域(gTLD)、國碼頂級網域(ccTLD)；根伺服器總共有 13 組（以英文字母 A 到 M 依序命名），起初是由美國政府授權 ICANN 管理，不過隨著 2016 年網路號碼指派機構（Internet Assigned Numbers Authority, IANA）監理權的移轉，ICANN 對於 IP 位址發放已無實質管理權力。

3. 網路治理概念的轉變

講者以在網際網路發展中重要人士的看法來說明網路治理概念的轉變。開發出 World Wide Web 的 Tim Berners-Lee 認為網路的規範就是讓電腦可以相容地共同運作的一套規則；與 IETF（Internet Engineering Task Force，網際網路工程任務組）成立息息相關的 Dave Clark 則在 1992 年提出我們不相信國王、總裁、及投票。我們相信粗略共識、事實依據、及可執行的程式碼；此番宣言亦影響芝加哥學院的 Lawrence Lessig 於 1998 年提出了「Code is the Law」(程式碼即為法律)，凸顯出在過去 30 年以來，雖然程式碼的發展表面上不得觸犯當地法規，但網路空間的行為規範，大部分還是受到程式碼所影響。

4. 經濟制裁與網路治理

經濟制裁在國際衝突事件中是常見的抵制手段，透過限制經濟資源的移轉而達到制裁效果。制裁的種類可分為針對個別國家之制裁以及針對性的制裁，如恐怖主義份子、人口販運或特定法人、團體等。經濟制裁具有強制的法律效力，違反制裁可能面臨巨額罰鍰及相關刑責，因此被視為非常有效的抵制手段。

2022 年 2 月底俄烏戰爭爆發後，烏克蘭政府正式向 ICANN 提出要求對俄羅斯實施制裁，停止俄國頂級域名.ru、.pф 及.su 解析，並要求關閉位於俄國的 DNS 根伺服器。烏克蘭政府亦要求歐洲 IP 位址管理機構 RIPE NCC 取消其核發給俄國所有 IPv4 與 IPv6 位址的使用權。

對此，ICANN 與 RIPE NCC 均回應本身為中立機構，不會停止提供相關服務，亦不會刪除俄羅斯頂級國碼網域名稱。雖然 ICANN 與 RIPE NCC 拒絕烏克蘭的請求，但在可行的權限範圍內仍採取相關措施制裁俄羅斯，如 ICANN 移除頂級域名.su、RIPE NCC 凍結俄羅斯主要電信公司之 IP 位址以及 Cogent、倫敦網路交換中心（LINX）等單位對俄羅斯斷網。

俄烏戰爭的爆發，促使三十多位 ICANN 現任前任董事及網路主導者共同發表「網路治理制裁原則」，內容包含切斷國家與網路連結的制裁行為不符合比例原則、將軍事與宣傳機構基礎設施視為網路制裁目標、建立有效網域名稱與 IP 位址制裁清單，並將其列入限制接取的目標、以及建立具有正當性的多方利害關係人審議程序等。當未來再度發生戰爭時，希冀透過網路治理制裁原則能夠為相關網路理機構建立一具有正當性的審議程序，使網路治理制裁得以奠定基礎。

問與答：

提問一：RIPE NCC 對俄羅斯所實施的相關限制措施是否根據聯合國的制裁令？

回覆一：聯合國並未發出正式的制裁令，僅有 111 個國家共同發出譴責聲明。由於 RIPE NCC 位於歐洲境內，因此必須遵守歐盟發出的經濟制裁命令，凍結俄羅斯移轉或申請IP位址。但是已註冊使用的IP只要沒有移轉均不會受到影響，仍可正常運作。目前相關制裁措施頻繁的更新，也是值得網路治理社群持續討論的重點議題。

二、 案例探討

(一) 平臺規範時代來臨了？

講者：曾更瑩／理律法律事務所 合夥律師

1. 前言

講者以近期熱門的「特斯拉（Tesla）執行長伊隆·馬斯克（Elon Musk）收購 Twitter」新聞事件做為案例。特斯拉 Tesla 執行長伊隆·馬斯克（Elon Musk）向來以愛用 Twitter 聞名，時常在 Twitter 上發文與網友互動，曾發文詢問網友：「你認為 Twitter 有嚴格遵守言論自由嗎？」要網友投票表決。也多次發布推文影響加密貨幣與公司股價，其發表的言論常引發網友論戰。

從 The Economic Times 所做的時間表中可看出 Musk 從 2022 年 1 月 31 日開始進行收購 Twitter 股票的動作，期間雖然 Twitter 曾試著抵抗 Musk 的敵意收購，在經過多次溝通／討論後，Twitter 董事會在美國時間 4 月 25 日宣布，同意以 440 億美元的價格將 Twitter 公司出售。當天 Musk 也用自己的 Twitter 帳號發表聲明：「言論自由是民主政治的基礎，Twitter 就像一座網路言論自由廣場，讓使用者可以在這裡討論攸關人類未來發展的問題。」，聲明中並提到他收購 Twitter 後要做的事情，包括公開演算法以獲得大眾的信任、對抗發垃圾訊息的機器人、對所有用戶進行身分驗證、是包容言論自由的地方以及政治中立。

2. Content Moderation – Lossen or Tighten?

雖然 Musk 希望可以放鬆控制網路上言論自由的力道，但歐盟執委會（European Commission，EC）則在 2020 年公布了兩項與數位政策有關的法案，分別是《數位服務法》（Digital Services Act，DSA）與《數位市場法》（Digital Markets Act，DMA），前者是用來保護數位服務的用戶，希望藉此來規範平臺業者及保障一般人使用數位內容的權益，後者則保障市場的

競爭。

在《數位服務法》中要求網路平臺提供業者在收到非法內容投訴之後，必須立即採取行動，包含移除非法或有害內容。其他內容審核義務包括了要求業者在發現使用者於平臺有違法行為時，就需主動跟主管機關作檢舉/報告；當主管機關要求業者提供必要的使用者個資，平臺業者也需要遵守；使用者發表的言論遭平臺下架時，業者除需告知使用者下架原因外，也要提供充分的申訴管道。另外，也規範業者需每年對平臺做系統性的風險評估。歐盟嚴格規範大型網路服務平臺，並且要求這些平臺業者必須承擔更多責任與義務，不能以平臺提供者身分來規避責任。

雖然 Musk 對於內容審核規範標準與歐盟的期望有所落差，但在是否公開「演算法」看法上確有相似之處。Musk 希望 Twitter 決定移除或推廣某篇內容時，都應該公開透明化，強調不論是利用演算法或人為方式，都不可以在幕後操縱其內容。在歐盟的 DSA 中則提到將阻止平臺使用基於性別、種族或宗教等資料演算法針對使用者、禁止對青少年/兒童投放廣告，另外也提到歐盟有權利要求業者對歐盟揭露演算法。

我國國家通訊傳播委員會（NCC）已於 2021 年底發布新聞稿公布「數位通訊傳播服務法」草案原則。NCC 指出數通法草案參考 DSA 等國際相關法制規範，以數位通訊傳播中介服務提供者為規範對象，並以自律先行，強化規管對象之義務及資訊透明度，並加入他律、法律等公私協力概念與作為，以彰顯多方參與的網際網路治理（Internet Governance）精神；該草案共 11 章，規範要項包括：基本權利維護、數位通訊傳播中介服務提供者之免責要件、數位通訊傳播中介服務提供者之義務、線上平臺及指定線上平臺之義務、公私協力合作、專責機構之設立及相關罰則等。

數通法草案要求中介服務提供者提出透明度報告、通知及回應等相關義務。此外，為強化對使用者之保障，該草案要求線上平臺如移除使用者貼文，或對使用者處以停權等相關限制行為時，必須說明原因，並提供異議機制，以保障使用者權益。更重要的是，草案課予業者將資訊限制登載

於共同資料庫的資訊透明義務。

3. 現行法律是否允許線上平臺被少數人收購？

歐盟 2022 年 3 月 24 日通過的 DSA 姊妹法案—《數位市場法》（Digital Markets Act，DMA），它的目的在於確保公平且開放的數位市場，把大型的網路平臺稱為守門人（Gatekeeper），並針對這些守門人進行規範及課以各種義務，確保公平競爭。只要是有強大的經濟地位，對歐盟市場有重大影響力，或是有強大的媒介地位，都會被視為守門人，受到 DMA 的規範。但 Musk 現在所經營的事業無一屬於被規範的大型線上平臺，看起來似乎就不在 DMA 的規範中。

美國的FTC近期對於Musk在公開宣布收購Twitter前收購的Twitter 9%股權行為展開調查，確認Musk是否漏未向FTC申報收購Twitter股權。另外許多美國學者則表示本件交易要完成，還是有可能要向美國競爭法主管機關提出 anti-trust filing，並於申報期間經過，主管機關未提出異議後，始得進行交割。也有學者認為馬斯克經營的 Starlink 提供網際網路接取服務，應該算是與 Twitter 有垂直競爭關係，但是如此一來，因為所有公司都有使用網際網路，都會跟提供網際網路接取服務的業者處於垂直競爭關係。

4. 平臺的所有權是否應有特殊規範？

傳統媒體受所有權限制，如臺灣規定黨政軍不得涉入媒體；廣播電台、無線電視不得有外資、媒體收購均受到主管機關嚴審、審查資金來源、防止大財團壟斷媒體（異業結合）、也防止過多媒體集中在同一集團手上（水平結合）等。但是社群媒體或其他線上平臺不受以上法規規範，主管機關依照公平交易法審核。但，按照歐盟 DMA，平臺收購一律要受規管，因此 Musk 購買 Twitter 案可以讓我們思考是否有制訂新規則來管理媒體社群平臺所有權之必要？

三、專題探討

(一) GAC 對 ccTLD 的準則及綱領

講者：吳國維／臺灣網路治理論壇 理事長

1. 域名系統的基本原理

講者首先以 Jon Postel 於 1994 年發表的《Domain Name System Structure and Delegation》技術文件（RFC1591）介紹域名系統的運作。日常生活中只要使用網路，均會涉及 IP 位址與域名，而 IP 位址與域名被稱為「唯一識別碼（Unique Identifier）」（類似手機號碼），也就是同一時間不能有 2 個相同的 IP 位址與域名，否則無法辨別資料究竟要傳輸給誰，或是導致無法解析。管理 IP 位址與域名的權威組織為網路號碼指派機構（Internet Assigned Numbers Authority, IANA），分配 IP 地址和頂級、次級域名則是由區域網際網路註冊機構（Regional Internet Registry，RIR）來負責。

2. 頂級域名的定義與管理

RFC1591 清楚定義了頂級域名分為兩種，分別是通用頂級域名（Generic Top-level Domain, gTLD）如.edu、.com、.org 等；另一種為國碼頂級域名（Country code top-level domain, ccTLD），此是根據 ISO 3166 列表制定，如.tw、.fr 等。

此份文件亦進一步闡述負責管理 ccTLD 的機構必須需具有良好的營運和技術能力，在提供相關服務時需秉持公平、非歧視的原則處理所有用戶之需求。ccTLD 亦代表著國家主權的延伸，當發生重大利益衝突事件時，IANA 僅扮演向衝突雙方傳遞訊息的角色，對其無責任義務亦盡量不涉入相關爭議。然而 RFC1591 為技術文件，實質上並無強制約束力，僅能作為營運頂級域名的參考而已。

3. 國碼頂級域名（ccTLD）的治理

講者以 2005 年 ICANN 政府諮詢委員會（GAC）發表的《ccTLDs 授權與管理之原則和指南》（Principles And Guidelines For The Delegation And Administration Of Country Code Top Level Domains），說明國碼頂級域名（ccTLD）究竟該由誰來管理。此文件主要是為國家政府、ICANN 以及 ccTLD 註冊機構之間的關係提供基本原則與框架。其內容主要提到幾項要點，包含 ccTLD 的政策應由該國家訂定，其相關爭議也應根據該國家法律由當地相關社群來共同解決；ccTLD 的發展應由多方利害關係人如政府、私部門、民間團體等共同參與及合作；ccTLD 的相關權利屬於當地政府與機構，受當地法律所規範。根據上述，可見 ICANN 對於 ccTLD 的管理十分有限，主要管理的責任在於當地政府以及註冊管理機構，因此許多國家透過此份文件宣告 ccTLD 為其數位主權的延伸。

4. 俄烏戰爭的爭議與思考

2022 年 2 月底俄烏戰爭爆發後，烏克蘭政府正式向 ICANN 提出要求對俄羅斯實施制裁，停止俄國國碼頂級域名.ru、.pф 及.su 解析，但 ICANN 正式回覆 ICANN 基於中立原則不會刪除俄羅斯頂級國碼網域名稱。講者表示根據上述兩份文件內容，並無賦予 ICANN 有正當性的權力得以執行制裁。目前歐盟和美國對俄羅斯實施經濟制裁，若 IP 位址與域名有被列為制裁的經濟資源之一，ccTLD 則有可能因為當地法院的正式判決而遭停止解析。

關於俄國頂級域名的爭議，可延伸思考 ccTLD 與數位主權的議題以及目前 ICANN 和 RIPE NCC 對於俄國的抵制，是否導致俄國逐漸走向分離全球網路的狀況，而形成網路分裂的問題。講者亦進一步舉例請學員思考，倘若烏克蘭要求 ICANN 停止解析俄國 ccTLD 一事成真，他日中國大陸是否也能聲稱臺灣為其領土的一部份，而奪走.tw 的管理權？這將是涉及數位主權、域名管理機制等值得深入探討的政治議題。

問與答：

提問一：課程中有提到國家對於國碼頂級域名具有管轄權，若是有國家意圖將 ccTLD 授權給私人機構營運（如吐瓦魯將.tv 授權給 VeriSign），是否有相關限制？

回覆一：根據課程中講解過的文件，ICANN 對於ccTLD 並無管轄權，因此將 ccTLD 授權給私人機構營運並無任何限制。營運 ccTLD 需要極高的維運成本，許多規模小的國家無力承擔，因此將 ccTLD 授權給私人公司營運，亦可藉此獲得一筆授權金，可用於建設其國內基礎建設，甚至成為該國家的主要收入來源之一。

提問二：吳理事長有提到透過經濟制裁可以限制俄羅斯的 IP 位址，但該項禁止措施是否僅在制裁令實行區域內有效，其他無須遵守制裁令的國家如中國大陸，是否仍可與俄羅斯正常連線？

回覆二：目前所有區域網路註冊管理機構（Regional Internet Registry，RIR）均規定所有 IP 位址都需要有資源公鑰基礎建設（Resource Public Key Infrastructure，RPKI)的認證。假設俄羅斯的某 IP 位址被 RIPE NCC 撤回，則其他 RIR 會認為該 IP 位址失去 RPKI 認證，並不合乎程序正當性而不允許其成功轉址。但若是與俄羅斯友好的國家接受未經 RPKI 認證的 IP 位址，並同意其轉址，此被撤銷的IP仍可在該國內繼續運作。由於被撤銷IP位址僅在其國內運作，ICANN 與 RIR 並無強制力可介入，這也是一個值得繼續探討的議題。

提問三：若俄羅斯的 IP 位址被撤回，是否意謂俄國可利用與其友好的國家如中國大陸、北韓等進行轉址，使其網站仍可正常運作，但卻不受外部相關網路機構的規範？

回覆三：此問題涉及「網路分裂」議題，以技術上而言，中國大陸、俄國和北韓等國確實可無視現行網路的運作規範，與自由民主的國家完全分離，創造一個獨立的網路空間。但現行網路空間所帶來的經濟效益十分龐大，若是中國大陸、俄國等國家完全脫離，極可能喪失極大的經濟利益，

也因此目前仍不太容易發生網路分裂，意圖實行網路分裂的國家必須考量政治與經濟的因素。

四、分組演練

(一) 線上分組方式

執行單位係利用 Webex 商業版軟體內建的分組討論功能，預先建立分組討論的會議室數量，並依照學員填回「線上出席調查表」時所選取欲參加的討論分組，將學員分配到指定的組別。

當會議主持人（執行單位）啟動分組討論功能時，Webex 會自動將線上會議室的所有參加者移動至所屬的分組會議室，參加者的系統畫面會顯示分組討論已持續的時間，以及所屬組別中的成員姓名（參閱圖 7-7）。為協助各組進行討論，執行單位亦在活動當日於各分組會議室中安排 1 名助教，提供即時的行政支援。



圖 7-7 Webex 分組會議室示意圖

分組討論時間結束後，Webex 會自動將所有參加者移動至原先的主會議室，參加者完全不需進行額外的系統設定或操作。

(二) 小組成果報告

本次分組演練課程將學員分成：網路人權、平臺規範以及網路安全，3 個主題組別，由講習課程的各主題講者提供討論題目，並全程指導該組學員透過多方利害關係人的角色扮演方式進行演練。

每組約 7～9 位學員，經過 90 分鐘的討論後，再由各組指派代表報告討論結果，主要重點彙整如表 7-3。

表 7-3 研習營學員成果報告彙整表

組別	1. 網路人權
題目	如何促進台灣數位人權？
共識	本組認為數位人權的提升需要多方利害關係人共同努力。例如像是公民社會下的所有網路使用者必須具有資訊素養以及自律的能力；學術界則需要透過教育來提升資訊素養；政府部門需建立相關政策來改善數位落差，達到數位機會的均衡，也應訂定相關法律來歸管數位暴力；平臺則須建立相關自律或是相關機制，使網路世界成為透明、更公開、可信賴的場域。
組別	2. 平臺規範
題目	民營的數位平臺是否適合或是管理平台上的言論？
共識	本組認為平臺必須適時管控內容。主要原因是平臺的審核時效快速，對惡意內容的遏止速度遠比政府的行政效率來得迅速。對使用者而言，如果對於平臺的管制措施不滿，隨時可改用其他平臺，但若是由政府來控制內容，如要改革難度較高，因此本組認為平台管理言論是不可避免的。本組針對平臺管制言論的做法亦提出幾項建議，例如民主化審查、利用演算法自動審查、建立申訴機制等。
組別	3. 網路安全
題目	網域註冊是否需要實名驗證？／有犯罪紀錄者是否可以列管其電磁紀錄，並禁止其註冊網域？
粗略	• 網域註冊是否需要實名驗證？

共識	本組大致認為如註冊網域強制實名驗證，可能侵害了使用者的言論自由及隱私權，也將導致個人資料遭到濫用、外洩的可能性提高。此外，網路安全和實名驗證的實施之間的必要性不足，不符合比例原則。因此不贊同實名驗證的實施。
	• 有犯罪紀錄者是否可以列管其電磁紀錄，並禁止其註冊網域？
無共識	本組針對此議題並無取得共識。後針對此議題提出粗略共識的結論為僅針對重大網路犯罪者進行管制，且須設立落日條款，分階段逐步減少對其權力的干預。但亦有組員表示該做法和實施網路實名制一樣恐侵害使用者基本權利。

第四節 圖文影音紀錄

一、各式設計物

配合原先規劃辦理實體研習營之活動需求，執行單位製作之設計物包含：展架海報、研習證明書以及參與人員名牌，成品如圖 7-8～7-10 所示。



圖 7-8 研習營展架海報



圖 7-9 研習證明書



圖 7-10 參與人員名牌

二、活動記錄



圖 7-11 研習營活動紀錄

三、 課程簡報與錄影檔

經講師同意授權公開之課程簡報資料及錄影檔，均已彙整於本研習營網站的「學習資源」專區（https://igcamp.tw/學習資源，參閱圖 7-12），供各界自行參考使用。



一、2022課程資料

(一)影片
課程影片，主題分別如下：
(1) 全球網路自由度及政策趨勢─陳文生顧問（NII產業發展協進會）
(2) 平臺規範的時代來臨了？─ 曾更瑩 合夥律師（理律法律事務所）
(3) 俄烏戰爭對網路治理規則的影響─黃勝雄 執行長（台灣網路資訊中心）

(二)簡報
(1) 全球網路自由度和政策趨勢
(2) 平台規範的時代來臨了？
(3) 俄烏戰爭對網路治理規則的影響

圖 7-12 研習營課程簡報資料與錄影檔

第五節 實習意願調查及課後測驗

本次培訓課程須進行實習意願調查及課後測驗，並協助有意願的結訓學員前往實習。

課前為了確保學員權益及避免浪費學習資源，錄取學員須填寫「出席保證書」，並同時回覆參與優秀學員遴選及實習意願。本屆 21 位結業學員（不含公務人員）當中，有 18 位表達同意參加優秀學員甄選，另有 20 位回覆願意參加實習。

課後為能更完整了解學員的學習情況，本次研習活動參考柯氏（Kirkpatrick）學習評估模式，以課後問卷調查作為活動及學習成效的評估方式。由於本次活動為 1 天短期課程，因此，學習成效評估的合理範圍應是層級一「反應」(如學員的滿意度、參與度）和層級二「學習」的部分範圍（如知識、技巧）。

本次課後測驗與問卷調查皆採線上填寫，並於結業式後進行。課後測驗則以講師授課內容以及課前所提供的學員手冊內容為出題範圍，一共設計了 10 題選擇題，測驗分數達 60 分的學員即可取得結訓資格。問卷內容分為：課程內容滿意度、學員自我評估，以及其他等單元。

本次課後調查共計收回 24 份問卷（回收率 100%），共 24 人通過課後測驗，測驗結果及問卷統計說明如下。

一、 測驗結果

「測驗」也可視為學習的一部份，為讓學員在學習過程中了解自己是否真的將課程內容融會貫通，執行單位請本次 4 位講師協助設計 10 題線上測驗題目，讓學員進行課後測驗，以確認學員的學習成效。統計結果共有 24 位學員（含 3 位公務人員）作答，並悉數通過測驗，平均分數為 89.12 分，當中滿分 7 人、90 分 12 人、80 分 1 人以及 70 分 4 人。課後測驗分數

分布詳圖 7-13；課後測驗答題結果如圖 7-14 所示。

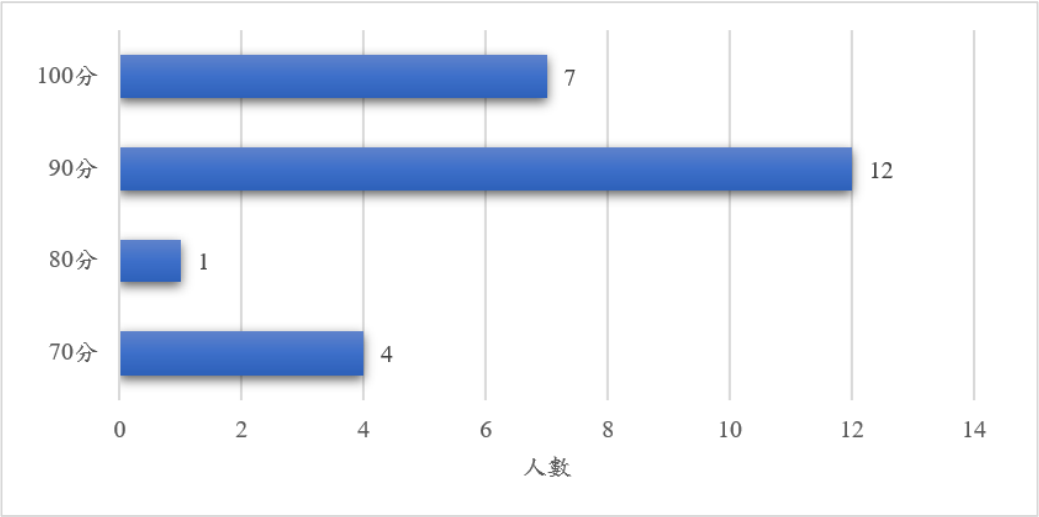
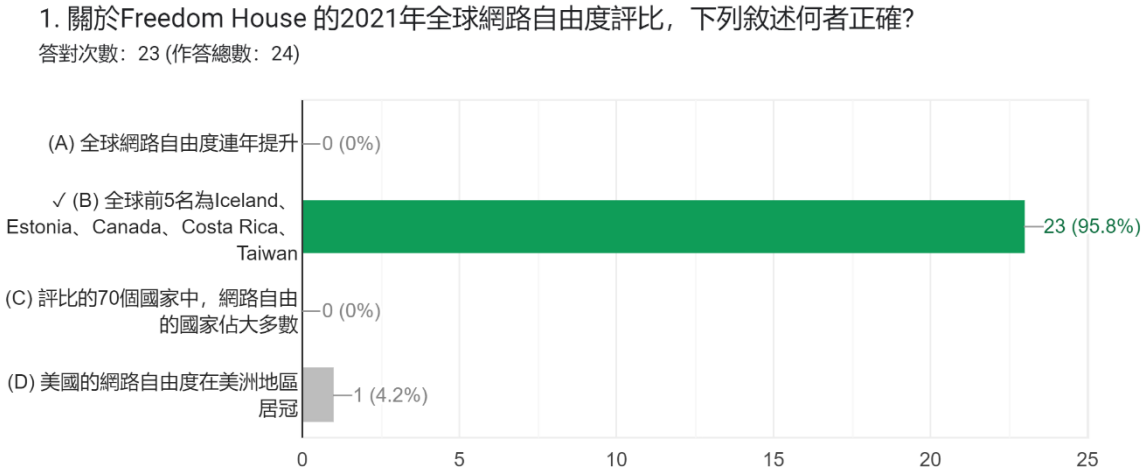
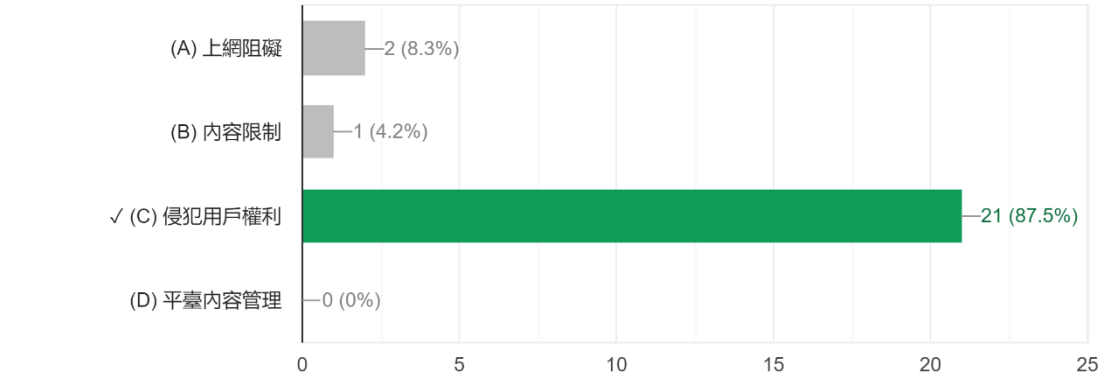


圖 7-13 課後測驗分數分布



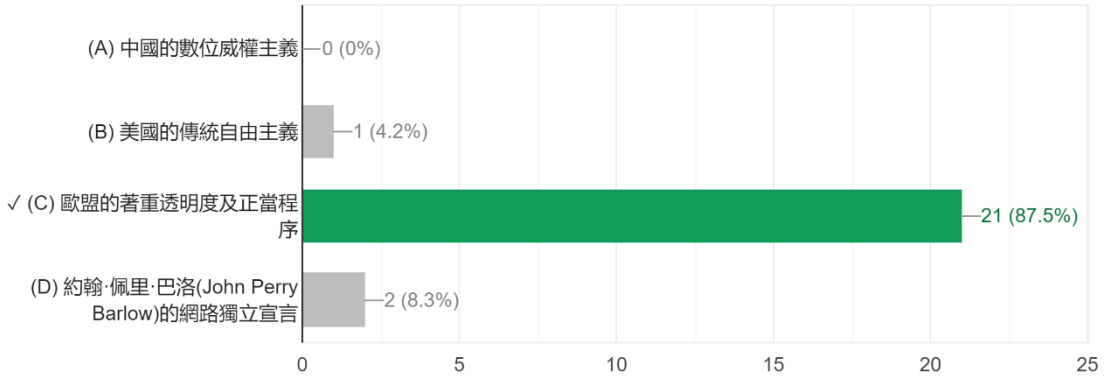
2. Freedom House 全球網路自由度評比的三大類指標中，臺灣表現最差的是哪一類?

答對次數：21 (作答總數：24)



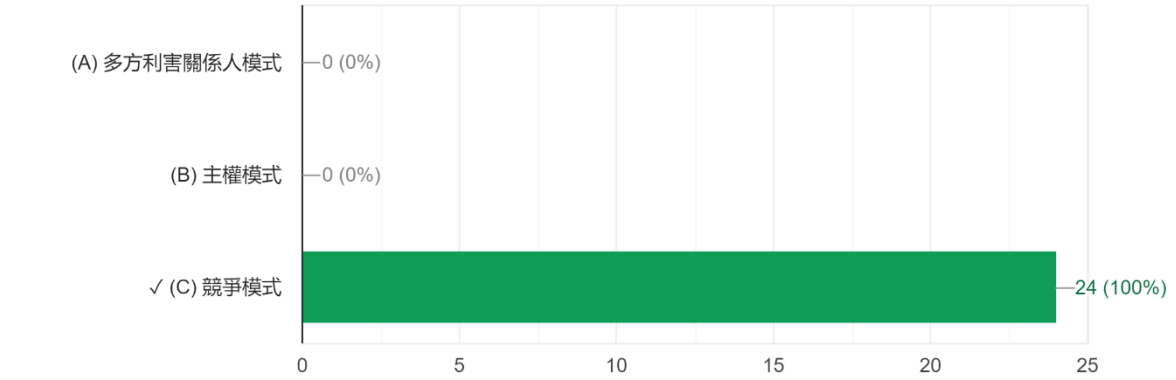
3. 網路治理的方式中，被公認為較佳的模式為下列哪一種?

答對次數：21 (作答總數：24)



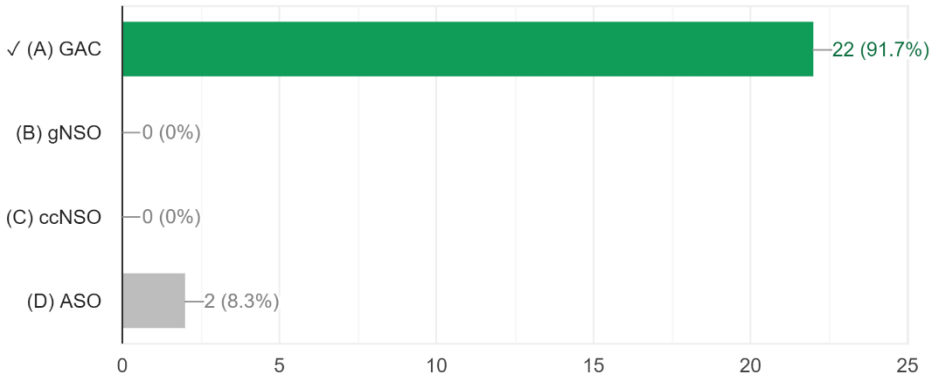
4. 下列何者非網路治理模式?

答對次數：24 (作答總數：24)



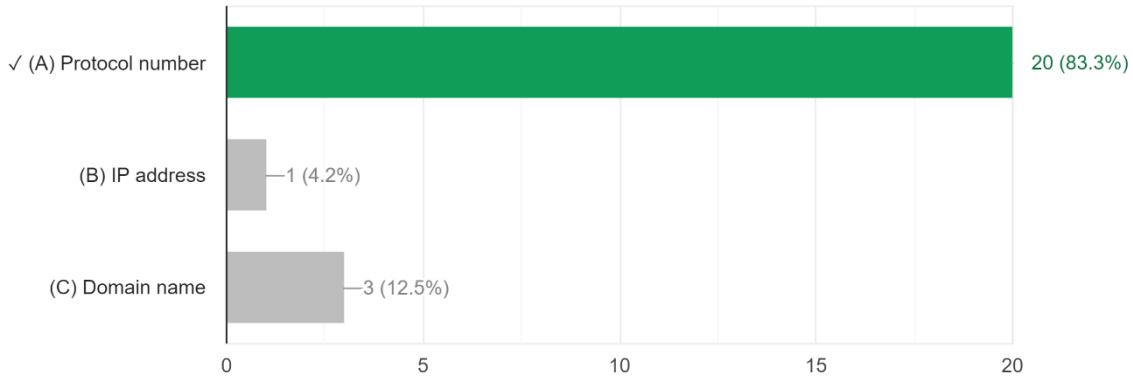
5. 下列何者非ICANN支援組織?

答對次數：22 (作答總數：24)



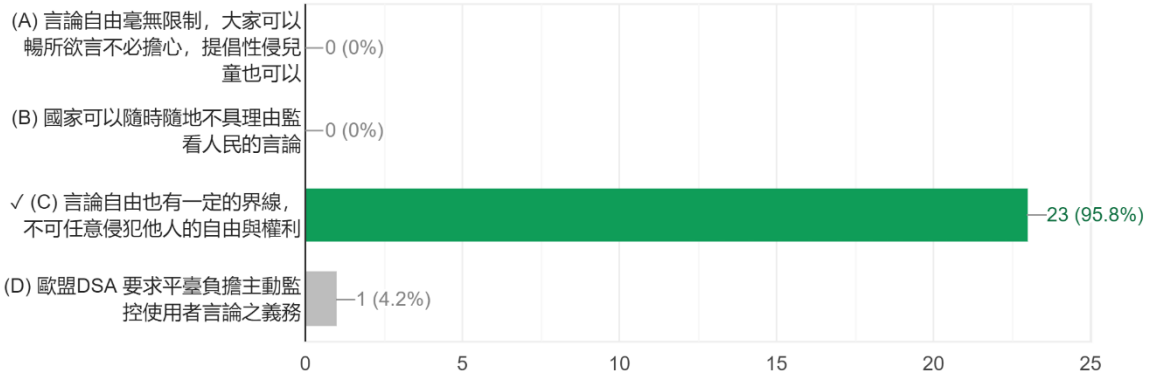
6. 下列何者非經濟制裁範圍?

答對次數：20 (作答總數：24)



7. 言論自由乃普世認同的基本人權，以下對於言論自由的敘述何者正確?

答對次數：23 (作答總數：24)



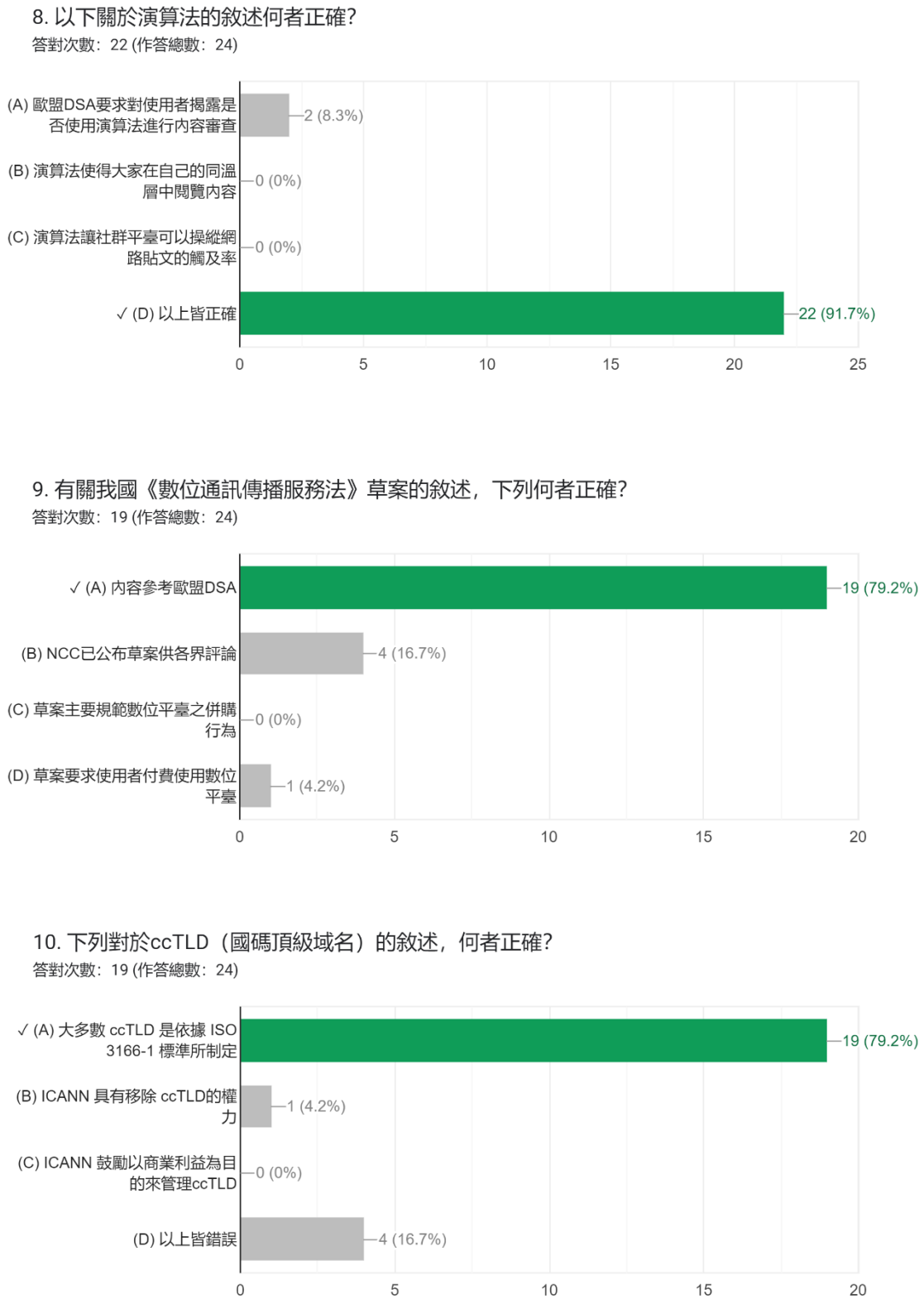


圖 7-14 課後測驗作答結果

二、課程內容滿意度

本年度學員對於整體課程安排、分組演練設計及授課內容之滿意度（包含非常滿意及滿意，參閱圖 7-15）分別為 96%、92%及 100%，顯示學員對課程內容以及整體課程安排予以高度肯定。

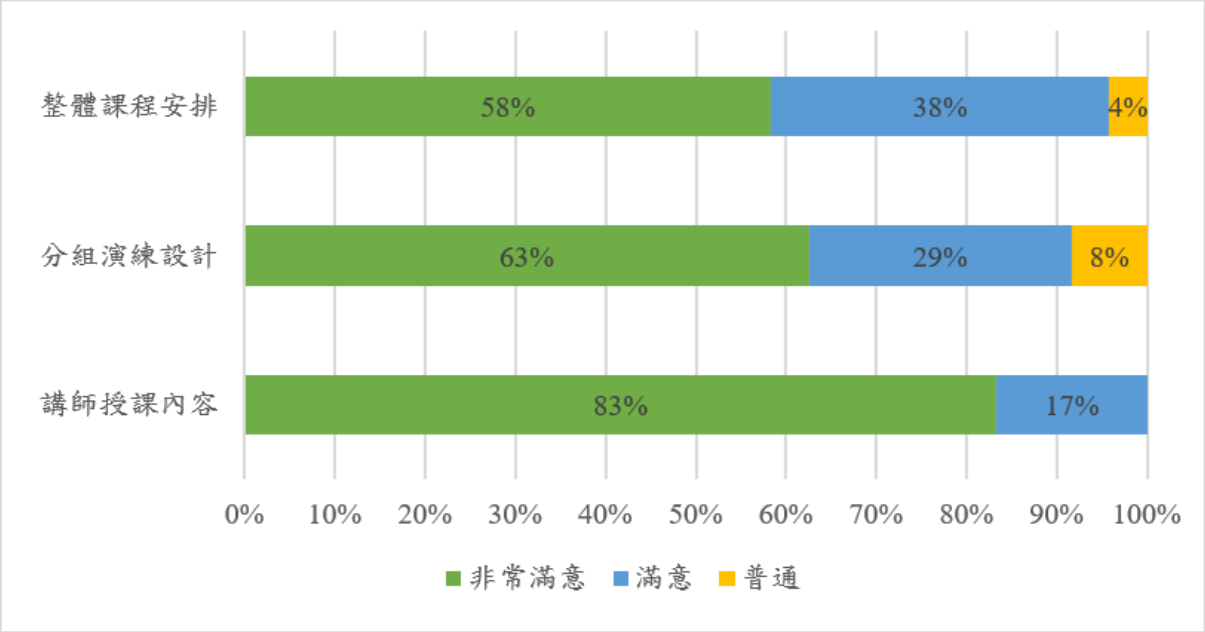
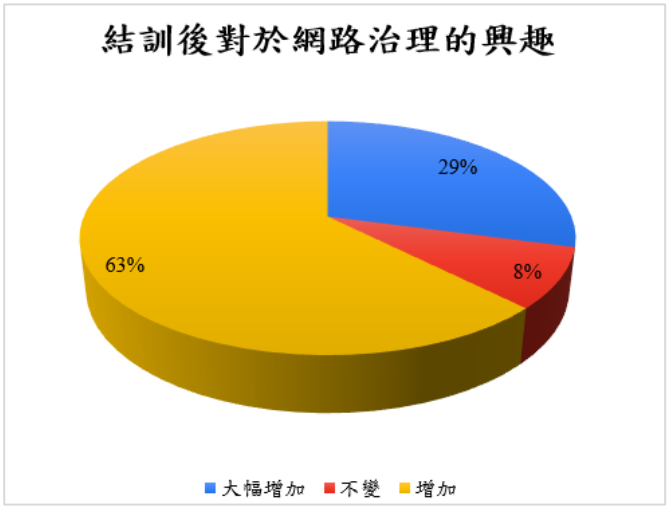


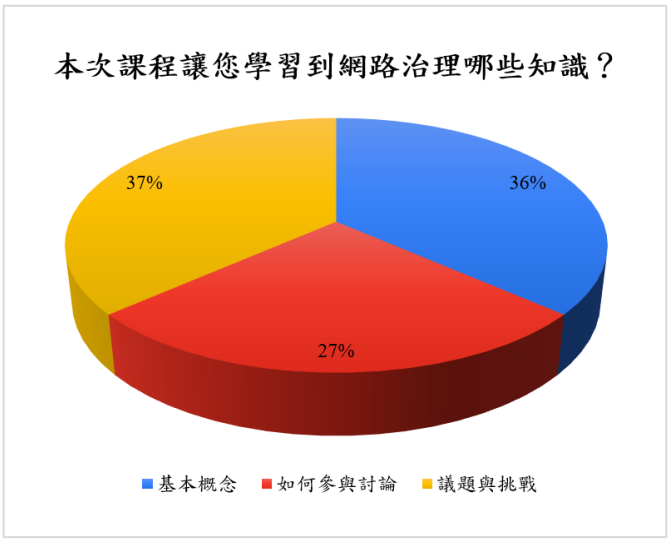
圖 7-15 研習營「課程內容」滿意度

三、學員自我評估

為確認本研習營對於學員是否具有實質助益，問卷中針對：結訓後對於網路治理的興趣、本次課程讓您學習到網路治理的哪些知識，以及未來願意參加的網路治理活動等 3 個項目向學員進行調查（參閱圖 7-16）。

達 92%的學員表示對於網路治理的興趣增加（包含增加與大幅增加）；學習到的網路治理知識則以「基本概念」及「議題與挑戰」最多，約各占 36 及 37%；所有學員皆表示未來有興趣參加其他網路治理活動，其中又以國內的「臺灣網路治理論壇」占比達 44%為最高。





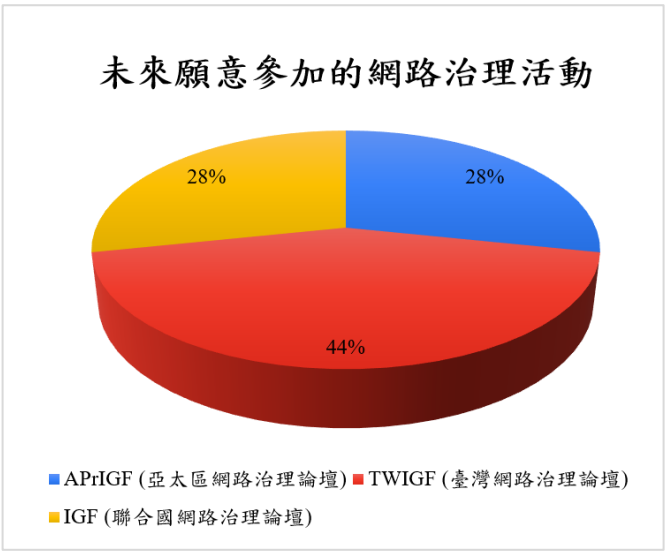


圖 7-16 研習營學員課後自我評估

四、其他建議

問卷的最後一個單元，則是針對本次研習營收穫最多的分別是哪幾堂課程進行調查（參閱圖 7-17），其中收穫最多的課程以「平臺規範的時代來臨了？」最高，達到 79%。其他專題課程的比例亦達 70%以上，顯示授課內容頗受學員喜愛。

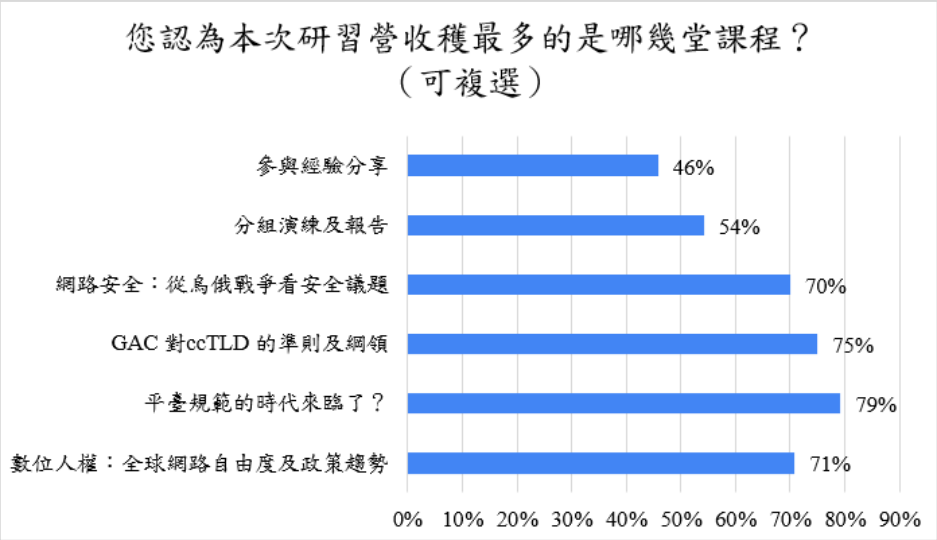


圖 7-17 其他建議調查結果

問卷最末亦設計開放性的問答題，邀請學員針對本次研習營之辦理給予執行單位具體的意見回饋，做為未來規劃相關活動之精進參考，回覆結果彙整如下。

- 因疫情改為線上實施，較為可惜。
- 扮演多方利害關係人的橋段令人印象深刻，未來如能有更多時間參與這個部分，應該會更有收穫。
- 希望之後能夠繼續參加更多網路治理相關活動。
- 可以依照學員專長(或所學)來分組，分組討論時能較快入主題。
- 課程安排稍嫌緊湊，希望未來可以增加講者 QA 時間。

第六節 學員遴選及後續活動安排

一、遴選優秀學員參與國際會議

本屆 21 位結業學員（不含公務人員）當中，有 18 位表達同意參加優秀學員甄選的意願。本次評選小組從角逐學員中遴選 1 位優秀學員參加 APrIGF 2022 國際會議。

本次評選會議於研習營分組報告結束後另闢線上會議室舉行，評選小組針對結業學員的學習熱忱、論述與表達能力、英文程度等項目，進行綜合評估。

經過講師的共識決，本屆優秀學員為洪同學（陽明交通大學資訊工程學系），他亦如期出國參與 9 月 12 至 14 日於新加坡召開的 APrIGF 2022 會議，並交付出國報告（參閱附錄三），報告刊載於研習營活動網站（https://igcamp.tw/學習資源）。洪同學非常積極全程參與三天會議，並於「在網路治理議題上強化身障人士的發聲」場次，主動分享看法（日本媒體近年推出 Barrier-free 影片，不僅讓聽障者可觀賞影片，也嘉惠日語的學習者）。

二、安排實習學員的實習活動

本屆 21 位結業學員（不含公務人員）當中，有 20 位表達同意參加實習學員甄選的意願。評選小組共選出 4 名實習學員，分別為李同學（國立陽明交通大學科技法律研究所）、徐同學（淡江大學教育心理與諮商研究所）、韋同學（國立陽明交通大學資工系）以及江同學（高雄醫學大學牙醫學系）。

本計畫安排實習學員參加 6 月底至 8 月份的國內外網路治理會議（詳表 7-4），並請學員撰寫會議摘要（參閱附錄四），最後還於 8 月 31 日舉辦

線上交流會，請學員分享參與會議的收穫（圖 7-18）。總計實習時數約 12 小時，提供每人新臺幣 2 千元的實習津貼。學員的會議摘要亦刊載於研習營活動網站（https://igcamp.tw/學習資源）及網路治理觀測站網站（https://igwatch.tw/）。

表 7-4 實習學員分工表

姓名	參與場次
江同學	• Focus Area 1, Subtopic 1: The European vision of digital sovereignty: From principles to action.（EuroDIG） • Focus Area 4, WS 6: The Declaration for the Future of the Internet.（EuroDIG） • 元宇宙的新維度治理框架（台灣網路講堂）
李同學	• Focus Area 1, Subtopic 2: Digital Sovereignty impact on the Internet infrastructure.（EuroDIG） • Focus Area 4, Subtopic 1: Responding to disinformation in times of COVID-19 and geopolitical conflict.（EuroDIG） • Beyond the Encrypted Content Debate.（IGF-USA 2022）
韋同學	• Focus Area 1, WS 3: International Connectivity: European Data-Gateway Platforms and the Global Gateway.（EuroDIG） • Focus Area 4, Subtopic 2: Sovereignty and the Internet: a risk of fragmentation.（EuroDIG） • 「公共空間的人工智慧應用與隱私隱憂」專題講座
徐同學	• Focus Area 1, Subtopic 3: Digital sovereignty - is Europe going in the right direction to keep Internet infrastructure secure and open? （EuroDIG） • Focus Area 3, Subtopic 1: Regulating emerging technologies: artificial intelligence and data governance.（EuroDIG） • 從拜登的數位資產政策中，臺灣數位金融之機會與挑戰(台灣網路講堂)

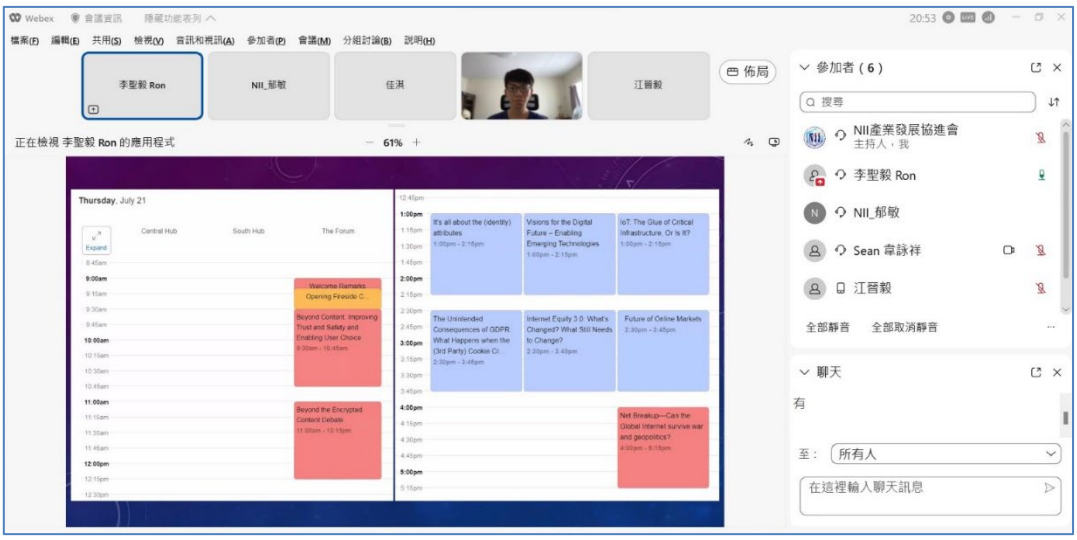


圖 7-18 實習學員線上交流會會議畫面

三、 實習學員心得回饋與未來建議

多數學員表示參加 EuroDIG 會議有助提升國際觀，在參與會議過程中，理解與談內容需克服語言和不同專業背景的挑戰。而在撰寫會議摘要方面，將全英文的座談內容轉化為淺顯易懂的中文短文，亦須投注大量時間與心力，儘管費時但學員皆表示有助於強化學習。

學員亦針對未來實習規劃提出建議，包含以導師制度帶領實習、更多的學員交流、提供議題的文獻資料、提供相關的就業資訊及依學員的專業安排實習等。

本次計畫原規劃安排至本會、臺灣網路資訊中心（TWNIC）或臺灣網路治理論壇（TWIGF）等執行網路治理相關業務的單位進行實習，但因各單位內部業務及人力規劃另有安排，加上學員本身也有工作或學業需兼顧，因此以參與國內外的網路治理會議，並撰寫會議紀錄的方式來執行。目前網路公司的實習機會競爭激烈且和網路治理無關，而公民團體或 NPOs 則無餘力可安排帶領實習生，以致難以媒合。建議 NCC 和數位部協調其所捐助成立或主管的 NPOs（如 TWNIC、TTC）提供實習機會。

第八章 課程影片製播

第一節 執行概況

本工作項主要係將「2022 網路治理研習營」全日課程剪輯成為 2 小時以上之視訊課程，並從中製作 3 支 5 分鐘以上的精華短片，將影片上傳至 Youtube 以做為網路治理議題的數位教材（參閱表 8-1）。其中 3 部精華短片皆有字幕、影片標題中有網路治理或相關關鍵字，以利大眾搜尋與學習。

表 8-1 課程影片製播總表

序號	類型	影片內容/講者	關鍵字	片長
1	2 小時視訊課程	2022 網路治理研習營—課程影片	#數位人權 #網路自由度 #數位平臺 #數位服務法 #歐盟 #網路安全 #資安即國安 #烏俄戰爭 #DNS #網路內容	2 時 15 分
2	精華短片	《數位服務法》簡介與評析（曾更瑩 律師／理律法律事務所）	#網路治理研習營 #數位服務法 #DSA #網路治理 #平臺責任 #網路內容 #演算法	8 分 06 秒
3	精華短片	網路治理的發展軌跡（黃勝雄 執行長／台灣網路資訊中心）	#網路治理研習營 #網路治理 #TCPIP #WorldWideWeb #ICANN #IGF #Internetgovernance	5 分 48 秒
4	精華短片	數位人權：全球相關政策趨勢（陳文生 顧問／NII 產業發展協進會）	#網路治理研習營 #網路治理 #Internetgovernance #數位人權 #資料監管 #網路監管	7 分 33 秒

執行單位於本計畫執行期間亦定期查看 YouTube 頁面是否有新增留言且迅速回應。

第二節 2 小時視訊課程

一、製播方式

本計畫於線上辦理「2022 網路治理研習營」課程時，即同步利用 Webex 商業版軟體內建的錄影功能進行課程錄影，待完成影片錄製後，再搭配使用其他的影片剪輯軟體進行影片的後製。

使用 Webex 錄影時，可依需求選擇不同的畫面布局（參閱圖 8-1）。執行單位所選用之布局為：當課程具有共用的內容，例如講師在分享簡報時，選擇使用圖 8-1 上排中央的「聚焦的內容和目前發言人」模式，以簡報內容為主，講師的鏡頭為輔；若講師無需分享簡報時，則選擇圖 8-1 下排的「焦點」模式，把畫面集中在講師的鏡頭。

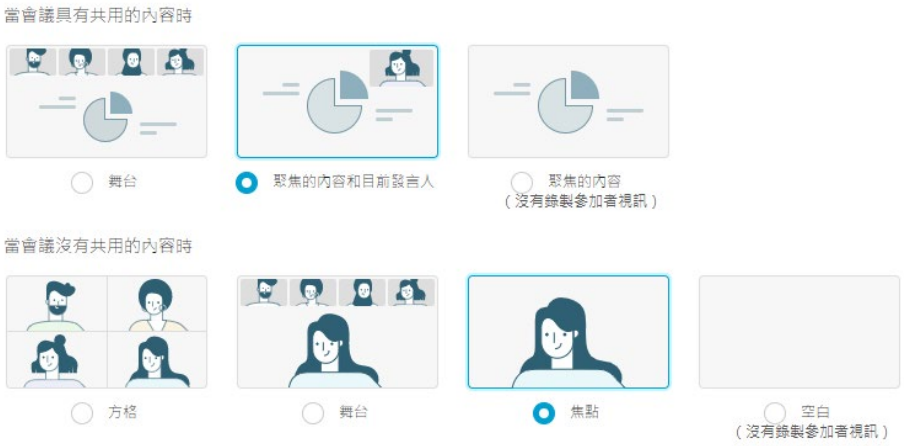


圖 8-1 Webex 錄影畫面布局

這樣的畫面布局，也可以確保不會將學員的畫面錄製到影片中，可避免後續在製作影片時衍生的肖像權等問題。至於講師方面，執行單位在課程辦理前均已請講師簽署錄影及公開影片的同意書，若未獲得講師同意，便不會將其影片納入剪輯內容當中。此外，影片中亦不會包含課堂提問、分組討論或小組報告等有學員出現的畫面，以保護學員的個人資料。

二、影片內容

課程影片在取得講師的同意下，除吳國維理事長外，由 3 位講師的課程內容剪輯而成，每個課程主題之間均插入以研習營主視覺設計的標題圖卡做為過場特效，讓課程影片的段落更加分明。影片的片頭及片尾亦採用相同風格的視覺設計，使得整部影片具有一致性的美感（參閱圖 8-2）。

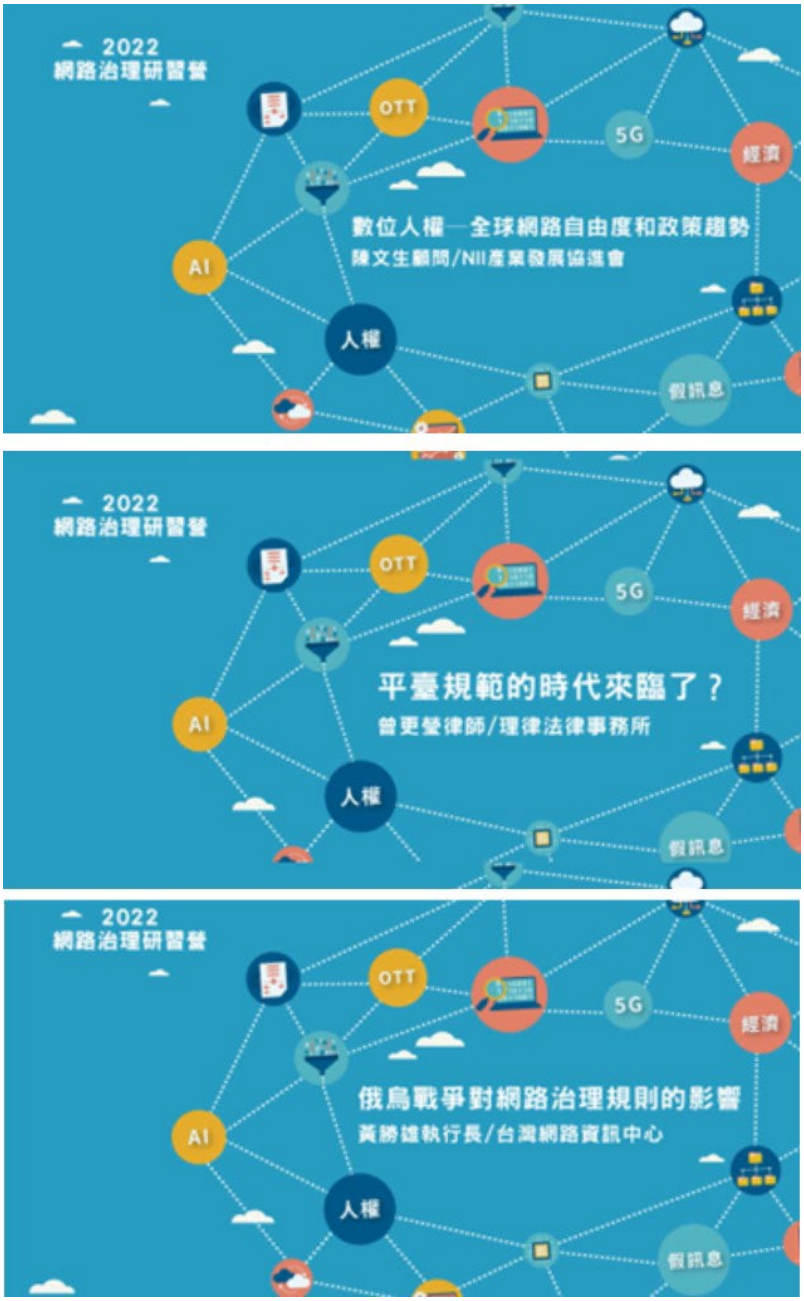


圖 8-2 課程影片視覺設計

本課程影片相關資訊彙整如下：

- 片名：2022 網路治理研習營—課程影片
- 片長：2 小時 15 分
- 網址：https://youtu.be/AB9sNYcNDkc
- 課程內容：

  ✧數位人權：全球網路自由度及政策趨勢

  講者：陳文生／NII 產業發展協進會 顧問

  ✧案例探討：平臺規範的時代來臨了？

  講者：曾更瑩／理律法律事務所 合夥律師

  ✧網路安全：從烏俄戰爭看安全議題

  講者：黃勝雄／台灣網路資訊中心 執行長

- 關鍵字：#網路治理研習營 #igcamp #網路治理 #數位人權 #網路自由度 #數位平臺 #數位服務法 #歐盟 #網路安全 #資安即國安 #烏俄戰爭 #DNS #網路內容
- 公開日期：2022 年 6 月 17 日

第三節 精華短片

一、 製播方式

本工作項係以前述 2 小時視訊課程影片為素材，從中剪輯製成 3 支 5 分鐘以上的精華短片，提供大眾作為認識網路治理議題的數位教材。

二、 短片內容

(一) 精華短片 1

本短片係剪輯自 2 小時視訊課程影片，摘錄理律法律事務所曾更瑩合夥律師課程「平臺規範的時代來臨了？」當中提及有關《數位服務法》的簡介與評析段落。

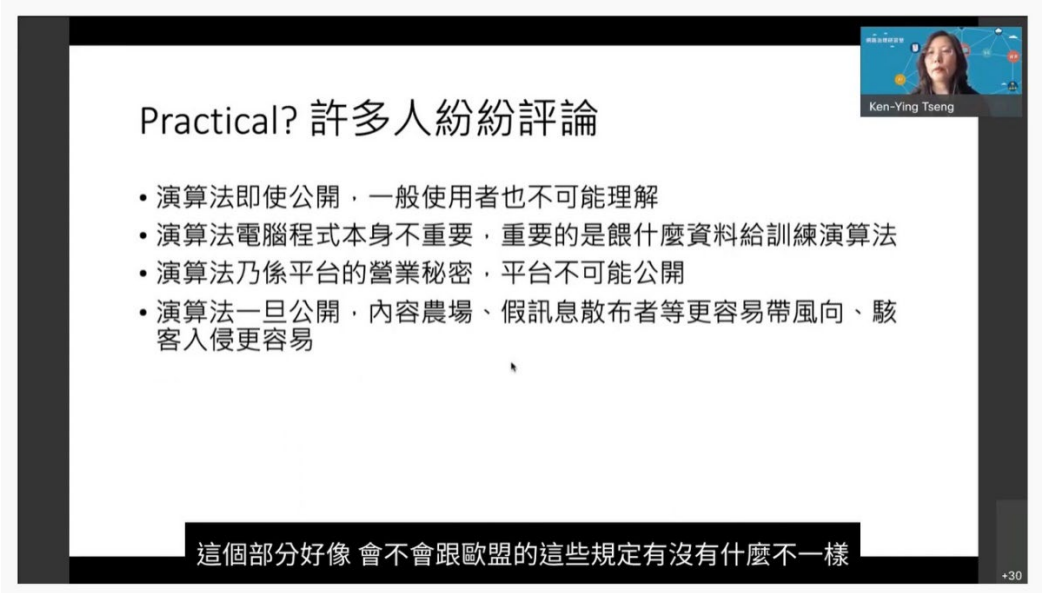


圖 8-3 精華短片 1 示意圖

本短片相關資訊彙整如下：

- 片名：2022 網路治理研習營—課程精華（一）：《數位服務法》簡介與評析
- 片長：8 分 06 秒
- 網址：https://youtu.be/NoeI6P-cAew

- 關鍵字：#網路治理研習營 #數位服務法 #DSA #網路治理 #平臺責任 #網路內容 #演算法
- 公開日期：2022 年 8 月 3 日

(二) 精華短片 2

本短片係剪輯自 2 小時視訊課程影片，摘錄 TWNIC 黃勝雄執行長課程「網路安全：從烏俄戰爭看安全議題」當中提及有關「網路治理的發展軌跡」段落。



圖 8-4 精華短片 2 示意圖

本短片相關資訊彙整如下：

- 片名：2022 網路治理研習營—課程精華（二）：網路治理的發展軌跡
- 片長：5 分 48 秒
- 網址：https://youtu.be/5G-3HxoJzbw
- 關鍵字：#網路治理研習營 #網路治理 #TCPIP #WorldWideWeb #ICANN #IGF #Internetgovernance

- 公開日期：2022 年 8 月 31 日

(三) 精華短片 3

本短片係剪輯自 2 小時視訊課程影片，摘錄 NII 陳文生顧問課程「全球網路自由度及政策趨勢」當中提及有關「數位人權：全球相關趨勢」段落。



圖 8-5 精華短片 3 示意圖

本短片相關資訊彙整如下：

- 片名：2022 網路治理研習營—課程精華（三）：數位人權：全球相關政策趨勢
- 片長：7 分 33 秒
- 網址：https://youtu.be/fxzOp08PUu0
- 關鍵字：#網路治理研習營 #網路治理 #Internetgovernance #數位人權 #資料監管 #網路監管
- 公開日期：2022 年 10 月 5 日

第四節 流量統計分析

以下針對本計畫產出之 2 小時視訊課程影片及 3 支精華短片流量進行分析，相關數據均來自 YouTube 平臺。配合本報告期末送審時程，流量及相關數據計算至 10 月 17 日，合先敘明。

一、觀看次數與時間

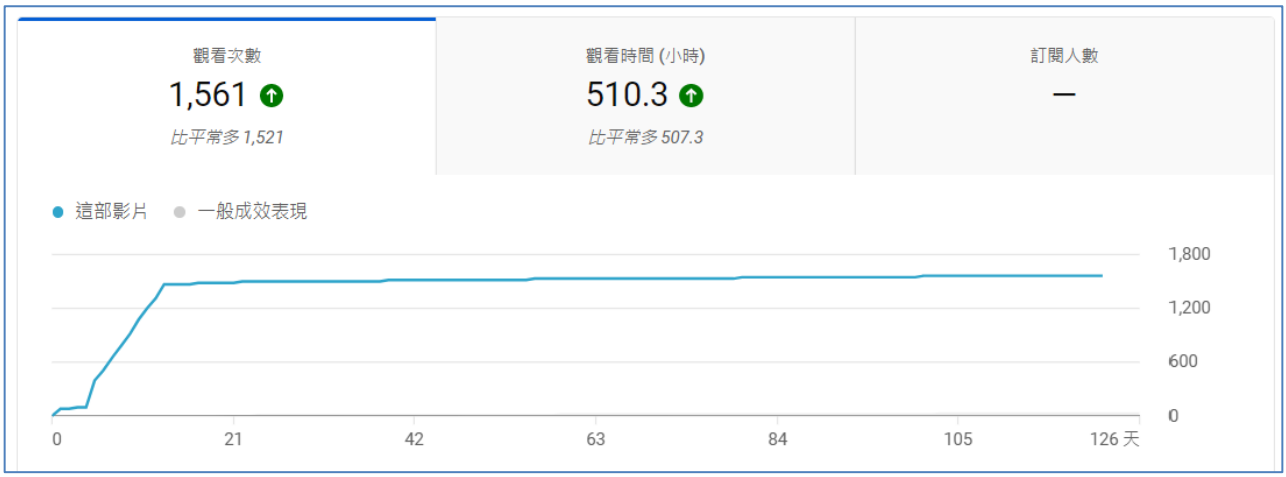
2 小時視訊課程影片的觀看次數為 1,561 次，累積觀看時數達到 510.3 小時；3 支精華短片觀看次數則依序為 191 次、271 次及 181 次；累積觀看時數依序為 9.8 小時、15.9 小時與 12.8 小時。

其中以 2 小時視訊課程影片的總觀看次數最高，原因是該片製作製播時，本計畫尚未影片數位行銷之要求，因此該片有購買 Youtube 廣告以提升影片能見度，觀看次數與累積時數與另外 3 支精華短片相比，數字自然較為理想。

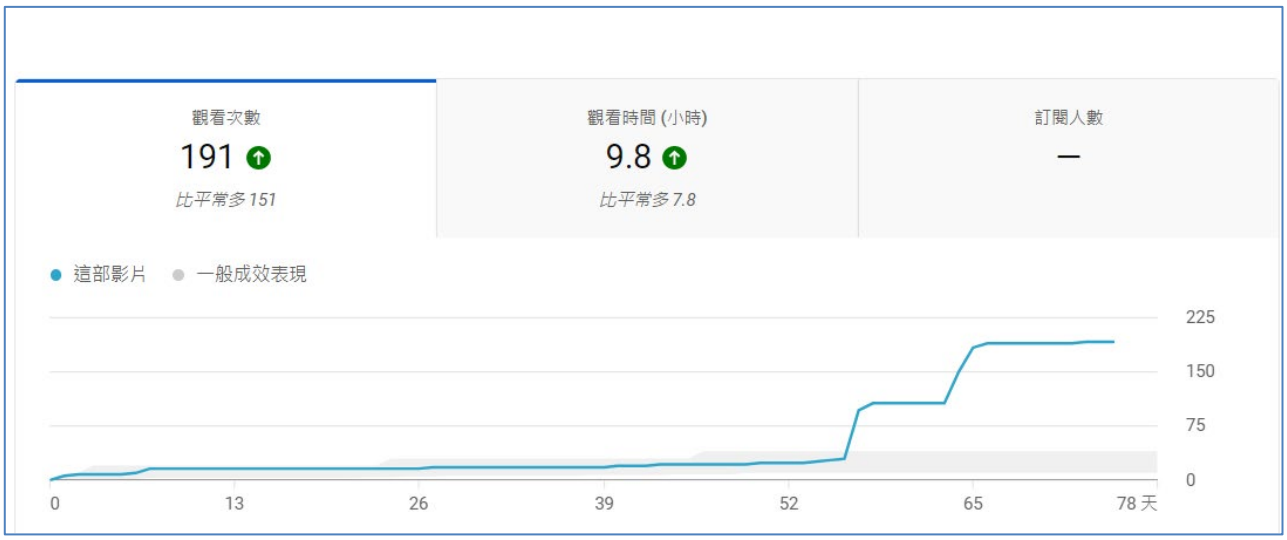
表 8-2 影片觀看次數與累積觀看時數彙整表

序號	類型	影片標題	總觀看次數	累積觀看時數
1	2 小時視訊課程	2022 網路治理研習營—課程影片	1,561 次	510.3 小時
2	精華短片	《數位服務法》簡介與評析	191 次	9.8 小時
3	精華短片	網路治理的發展軌跡	271 次	15.9 小時
4	精華短片	數位人權：全球相關政策趨勢	181 次	12.8 小時

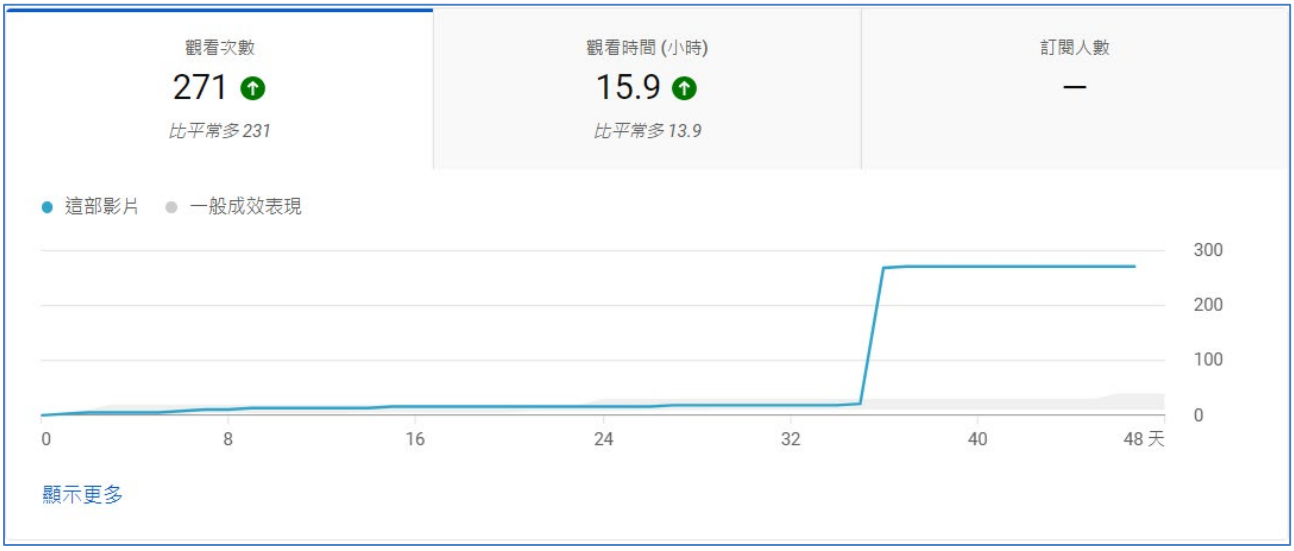
2 小時課程影片



精華短片 1：《數位服務法》簡介與評析



精華短片 2：網路治理的發展軌跡



精華短片 3：數位人權：全球相關政策趨勢



圖 8-6 影片觀看次數與累積觀看時數

二、曝光次數與點閱率

YouTube 統計的影片「曝光次數」，係指影片縮圖顯示在使用者畫面的時間超過一秒，且至少有一半以上的部分出現在畫面中，以下亦列出因曝光而產生的點閱率。根據統計結果，2 小時視訊課程影片獲得 YouTube 自動顯示的曝光次數為 1 萬次，3 支精華短片則依序為 503 次、314 次及 198 次。來自曝光次數的點閱率，2 小時視訊課程影片為 1.4%，3 支精華短片則依序為 4.4%、3.2%及 5.1%。

表 8-3 影片曝光次數與點閱率彙整表

序號	類型	影片標題	曝光次數	點閱率
1	2 小時視訊課程	2022 網路治理研習營—課程影片	1 萬次	1.4%
2	精華短片	《數位服務法》簡介與評析	503 次	4.4%
3	精華短片	網路治理的發展軌跡	314 次	3.2%
4	精華短片	數位人權：全球相關政策趨勢	198 次	5.1%

2 小時課程影片



精華短片 1：《數位服務法》簡介與評析



精華短片 2：網路治理的發展軌跡



精華短片 3：數位人權：全球相關政策趨勢



圖 8-7 影片曝光次數與點閱率

三、觀眾性別與年齡

根據 Youtube 針對 2 小時視訊課程影片及 3 支精華短片之綜合統計，4 支影片觀眾以男性為主（85.9%），而女性僅有 14.1%；在年齡層方面，以 65 歲以上最多（24.6%），次之為 55～64 歲（23.1%）。

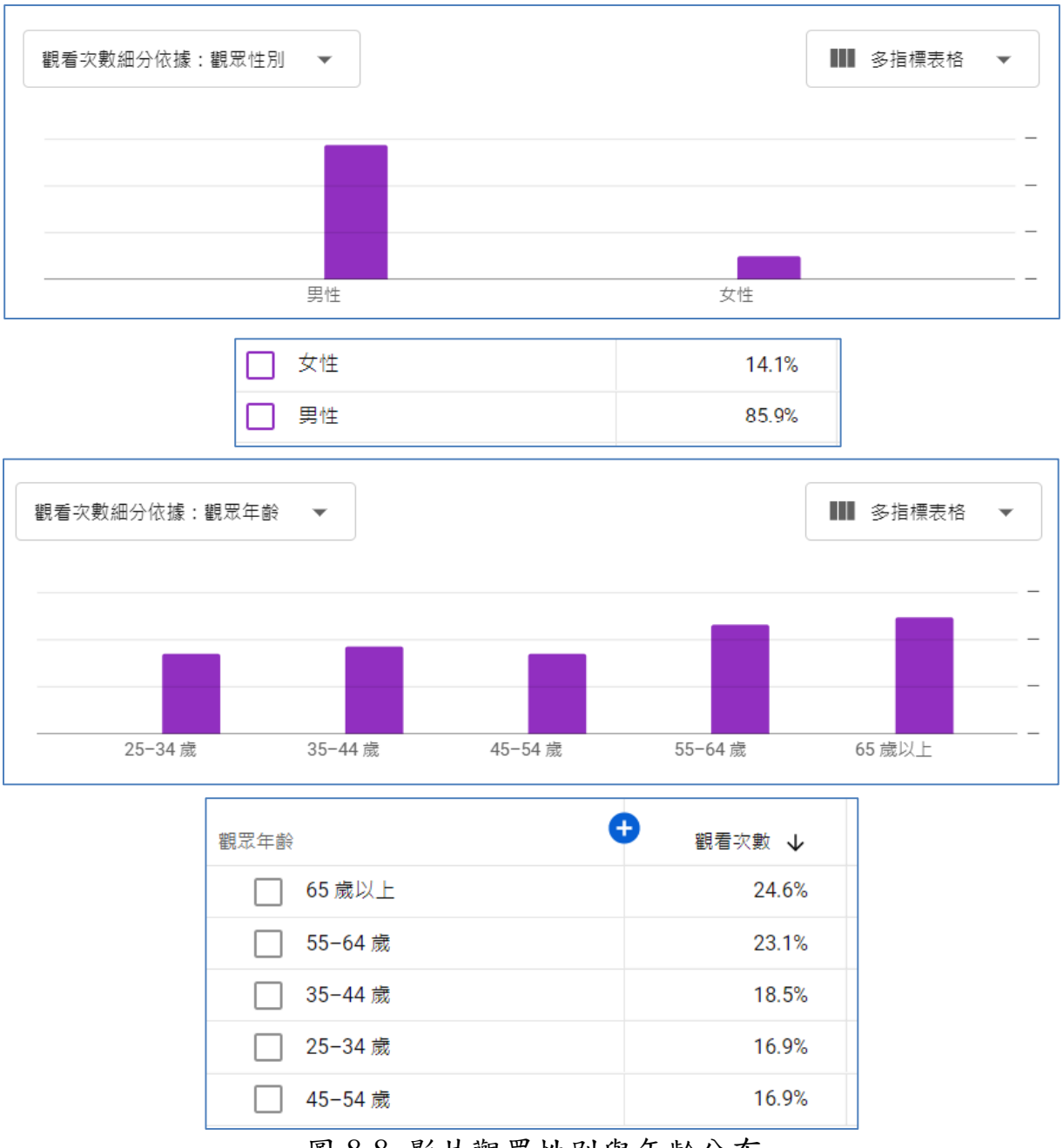


圖 8-8 影片觀眾性別與年齡分布

第九章 國際會議 APrIGF 參與

第一節 會議簡介

一、會議背景

APrIGF 為亞太地區網路治理政策討論、意見交換、促進合作的平臺，以推動亞太地區網路治理的發展為目標，自 2010 年起已分別於香港、新加坡、東京、首爾以及臺北等地舉辦，疫情爆發前，每年皆吸引亞太地區 20 多國的 2~3 百位各界人士參與。多方利害關係人模式是 APrIGF 的核心原則，並著重於參與者的多樣性與討論議題的開放性。每年的大會主題與各個座談場次，皆為公開徵求，並由多方利害關係人代表共同決定。會議結束後並彙整成綜合報告 (Synthesis Document)，向全球傳達亞太地區的網路治理觀點。

二、2022 年會議資訊

受到 COVID-19 疫情持續的影響，APrIGF 2022 採虛實混合（hybrid）型式，於 2022 年 9 月 12 日至 14 日由 APrIGF 秘書處和 APNIC 共同主辦，實體會議的地點同 APNIC 54，皆為新加坡。

本次大會主題為「以人為本：展望社群引領的包容性、永續性和可信賴的網路」（People at the Centre: Envisioning a community-led Internet that is inclusive, sustainable and trusted），討論主題即是大會主題所指的「包容性」、「永續性」、「可信賴」3 大類別。會議包含開閉幕、座談（Workshop）、演講（Showcases，以個人或單位名義發表 30 分鐘演講）等共近 30 場，議程請詳 https://ap.rigf.asia/news/2022-program-schedule/。

本計畫由計畫主持人梁理旋赴新加坡實地與會，參與的場次如下表 9-1 所列，並於後續章節摘要相關討論重點。

表 9-1 APrIGF 2022 參與場次

編號	場次名稱
--	APrIGF 2022 Opening Plenary 開幕典禮
S13	Combating Disinformation from COVID-19 to the General Election: Multistakeholder Digital Literacy vs Legislation & Censorship? 打擊從 COVID-19 到選舉的虛假訊息：多方利害關係人的數位素養 vs 立法和審查？
S08	Towards an EcoInternet - A Multistakeholder Dialogue on Policy Making and Strategising for a Sustainable and Energy Efficient Internet 邁向節能網路——永續和節能網路政策和策略制定的多方利害關係人對話
S21	LEO Satellite Constellations - Will They Bring Better Internet Access and a More Resilient Internet? 低軌衛星星群 —— 它們會帶來更好的網路接取和更具韌性的網路嗎？
S11	Responding to changing digital rights priorities in a post-pandemic world 因應疫後世界數位人權優先事項的變化
S19	Locally Accessible Cloud Service (LACS) for e-resilience 建立本地可存取的雲端服務以提升網路韌性
--	APNIC Cooperation SIG and APrIGF APNIC 合作特別興趣小組與 APrIGF (討論多方利害關係人參與網路治理，如何受到近期地緣政治衝突和國家法規的影響)

第二節 會議重點摘要

一、開幕典禮

(一) 貴賓致詞

APrIGF 2022 開幕典禮除了有熟面孔的 DotAsia 執行長 Edmon Chung、APNIC 總裁 Paul Wilson 等貴賓外，還有首度於 APrIGF 致詞（影片）、甫上任不久的聯合國秘書長之科技大使 Amandeep Singh Gill。

Gill 表示，當前全球網路面臨分裂、不當內容等挑戰，如果不透過國際合作加以因應，恐將摧毀網路作為公共財的基礎。因此，聯合國秘書長推動於 2024 年《未來高峰會》（Summit of the Future），通過《全球數位協議》（Global Digital Compact, GDC），促進全球的數位合作。GDC 是網路共同價值觀——開放、自由、安全、包容的憲章，其內容並非只是一份指導原則，而是包含因應普及連網、假訊息、人權、AI 等問題的全球合作優先事項和方法。雖然 GDC 將採聯合國會員國的多邊程序，但因網路從開始發展至今，不論是基礎建設或內容應用層，皆是實施多方利害關係人（multi-stakeholder，以下簡稱多方）機制，因此，他的團隊會確保多方的觀點被納入多邊程序。

此外，致詞貴賓還有聯合國 IGF 秘書處代表 Chengetai Masango，以及新加坡通訊及新聞部部長 Dr. Janil Puthucheary。兩人皆提到數位落差的問題，可能使未上網人口失去基本權利，因此，他們也期許在網路社群的努力下，數位落差能獲得改善。

(二) 座談：以人為本的網路——我們如何正確做到？

開幕座談的主題為 People-centered Internet – How do we get it right。主持人——全球資訊網基金會（World Wide Web Foundation）亞太區主任 Anju Mangal 表示，網路的誕生是為了確保人們享有美好的生活，但多年來，我

們對技術的重視程度遠高於對人類。面對疫情蔓延、自然災害、地緣政治的挑戰，凸顯我們對於縮減數位落差的嚴重不足。我們需要將人置於網路、決策、政策制定和社群驅動倡議的中心，思考如何確保人人都能獲得有意義的連網。

巴布亞紐幾內亞的通訊與資訊科技部部長 Hon. Timothy Masiu 指出，由於巴國正處於建立數位基礎建設的階段，當務之急就是建立全國的網路接取，希望包括偏鄉學校和醫療院所在內的網路，都能於 2027 年前完成。

東南亞最大的叫車和外送平臺 Grab 創辦人之一的 Ilaria Chan 認為，「以人為本」就是滿足民眾的日常生活所需。她表示，Grab 的創立初衷是為了解決人們在馬來西亞搭乘計程車的安全疑慮；後來在營運過程中，又看到人們的不同需求，因而發展食物外送平臺、快遞、行動支付、金融科技、小額保險等服務。

Meta 南亞公共政策主任 Sarim Aziz 表示，新冠肺炎疫情加速數位轉型的腳步，但同時也凸顯數位鴻溝之大。Meta 早就意識到只有連線是不夠的，因此，著重於建立永續實惠的接取解決方案。Aziz 並認為，元宇宙應該像 TCP 一樣，成為一個具包容性、全球共享共用的標準，而不是由一家特定公司掌控或持有。

二、座談：打擊虛假訊息

「打擊從 COVID-19 到選舉的虛假訊息：多方利害關係人的數位素養 vs 立法和審查？」座談，由香港技術社群 Tech For Good Asia 創辦人，同時也是美國史丹福大學全球數位政策中心訪問學者 Charles Mok（莫乃光）申辦並主持。Mok 表示，虛假訊息（disinformation）已經成為亞洲和全世界最主要的信任威脅，本場座談從 COVID-19 和選舉的虛假訊息兩個角度，探討最佳的因應之道究竟是政府立法、業者自律，或是多方推動數位素養。討論重點如下：

(一) 經驗分享：業者自律和培養數位素養措施

Meta 亞太地區錯誤訊息政策主任 Alice Budisatrijo 分享業者自律的實例，簡介 Facebook 處理錯誤訊息（misinformation）和虛假訊息（disinformation）的方法包括：與事實查核機構合作、發布指南、限制政治廣告、移除惡名昭彰組織的帳戶或專頁等。她也坦言兼顧言論自由並非易事，業者需制定明確的原則，民眾也需培養數位素養。

公民團體 ICT Watch 執行長 Indriyatno Banyumurti，和聯合國兒童基金會（United Nations Children's Fund, UNICEF）專員 Rizky Ika Syafitri，則是分享打擊虛假訊息和建立民眾數位素養的措施，例如：提供線上課程、舉辦座談、製作電影和動畫、設計有趣吸引民眾的宣導資訊等。

(二) 講者對於是否該立法懲處，看法分歧

韓國高麗大學教授暨公民團體 Open Net 董事 Kyung Sin PARK 博士對於立法懲處虛假訊息，表達反對立場，認為此舉會對公眾言論產生負面影響，因為最大的問題始終來自國家支持的虛假訊息，它帶有合法性和壓迫性，導致真相被掩蓋，社會注意力被轉移到相對不重要的議題。PARK 強調，韓國近期才賠償上百位於數十年前因反對某些政策而入獄的政治犯，就是最好的教訓。

不過，聯合國兒童基金會的 Syafitri 提出不同看法。她表示，雖然數位素養是最佳方法，但這需要長期培養才能見效。因此，對於某些問題，如健康相關問題，可能還是需要法規對虛假訊息進行懲罰，尤其健康訊息並不像政治或選舉訊息那般的主觀。

三、座談：邁向節能網路

「邁向節能網路——永續和節能網路政策和策略制定的多方利害關係人對話」座談，由香港的技術社群 DotAsia Organisation 申辦，其執行長 Edmon Chung 主持，我國數位發展部部長唐鳳也受邀擔任講者。主持人

Chung 表示，本場座談旨在分享友善環境的故事，以及公共政策如何回應節能網路議題。討論重點如下：

(一) 節能網路的政策案例分享

我國數位發展部唐鳳部長分享臺灣以數位轉型推動減碳的作法。她表示，臺灣訂下 2050 淨零排放的目標，目前具體措施如數發部「臺灣雲市集」平臺，當中的雲端方案包括電能管理、溫室氣體盤查的系統或解決方案等，方便中小企業導入，而非只有大企業才能做到節能減碳。此外，通訊傳播委員會規劃 3G 網路於 2024 年落日，屆時臺灣一年將可減少約 1 億度用電。

紐西蘭國碼頂級域名（ccTLD）管理維運單位 InternetNZ 的首席顧問 Ellen Strickland，也分享紐西蘭從再生能源角度切入的環保策略。她表示，紐西南推動 2030 年前達成 90% 再生能源的目標，屆時即使伺服器和機房等網路維運設備和場所的節能效果有限，整體社會仍能達到降低氣候變遷衝擊的目標。

(二) 人人可響應的節能網路措施

德國技術評估和系統分析研究機構（Institute for Technology Assessment and Systems Analysis）研究員 Jaewon Son 表示，人人都可以響應節能網路，例如：我們可以取消不再閱讀內文的 email 訂閱，此舉可以同時減少網路頻繁傳輸和伺服器儲存的耗能。此外，在各種網路治理會議、課程，以及網路社群，應該多推廣此議題，讓更多人知道網路對環境的影響。

(三) 網路對環境的影響需視其取代的耗能活動而定

主持人 Chung 介紹 DotAsia 的網路對環境影響研究計畫，並指出初步研究結果顯示，如果只看網路碳足跡（Internet Footprint）恐怕會有所誤導，因為這項數字只會隨著我們使用更多的網路應用而越來越高。例如：使用視訊會議軟體Zoom時，筆電或手機的電池消耗得更快，但我們要思考的是，它是否取代更耗能的傳統活動，或有效減少實體碳足跡（Physical Footprint）。此外，也要思考我們是否建設過多的寬頻網路，因為維運一條寬頻網路遠

比傳輸資料更加耗能。

四、演講：低軌衛星的機會與挑戰

「低軌衛星星群——它們會帶來更好的網路接取和更具韌性的網路嗎？」演講，由跨國技術社群 ISOC（網際網路協會）申辦，講者為 ISOC 低軌衛星（Low Earth Orbit Satellite，簡稱 LEOs）網路系統計畫主持人 Dan York，以及 ISOC 亞太地區副主席 Rajnesh Singh，兩人以來回輪流方式演講，內容重點如下：

(一) LEOs 的興起和現況

SpaceX 在烏克蘭提供 LEOs 網路服務是數月前的熱門新聞，但它只是 LEOs 的其一，Amazon 的 Kuiper 計畫也將在 2022 年末發射衛星，還有中、印等各國也都有 LEOs 計畫。LEOs 需要大量佈署，故稱為星群(constellation)。如 SpaceX 的 Starlink 計畫預計發射 15,000 顆衛星，目前的進度是 2,800 顆。

LEOs 之所以蔚為風潮，原因包括：連線低延遲、火箭科技的進步降低發射費用、設備元件小型化讓衛星得以量產，以及出現能夠同時提供衛星和發射服務的企業。

(二) LEOs 的機會與挑戰

LEOs 帶來許多潛在機會，例如：為偏遠地區的個人、圖書館、學校、小島提供網路服務；為社區網路提供回載（backhaul）；為天然災害地區提供網路通訊等。但同時也伴隨如下的商業面、政策面和技術面的挑戰。

- 商業面挑戰：可負擔性、容量（是否會擁塞）、競爭（若市場競爭不足，價格將居高不下）、合併（未來是否形成少數企業壟斷）。
- 政策面挑戰：頻譜配置、干擾（來自軍方、航空業、行動通訊業的干擾）、軌道配置（目前國際規則模糊不清）、各國法規限制（如須向每個國家各別申請頻譜）。

- 技術面挑戰：安全、隱私、開放標準、互通性、太空垃圾。

(三) LEOs 的未來

LEOs 產業才剛開始起步，故有諸多問題 ISOC 目前也無答案。例如：可持續的商業模式為何？又對現有 ISPs、地球環境、天文學將造成什麼影響？儘管如此，為了共同塑造 LEOs 的未來，ISOC 最後也呼籲大家，分享 LEOs 的資訊或協助回答相關問題；如果是相關產學界人士，也請分享佈署或試點計畫的經驗。

五、座談：因應數位人權議程改變

「因應疫後世界數位人權優先事項的變化」座談，由跨國公民團體——進步通訊協會（Association for Progressive Communications, APC）亞洲數位權利主任 Pavitra Ramanujam 申辦並主持。Ramanujam 表示，疫情加速政府導入數位科技，網路讓公共參與更容易，但也讓政府更方便地控制數位空間、破壞數位人權。因此，本次會議將探討疫情如何改變數位人權的議程，又該如何因應。討論重點如下：

(一) 馬來西亞整體數位人權倒退，但個資隱私保護意識提升

英國諾丁漢大學馬來西亞分校助理教授 Gayathry Venkiteswaran 表示，馬來西亞的特殊情況是對抗疫情的同時，也面臨政黨輪替。然而，新政府卻濫用緊急命令，加強對網路言論的控制和限制，尤其涉及種族、宗教、皇室的言論更是敏感，且遭到調查、審判和內容下架的案件大增，猶如回到威權時代。另一個特殊情況為 2021 年發生重大的個資外洩事件，但也因此喚起民眾保護個資和隱私的意識。例如：民眾對於對抗疫情的 Apps 功能，從原本的接觸追蹤擴大到器官捐贈等，已經有所疑慮，並要求政府提出保護措施。

(二) 泰國政府建構數位威權主義生態系統

泰國公民團體 Thai Netizen Network 專案經理 Darika Bamrungchok 指出，雖然網路讓社會運動得以快速動員，但網路也成為政府監控民眾和打壓人權的武器。Bamrungchok 以泰國 2020~2021 年爭取民主的抗議活動為例，歸納出泰國政府透過司法騷擾和起訴、網路和媒體審查、數位監控、資訊戰等 4 大手段，建構數位威權主義生態系統，掌控並操弄能夠影響公眾輿論和政治意向的資訊。

(三) 韓國防疫有成，但過度蒐集個資可能不符國際人權標準

韓國公民團體 Korean Progressive Network Jinbone 主席 Byoung-il Oh 表示，防疫和保障數位人權的確是兩難，為了公共健康可能需要限制某部分的人權，但防疫政策也應該基於最小侵害原則，不該獨斷推行。韓國採取所謂的 3T 防疫策略，也就是篩檢（test）、追蹤（trace）、治療（treat），雖然被視為成功控制疫情，但過程中民眾的手機位置、信用卡、交通卡等個資都被蒐集，形同曝露習慣和喜好等隱私。因此，韓國的防疫政策並不符合國際人權標準的比例原則。

六、演講：LACS 提升網路韌性

「建立本地可存取的雲端服務以提升網路韌性」演講，由日本的國際電氣通信基礎技術研究所（Advanced Telecommunications Research Institute International, ATR）Toshikazu Sakano 博士主講，內容重點如下：

(一) LACS 可立即為災區提供通訊網路服務

有鑑於地震、海嘯、颱風等天災發生時，容易對電力和通訊網路設施（如電纜、路由器、傳輸設備等）造成嚴重破壞，導致通訊中斷，進而影響救災和民眾生活，日本 ATR 研究開發本地可存取的雲端服務（Locally Accessible Cloud Service, LACS），以立即提供災區網路通訊服務。

LACS 是一種便於攜帶的伺服器系統，大小猶如手提行李箱，裡面裝有小型電腦、Wi-Fi 接收器、電池、太陽能充電板、網路交換器等，可隨

時隨地在任何網路環境中，提供雲端通訊服務，包括：政府部門公告重要訊息、用戶分享資訊（類似社群媒體服務）、用戶雙向通訊（類似通訊軟體服務）。儘管服務地區和人數有限，但只要用戶透過手機等裝置的 Wi-Fi 功能，就可使用 LACS 處理文字、語音、影像、動畫等資料。



圖片來源：Dr. Toshikazu Sakano

圖 9-1 LACS（本地可存取的雲端服務）系統的外觀和裝置

(二) LACS 還可用於普及服務、線上教育，已通過實驗且產品即將上市

除了災後救助和復原外，LACS 平時亦能作為開發中國家或一般偏鄉地區的社區網路，為當地民眾提供基本的連線服務，並可用於數位醫療和線上教育，有助於消弭數位落差。此外，亦可在人潮聚集的活動，協助卸載流量，減輕核心網路的負擔。這些用途皆已在日本和菲律賓進行並通過概念性驗證（Proof of Concept, POC）實驗，不久後產品就可上市。

七、座談：APNIC 合作特別興趣小組和 APrIGF（地緣政治議題）

本場會議由 APNIC 的合作特別興趣小組（Cooperation SIG）主辦，並納入 APrIGF 議程。會議由該小組的主席、TWNIC（台灣網路資訊中心）丁綺萍副執行長主持，探討多方利害關係人（以下簡稱多方）參與網路治理過程中，如何受到近期地緣政治衝突和國家法規的影響。討論重點如下：

(一) 經驗分享：俄羅斯國際交流處境尷尬；阿富汗數位人權倒退

俄羅斯國碼頂級域名(ccTLD)相關單位的專案經理 Ilona Stadnik 表示，今年（2022）俄羅斯的網路治理教育推廣工作，因地緣政治衝突而面臨許多挑戰。例如：在俄羅斯舉辦課程和會議，邀請不到國際專業講者；而參與國際論壇，隨著各大會議從線上恢復為實體，卻有無法出國的問題，或出國後可能受到俄羅斯形象不佳的牽連。

阿富汗國家 IT 專業協會（National IT Professionals Association of Afganistan）主席 Mohibullah Utmankhil 則指出，雖然阿富汗仍有 77% 人口無法上網，但自從塔利班重新掌權以來，不但對某些地區進行斷網及阻斷連接特定網站，還對社群媒體的訊息進行監控，嚴重侵犯阿富汗的數位人權，甚至禁止舉辦網路治理論壇和課程。因此，呼籲國際社會和當地民間組織合作，共同改善阿富汗的寬頻接取、數位人權和能力建構。

(二) 專家：以人類仰賴網路的敘事，應對地緣政治的威脅

前 ICANN（網際網路名稱與號碼指配機構）總裁 Paul Twomey 博士表示，當前網路維持高效的運作，證明多方模式是管理全球網路的最佳方式，然而卻日益受到地緣政治衝突的挑戰。例如：俄烏戰爭迫使當地網路運營商將其流量從一組連接，重新定向到其他網路，且 BGP（Border Gateway Protocol，邊界閘道協定）表格也被更改，不但影響網路運作效能，也凸顯地緣政治和網路技術社群的運作方式發生衝突。

網路內容也是地緣政治衝突的其一領域。在多方模式下，網路成為公共財，但也發展出超級強大的平臺，並被反對多方模式的政治家指控「美國人控制一切，我們需要新的模式」。此外，美國及其盟友和中國大陸之間

的技術標準制定、5G 部署、晶片和各種貿易限制，也是另一場地緣政治衝突。為此，技術社群可以提出人類深度仰賴高效運作網路的敘事(narrative)，不論是教育、工作、生活、健康等各方面，藉由敘事發揮影響力，應對地緣政治的威脅。

(三) 專家：社群相互支持並捍衛多方模式，以因應數位威權的威脅

香港技術社群 Tech for Good Asia 創辦人暨美國史丹福大學的訪問學者 Charles Mok（莫乃光）表示，網路分裂比斷網還糟糕，那些切斷網路的政府是因為尚不知道分裂網路的技術和資源，一旦他們像中國大陸一樣掌握要領，根本就不必斷網，只要分裂網路即可。還有其他講者提到一些政府限制民眾發展數位素養和網路治理的能力，這是因為網路治理的多方模式，正是防止網路分裂和因應其他治理問題的好工具。

Mok 並指出，上述情況並非是威權國家獨有，而是也會發生在民主國家，香港就是一個證明，網路自由於一夕之間就消失，香港民眾的自我審查言論變成一種生存的行為。因此，來自各國的網路治理社群應該相互支持，共同面對這些挑戰，捍衛多方模式。尤其技術社群的與會者，在開發新產品或新服務時，務必要考量人權。

第三節 心得與建議

- **掌握《全球數位協議》因應網路問題之規畫，作為我國施政參考**

聯合國訂於 2024 年通過《全球數位協議》（GDC），以透過國際合作因應網路發展的挑戰。根據開幕致詞貴賓——聯合國秘書長之科技大使 Amandeep Singh Gill 所述，GDC 並非只是一份指導原則，而是包含因應普及連網、假訊息、人權、AI 等問題的全球合作優先事項和方法。因此，雖然我國無法簽署 GDC，但數位發展部仍應掌握其進展，及所規畫的網路問題因應方向和措施，以作為國內的施政參考，同時也尋求未來在國際合作實務上的臺灣參與機會。此外，由於 Gill 也承諾，將在聯合國以會員國為主的多邊程序中，採納多方利害關係人的觀點。因此，我國可透過網路治理國際會議的 GDC 相關場次，對 GDC 草案表達意見。

- **持續參與 APrIGF 進行國際政策交流，並將新資訊引進國內**

本屆 APrIGF 我國數位發展部唐鳳部長應邀擔任「節能網路」議題的講者，分享臺灣以數位轉型推動減碳的作法；而同場次其他講者的主張，例如：應向大眾推廣此議題、其效益不宜被網路碳足跡誤導等，相信數發部亦會作為其施政參考。

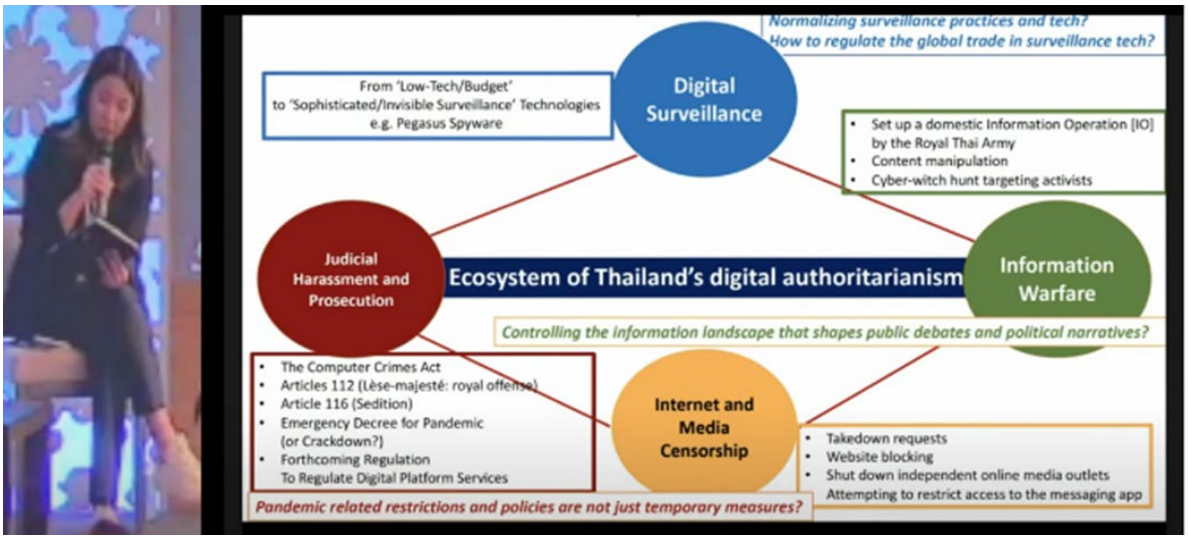
此外，本屆會議還有 ISOC 專家介紹「低軌衛星（LEOs）的機會與挑戰」，演講內容深入淺出，可作為科普教材。LEOs 亦是最近國內的熱門議題，數發部訂於 2022 年 11 月開放執照申請，明年或可於 APrIGF 申辦座談，進一步和其他國家探討政策面議題。

又日本的國際電氣通信基礎技術研究所（ATR）專家於本次會議介紹 ATR 研發的 LACS（本地可存取的雲端服務），雖然整套裝置只有手提行李箱的大小，但可為受災地區、偏遠地區、開發中國家，甚至是活動慶典場合，立即提供通訊網路服務。LACS 即將量產上市，建議數發部取得詳細資料，並評估我國電信普及服務是否有採購需求。

第四節 會議剪影







場次 S.13 打擊假訊息；場次 S.21 低軌衛星的機會與挑戰；場次 S.11 因應數位人權議程改變

第十章 結論與建議

第一節 案例研析 (1) 對俄斷網制裁的發展與影響

一、 結論

(一) 國際普遍反對「全面性」斷網制裁，但對多方機制實施制裁無共識

從 ICANN 和 RIPE 婉拒烏克蘭政府的斷網制裁政治訴求、40 多個公民團體聯合呼籲勿對俄羅斯斷網、美英兩國政府發布電信網通服務「通用許可」，以及專家學者對於網路資源治理得以維持政治中立的肯定，凸顯即使在強烈的挺烏反俄氛圍下，國際社會仍普遍反對對俄羅斯實施「全面性」的斷網制裁，以維護全球網路的正常運作，保障俄羅斯的人道通訊所需、獲取外界資訊，以及避免助長普丁的資訊控制。

至於部分專家聯合提出的「多方利害關係人實施網路制裁」，網路治理社群對此並無共識。反對方的理由如：網路制裁和經濟制裁不同，無法精準地不波及一般民眾；針對軍事和宣傳機構的制裁無效，因為可輕易轉換至民用網路和其他傳播管道；制裁的本質為國家政府的行為，而非其他利害關係人的消費者抵制運動；由「非國家行為者」制定基於政治目的的網路制裁清單，將破壞網路運營商的自治機制及全球網路的互連和韌性。

(二) 歐美國家排除或豁免電信網通制裁，我國法規方向亦和國際一致

不論是原本法規即排除民用電信網絡制裁的歐盟，或在公民團體聯合呼籲後發布「通用許可」豁免電信網通相關制裁的美國和英國，整體而言，除了受制裁或管制行業的實體和個人外，目前歐美各國沒有禁止對俄羅斯提供電信網通相關服務。我國亦加入制裁俄羅斯的國際行列，於 4 月 6 日公告並實施「輸往俄羅斯高科技貨品清單」(5 月 6 日增加白俄羅斯)，主管機關為經濟部（2022），內容主要是針對電子等 8 大類產品出口俄羅斯進行管制，但一般民眾使用的電腦、電信和資訊安全類別產品，不在管制

範圍。此規範可謂和歐美國家排除或豁免電信網通制裁的法規方向一致。

(三) 斷網制裁加上「數位孤立」，全球網路分裂危機更甚以往

雖然 ICANN 和 RIPE 維持俄羅斯關鍵網路資源的正常運作，且歐美和我國等也允許持續對俄提供電信網通服務，不過，多數國際資通訊大廠仍未恢復俄羅斯的業務或服務。加上普丁還以封鎖西方新聞媒體和社群平臺作為反制，進而形成雙向封鎖。因此，專家認為陷入「數位孤立」的俄羅斯將更積極推動網路主權，且更倚賴中國大陸的軟硬體，甚至可能淪為其網路主權倡議的追隨者；其他獨裁國家也會對俄羅斯的處境引以為鑑，尋求數位自主，以為脫離全球網路做準備；而全球網路也因此更趨向分裂，可能形成依國界劃分、眾多無法互通的網路，甚至使用技術不相容的網路協議，或擁護不同的國際治理機構，以致全球網路互連的時代宣告終結。

二、 建議事項

(一) 立即可行：研議建立多方機制，為重大網路事件奠定即時決策基礎

雖然由部分專家聯合提出的「多方利害關係人實施網路制裁」，因為制裁的本質是否屬其他利害關係人不宜涉入的國家政府行為等論點，而未能廣獲網路治理社群的支持，不過，這並不代表多方的方式或程序遭到否定，反而《麻省理工科技評論》還指出，沒人能提出比現行多方方式更好的替代方案來治理全球網路資源——儘管因為採取共識決而導致進展非常緩慢（Ball, 2022）。

為此，此份聯合聲明所建議的「建立多方機制作為因應重大或緊急網路事件的即時決策基礎」，仍可供通傳會和數位發展部參考。惟建立一個合適的多方機制需先投入資源進行研議規劃，因為除了需掌握開放、平等、透明的參與原則；由下而上的運作過程；及共識決的決策方式等細節之外，還需因應常被詬病的效率低落等問題（TWNIC, 2019）。而針對後者，或許至少先界定不同情境下將採行的不同機制。如重大但非緊急事件，採取真

正的多方機制——從界定議題範圍、產出方案到決策執行；但緊急事件時，則回歸既有的行政程序，而多方僅扮演諮詢的角色。

此外，美國數位治理顧問 Farzaneh Badii（2022）也提醒，應避免多方機制被少數有權勢者控制。例如此份聯合聲明最後只有 4 成參與討論者簽署，另有高達 6 成未簽署，且不知他們是何許人也；加上 10 天內即從無到有火速完成所有作業，凸顯其運作和決策過程皆有問題，以致失去多方程序應帶來的不同思辨之優勢，且最終產出多項無效的建議。

(二) 中長期：於 ICANN 推動 ccTLD 政策修改，避免.tw 因政治而遭移除

ICANN 婉拒烏克蘭政府的斷網政治訴求，捍衛 ccTLD「政治中立」的治理原則，看似亦對我國有利，意即萬一中國大陸也要求撤銷我國.tw，ICANN 應會同樣基於中立立場而拒絕。然而，實際狀況恐非如此樂觀。

ICANN 表明無權撤銷俄羅斯的 ccTLD，除了其成立宗旨並未被賦予實施網路制裁的權力之外，另一方面，根據 GAC（政府諮詢委員會）的《ccTLDs 授權與管理之原則和指南》，ccTLD 屬於各國的當地議題，且發生爭議時是訴諸各國的當地法規，ICANN 維持中立立場。而 ccTLD 主要又是參照 ISO 3166 國碼標準所制定，但隸屬聯合國組織的 ISO 在 3166 國碼標準中，將我國標註為「中國大陸的一省」。

由於我國無法排除中國大陸於 GAC 援用此標準要求移除.tw 的可能性，因此，儘管難度很高，但代表我國參與 GAC 之數位發展部（原交通部和通傳會業務）仍可嘗試集結具有相似需求的其他國家，共同推動修改《ccTLDs 授權與管理之原則和指南》，藉由增加「尊重現狀、保護既有使用者權益」等條文（本計畫諮詢顧問曾更瑩律師之建議），降低.tw 因政治干預而遭移除的風險。

第二節 案例研析 (2) 解讀《未來網際網路宣言》

一、 結論

(一) DFI 承諾廣受肯定，具有數位政策「定位」和改善施政的意義

雖然 DFI 所承諾「開放、自由、全球化、可互通、可靠和安全」的網路願景，在過去的國際議程都曾出現，但專家認為，在當前數位威權主義興起和網路面臨分裂之際，重申這些承諾有其時代意義，尤其在面臨嚴峻的網路挑戰時，DFI 可為數位政策「定位」，避免推出偏離的政策措施。此外，DFI 還在美國內部發揮政策改善的具體價值，美國學者表示，最近美國在促進隱私（公布《美國資料隱私和保護法》草案）和確保國際資料流通（和歐盟達成《跨大西洋資料隱私框架》協議）等方面，已取得實質進展。

(二) DFI 無約束力和實施機制，未來前景不明

儘管本計畫嘗試拼湊出 DFI 推動方式的模糊輪廓——如透過 TTC（美歐貿易和科技委員會）等多邊場合、國務院成立新的「網路空間暨數位政策局」等；且有公民團體表示將促使政府信守 DFI 承諾；又美國官員也認為 DFI 可形成的國際常規和公民社會監督力量，不容小覷。不過，DFI 不具法律約束力、缺乏實施機制、尚未和全球既有進程建立關聯性等問題，也引發不少對其未來發展的質疑。例如：美國智庫「外交關係協會」(CFR）指稱「未來也仍無法藉由 DFI 實現全球網路的烏托邦願景」、公民團體 Access Now 認為「DFI 最終只會淪為空談，甚至佔用國際政策論辯的有限資源」。

(三) DFI 制定程序違背多方承諾，如何重建多方社群信任亦是考驗

DFI 以「由上而下」、僅有政府單位參與，且沒有公開向公民社會徵求意見的方式制定，違反其「強化多方利害關係人的網路治理」承諾及原則，

不但引發拜登政府的誠信問題，也破壞多方方法的可信度，喪失非政府利害關係人的聯合支持，甚至可能反而讓威權政府加以仿效。後續如何重建多方社群對 DFI 的信任和支持，亦仍是一大考驗。

(四) 民主和威權陣營對峙，全球網路治理更趨兩極化

目前 DFI 共有 61 個簽署國（加上歐盟則有 62 個簽署者），美國也持續尋求願意落實 DFI 承諾，且沒有斷網或封閉平臺等不良紀錄的國家加入。而就在 DFI 發布後的 2 個多月，中國大陸在北京成立「世界互聯網大會國際組織」（WICO），將一個已經舉辦 8 年的「國際會議」，升級為「常設國際組織」，以強化在全球推動國家控制網路的理念，被視為是對 DFI 的反擊。中共官媒聲稱，WICO 已有來自近 20 國的上百個網路相關機構、組織、企業及個人加入。雖然這並非美中雙方陣營的首次網路治理理念之爭，例如 2020 年美國推出「乾淨網路」計畫後，中國大陸也提出《全球數據安全倡議》作為抵制。不過，就 DFI 和 WICO 的目標來看，此次更凸顯自由民主和數位威權兩個陣營的對峙，也讓全球網路治理更趨兩極化的發展。

二、 建議事項

(一) 立即可行：將 DFI 原則轉化為具體政策措施，以履行簽署國承諾

雖然 DFI 不具約束力，但為了維護自由開放的網路共同願景，身為簽署國的我國應履行承諾，也就是落實其 5 大類 23 個子項的關鍵原則。因此，首要之務是由數位發展部籌組多方利害關係人專家小組，逐項確認、解讀這些原則的文義重點，之後識別各項原則的主責部門及對應的業務，進而將 DFI 原則轉化為具體的政策措施，並加以推行。

以 DFI 第 5 大類「強化多方利害關係人的網路治理」的第一項原則「保護和強化網路治理的多方利害關係人系統，包括主要技術協定和其他相關標準及協定的開發、部署與管理」為例，可能是指維護 IETF（Internet Engineering Task Force，網際網路工程任務組）和 IANA 的多方運作方式。

又其第二項原則「避免破壞攸關網路一般可用性及完整性的技術基礎設施」，可能是指維護 ICANN 掌管全球關鍵網路資源，避免將治理權移轉到由國家政府控制的 ITU。這 2 項原則應為數位發展部資源管理司（原通傳會射頻與資源管理處）的國際交流合作相關業務。至於如何在參與這些國際組織時，維護其多方運作方式，則需由該處（司）進一步研議。

(二) 中長期：定期評估我國 DFI 履行情況，做為對內改善對外貢獻基礎

身為網路自由度於全球名列前茅的國家，我國可考慮提高標準，針對前述 DFI 的 5 大類 23 個子項的關鍵原則，由轄下包含民主網絡司的數位發展部委託公正第三方，定期評估我國 DFI 履行情況，進而做為改善國內相關施政，及貢獻國際社會的基礎。

例如 DFI 第 1 大類「保護人權與基本自由」的其一原則為「……採取減少線上非法及有害內容的行動時，會符合……言論自由權，並鼓勵多元意見及多元主義，讓民眾免於言論審查、騷擾或恐嚇的恐懼」，如經評估認定期間內有「查水表」事件，數位發展部可基於履行 DFI 簽署國承諾，請執法單位予以改善。又如第 3 大類「推動包容和可負擔的網路連線」當中的「推動個人和企業可負擔、具包容性及可信賴的網路連線……」原則，如經評估認定已高度落實，則可將通傳會基礎設施與資通安全處（移撥數位發展部韌性建設司）所推動的數位基礎建設及縮短偏鄉數位落差相關計畫，透過國際會議或交流訪問等場合，提供他國參考，貢獻國際社會。

第三節 案例研析 (3)「公平分攤」網路成本的爭議

一、 結論

(一) 歐盟可能推出「公平分攤」網路成本規定，進而成為全球新標準

面對電信業者重提內容業者（CPs）應分攤網路建設成本的訴求，歐盟執委會已訂於 2023 年第一季正式商議此「公平分攤」政策議題。雖然目前無法確定商議後是否將提出法案，又如果提案是否和原先研擬的《連網基礎設施法案》（CIA）相關。另一方面，此訴求也面臨 CPs 和數十個公民團體的反對，指稱違反歐盟「網路中立」法規；而且專家們亦提出破壞全球數位常規、言論自由和流量產業發展等疑慮。不過，由於歐洲的 5G 佈署相對落後，可能衝擊 2030 年《歐洲數位十年》政策的兌現；加上近年歐盟的政策立場也轉向監管科技巨頭。因此，歐盟仍可能推出「公平分攤」網路建設成本的規定，《路透社》報導甚至認為歐盟此次有機會為網路建設成本豎立全球新標準。至於「網路中立」問題，有電信商表示不必擔憂，因為他們並不會限制網路流量，目標只是確保科技巨頭為飆升的網路成本作出貢獻，而小公司根本不必支付任何費用。

(二) 韓案例凸顯中小型國若率先針對科技巨頭，恐影響對美政經關係

韓國於 2020 年 12 月率先全球，實施被稱為 Netflix law 的《電信事業法》部分修正條文，藉由賦予大型 CPs 提供「穩定服務」的義務，讓科技巨頭向韓國 ISPs 支付網路使用費。然因「穩定服務」語意模糊，以致 Netflix 和 YouTube 迄今仍未付費，於是韓國國會議員陸續再提出相關修正草案，目前已有 7 案送至國會。韓國此項政策發展也成為歐洲電信業者津津樂道的案例，但卻引來美國的政治回應。相關事件如：美國直接對修法表達關切，致使一場法案公聽會從 4 月延宕至 9 月才召開；美國將此問題列為 2022 年美韓的貿易障礙之一；美國商務部於 9 月份雙方經貿會議暗示此問題造成緊張局勢；美國 4 月底推動的《未來網際網路宣言》韓國較各國延

後近一個月才得以加入（參見本報告第四章第三節）。此外，美國的電腦與通訊產業協會（CCIA）還列出韓國可能違反《韓美自由貿易協定》當中的數項條款。由此也凸顯中小型國家如果率先推出不利於科技巨頭的政策，美國勢必會有所回應，並可能影響雙方的政經關係。

二、 建議事項

(一) 立即可行：掌握「公平分攤」政策動向，以利國內政策順應國際潮流

國內電信業者亦相當關注國際間涉及網路建設成本分攤的議題，並曾呼籲讓電信業者可以向高流量的內容業者收取分潤費。因此，建議通傳會掌握國際「公平分攤」政策議題的動向和進展，以利國內相關政策能在第一時間順應國際潮流。當中，尤其要密切追蹤可能為全球豎立新標準的歐盟政策。依據歐盟執委會的時程規劃，其政策諮商將於 2023 年第一季啟動，預計 6 至 9 月期間發布政策方案。而在政策明朗化之前，歐盟電子通訊傳播監管機構（BEREC）訂於 3 月到 6 月發布的評估報告，亦值得關注，因為報告可能有助於釐清各方立場和各種意見的合理性。

此外，「公平分攤」的政策方向在歐盟和韓國皆被指稱違反「網路中立」原則。因此，亦可留意歐盟和韓國如何回應此項疑慮，以釐清「網路中立」的意涵或是否有新的解讀。至於美國《公平資助法案》，雖然立法進展難以預測，且美國「普及服務基金」的用途和籌資機制和我國有所差異，但一旦法案通過後，FCC 須於 180 天內完成可行性評估報告，屆時評估結果將攸關內容業者是否應承擔網路普及服務責任的國際新趨勢，並可作為數位部管理我國「電信事業普及服務基金」的參考。

(二) 中長期：普及連線概念已升級，我國數位平權計畫可參與 PNMA

美國《公平資助法案》（草案）的最終目的，是希望科技巨頭能夠資助普及服務基金（USF），以縮減數位落差。同樣地，我國電信普及服務亦是透過積極建設通信基礎設施，以消弭數位落差。不過，根據 IGF 資料，普

及連線（universal access）的概念已擴展至「有意義連網」（meaningful access），因為許多例證顯示，有些地區即使有網路覆蓋，人們也不使用。為此，IGF 於 2021 年成立「有意義連網政策網絡」（Policy Network on Meaningful Access, PNMA），期能透過專家工作小組的引領和全球多方利害關係人的討論，從網路基礎設施、使用者的意願和能力、內容和網路環境的公平和多樣性等層面，找出成功案例、識別推動障礙，並提出政策建議，以協助各國落實數位平權，消弭數位落差。

我國教育部自 2020 年起，實施為期四年的「邁向數位平權推動計畫」，整合包含通傳會（業務移撥數位部）等部會資源，建構人人享有數位平權且友善的數位環境。建議計畫主責和協辦部會派員參與 PNMA，和國際進行政策交流，並將最佳實踐引入國內，以促進我國實現數位平權計畫目標。

第四節 大專校園講座

本項工作要求於大專校園內辦理50人以上的網路治理實體講座，今年第一季疫情雖有趨緩，但4月份開始COVID-19疫情再次升溫，染疫人數逐日上升；加上中央疫情指揮中心的相關政策經常滾動式調整，導致各大專校院教學方式有所不同。因不確定性高，以致在聯繫校方相關行政事宜時，需耗費更多時間確認資訊。

近兩年也因疫情關係，老師逐漸熟悉線上授課模式，且學生也已適應線上課程，建議未來在校園講座的規劃上，可放寬辦理形式，除了實體講座之外，亦可包含線上方式辦理，一方面保留計畫執行上的彈性，另一方面，線上講座也不受區域性的限制，更可擴大講座辦理效益。

第五節 人才培訓課程

根據課後問卷調查結果，學員對整體課程安排滿意度為 96%，講師授課內容滿意度為 100%，且所有學員皆表示未來有興趣參加網路治理活動，顯示今年度的研習營課程內容規劃與整體活動執行受到學員肯定。惟部分學員反應 1 日的課程安排過於緊湊，也因為受限於課程時間太短，無法提供講師及學員充分時間進行問答。

本課程於規劃時，為避免學員因參加培訓而須請假，或因週末 2 天都需進修而無法充分休息，影響到課業或工作，故將專題講習、案例探討及分組討論濃縮在 1 日進行。建議未來可提高預算增加課程時數，在實體搭配線上課程的混合方式下，增加授課天數，不僅能提供更具深度與廣度的教學，也讓學員能擁有更多時間消化學習內容，同時有更充裕的時間與講師交流，有助於提升培訓效益。

全球疫情逐漸好轉，國際間的網路治理會議得以重返實體，本計畫按照規劃補助 1 名優秀學員至新加坡參加 APrIGF 2022 會議。本屆優秀學員參與 APrIGF 非常主動且積極，亦回饋從參與實體會議中獲得許多新知獲益良多。建議仍可延續提供優秀學員出國參加國際會議之獎勵，以吸引更多人才報名參訓。

本次計畫選出 4 名學員擔任實習學員，原規劃安排至本會、臺灣網路資訊中心（TWNIC）或臺灣網路治理論壇（TWIGF）等執行網路治理相關業務的單位進行實習，但因各單位內部業務及人力規劃已有安排，加上學員本身也有工作或學業需兼顧，因此以參與國內外的網路治理會議，並撰寫會議紀錄的方式來執行。目前網路公司的實習機會競爭激烈且和網路治理無關，而公民團體或 NPOs 則無餘力可安排帶領實習生，以致難以媒合。建議 NCC 和數位部協調其所捐助成立或主管的 NPOs（如 TWNIC、TTC）提供實習機會。

第六節 課程影片製播

本年度計畫的 2 小時課程影片及 3 支精華短片，囿於有限的預算均由本計畫團隊自行產出。以觀看數而言，3 支精華短片觀看次數平均在 200 次左右，相較於前幾年僅 2 位數觀看次數的成績而言，已屬佳績。不過，Youtube 平臺每日有數以萬計的影片上傳，網路治理主題影片對於大眾而言內容較為嚴肅，吸引力自然較低。若要追求較高的影片品質及推廣成效，在企劃影片內容、拍攝影片及選擇推廣通路時，相對必須投入較高的成本。建議未來若通傳會提高影片製播預算，可考量前 2 年計畫與知識型網紅合作拍攝相關影片的方式，借助網紅本身的高訂閱數以及號召力，應更能擴大推廣效果，亦可多加嘗試於 Youtube 以外的平臺進行宣傳，以增加能見度。

本項工作依據 RFP，主要是將課程影片剪輯為數位教材；然 RFP 又規定進行數位行銷（雖然後來取消）和流量分析等行銷推廣類影片的工作項目，而此類影片需要的是精心製作的內容和具相當流量的渠道。故建議釐清影片製播的目的，並調整相關的工作子項和所需的資源。

第七節 國際會議 APrIGF 參與

- **掌握《全球數位協議》因應網路問題之規畫，作為我國施政參考**

聯合國訂於 2024 年通過《全球數位協議》（GDC），以透過國際合作因應網路發展的挑戰。根據開幕致詞貴賓——聯合國秘書長之科技大使 Amandeep Singh Gill 所述，GDC 並非只是一份指導原則，而是包含因應普及連網、假訊息、人權、AI 等問題的全球合作優先事項和方法。因此，雖然我國無法簽署 GDC，但數位發展部仍應掌握其進展，及所規畫的網路問題因應方向和措施，以作為國內的施政參考，同時也尋求未來在國際合作實務上的臺灣參與機會。此外，由於 Gill 也承諾，將在聯合國以會員國為主的多邊程序中，採納多方利害關係人的觀點。因此，我國可透過網路治理國際會議的 GDC 相關場次，對 GDC 草案表達意見。

- **持續參與 APrIGF 進行國際政策交流，並將新資訊引進國內**

本屆 APrIGF 我國數位發展部唐鳳部長應邀擔任「節能網路」議題的講者，分享臺灣以數位轉型推動減碳的作法；而同場次其他講者的主張，例如：應向大眾推廣此議題、其效益不宜被網路碳足跡誤導等，相信數發部亦會作為其施政參考。

此外，本屆會議還有 ISOC 專家介紹「低軌衛星（LEOs）的機會與挑戰」，演講內容深入淺出，可作為科普教材。LEOs 亦是最近國內的熱門議題，數發部訂於 2022 年 11 月開放執照申請，明年或可於 APrIGF 申辦座談，進一步和其他國家探討政策面議題。

又日本的國際電氣通信基礎技術研究所（ATR）專家於本次會議介紹 ATR 研發的 LACS（本地可存取的雲端服務），雖然整套裝置只有手提行李箱的大小，但可為受災地區、偏遠地區、開發中國家，甚至是活動慶典場合，立即提供通訊網路服務。LACS 即將量產上市，建議數發部取得詳細資料，並評估我國電信普及服務是否有採購需求。

中英文對照表

簡稱	英文	中文
APNIC	Asia Pacific Network Information Center	亞太網路資訊中心
APrIGF	Asia Pacific Regional Internet Governance Forum	亞太區網路治理論壇
AS	Autonomous System	IP 位址及自治系統
BEREC	Body of European Regulators for Electronic Communications	歐盟電子通訊傳播監管機構
BGP	Border Gateway Protocol	邊界閘道協定
BIS	Bureau of Industry and Security	美國商務部工業與安全局
CCIA	Computer & Communications Industry Association	電腦與通訊產業協會
ccNSO	Country Code Names Supporting Organization	國碼域名支援組織
ccTLD	Country Code Top-level Domain	國碼頂級域名
CDN	Content Delivery Network	內容傳遞網路
CENTR	Council of European National Top-Level Domain Registries	歐洲國家頂級網域管理局
CEPA	Center for European Policy Analysis	歐洲政策研究中心
CFR	Council on Foreign Relations	美國智庫—外交關係協會
CIA	Connectivity Infrastructure Act	《連網基礎設施法案》
CIRs	Critical Internet Resources	關鍵網路資源
CISA	Cybersecurity and Infrastructure Security Agency	美國國土安全部網路安全暨基礎設施安全局

CPs	Content Providers	內容供應商
DDoS	Distributed Denial of Service	分散式阻斷服務
DFI	The Declaration for the Future of the Internet	《未來網際網路宣言》
DMA	Digital Markets Act	歐盟《數位市場法》
DNS	Domain Name System	網域名稱系統
DSA	Digital Services Act	歐盟《數位服務法》
EC	European Commission	歐盟執委會
ETNO	European Telecommunications Network Operators'Association	歐洲電信網路營運商協會
EuroDIG	European Dialogue on Internet Governance	歐洲網路治理論壇
FCC	Federal Communications Commission	美國聯邦通訊委員會
FIRST	Forum of Incident Response and Security Teams	資安事件應變小組論壇
FOC	Freedom Online Coalition	網路自由聯盟
FTC	Federal Trade Commission	美國聯邦貿易委員會
G20	Group of Twenty	二十國集團
G7	Group of Seven	七大工業國家組織
GAC	Governmental Advisory Committee	政府諮詢委員會
GDC	Global Digital Compact	《全球數位協議》
GÉANT	GÉANT	歐洲學術研究網路
IANA	Internet Assigned Numbers Authority	網路號碼分配機構
ICANN	Internet Corporation for Assigned Names and Numbers	網際網路名稱與號碼指配機構
IETF	Internet Engineering Task Force	網際網路工程任務組
IGF	Internet Governance Forum	聯合國網路治理論壇
IoT	Internet of Thing	物聯網

IPEF	Indo-Pacific Economic Framework	印太經濟框架
IPv6	Internet Protocol version 6	第 6 版網際網路協定
ISOC	Internet Society	網際網路協會
ISPs	Internet Service Providers	網路服務供應商
ITU	International Telecommunications Union	國際電信聯盟
IXP	internet exchange point	歐洲網路交換中心
KCC	Korea Communications Commission	韓國國家通訊傳播委員會
LEOs	Low Earth Orbit Satellite	低軌衛星
LINX	London Internet Exchange	倫敦網路交換中心
MANRS	Mutually Agreed Norms for Routing Security	路由安全共同協議規範
NIR	National Internet Registry	國家級註冊管理機構
NTIA	National Telecommunications and Information Administration	美國商務部國家電信暨資訊管理局
OECD	Organisation for Economic Cooperation and Development	經濟合作暨發展組織
OFAC	Office of Foreign Assets Control	美國財政部外國資產控制辦公室
OFSI	Office of Financial Sanctions Implementation	英國財政部金融制裁執行辦公室
PNMA	Policy Network on Meaningful Access	有意義連網政策網絡
RIPE	Réseaux IP Européens Network Coordination Center（RIPE NCC）	歐洲 IP 網路資源協調中心
RIRs	Regional Internet Registries	區域網路註冊中心
RPKI	Resource Public Key Infrastructure	資源公鑰基礎建設
SIG	Special Interest Groups	特別興趣小組

TTC	U.S.-EU Trade and Technology Council	美歐貿易和科技委員會
USAID	United States Agency for International Development	美國國際開發總署
USF	Universal Service Fund	普及服務基金
WICO	World Internet Conference organization	世界互聯網大會國際組織
WSIS	World Summit on the Information Society	聯合國資訊社會世界高峰會
WTO	World Trade Organization	世界貿易組織

附錄

附錄一：大專校園講座簡報

- 政治大學
- 東海大學／中正大學

附錄二：「2022 網路治理研習營」課程簡報（僅提供講師授權公開部分）

- 數位人權：全球網路自由度及政策趨勢／陳文生顧問
- 平臺規範時代來臨了？／曾更瑩合夥律師
- 俄烏戰爭對網路治理規則的影響／黃勝雄執行長

附錄三：優秀學員參與 APrIGF 2022 會議摘要報告

附錄四：實習學員參與網路治理會議摘要報告

附錄一：大專校園講座簡報

Internet Policy

地緣政治衝突時代的網路治理

Kenny Huang, Ph.D. 黃勝雄博士

APNIC EC, TWNIC Board & CEO, NII Chair

2022 May 12

Internet Governance

網路治理軌跡

- 階段1：軍事發展 (1957-1970s)
  - DARPANet
- 階段2：學術研究 (1970-1990s)
  - TCP/IP
- 階段3：商業發展 (1990s-2000s)
  - WWW
- 階段4：大量媒介 (2000s-2010s)
  - WSIS
- 階段5: 所有人及所有物件 (2010s-2020s)
  - New internet complexity (IoT, AI, Big data..)

資訊社會發展

- 農業社會 (封建主義)
  - 要素： 土地與勞工
  - 君主制度
- 工業社會 (資本主義)
  - 要素: 土地、勞工、資本
  - 權力分散：行政權、司法權、立法權
  - 權力移轉：從皇宮移轉國會
- 資訊社會 (數據主義)
  - 要素: 土地、勞力、資本、數據
  - 權利分散: 決策權高度分散化
  - 權力移轉: 從政府治理模式移轉至多層及多方利害關係人治理模式

Internet 特性

- 技術架構
  - 植基於端點對端點原則(end-to-end)之分散網路組合的網路
- 資源
  - Protocols, names 及 numbers 盡乎無限資源 (IPv6), 無領土概念並可重複使用資源
- 法規
  - 在本國法、國際法之上的程式碼規範、 自律、及他律的混合型態

Protocols 及組織

Protocols

- 1969 RFC (Steve Crocker)
- 1971 @ (Roy Tomlinson)
- 1974 TCP/IP (Vint Cerf, Bob Kahn)
- 1982 SMTP (Jon Postel)
- 1985 DNS (Paul Mockapetris & Postel)
- 1991 HTML (Tim Berners-Lee)

組織

- 1975 IAB
- 1986 IETF
- 1989 IANA
- 1992 ISOC
- 1992 RIPE
- 1993 APNIC
- 1993 W3C
- 1998 ICANN
- 1999 TWNIC
- 2004 NRO
- 2005 IGF

DNS: 網路空間領域

- IP 位址
  - IPv4 : 32 bits, 43 億
  - IPv6 : 128bits, 無限
- 網域名稱
  - gTLD 通用頂級網域
  - ccTLD 國碼頂級網域
- 根伺服器 root server
  - 13 字元 (A-M)
  - 美國政府角色 : 授權頂級網域 zone file發布
  - 2016 年IANA 監理權移轉
    - Protocol : IETF
    - Number : RIRs
    - Names : ICANN 代管
- 管理
  - 1998年前: Jon Postel 管理 IANA, NSI 代管 root zone
  - 1998年後: root zone 改由美國政府委託 Versign 代管

網路治理概念

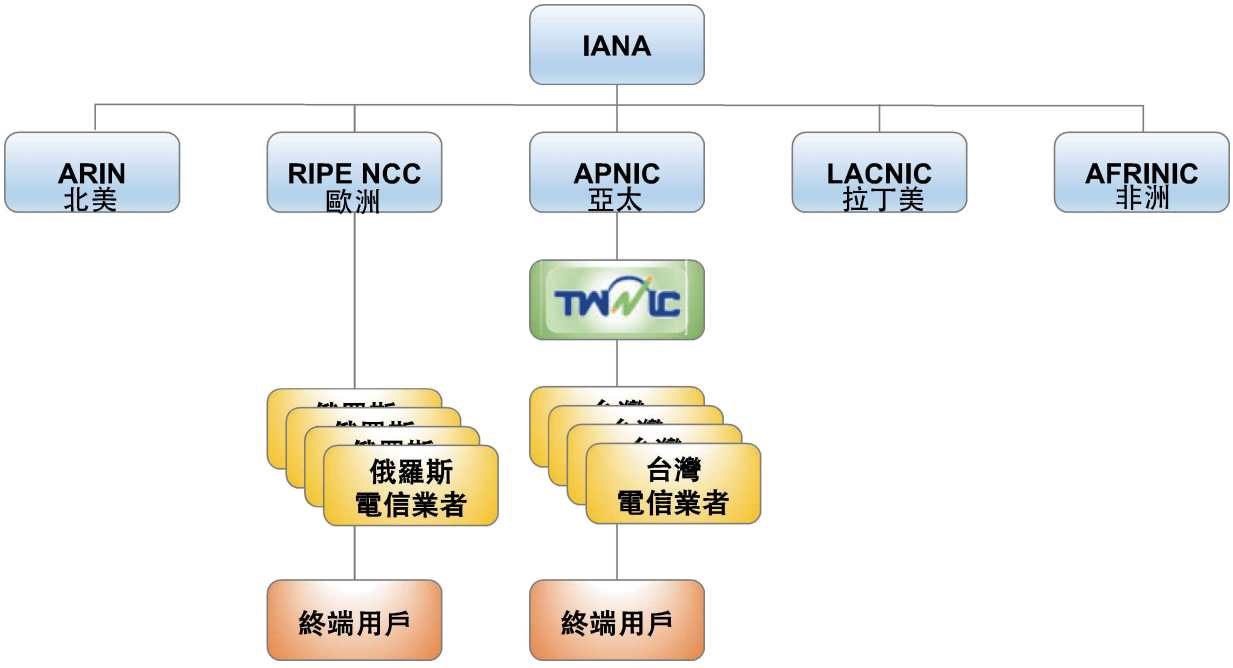
- 1991 Tim Berners-Lee (WWW)
  - 我們設計的網路是研究一種規則，讓電腦可以相容地共同運作。就如同社會規範就是研究一種規則讓人們可以和諧地共同工作。
- 1992 Dave Clark (IETF)
  - 我們不相信國王、總裁、及投票。我們相信粗略共識、事實依據、及可執行的程式碼
- 1996 John Barlows 網路獨立宣言
  - 我來自網路空間，心靈所在之處。我代表未來向政府提出宣言，希望你讓我們獨自留在網路空間，在網路空間你並不受到歡迎，網路空間沒有你的管轄權。
- 1998 Lawrence Lessig (Code is the Law)
  - 我們必須了解在網路空間如何利用程式碼規範軟體行為, 我們可以經由設計、發展出我們認同價值的網路空間。或者我們放棄設計符合社會價值的網路空間。程式碼不會憑空產生，它只能透過我們設計才能產生。

ICANN (1998)

- ICANNs mandate
  - Root Server
  - Domain names
  - IP addresses
- ICANN架構
  - 董事會
  - 支持組織 (supporting organizations)
    - gNSO, ccNSO, ASO
  - 諮詢委員會
    - GAC, ALAC, RSSAC, SSAC, TLG)
  - 究責機制
    - AoC Review, Reconsideration ..
- ICANN 運作原則
  - 安全與穩定 Security & stability
  - 由下而上政策制定機制
  - 多方利害關係人模式

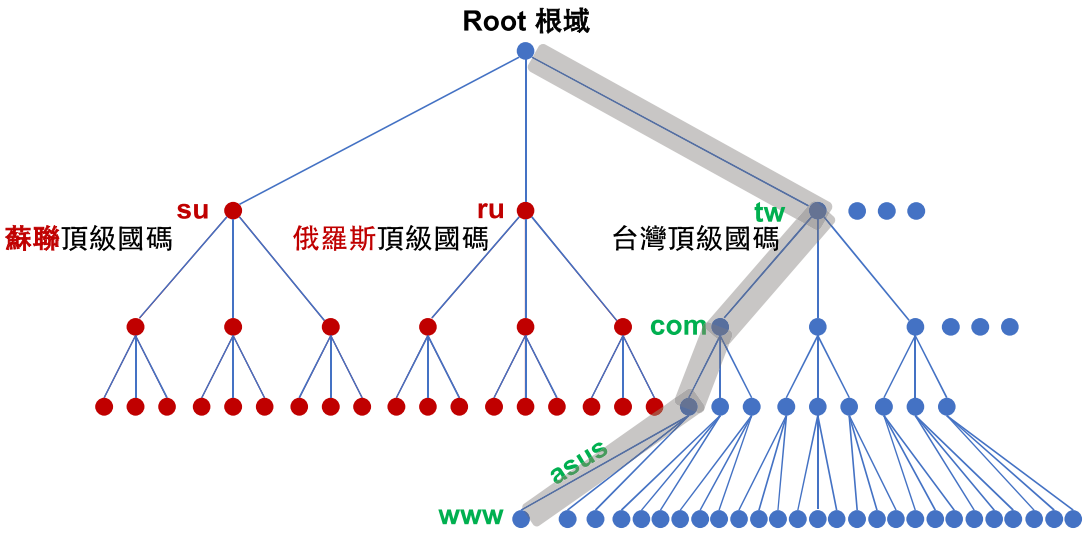
9

IP位址發放結構



10

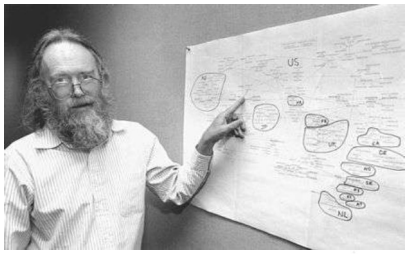
網域名稱結構

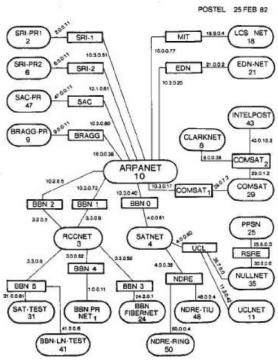


11

Jon Postel 與根伺服器管理機構

name		Operator 所有權人
A-Root		Verisign, Inc.
B-Root		Univ. of Sothern California, Information Sciences Inst.
C-Root		Cogent Communications
D-Root		Univ. of Maryland
E-Root		NASA Ames Research Renter
F-Root		Internet Systems Consortium （ISC）
G-Root		U.S. DoD Network Information Center
H-Root		U.S. Army Research laboratory
I-Root		Netnod
J-Root		Verisign, Inc.
K-Root		RIPE NCC
L-Root		ICANN
M-Root		WIDE project & JPRS





12

Jon Postel 變更根伺服器路徑



8 位根伺服器管理者(組織)

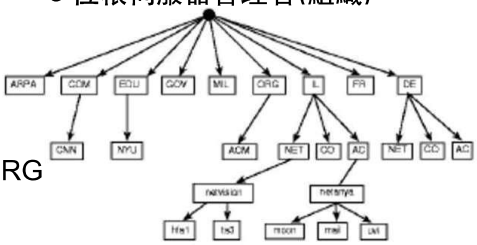


1998.01.28





IANA組織
DNSROOT.IANA.ORG



美國政府：
Postel 變更 root server 路徑沒有經過任何人授權同意。這次事件引起政府高度關注。美國強烈要求root server 路徑指向必須回復更動前的路徑指向。

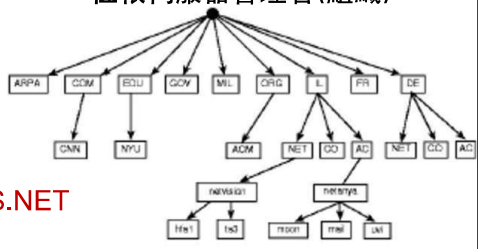
一週後, NTIA 公布改善網路域名及位址管理新計畫。
同年9月 ICANN 正式成立



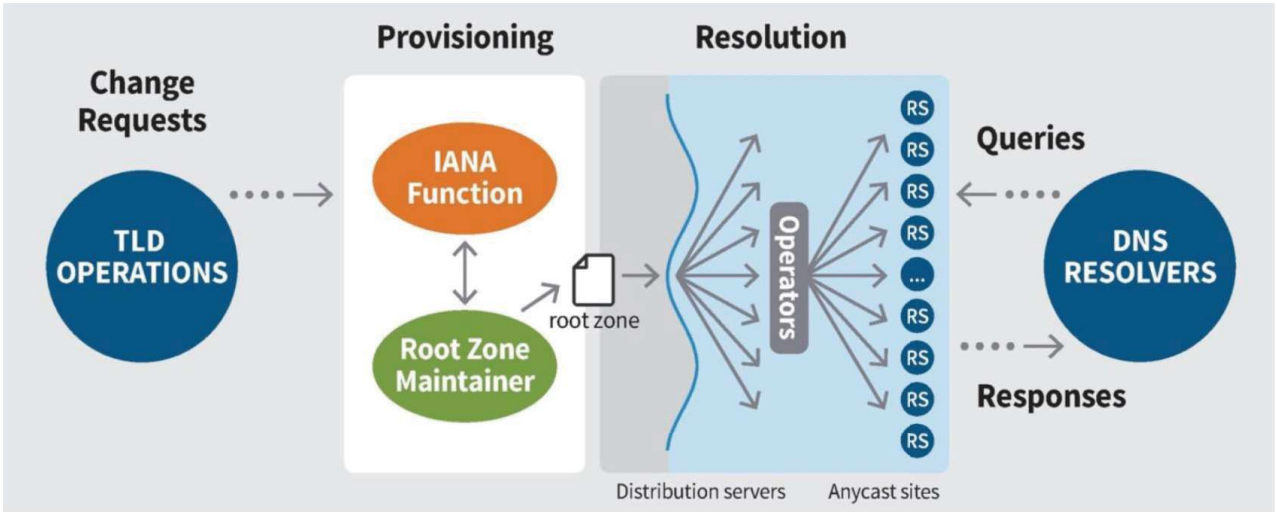
4位根伺服器管理者(組織)



NSI 公司
A.ROOT-SERVERS.NET



網域名稱註冊與解析架構



網際空間主軸演化

Previous Decades
過去數十年主軸

Infrastructure

基礎建設

Last Decade
過去十年主軸

Technical Innovations

技術創新

Next Decade
未來十年主軸

Policy, Regulations & Governance

政策法規、治理

15

網路治理模式

多方利害關係人模式
Multistakeholder model

- ICANN
- 區域網路資訊中心 RIRs
- 網路標準機構 IETF
- ccTLDs, gTLDs, Registrars



多方利害關係人依其原則、規範、政策程序推動網際網路之發展與使用

有限介入模式
Limited intervention

- 英國調查權力法 (investigatory Powers Act)
- 美國 41條規則 (rule 41)
- 澳洲反加密法 (anti-encryption law)



網際主權模式
Cyber sovereignty

- 中國防火長城
- 俄羅斯網路獨立法
- 高密度網路審查國家



政府訂定網際空間範疇，實施控制措施以主張其網際空間管轄權

16

Cyber Jurisdiction Case: China Intranet



中國 Internet 非常類似企業 Intranet, 並且具下列優點

1. 中國可以強制網路審查權
2. 一旦面臨外部威脅，中國隨時可以切斷國際網路，並維持Internet局部接取功能
3. 國內訊務永遠不會離開國境

中國網路治理可跨越管轄權

- 一帶一路跨境基礎設施
- 中國電信、移動全球市場
- 華為、抖音、騰訊平台

17

Cyber Norms

18

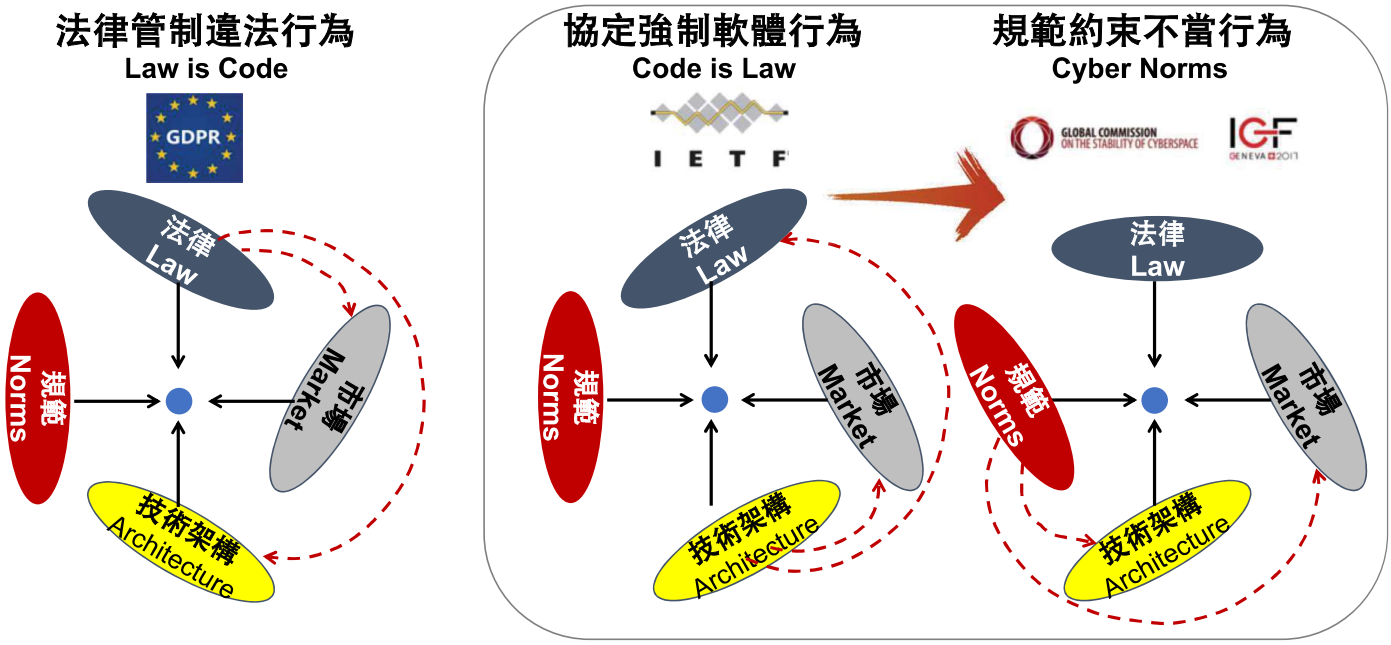
公共政策治理模式

	政策治理能力與能量		
私部門	✗	✓	✓
政府機構	✓	✓	✗
治理模式	政府法規 State regulation (Neoliberalism)	合作 (Knill, 2002) 共同規範 (Tanja Borzel, 2007) 代理規範 (Tanja, Borzel, 2007)	自律規範 Private self regulation (Knill, 2002)

19

New Chicago School Theory

How to regulate cyberspace



* Norm: shared expectations of appropriate behavior

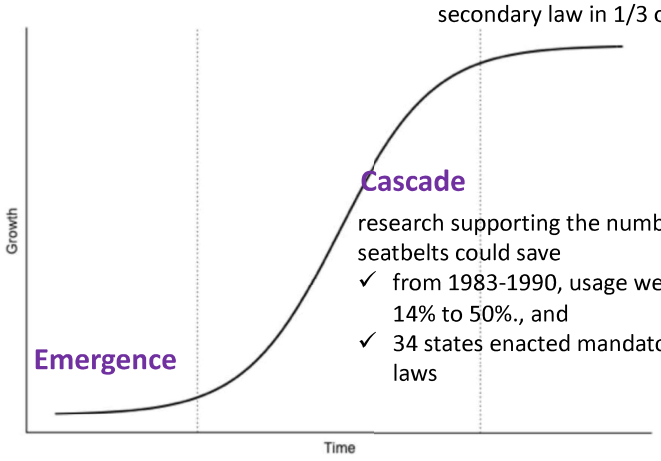
20

Case: US car seat belt



1968 – National Highway Safety Bureau requires seat belt fastening

Battles over regulation and civil liberties infringements



Entrenchment

In US, 87% of adults wear seatbelts all the time, despite it being a secondary law in 1/3 of states.

Cascade

research supporting the number of lives seatbelts could save

- ✓ from 1983-1990, usage went from 14% to 50%., and
- ✓ 34 states enacted mandatory usage laws

21

網路政策參考框架

characteristics	ICANN	ITU	IGF	APNIC	TWNIC	IETF	NATO
multistakeholder	x		x	x	x		
bottom-up model of governance	x		x	x	x	x	
standard setting	x	x		x	x	x	
operates based on contractual compliance	x			x	x		
governmental		x					x
sets internationally enforceable obligations for states		x					x

22

Intermediary Responsibility

Power of Enforceability 強制力
Well-positioned to impose internet policy or regulatory functions

Internet Intermediaries 網路中介者

電信管理法

網路中立、
普及原則



電信業者　註冊管理機構　平台業者　搜尋引擎

Communication Decency Act
CDA Sec. 230

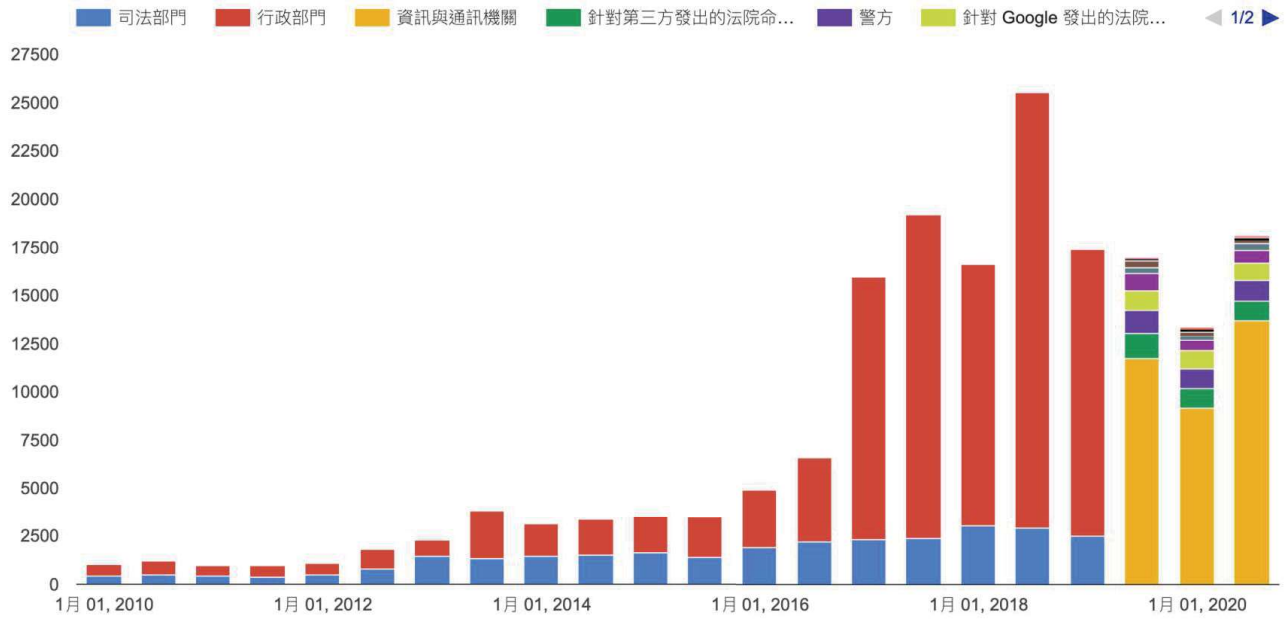
第三方內容免責、
用戶規約

多方利害關係人模式
Fiduciary duty 信託責任

Manila principles

1. 中介者豁免對第三方內容承擔責任
2. 沒有司法機關命令，不得提出內容限制請求
3. 內容限制之請求必須清晰明確，符合正當程序
4. 內容限制命令必須符合比例原則檢驗
5. 內容限制政策必須遵循正當程序
6. 內容限制政策必須具備透明度與問責機制

Google content removal requests by the numbers

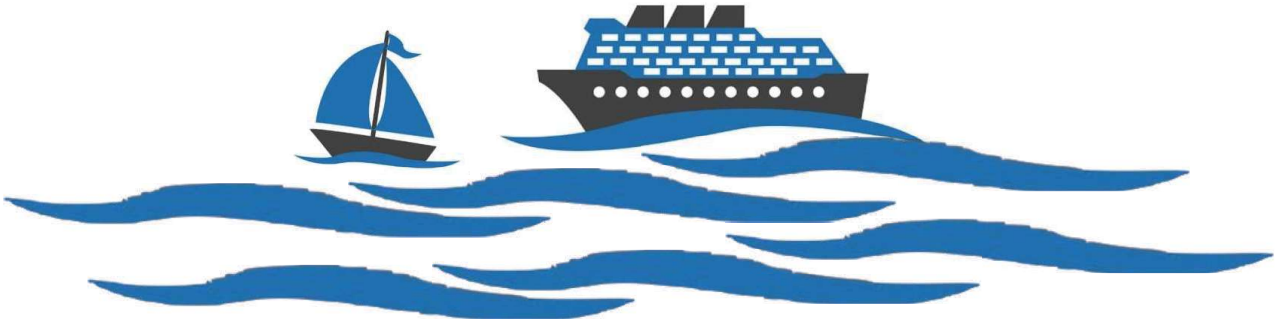


Source: Google Transparency Report

系統性風險 vs. 非系統性風險

非系統性風險

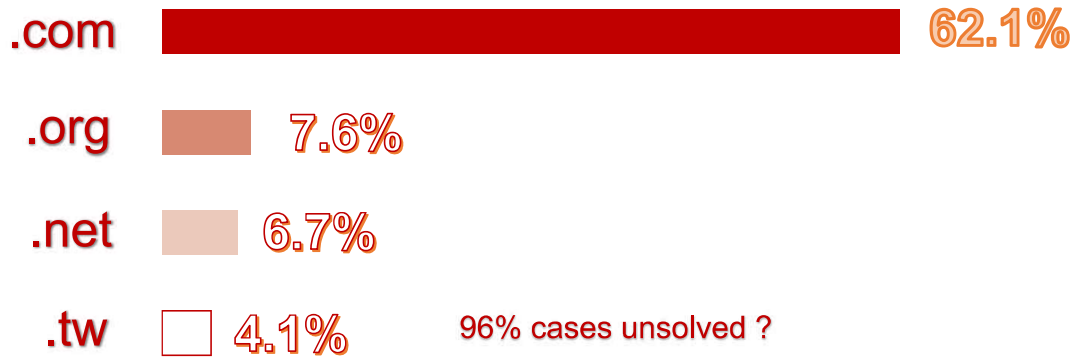
組織管理 資本支出、營運支出、管理制度、系統漏洞、技術與人才



系統性風險

網路治理 網路協定、全球網路結構障礙 、網路治理、網路規範、國際公約、 國內法規

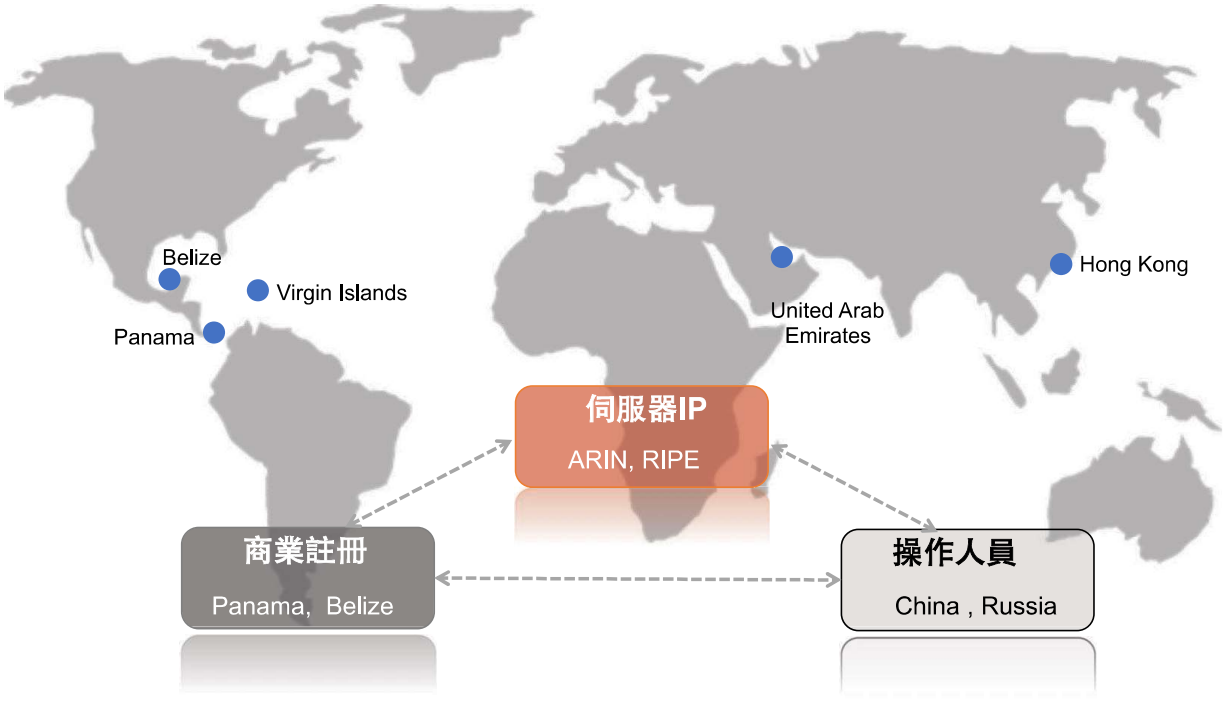
網路犯罪頂級域名統計



資料來源: CIB, 2020 Jan-Aug

27

網路犯罪： 多層斷鏈



28

Dilemma of criminal procedure

公訴要件 §刑事訴訟法264

1.  犯罪行為人個資 — Not Available
2. 

犯罪事實證據

29

網路管轄權 Internet jurisdiction

Borderless Internet



網際網路具跨境特性



National laws confined to territorial limits

法律與管轄權具地理限制



30

現有解決方案

司法互助
MLAT

- 緩慢且複雜



布達佩斯協定
Budapest Convention

- 緩慢且複雜
- 擴充性不足



法律合作
Legal Cooperation

- 透明度不足
- 證據可採納性
- 法律衝突Conflicts of laws



31

情境：社群平台發布仇恨言論; deepfake 影像/圖片; 一頁式詐騙廣告

	Effective	Quick	Simple	Precise	Proportional	Cost-Effective
電信業者	✓	✗	✗	?	✗	✗
內容遞送網路	?	?	?	?	✗	✗
主機代管	✓	✗	✗	✗	✗	✗
平台	✓	✓	✓	✓	✓	✓
受理註冊商	✓	✓	✓	✗	✗	✗
註冊管理機構	✓	✓	✓	✗	✗	✗

32

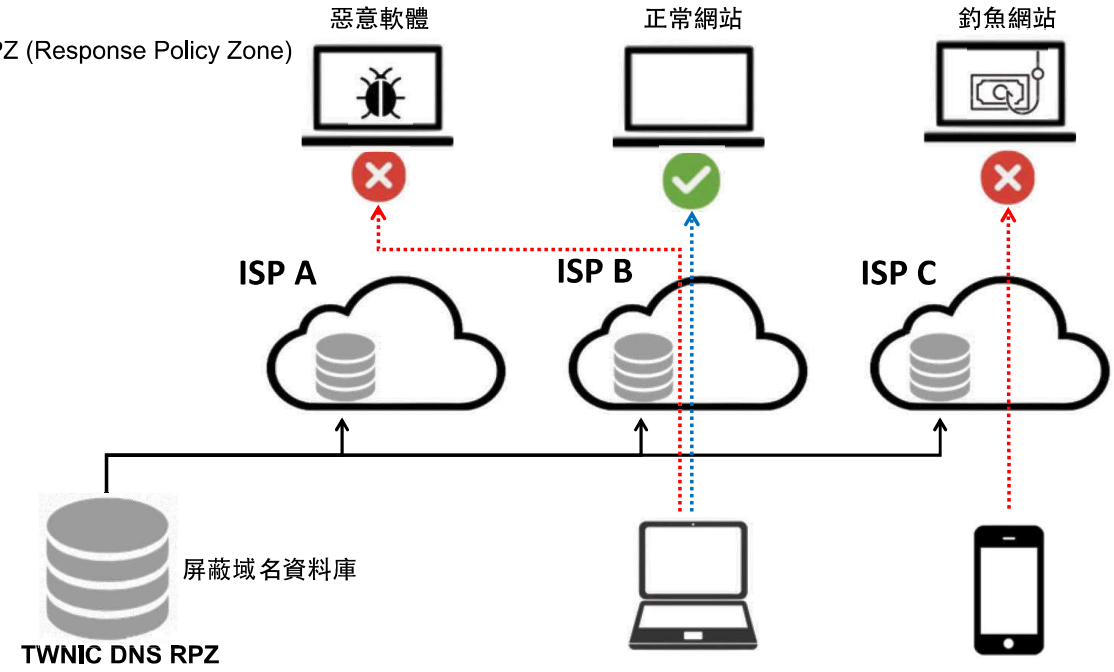
情境：殭屍電腦命令控制伺服器 C2 Server; 侵權網站

	Effective	Quick	Simple	Precise	Proportional	Cost-Effective
電信業者	✗	✗	✗	?	✓	✗
內容遞送網路	✗	?	?	?	✓	?
主機代管	✗	?	✓	✓	✓	✓
平台	?	?	?	?	?	?
受理註冊商	✓	✓	✓	✓	✓	✗
註冊管理機構	✓	✓	✓	✓	✓	✓

33

TWNIC RPZ 技術架構

回應政策域 RPZ (Response Policy Zone)



34

網域名稱加入RPZ屏蔽名單情況

	情況(一)	情況(二)
情況	網域名稱係法院判決/裁定或行政機關命令停止解析者	網域名稱係有資安疑慮且影響資安重大者
移除性質	依據法律 + 因應法律規定採取行動	法律認定關鍵基礎設施或電信事業有維護資安義務 資通安全管理法第10條、第16條第2項、實施細則第6條第1項、通傳會所管特定非公務機關資通安全管理作業辦法第2條第1項、電信管理法第15條、電信事業資通安全管理辦法第2條 + 因應法律規定採取行動

域名濫用框架 DNS Abuse Framework

Technical Regime
.TW DNS query : 1.2T queries =>0.6T abuse queries
TWCERT : 920K cases / year

Law Regime
Disinformation cases
通報>10000, 提報 2953, 偵辦 589, 移送地檢 93

Gap assessment

From intermediary liability to **intermediary responsibility**

域名濫用治理框架

技術
1 malware
2 botnet
3 phishing
4 pharming
5 spam

規範
1 MANII 中介者爭議處理規範
2 iWin 兒少安全防護規範
3 **Emergent abuse**
(1) public order
(2) personal injury
(3) monetary damages
(4) child abuse *
(5) illegal trade
(6) threat of illegal activity

法律
1 法院裁判
2 扣押命令
3 行政處分

網路管轄權

現行解決方案
1. 司法互助 MLAT
2. 布達佩斯協定Budapest Convention
(1) 緩慢
(2) 無擴充性
3. 法律合作 Legal cooperation
(1) 透明度不足
(2) 證據可採納性
(3) 法律衝突 conflicts of laws

域外效力
1 兒少法46
2 動防條例 38-3

違法境外網站採限制接取取代司法互助網域移除

依據英國 CDPA 法，提起侵權訴訟的成本很高，除了難以要求境外註冊管理機構或受理註冊商強制執行網站下架外，違法網站容易複製更新網域名稱。**近年來，透過國內電信業者直接封鎖可以更快速達成犯罪防制效果。**

nsw2u.xyz、nsw2u.org、nsw2u.com、nsw2u.net、nswrom.com
六家網站提供盜版任天堂Switch ROM 下載

任天堂向英國法院提出訴訟限制電信業者接取境外侵權網站，**法院裁定(injunction)英國六大電信業者兩年間限制接取Switch非法下載境外網站。**

Dec 2021

37

Sanctions

38

Sanctions

- Definition
  - Political trade tools put in place against targeted countries with the aim of restoring international peace and security.
  - Change the behavior of the target country's regimes individuals or groups in a direction which will improve the situation of that country. Such as an arms embargo and a ban on the export on certain items could be aimed at supporting a peace process.
- Types of sanction
  - Country based sanction : embargos to the actual countries
  - List-based sanction: individuals such as terrorists, traffickers, corrupt leaders
  - Target-based sanction: individuals or organizations
- The most frequently applied sanctions
  - Sanctions on exporting arms and associated technical assistance, training, financing
  - A ban on exporting equipment that might be used for internal repression
  - Financial sanctions on individuals, government bodies and associated companies.
  - Travel ban on named individuals

39

Sanction regimes

- Financial sanctions
  - Prohibiting the transfer of funds to a sanctioned country
  - Freezing the assets of a government, companies, or residents
  - Prohibiting providing other financial services, such as insurance
- Sanction regimes
  - EU: uphold international security order; defending human rights and democracy
  - UN SC: threats to peace; security and stability; violations of human rights
  - US OFAC (Office of Foreign Assets Control)



46% Global GDP

40

Non-compliance to Sanctions

- It is a criminal offence to breach a sanction without authorization from the appropriate sanction regime
- Non-compliance to sanctions will be a serious threat to national security and foreign relations
- Breaching sanctions can face severe legal repercussions
  - Fines range up to millions of dollars
  - Prison sentences for the liable parties involved if the breach is considered to be taken place willfully.



41

Do sanctions work ?

- Sanctions are playing a growing role in modern geopolitics
- Short term sanctions have an effective outcomes
  - Evidence shows that the longer sanctions last the less likely they are to succeed

42

Sanctions and IG

ICANN and RIPE NCC

- 烏克蘭GAC代表請求 ICANN 實施俄羅斯的制裁. 關閉俄羅斯頂級網域名稱.ru, .рф, .su解析
- 關閉俄羅斯根伺服器



- 烏克蘭要求 RIPE NCC 取消核發給俄羅斯的所有IPv4與IPv6位址。



But





- ICANN移除 .su，說明因.su 已不在ISO3166-1, 不再符合 ccTLD 資格
- 依據註冊商授權合約第3.7.5.1條，烏克蘭無力付款續約可免除取消域名
- 三十多位ICANN現任前任董事及網路主導者共同發表網路治理制裁原則
- 歐洲代管.UA 烏克蘭頂級網域
- CENTR歐洲國家頂級網域管理局拒絕俄羅斯會員資格
- Godaddy 停止銷售.ru網域
- CA 不接受俄羅斯憑證更新

- 凍結俄羅斯最終受益人UBO之IP位址, 包含俄羅斯主導電信公司
- LINX 交換中心斷網
- GÉANT研究網路斷網
- COGENT國際轉訊斷網

45

網路治理制裁原則 Multistakeholder Imposition of Internet Sanctions

- 切斷國家與Internet連結的網路制裁不符合比例原則並且不適當
- 網路制裁有效性應該被評估
- 網路制裁必須精確，將無法預期結果可能性最小化
- 可將軍事與宣傳機構基礎設施視為網路制裁目標
- Internet 基於跨國特性及多方利害關係人治理架構，不適合執行網路制裁
- 政府嘗試操作網路治理機制實施網路制裁是不適當
- 部分適當有效且具體措施，網路治理社群於網路制裁審議過程可列入考量。
- 包含建立有效網域名稱與IP位址制裁清單，制裁清單可以列入限制接取之制裁方案，比照網路管理者阻擋垃圾郵件或惡意軟體方式執行。
- 建立多方利害關係人審議程序，制裁俄羅斯軍事及宣傳機構IP位址與網域名稱，並為未來面臨嚴重性急迫性決定奠定基礎。

46

外國資產控制辦公室網路制裁令



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

OFFICE OF FOREIGN ASSETS CONTROL

Russian Harmful Foreign Activities Sanctions Regulations
31 CFR part 587

GENERAL LICENSE NO. 25

Authorizing Transactions Related to Telecommunications and Certain Internet-Based Communications

(a) Except as provided in paragraph (c) of this general license, all transactions ordinarily incident and necessary to the receipt or transmission of telecommunications involving the Russian Federation that are prohibited by the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587 (RuHSR), are authorized.

(b) Except as provided in paragraph (c) of this general license, the exportation or reexportation, sale, or supply, directly or indirectly, from the United States or by U.S. persons, wherever located, to the Russian Federation of services, software, hardware, or technology incident to the exchange of communications over the internet, such as instant messaging, videoconferencing, chat and email, social networking, sharing of photos, movies, and documents, web browsing, blogging, web hosting, and domain name registration services, that is prohibited by the RuHSR, is authorized.

- 依據俄羅斯有害外國活動制裁法(RuHSR)，除通用許可規定外，禁止所有涉及俄羅斯發送或接收之電信服務。
- 除通用許可規定外，禁止美國或美國人直接或間接向俄羅斯出口、銷售、提供服務、提供軟體、硬體、及禁止提供網際網路交換涉及技術，例如即時軟體、視訊會議、聊天對話、電子郵件、社群網路、照片分享、電影、文件、網頁瀏覽、部落格、網站代管、網域名稱註冊服務等。
- 人道需求之通訊豁免制裁

47

Internet Governance Regime and Sanctions

Internet Resources	Activity	Sanctioned ? US,EU,G7
IP addresses	new registration	yes
	in use	no
	transfer	yes
Domains	new registration	yes
	in use	no
	transfer	yes

48

Internet Governance Regime and Sanctions

Internet Resources	Sub element	Sanctioned ? US,EU,G7
IP addresses	RPKI RoA	?
	RPKI validation	?
	BGP	?
	Connectivity	yes
	Peering	yes
	Transit	yes
Domains	DNSSEC	?
	Email	?
	Resource records	?
	DNS	?
	Resolvers	?
	DANE	?
	Hosting	yes

49



谁有权没收你的互联网IP地址?

本报特约记者 谭亚凌

编者的话："谁偷走了非洲的互联网IP地址资源？人们把手指指向中国"，美联社等西方媒体近日的一篇报道，用充满偏见的语言描述了非洲发生的一起互联网IP地址纷争，并不顾"没有任何中国官方机构涉及该纠纷"的事实，给中国扣上一顶"数字殖民主义"的帽子。外媒报道不值一驳，但抛开国际政治因素，从科技角度来看，它也是一件不容忽视的大事，也是将于6日至10日举行的联合国互联网治理论坛（IGF）关注的焦点之一，因为它提出了一个越来越避不开的话题：谁有权没收你的互联网IP地址？

THIS WEBSITE HAS BEEN SEIZED

تم الاستيلاء على هذا الموقع

The domain presstv.com has been seized by the United States Government in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, and 50 U.S.C. 1701-1705 as part of a law enforcement action by the Bureau of Industry and Security, Office of Export Enforcement and Federal Bureau of Investigation.

"没收IP地址或域名"是怎样做到的

域名、IP地址及其服务系统等是互联网最重要的基础资源，为互联网提供关键的核心服务。

据介绍，IP地址是用来唯一标识互联网上计算机的逻辑地址，让计算机之间可以相互识别并通信，每台联网计算机都依靠IP地址来互相区分，相互联系。目前互联网上主流的是IPv4地址，也就是由三个小数点分隔开的四段数字。

由于IP地址是数字标识，使用时难以记忆和书写，因此在IP地址的基础上又发展出一种符号化的地址方案，来代替数字型的IP地址。每一个符号化的地址都与特定的IP地址对应，这样网络上的资源访问起来就容易多了。这个与网络上的数字型IP地址相对应的字符型地址，就被称为域名。比如被美国没收的伊朗新闻网站域名就是presstv.com。

虽然大家都知道美国控制着互联网域名管理和IP地址的分配，但它"没收"其他国家的域名在技术上是怎么样实现的呢？

据中科院计算机网络信息中心研究员王伟博士介绍，网站都是通过域名访问，域名对应该网站的公网IP地址，域名到IP地址的映射关系是通过DNS解析来实现的。这次被美国关停的伊朗相关新闻网站涉及到4个域名后缀：.com、.net、.tv和.org，它们分别被两家美国公司Verisign和PIR所管理。

以presstv.com为例，6月22日之后，管理.com的美国公司Verisign的第一个操作是，把域名解析的地址改变了。这相当于把指路的路标拧了一下，本来是往东指的，现在却指到西边去了，这样即使输入正常的域名，却也解析不到原本的IP地址208.93.18.215，而是被指向受美国控制的一台服务器，而网站封禁的图片就挂在该服务器上。

第二个操作，Verisign把相关的域名所对应的IP地址改掉了，这几个IP地址，已经到了美国亚马逊机房的IP地址了。

中科院计算机网络信息中心得到的结论是，从技术层面，美国司法部一纸命令，这两个注册管理机构——Verisign和PIR没有征得用户的同意，就单边地把这两个数据NS一改（NS是DNS数据库的一条资源记录，用于记录域名和IP地址的对应关系，服务于DNS解析），IP地址一改，伊朗的那些网站就从互联网世界消失了。

中国用户的域名或IP地址有被没收的风险吗？答案是有，对于域名来讲，如果注册的是.com或.net等国际通用域名，就会有风险。如果使用我国管理的.cn域名，其他国家就不好没收了，除非直接"没收".cn顶级域，但这样一来，影响太大，迄今也未有过先例。对于没收IP地址来看，上述"IP地址被没收"事件可说是目前唯一仅见的案例，一个异常危险的先例。

不过，大国从来不把命运假手他人，有些国家已经未雨绸缪。俄罗斯近几年就在全力打造"主权互联网"，实现互联网和本国数据的自主可控，减少对境外网络服务的过分依赖。▲

"美国没收伊朗网站域名"和"非洲互联网络信息中心IP地址纠纷"是今年互联网治理领域的两件大事，它们充分暴露了互联网基础资源的重要性和治理机制的不完善。

"互联网基础资源有一个最根本的问题一直没有解决，就是IP地址、域名是不是一种数字资产，如果不是，那么它是什么，如果是的话，所有权是谁的？"中科院互联网信息中心研究员王伟博士表示，以前人们说，IP地址所有权是全体网民的，所以大家只有使用权，因此不会说卖IP地址给你，是说你是会员，给你IP地址让你用。可是，由于权属不明确，一旦上层的IP地址分配机构由于某些政策原因或者法律原因要收回的话，利益怎么判断？你有没有权利抗争？在互联网发展早期，基础资源充沛的时候，大家意识不到这个问题的存在，但现在互联网基础资源开始稀缺了，一个IP地址从几块钱变成几十美元的时候，有意或无意的地址资源争夺开始对既有的互联网治理模式构成挑战。

世界互联网治理面临挑战

据介绍，当年科学家们设计的IPv4地址容量为2的32次方，大约37亿多个可分配IP地址，当时认为已经绰绰有余了。结果只过了20年的时间，IPv4地址已不敷分配。网络要扩张，数字经济要发展，而互联网基础资源则成为稀缺资源，利益的争夺随之开始，原有的治理模式的问题开始暴露。

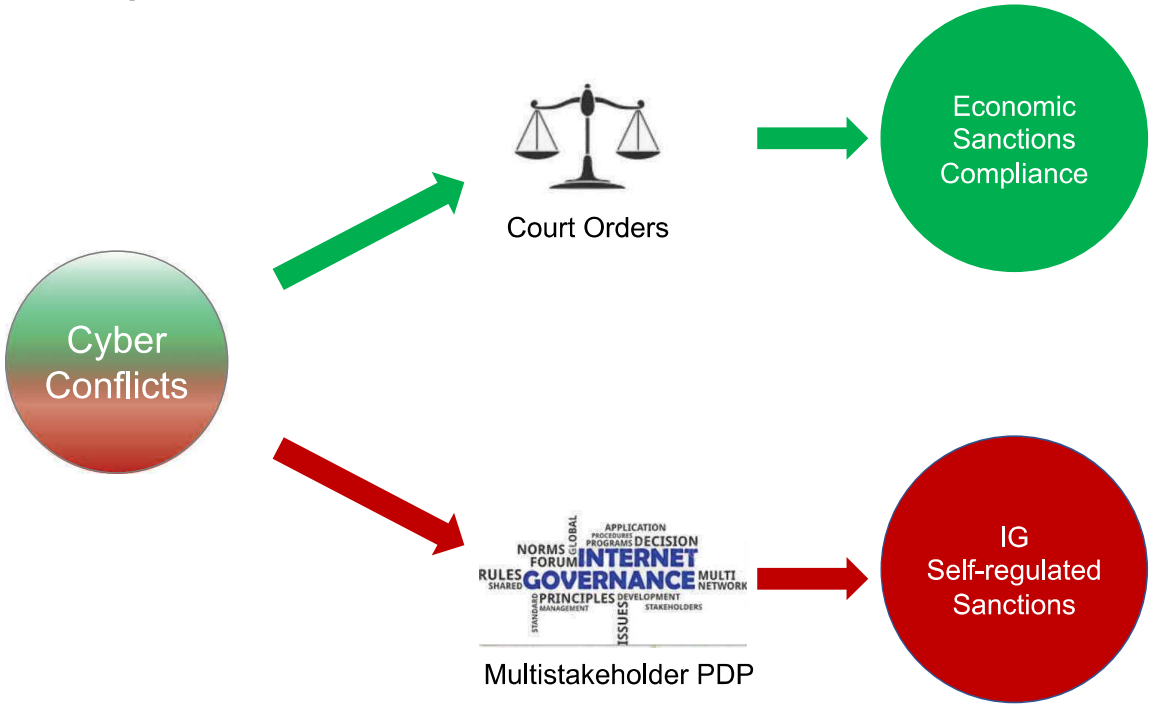
中国社会科学院世界经济与政治研究所研究员郎平认为，从治理角度和应用角度来看，互联网基础资源治理与国家利益之间是存在张力的：一方面，互联网基础资源是有限的，而国家之间就全球资源的分配存在竞争关系；另一方面，国际顶级域名是归ICANN负责分配，而从事域名管理的公司和机构是有国别、有国家属性的，域名的使用者也是有国别的，这意味着有关域名的活动，也是有主权属性的。

由此，郎平认为，未来在大国竞争的趋势下，我们的域名和IP地址治理，在全球治理层面应该怎么推进，在新形势下我们需要认真思考，"它是不是能够适应新的形势"。▲

业氢能 点亮世界
鸿达兴业
股票代码：002002
www.002002.cn
制氢-储氢-储能-运氢

50

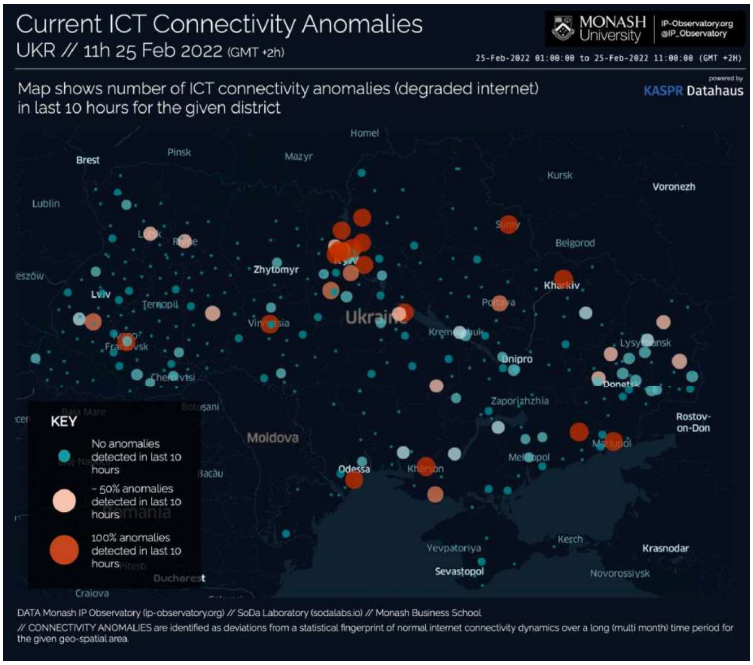
Future cyber conflicts



51

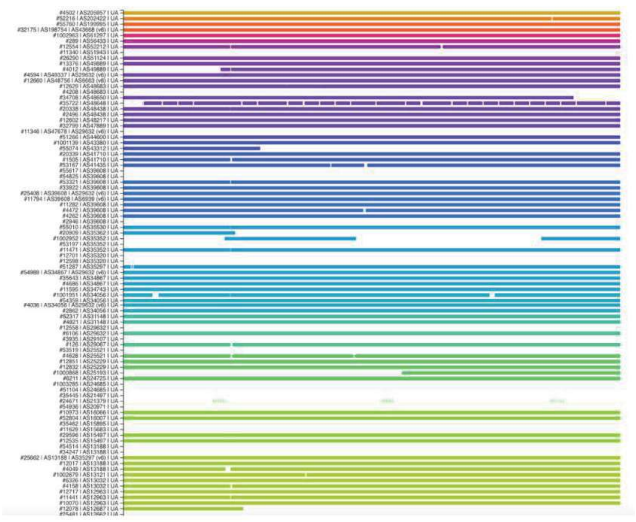
Evolving IG & Digital Policy

52



烏克蘭網路基礎設施在10小時內呈現高度異常現象 (2/25)

武裝衝突造成網路阻斷



戰爭以來RIPE持續量測基輔網路可用性



烏克蘭網路業者在攻擊後搶修網路作業

美國從俄烏戰爭重新檢視 DNS 重要性

美國國會研究報告 2022.03.23



A Revisit of the Domain Name System After Russia's Invasion of Ukraine

March 23, 2022

- 美國政府NTIA在2016年後停止全球DNS控制權，國會此時應該重新評估美國政府與ICANN關係，並維持美國在ICANN的領導地位。
- 美國應重新檢視美國政府在ITU的領導地位，俄羅斯積極倡議將全球網路治理由ICANN移轉到 ITU 由多國治理。2022年9月ITU秘書長即將改選，美國政府應支持美方候選人Bogdan-Martin以對抗俄羅斯支持的候選人，秘書長勝選者四年任期內對ITU在網路治理政策、範疇與方向具有重大影響

55

.UA 烏克蘭頂級國碼國際重新配置



- 烏克蘭國家頂級網域名稱 .UA 註冊管理機構(Hostmaster Ltd)過去域名伺服器在基輔，2022.03起已轉移到國外的伺服器
- 烏克蘭國家頂級網域名稱註冊管理機構已將 com.ua 和 kiev.ua二級網域使用Cloudflare DNS 防火牆保護。為保護.UA其他公共網域名稱

Name Servers 2022 May 06

HOST NAME	IP ADDRESS(ES)	
ho1.ns.ua	195.47.253.1 2001:67c:258:0:0:0:0:1	San Jose; US
pch.ns.ua	204.61.216.12 2001:500:14:6012:ad:0:0:1	Berkeley; US
cd1.ns.ua	194.0.1.9 2001:678:4:0:0:0:0:9	Strasbourg; FR
in1.ns.ua	74.123.224.40 2604:ee00:0:101:0:0:0:40	Santa Clara; US
rcz.ns.ua	193.46.128.10 2a02:850:ffe0:0:0:0:0:10	Wien; AT
bg.ns.ua	185.136.97.185 185.136.96.185 2a06:fb00:1:0:0:0:4:185 2a06:fb00:1:0:0:0:2:185	Slaskie; PL

56



BLEEPINGCOMPUTER.COM

Russia creates its own TLS certificate authority to bypass sanctions

- 對俄羅斯實施制裁國家所在地的憑證權威機構(CA: Certificate Authority)不得接受俄羅斯憑證到期更新付款。憑證過期後網頁瀏覽器會以全頁面顯示網站不安全警語促使多數使用者離開。
- 俄羅斯數位發展部建立自己的憑證權威機構CA來發放憑證
- CA必須獲得所有瀏覽器信任，瀏覽器公司審查作業需要相當久的時間(遑論制裁令)，為此俄羅斯又開發自己Yandex瀏覽器與Atom產品
- 許多人認為，俄羅斯切斷全球網路使用獨立網路Runet 時機已經到了。



THEATLANTIC.COM

The Russian Invasion Touches Outer Space

The long-held idea that earthly conflict can't tarnish ...

- 即便國際衝突不斷，美俄兩國在國際太空站合作的價值一直堅持相同立場：國際太空站是國際合作的堡壘。
- 美國提供太空站所需電力，俄羅斯推進器定期將太空站推升到更高高度。如果俄羅斯停止合作時太空站將面臨極度危險。
- 英國首相表示雖然地緣政治存在衝突，他仍支持與俄羅斯在藝術與科學領域合作。

Starlink 星鏈支援烏克蘭網路





59

星鏈改變未來戰爭型態



- 烏克蘭副總理費多羅夫於戰爭一開始呼籲SpaceX創辦人馬斯克，將烏克蘭連接到星鏈。馬斯克立即宣布免費開通星鏈在烏克蘭的服務，並向烏克蘭發放上千份的星鏈終端。
- 烏克蘭炮兵使用無人機夜視功能觀察俄羅斯位置時，無人機經由星鏈將信號傳輸給炮兵部隊，根據這些資訊炮兵進行火炮矯正，發動更精準的攻擊。
- 星鏈低成本、不易被干擾、可替代全球定位系統GPS, 且精確度更高

60

被高估的網路戰爭



LAWFAREBLOG.COM

Cyber Realism in a Time of War

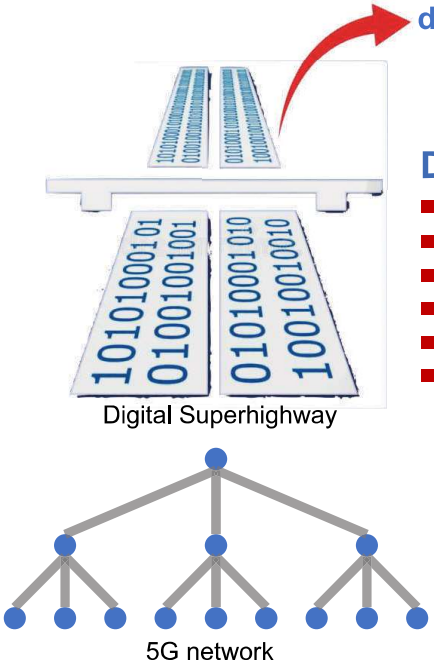
Activity in the digital domain may affect the war in Ea...

- 1993年以來，不乏網路戰爭對未來戰爭重要性的討論。
- 過去十年來俄羅斯來多次對烏克蘭實施網路攻擊行動，但對烏克蘭網路核心基礎設施幾乎沒有影響
- 俄烏衝突中烏克蘭已成為俄羅斯網路遊戲場。隨著能源中斷、銀行終止支付、戰亂對公民的衝擊，網路戰產生的影響已經無關緊要。
- BBC: 俄烏衝突顯示網路攻擊已非主要方案。要摧毀基礎設施，導彈效果比程式碼更加直接。即便要破壞對方資訊系統，網路攻擊效果比不上一顆飛彈。

Taiwan Beyond 5G

Digital attributes

- Digital transformation
- Edge computing
- AIoT
- Streaming
- Metaverse
- Blockchain & crypto
- Cybersecurity



Digital policy directives

- Dual-use technologies
- Evolved Geopolitics
- Space & Ocean digital agenda
- Multistakeholder model
- Governance, policy & regulations
- New digital ministry

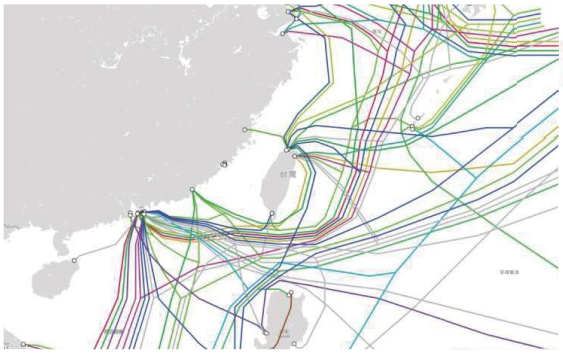
Space and ocean digital agenda

Undersea cable grouping model

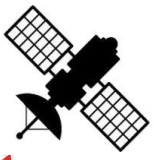
Group 1: North-South Taiwan bypass infra

Group 2 : one leg migration

Group 3: grandfathered operators









Space zoning strategy

Zone 1 : 100-2000KM

Zone 2 : 2000-35000KM

Zone 3: 35000-360,000KM

63

Space Digital Agenda

Applications

- Remote monitoring
- Weather forecast
- Disaster monitoring
- Data communication ?

Policy

- Goals and beneficiaries
- Output, outcome and impact assessment
- Efficiency and effectiveness assessment
- Policy alternatives

Governance

- Colonial logic pattern ?
  - exploration, extraction, discarding?
- Satellite orbit, spectrum assignment
- Maximize stakeholder's value
- Public private partnership

Regulations

- Space law
- Authority : Ministry of Science and Technology
- Spacecraft launch site selection
- Spacecraft registration
- Liability and responsibility of space disaster

64

What if …



TESLARATI.COM | BY SIMON ALVAREZ

Elon Musk sends Starlink terminals to Ukraine after official's request

- 違反電信管理法第36條第5項
- 違反電信管理法第53條
- 違反公眾電信申請及審查辦法第13條
- 違反電信管制射頻器材製造輸入及申請作業管理辦法
- 或戰備各階段公民營通信設施支援軍事管制運用辦法第九條第一項?
  - 衛星資通電路接入核定節點

Wall Street Journal 2022 April 18



THE WALL STREET JOURNAL.

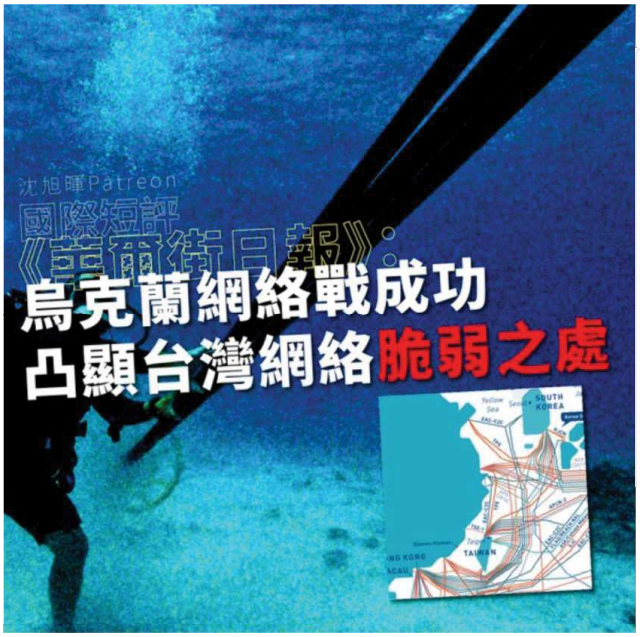
World U.S. Politics Economy Business Tech Markets Opinion Books & Arts Real Estate Life & Work WSJ. Magazine Spo

Ukraine War Stokes Concerns in Taiwan Over Its Fragile Internet Links

Kyiv's successful use of internet to counter Moscow highlights Taiwan's reliance on undersea internet cables that China could cut

Related Video

- 華府智庫CSIS高級顧問Ivan Kanapathy表示，烏克蘭對媒體的高度有效利用，北京當局如果發動攻台，透過切斷台灣與世界的聯繫將大大提高成功的機率
- "We're very vulnerable," said Kenny Huang, chief executive of Taiwan Network Information Center



堅離地城：沈旭暉國際生活台 Simon's Glos World

6h ·

【#Patreon國際短評🇹🇼🇨🇳🇺🇸】假如敵軍派遣潛艇或潛水員，攻擊或物理切斷這些電纜，或者襲擊上述4處登陸站的網絡設施，台灣將會面臨幾乎完全斷網。《華爾街日報》形容這4處登陸站「疏於防衛」（lightly protected），並引述台灣網絡資訊中心CEO黃勝雄的講法，指出台灣在這方面確是「十分脆弱」.....

https://www.patreon.com/posts/65532271

2022 May 05

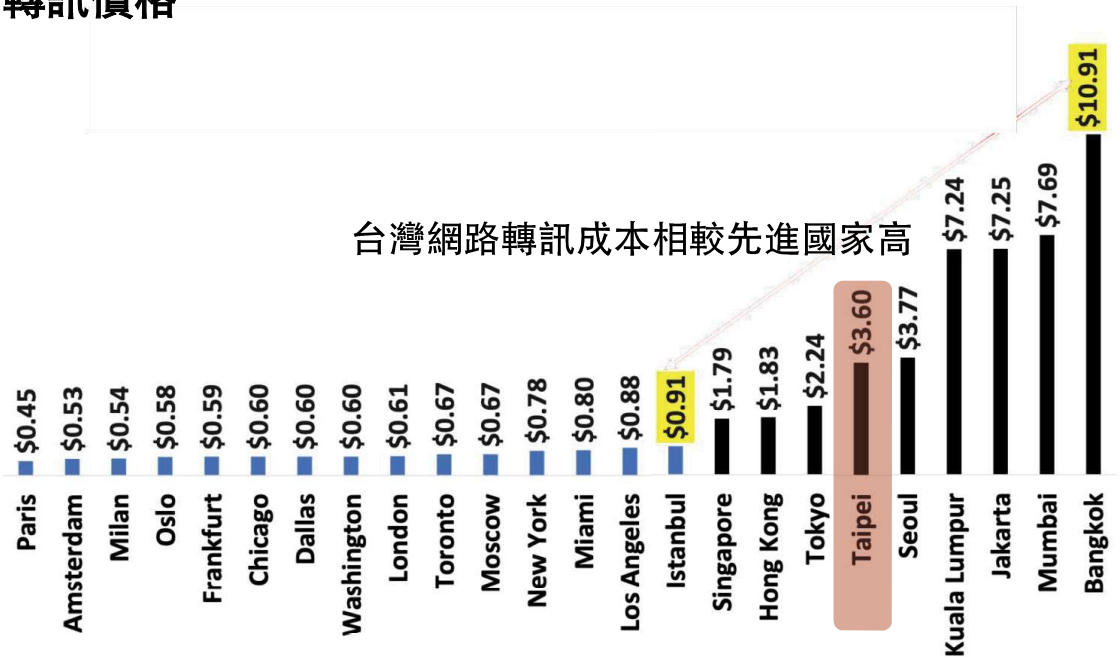
美國海軍研究所《議事錄》



2022 May 01

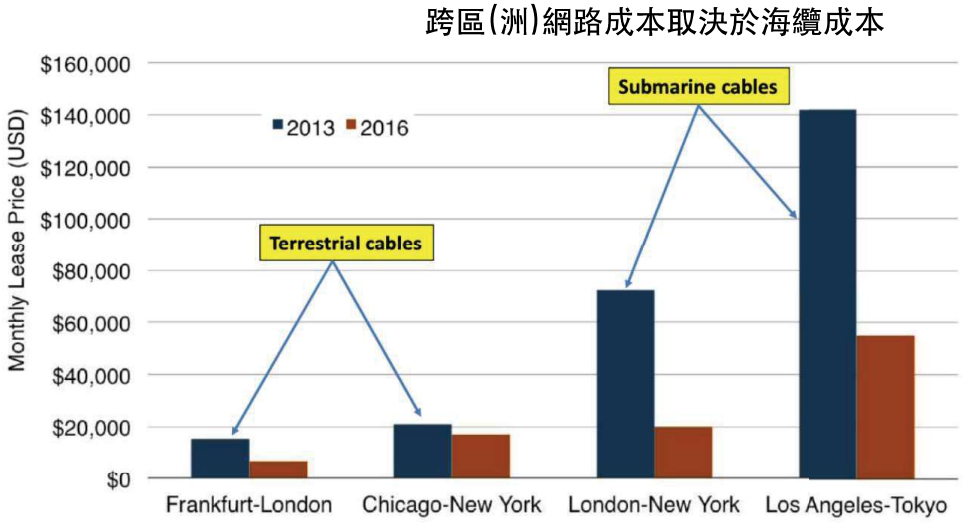
- 若台灣被中國入侵，美國海軍陸戰隊應摧毀台灣的資料中心、以及試圖將資料傳回中國的管道，如此將削弱中國在台灣島上建立中國式的監控能力，也讓美國和盟軍有足夠時間在更廣的戰區擊退中國。
- 海軍研究所進一步建議瞄準台灣的海纜登陸點，特別是海纜登陸點與中國間的連結。如果台灣被入侵，美國軍隊要破壞台灣的網路基礎設施以切斷中國可能運用，為反抗力量的東山再起做準備。

網路轉訊價格



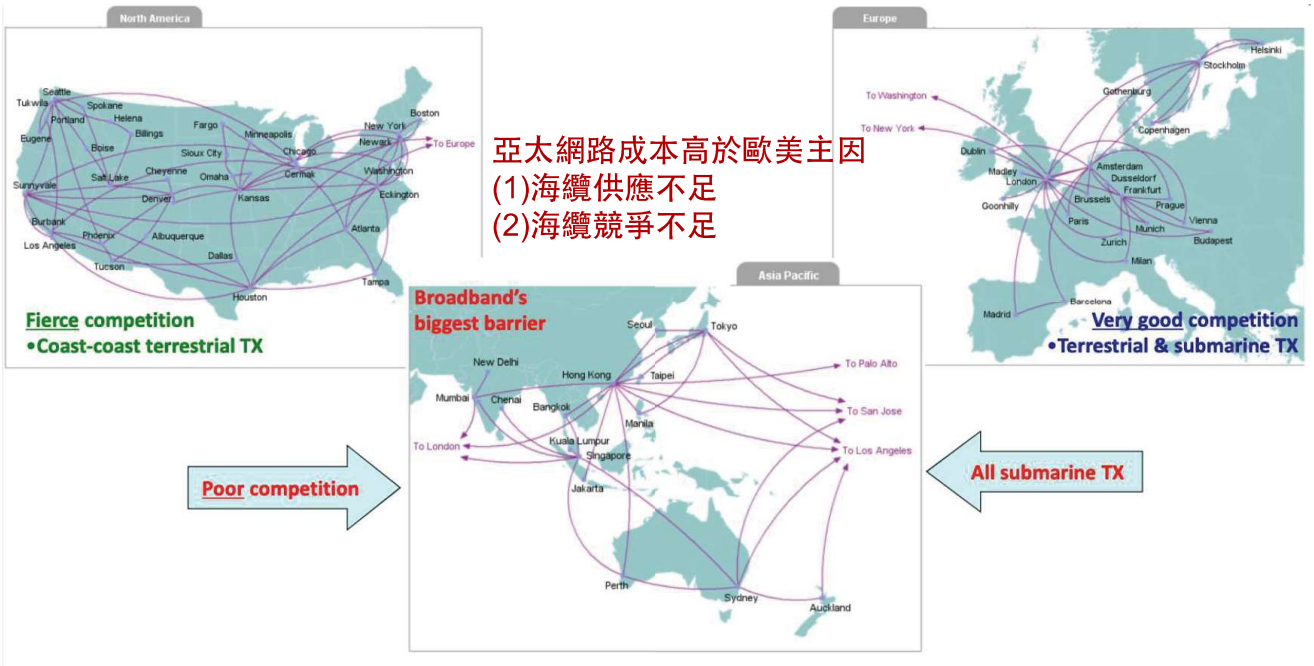
資料來源：TeleGeography 2017

海纜成本決定跨區(洲)網路成本



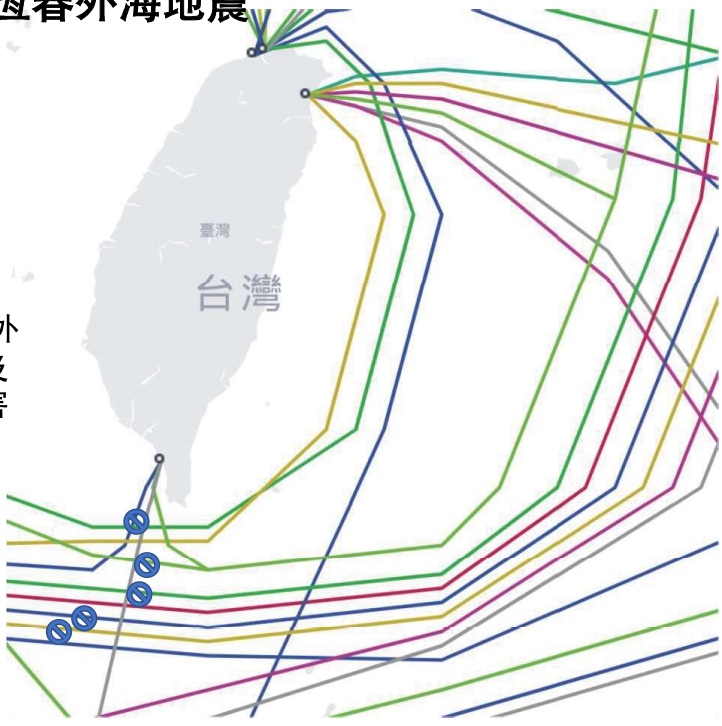
資料來源：TeleGeography 2017

亞太區網路成本高於歐美主因



2006年12月 恆春外海地震

2006年12月恆春外海地震造成亞太及全球網路重大災害

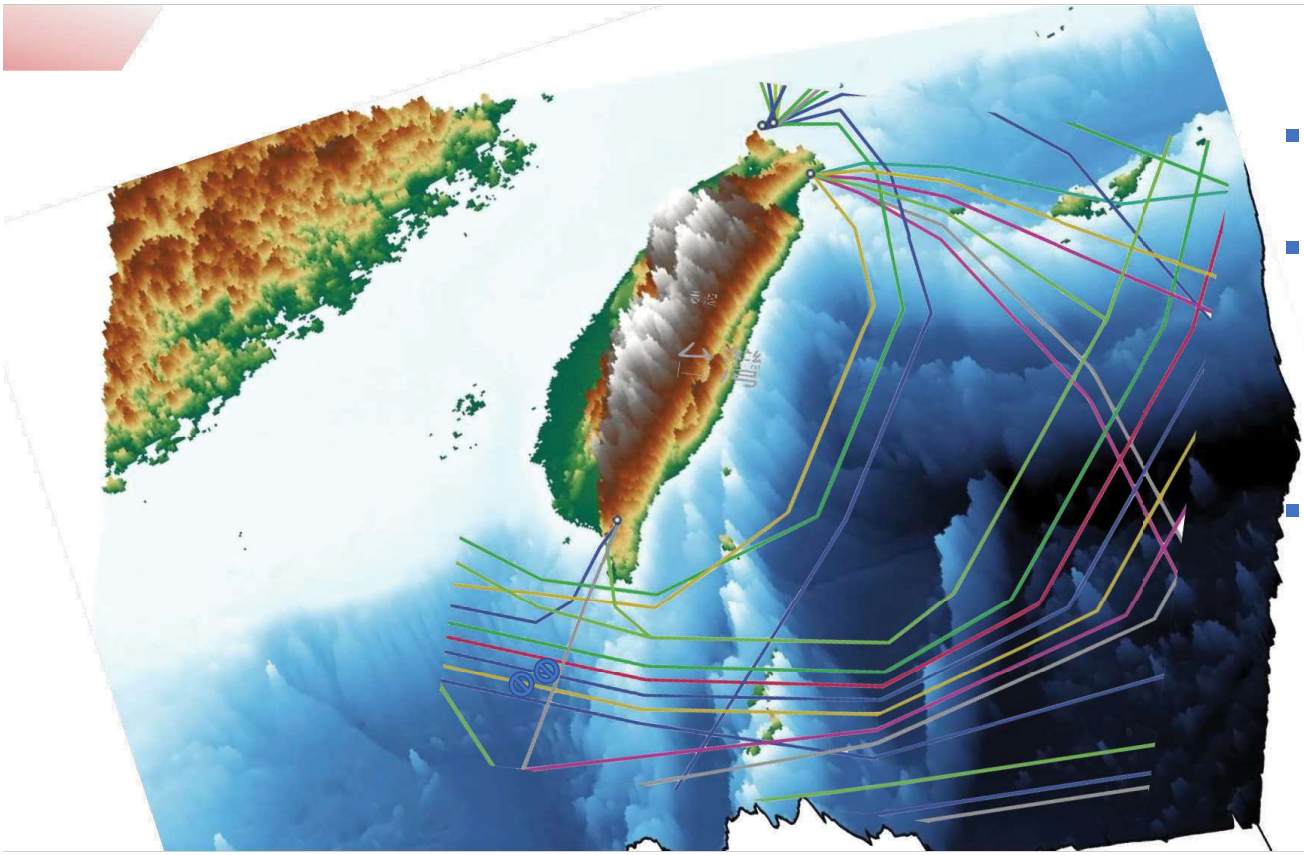


6.7 Richter Scale

2006/12/26	UTC+8
CH-US(W2)	20:27
SMW3(S1.8)	20:27
SMW3(S1.7)	20:41
APCN2(S7)	00:06

5.0 Richter Scale

2006/12/27	UTC+8
APCN2(S3)	02:00
APCN System1	02:16
CH-US(S1)	03:02
APCN System2	04:55



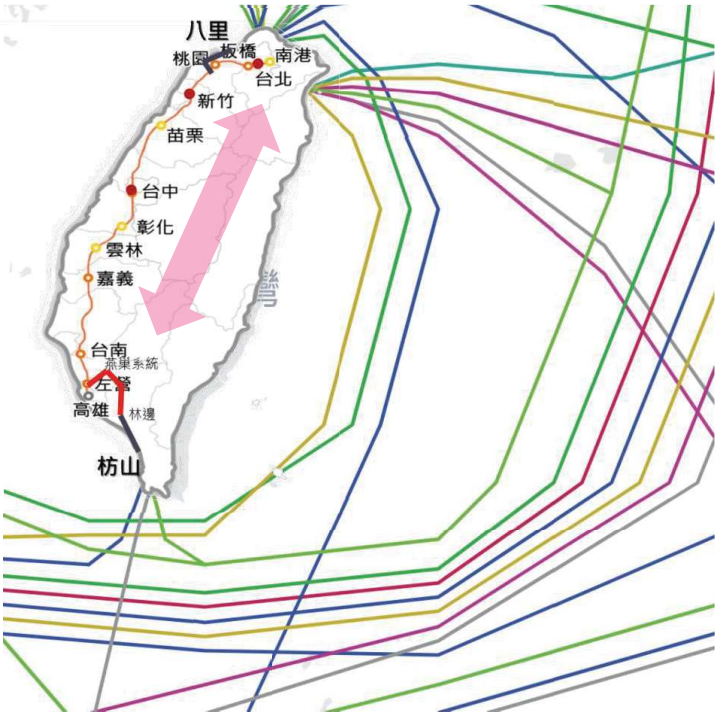
- 台灣為亞太區海纜重要節點
- 台灣海面下山脈多，周邊海域有很多斷層海溝，海纜容易因地震或洋流斷裂。
- 亞太區海纜迫切需要技術可行備援方案

73

台灣光纜通道提升海纜韌性

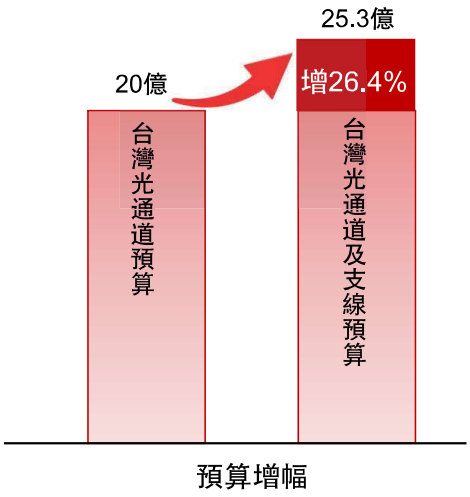
政策效益Policy Impact

1. 國際投資
   Global investment
2. 儲備稀少性戰略資源
   Accumulation of rare strategic resources
3. 鞏固台灣網路空間戰略地位
   Strategic value proposition of cyberspace via geographic advantage

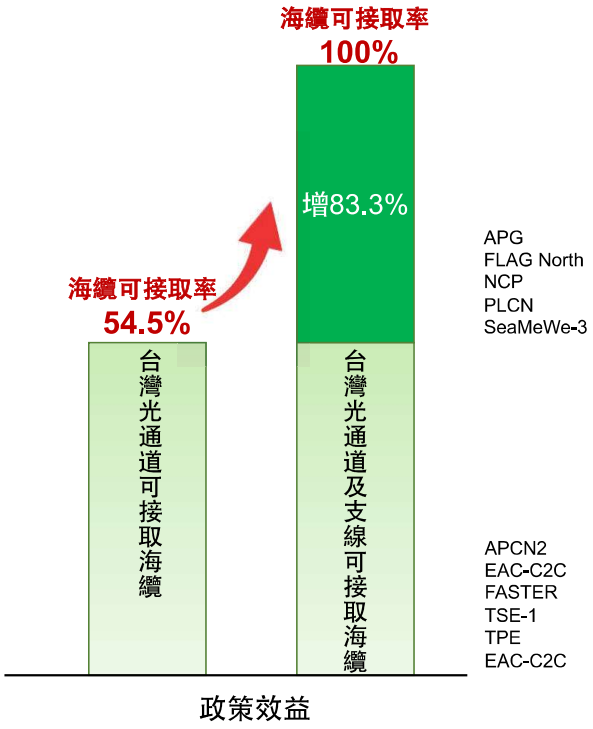


74

政策重要性



預算增幅



政策效益

75

政府介入重要性

先進網路政策模式

規劃模式	目標	介入措施
策略規劃模式	設定願景目標	調整法規框架
凱因斯激勵模式	創造就業機會 提振經濟	政府補貼
政府介入模式	介入競爭不足區域 提供管道鼓勵競爭	政府建置管道 基礎設施

76

政策定位與機會

政府是否介入		公共網路模式是否可持續營運並且獲利：是	公共網路模式是否可持續營運並且獲利：否
	是	與私部門競爭(德國，瑞士，荷蘭)	公共設施降低市場限制鼓勵業者投資 ← 政策方向 公共網路腐蝕公共預算未促進競爭(瑞典)
	否		新業者無法與既有業者競爭(Supplier of Last Resort)

77



78

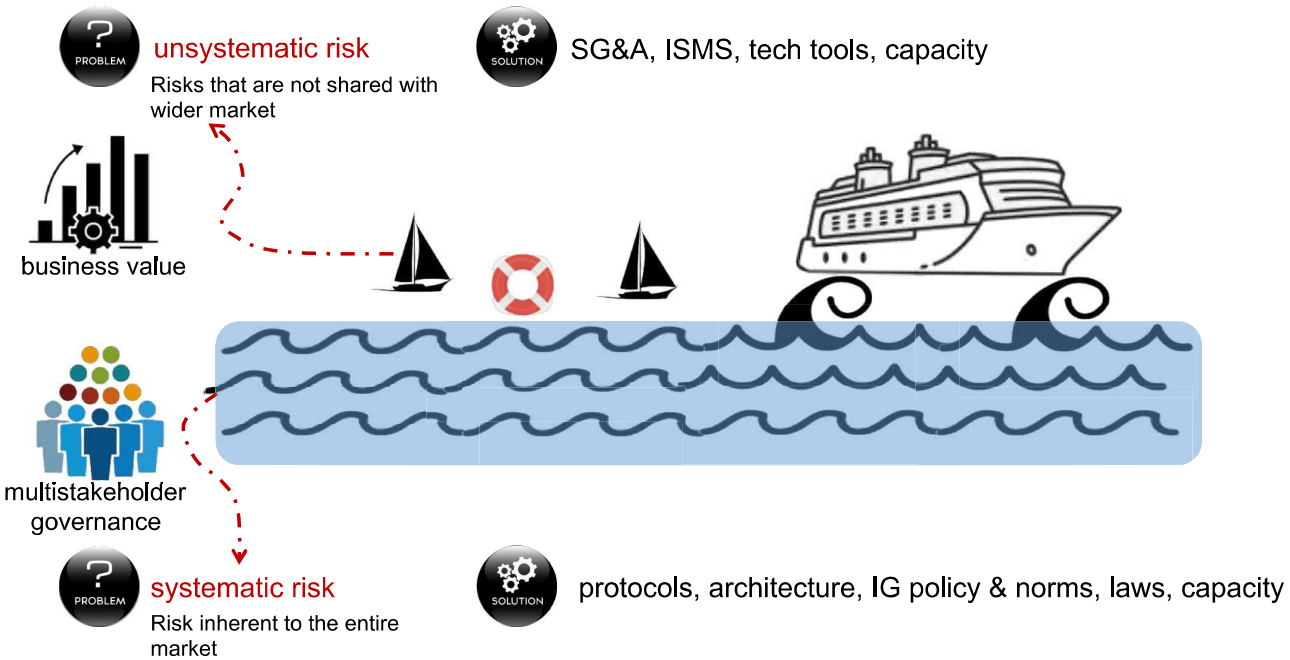
地緣政治衝突時代的網路治理

Dr. Kenny Huang 黃勝雄博士

CEO & Board Director, TWNIC
Executive Council, APNIC
Chair, NII

2022 Sep

design thinking of threat mitigation



2

unsystematic risk examples

unsystematic risk

Risks that are not shared with wider market

SG&A, ISMS, tech tools, capacity

SG&A





ISMS





tech tools





systematic risk examples

systematic risk

Risk inherent to the entire market

protocols, architecture, IG policy & norms, laws, capacity

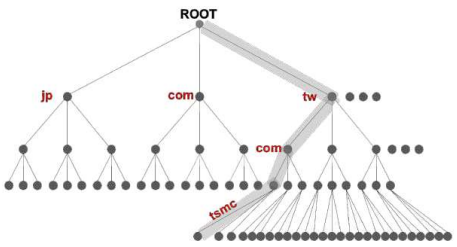
protocol





architecture





policy/ norms

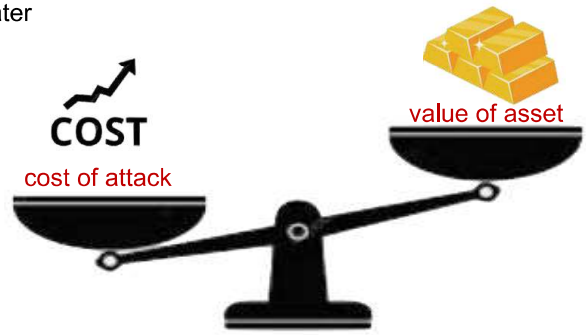




Cybersecurity – misaligned incentives



Goal : making cyber attack uneconomical
when cost of the attack is greater
than the return from an attack.



example: password length

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years

5

Issues in the cyber regime

	Depth	Breath	Compliance
DNS/standards			
Crime			
War			
Espionage			
Privacy			
Content control			
Human rights			

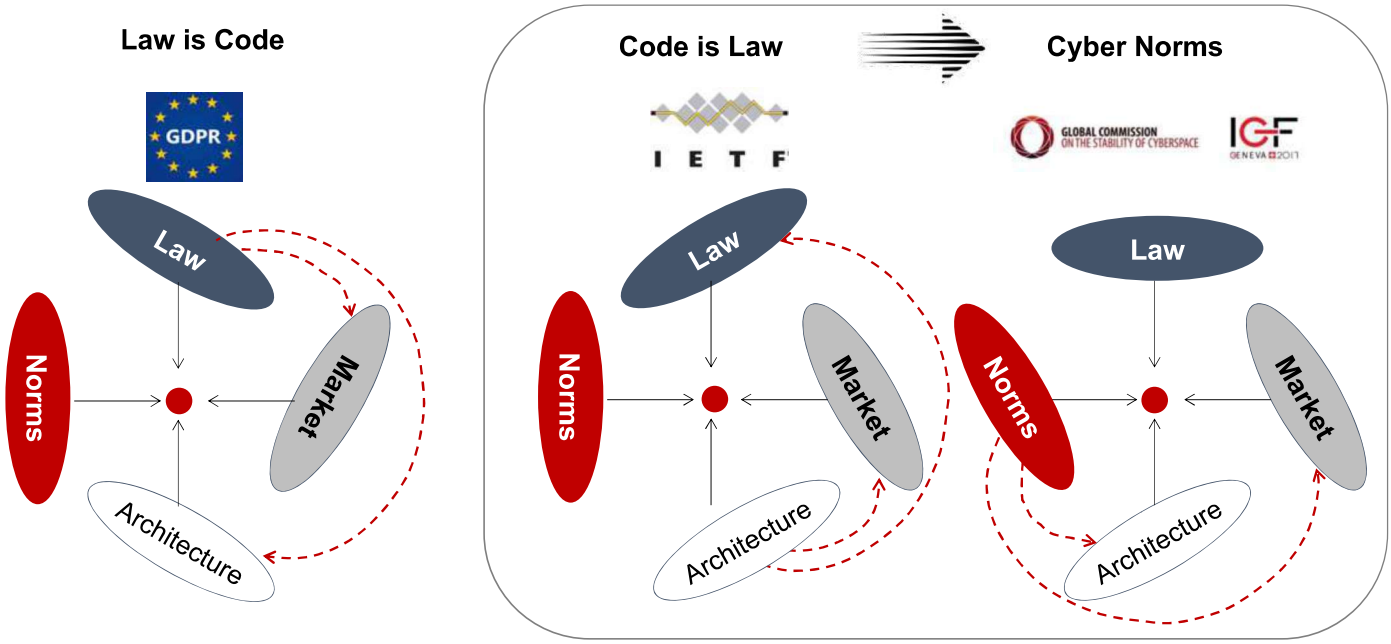
Source: Harvard University

- Depth refers to the hierarchical coherence of a set of rules
- Breadth refers to the scope of the numbers of state and non-state actors that have accepted a set of norms.
- Compliance refers to how widespread is the behavioral adherence to a set of norms

6

How to regulate cyberspace

New Chicago School Theory



* Norm: shared expectations of appropriate behavior

public policy & cyber policy reference model

public policy

	Governance Capacity and Capability		
Private sector	👎	👍	👍
Public sector	👍	👍	👎
Governance Model	State regulation (Neoliberalism)	Cooperation (Knill, 2002) Co-regulation (Tanja Borzel, 2007) Delegation (Tanja, Borzel, 2007)	Self regulation (Knill, 2002)

cyber policy reference model

characteristics	ICANN	ITU	IGF	APNIC	TWNIC	IETF	NATO
multistakeholder	x		x	x	x		
bottom-up model of governance	x		x	x	x	x	
standard setting	x	x		x	x	x	
operates based on contractual compliance	x			x	x		
governmental		x					x
sets internationally enforceable obligations for states		x					x

A Declaration for the Future of the Internet



Internet governance model

Multistakeholder model

- ICANN
- RIRs
- IETF
- ccTLDs, gTLDs, Registrars



Multistakeholder shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

Limited intervention

- UK Investigatory Powers Act
- US Rule 41
- AU Anti-encryption Law



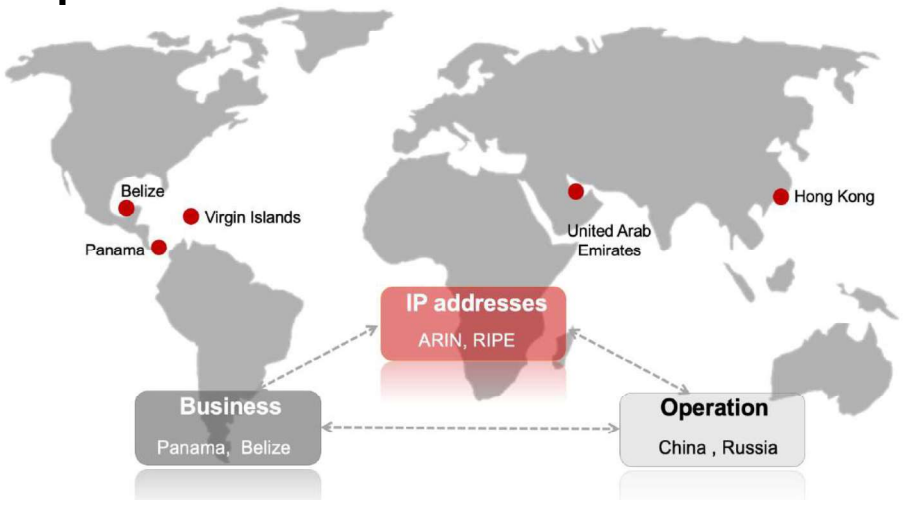
Cyber sovereignty

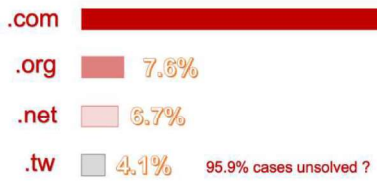
- Great firewall of China
- Russia Internet Isolation Bill



Government determines cyberspace, control mechanism and cyberjuridiction.

cybercrime operations





Cybercrime statistics

source: CIB, 2020 Jan-Aug

Cyber jurisdiction

PROBLEM



Borderless Internet



National laws confined to territorial limits



SOLUTION

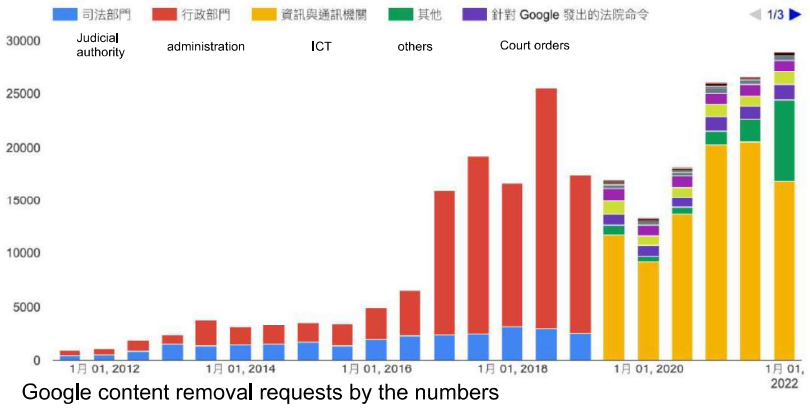
MLAT	Budapest Convention	Legal Cooperation
▪ Slow and complex	▪ Slow and complex ▪ Lack of scalability	▪ Lacks transparency ▪ Admissibility of evidence ▪ Conflicts of laws



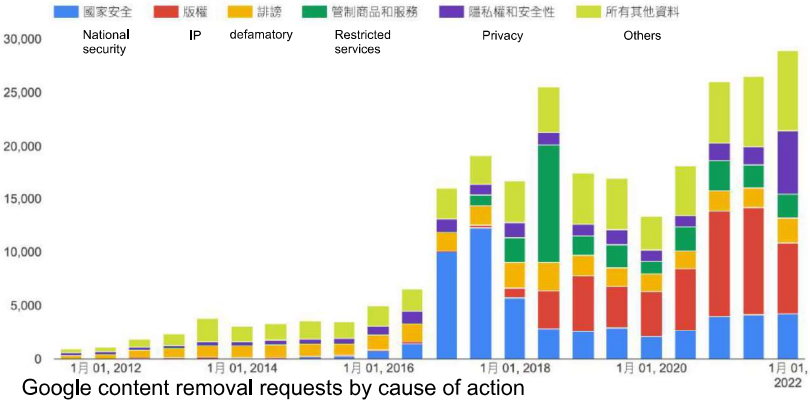






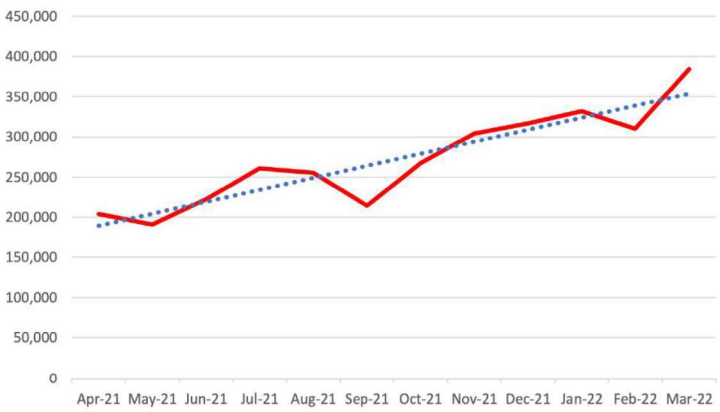


Google content removal requests by the numbers

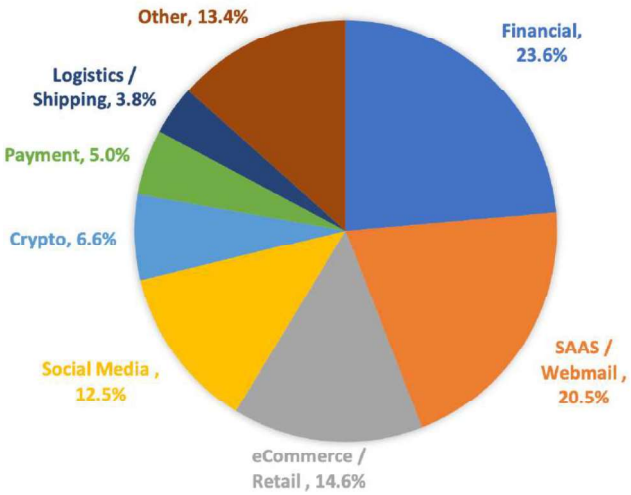


Google content removal requests by cause of action

Phishing BEC targets



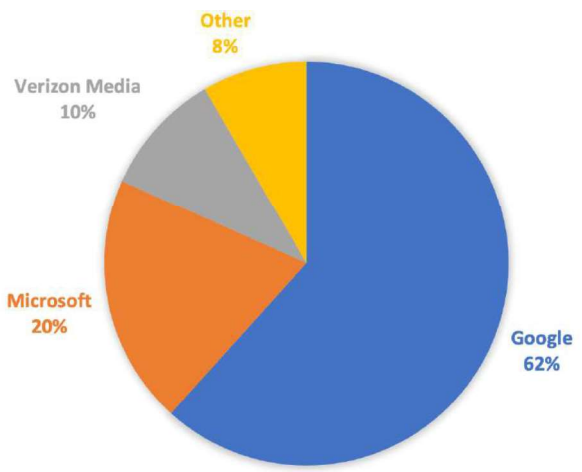
Most targeted industries



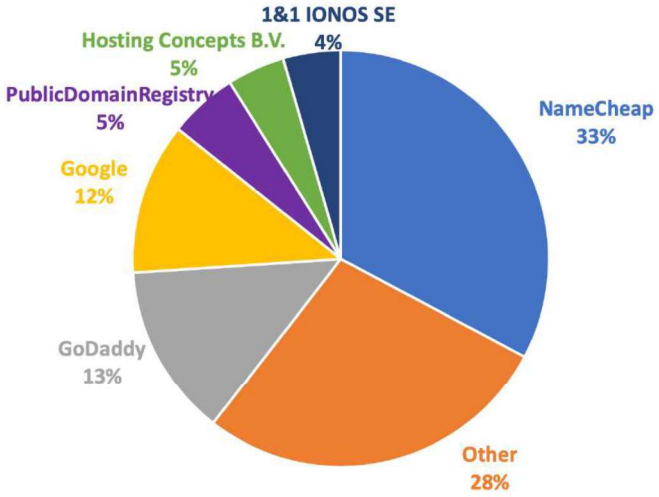
APWG 2022 Q1

BEC providers and domain registrars

Webmail providers used in BEC attacks



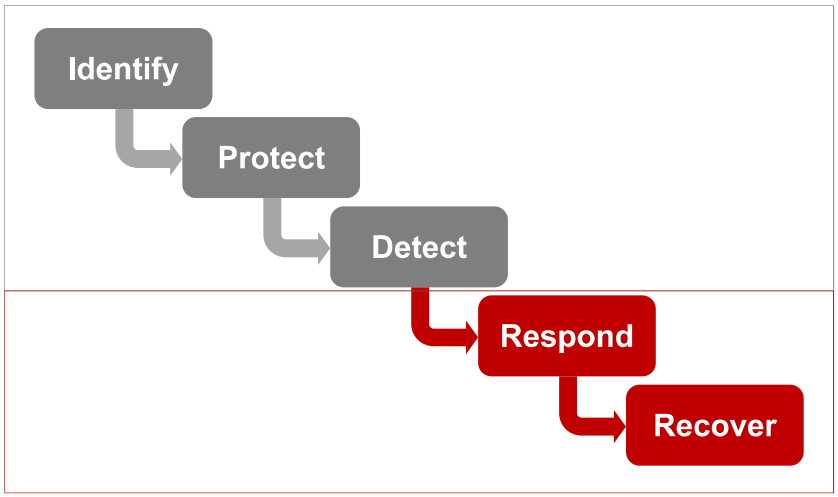
Registrars used to register BEC attack domains



APWG 2022 Q1

15

NIST Cybersecurity Framework



Advancement in technology
Research, Development & Innovation
- Correlation
- Artificial Intelligence
- Machine Learning

People & Process Challenge
- Domain take-down
- Cross Border Organized Crime
- State-sponsored attacks
- Command & Control Server take-down

16

End user targeted attacks

42% Misconfiguration

- Configuration errors
- Weak defaults
- Easy passwords

6% Vulnerable codes

- Bugs
- Input validation

32% End user error

- Install suspect applications
- Clicking malicious links

6% Targeted attack exploded

- Phishing emails
- Watering hole attacks

15% Undetermined

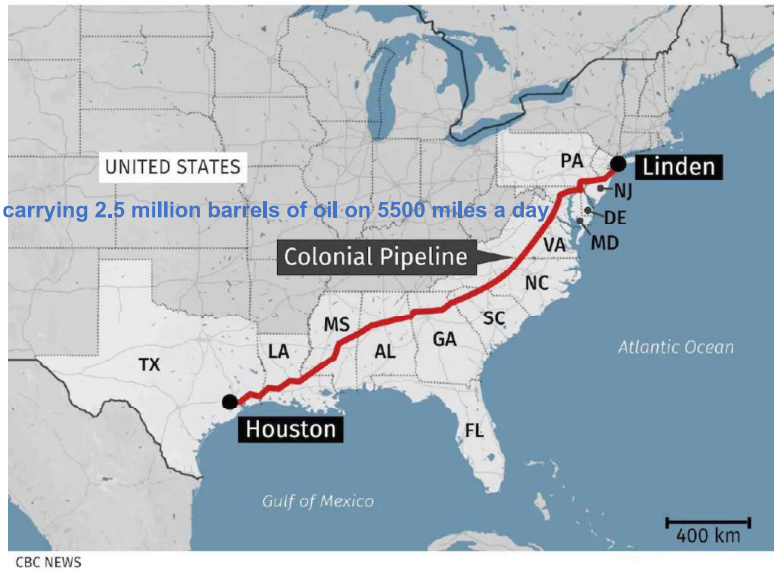
50% End user targeted

- Users are one of the greatest weakness in the defense against cyber attacks.
- Account for almost half of breaches.
- Most are non-malicious but using poor practice.
- Will become the norm to see security hygiene as part of job description.

17

Colonial Pipeline ransom attack

Major U.S. gasoline pipeline hit by cyberattack



CBC NEWS

The company was breached through a leaked password that had access to the VPN

Colonial Pipeline billing system was compromised by ransom attack on May 7 2021. Company shut down pipeline operation due to concern that hackers might further attacks on vulnerable parts of the pipeline.

< 7 hours
company paid 75 Bitcoin or USD 5M

Pipeline restart operation on May 12 2012. Gas price rose to to the highest ($3 a gallon) it's been in over six years.

→ **Cyber Hygiene**

18

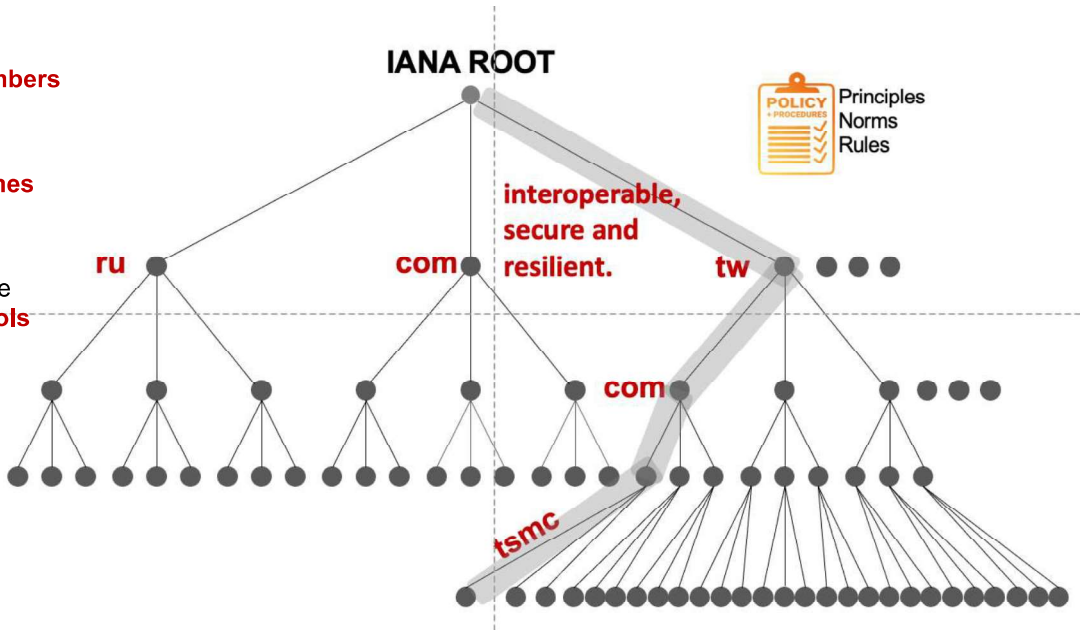
Technical internet governance

TIG is focused on how the Internet operates with the common goal of ensuring that the Internet remains **singular, unified, interoperable, secure and resilient.**

singular, unified **numbers**

singular, unified **names**

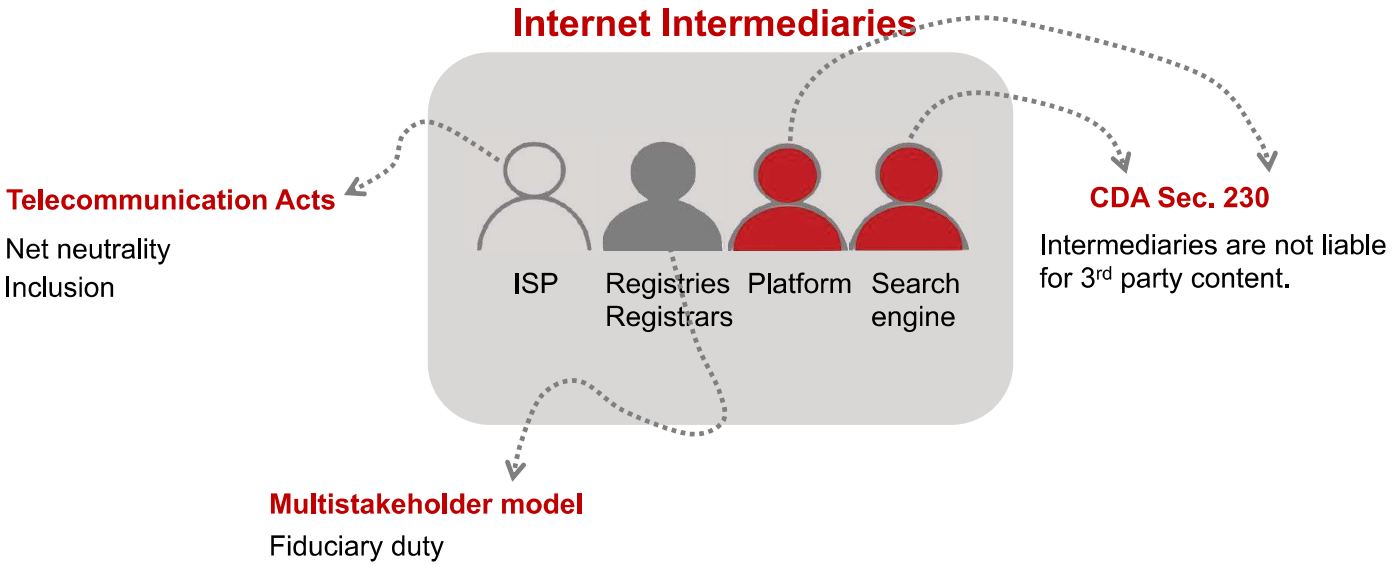
Interoperable, secure and resilient **protocols**



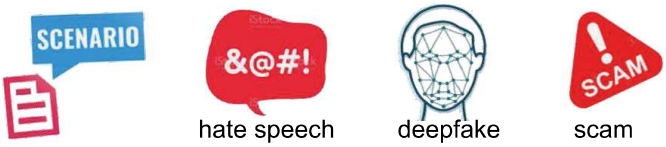
Internet governance vs. cybersecurity governance

IG vs. CG	
Same	Different
cross-border governance demand	centralized architecture (e.g., root)
technology interoperability	global coordinated system
distributed responsibility	criminal sanctions
private sector lead	

Internet intermediary governance model



scenario assessment



	Effective	Quick	Simple	Precise	Proportional	Cost-Effective
ISP	✓	✗	✗	?	✗	✗
CDN	?	?	?	?	✗	✗
Hosting	✓	✗	✗	✗	✗	✗
Platform	✓	✓	✓	✓	✓	✓
Registrar	✓	✓	✓	✗	✗	✗
Registry	✓	✓	✓	✗	✗	✗

scenario assessment





C2 server



botnet



pirate site

	Effective	Quick	Simple	Precise	Proportional	Cost-Effective
ISP	✗	✗	✗	?	✓	✗
CDN	✗	?	?	?	✓	?
Hosting	✗	?	✓	✓	✓	✓
Platform	?	?	?	?	?	?
Registrar	✓	✓	✓	✓	✓	✗
Registry	✓	✓	✓	✓	✓	✓

Law Enforcement & DNS RPZ



Jurisdiction



Law

Court Order

Injunction

Administrative Order

TWNIC RPZ

TIG Norms

TIG Norms

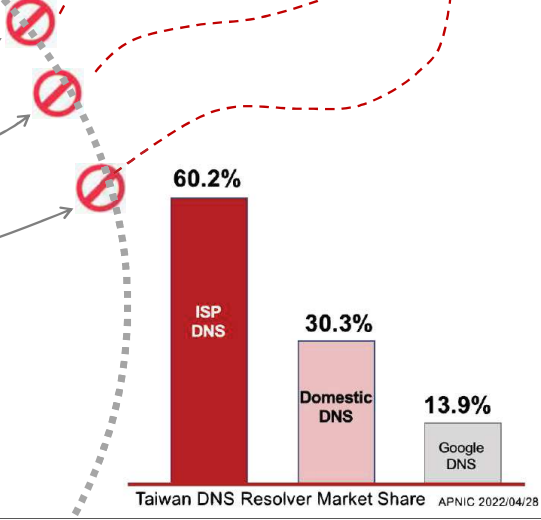


Cyber Norm Dispute Resolution Mechanism

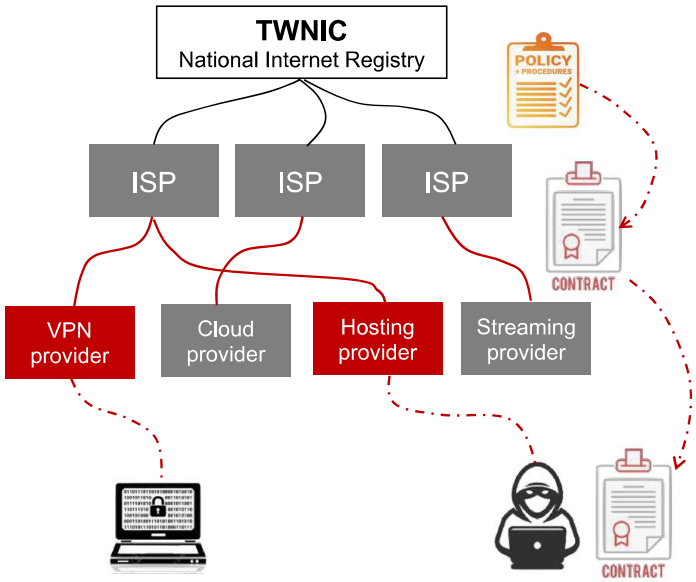
Threat Intelligence Suppliers



Potential Cyber Norms
Disrupt public order
Personal injury
Monetary damages
Child abuse
Illegal trades
Threats of illegal activity



IP Address Policy



Cybercrime Mitigation Strategy

TIG Norms

- Information disclosure : address holder should be registered in WHOIS database if allocation > /30
- Abuse contact validation every 6 months

Contractual Compliance

- Inform address holder's responsibility conducting cybersecurity clearance
- deploy required measures to against cyber threats.
- transparency and accountability mechanism.

Norm Enforcement

- Q/A methodology : official notice and timely response until issue resolved.
- Address holder's resources can be frozen if it fail to fulfill contractual obligations.

25

Extraterritorial operation

TWNIC x www.asia

POLICY

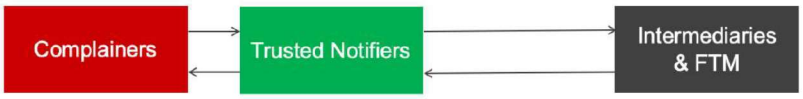
TWNIC – DotAsia Collaboration Against DNS Abuse

Expedited Response on Anti-Phishing Efforts: Mutual Recognition as Trusted Notifier
Illegal & Fraudulent Activities including Phishing and Willful Distribution of Malware
Future expansion to other ccTLDs & security community organizations

APAC DNS FORUM 2022
ICANN APAC – TWNIC ENGAGEMENT FORUM 2022
www.asia

Value to intermediary :

- Risk reduction : better evidenced
- Cost reduction : transfer evaluation cost to TNs
- Firm value : consumer trust



Value to trusted notifier:

- Efficiency : faster
- Effectiveness : enforceability

26

TWNIC DNS abuse

Technical Regime
.TW DNS query : 1.7T queries =>1.2T abuse queries
TWCERT : 200K cases / month

Law Regime
Disinformation cases
notice>10000, report 2953, investigation 589, prosecutor's office 93



Gap assessment

From intermediary liability to intermediary responsibility

Abuse framework			Cyber Jurisdiction
Technical abuse 1 malware 2 botnets 3 phishing 4 pharming 5 spam	**TIG norms** 1 DNS RPZ 2 iWin 3 **Emergent abuse** (1) public order (2) personal injury (3) monetary damages (4) child abuse * (5) illegal trade (6) threat of illegal activity	**Unlawful abuse** 1 court order 2 injunction 3 administrative order 4 threat Intelligence	**Current solutions** 1. MLAT 2. Budapest Convention (1) slow (2) not scalable 3. Legal cooperation (1) lack of transparency (2) admissibility of evidences (3) conflict of laws **Extraterritorial effectiveness** 1 DNS RPZ 2 Registry MoU

27

expanded domain rebranding

The Pirate Bay

piratebay.se
thepriatebay.se

2 domains seized ›
6 domains expanded

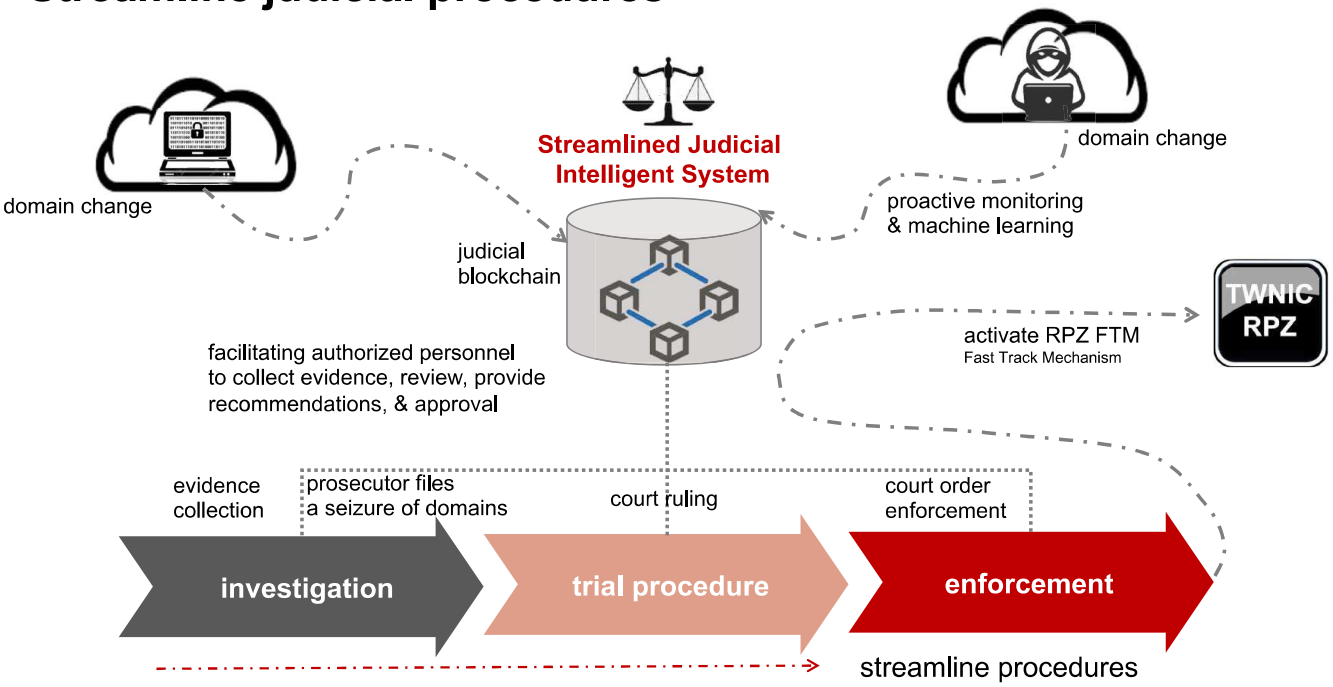


piratebay.gs
piratebay.la
piratebay.vg
piratebay.am
piratebay.mn
piratebay.gd

The expanded domains are outside the jurisdiction of Sweden

28

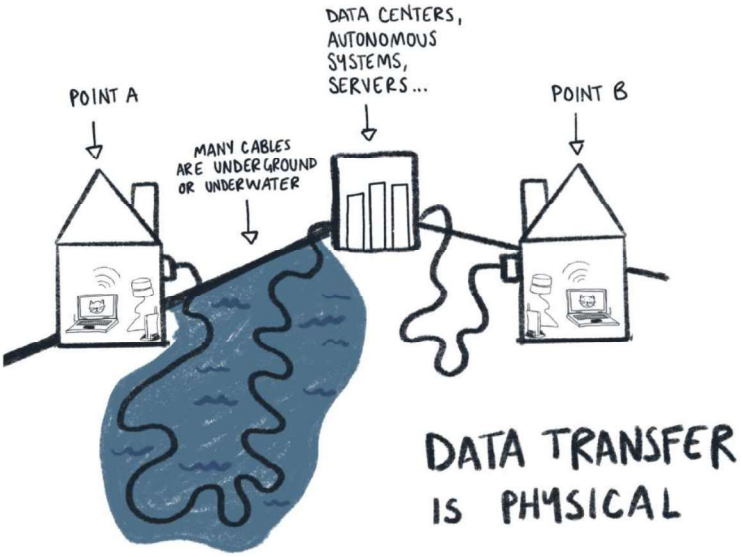
Streamline judicial procedures



How the Internet works: undersea cables, DNS, data center



Defector, 2021/10/22



How world war III could start: cut the cable



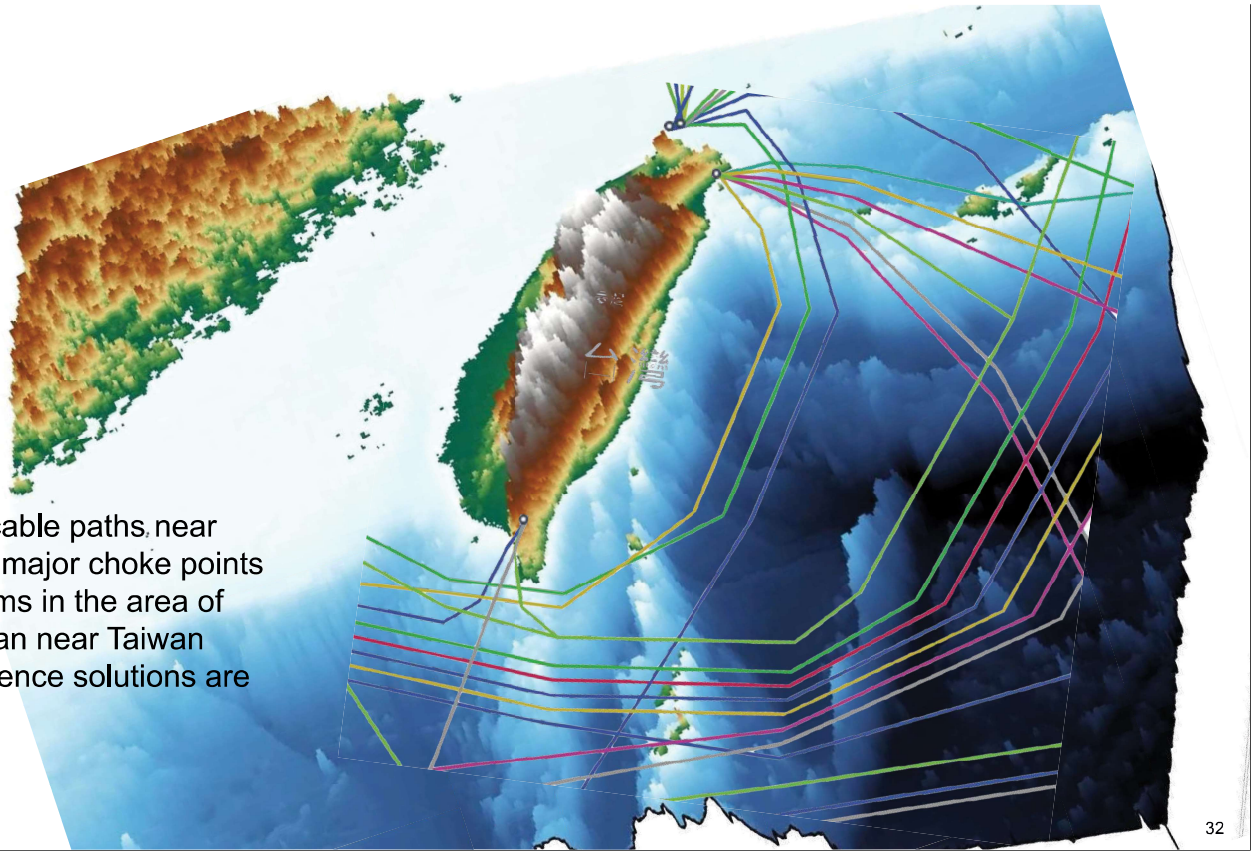
January 7, 2018 | *Topic:* Security | *Blog Brand:* The Buzz | *Tags:* China, Russia, America, War, Military, Technology, World

How World War III Could Start: Cut the 'Cable"

The National Interest, 2018/07/07

- More than 95% of everything that moves on the global Internet passes though just 400 undersea cables. US, Russia, China are are focusing on undersea cables as sources of intel as well as targets in war.
- Gray legal zone: UNCLOS declares that undersea cable attack is not hostile acts : undersea cables can be identified as legitimate military target.
- Luzon strait near the Philippines where all undersea cables connecting Taiwan, Korea, Japan pass are highly vulnerable chokepoints.

31



- Undersea cable paths near Taiwan are major choke points
- Deep chasms in the area of Pacific ocean near Taiwan
- Cable resilience solutions are needed

32

Communications during Ukraine war

- Ukraine ask for support from Starlink at the beginning of the war with Russia
- Elon Musk sent Starlink terminals to Ukraine and activated Starlink service in Ukraine.





US identified the strategic importance of DNS after Russia‘s invasion of Ukraine

Congressional Research Service
Informing the legislative debate since 1914
INSIGHT

A Revisit of the Domain Name System After Russia's Invasion of Ukraine

March 23, 2022

Congressional Research, 2022/03/23

- US NTIA hand over the control of global DNS since 2016. US should review the relationship between US government and ICANN and fight for US leadership in ICANN.
- US should review US leadership in ITU. Russia advocated that transferring control of Internet to ITU for multilateral governance. US should participate ITU secretariat-general election in 2022.

What if it happened to Taiwan (WSJ)


THE WALL STREET JOURNAL.

World U.S. Politics Economy Business Tech Markets Opinion Books & Arts Real Estate Life & Work WSJ. Magazine Spo

Ukraine War Stokes Concerns in Taiwan Over Its Fragile Internet Links

Kyiv's successful use of internet to counter Moscow highlights Taiwan's reliance on undersea internet cables that China could cut

Related Video

- If China invades Taiwan, disconnecting Taiwan from the world by cutting undersea cables would greatly improve China's chances of success.
- "We're very vulnerable," said Kenny Huang, chief executive of Taiwan Network Information Center

WSJ, 2022/04/18

US Naval Institute Proceeding 2022.05.01



Preparing a Post-Invasion Taiwan for Insurgency

The Marine Corps must be ready to assist Taiwan in destroying infrastructure to thwart Chinese surveillance capabilities and ensure success in a broader conflict.

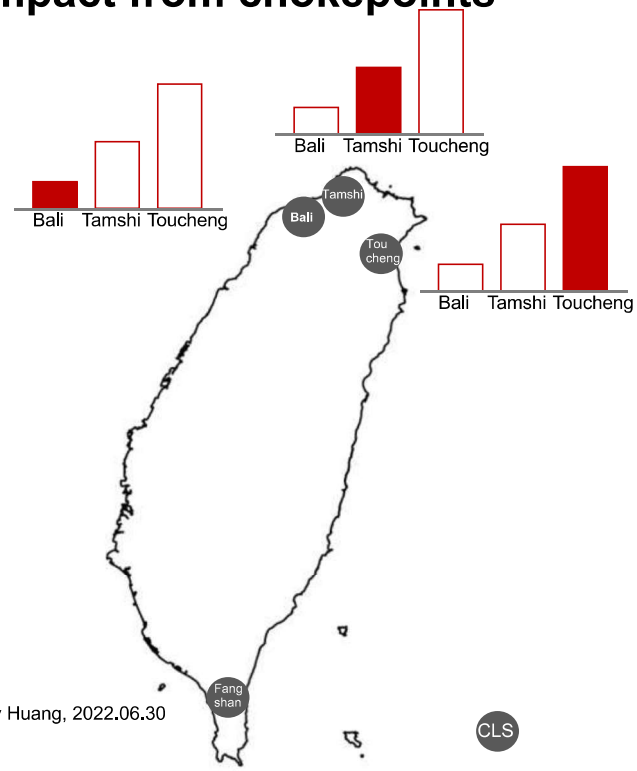
By Christopher Booth

May 2022 | Proceedings | Vol. 148/5/1,431

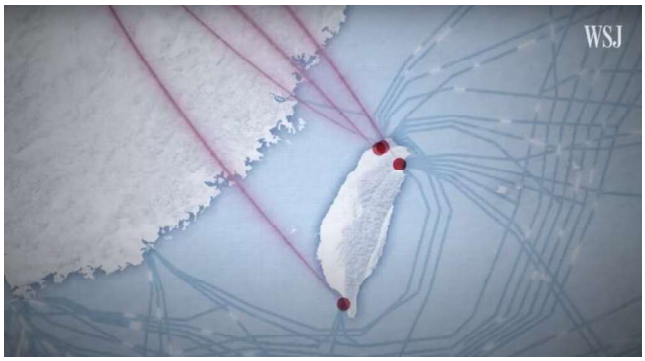
- If China invades Taiwan, US Marine Corps should help destroy with Taiwan CLS and data centers to eliminate the PLA's ability to repurpose it.
- Major choke points need to target are cable landing stations as 99% internet data is routed through these cables.

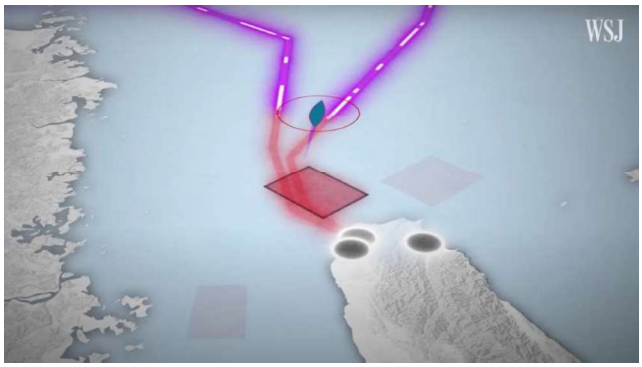
US Naval Institute, 2022/05/01

Impact from chokepoints



Dr. Kenny Huang, 2022.06.30

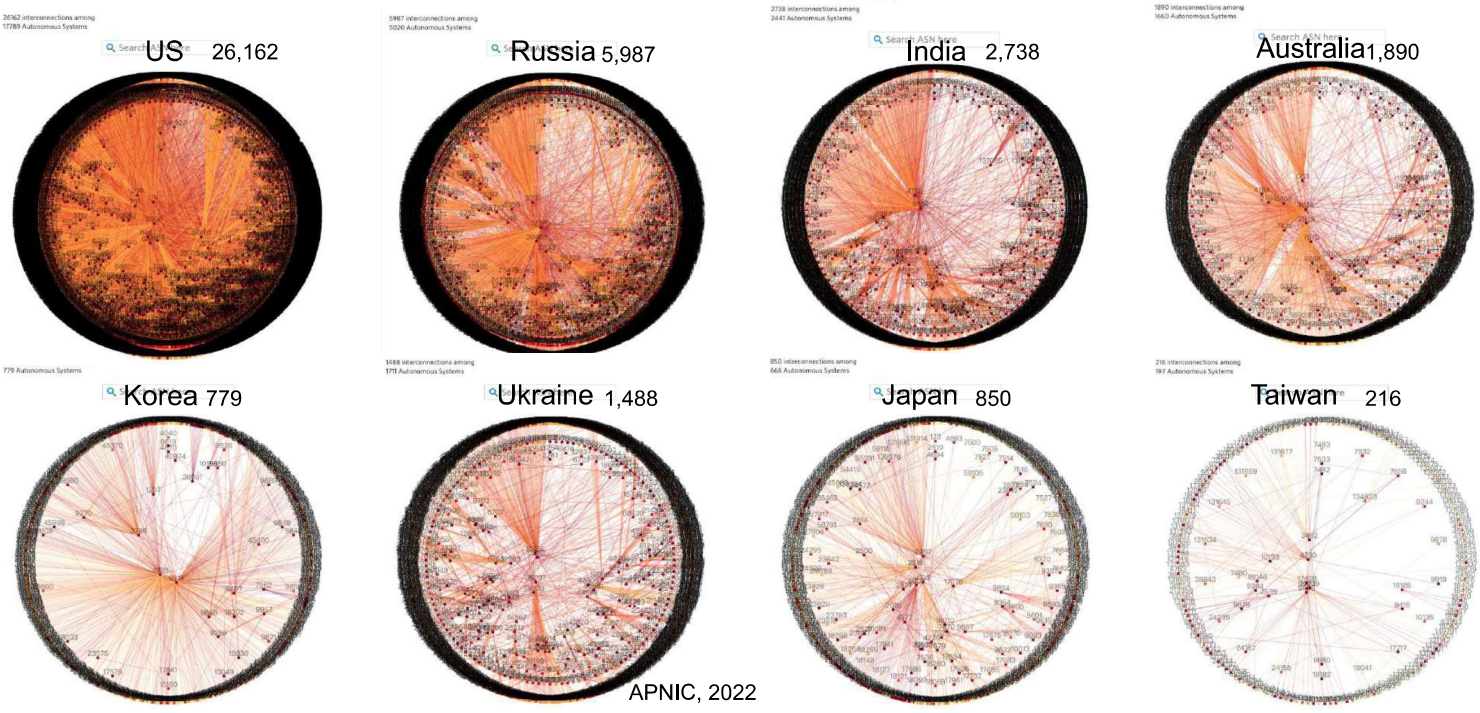




WSJ, 2022.09.21

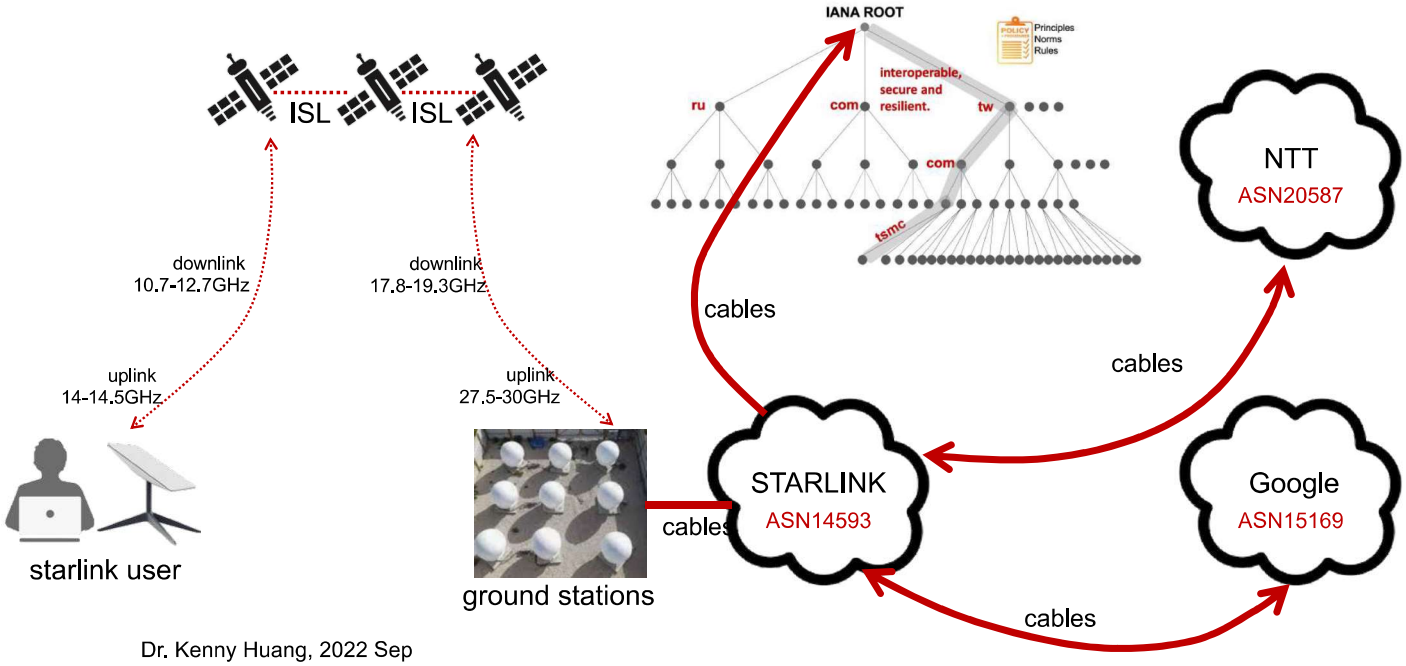
37

network connectivity and resilience



APNIC, 2022

Starlink ISL Topology

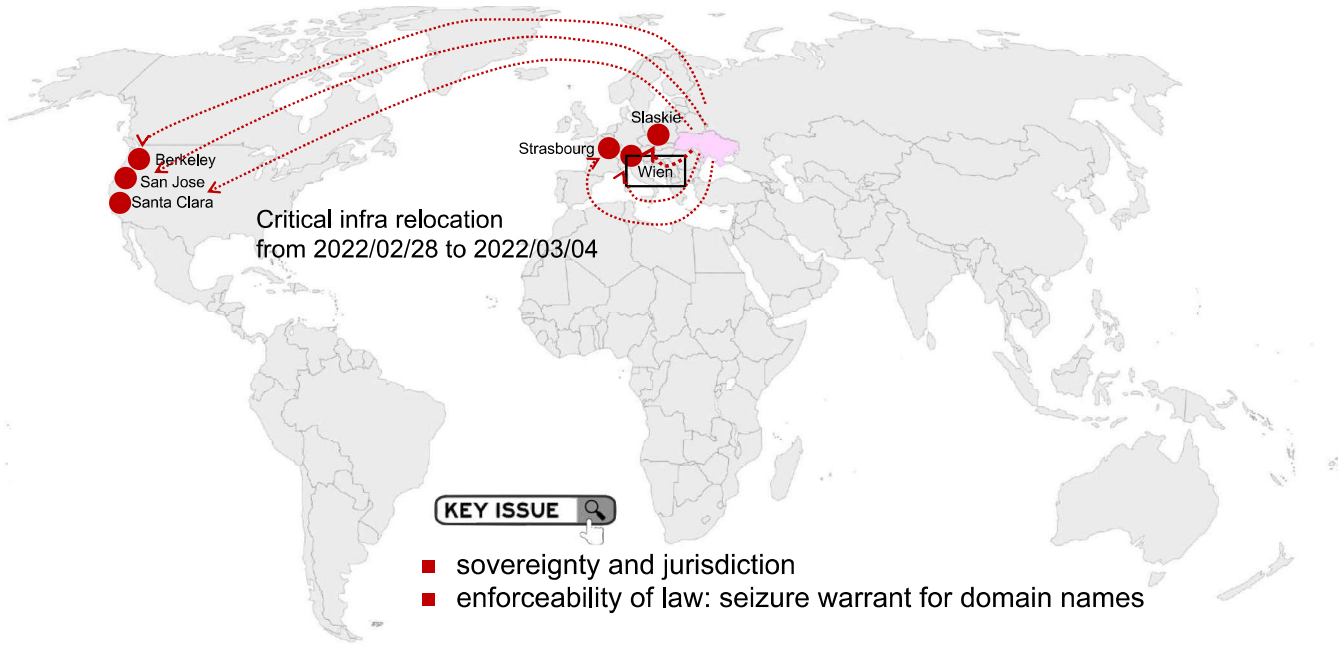


Dr. Kenny Huang, 2022 Sep

Chokepoints resilience : policy intervention model

Government Intervention ?		Is public infra financially sustainable ? Yes	Is public infra financially sustainable ? No
	Yes	public infra competes with private infra (Germany, Swiss, Netherland)	public infra reduce entry barrier and stimulate investment public infra erodes gov. budget and doesn't improve competition
	No		Supplier of Last Resort

Ukraine critical infra relocation (.ua ccTLD)



KEY ISSUE

- sovereignty and jurisdiction
- enforceability of law: seizure warrant for domain names

First internet sanction

- Ukraine requested ICANN to remove Russia ccTLDs (.ru, .рф, .su)
- Shutdown root servers in Russia

ICANN REJECTED

- Ukraine requested RIPE NCC to revoke Russia's IPv4 and IPv6 addresses。

RIPE NCC REJECTED

BUT

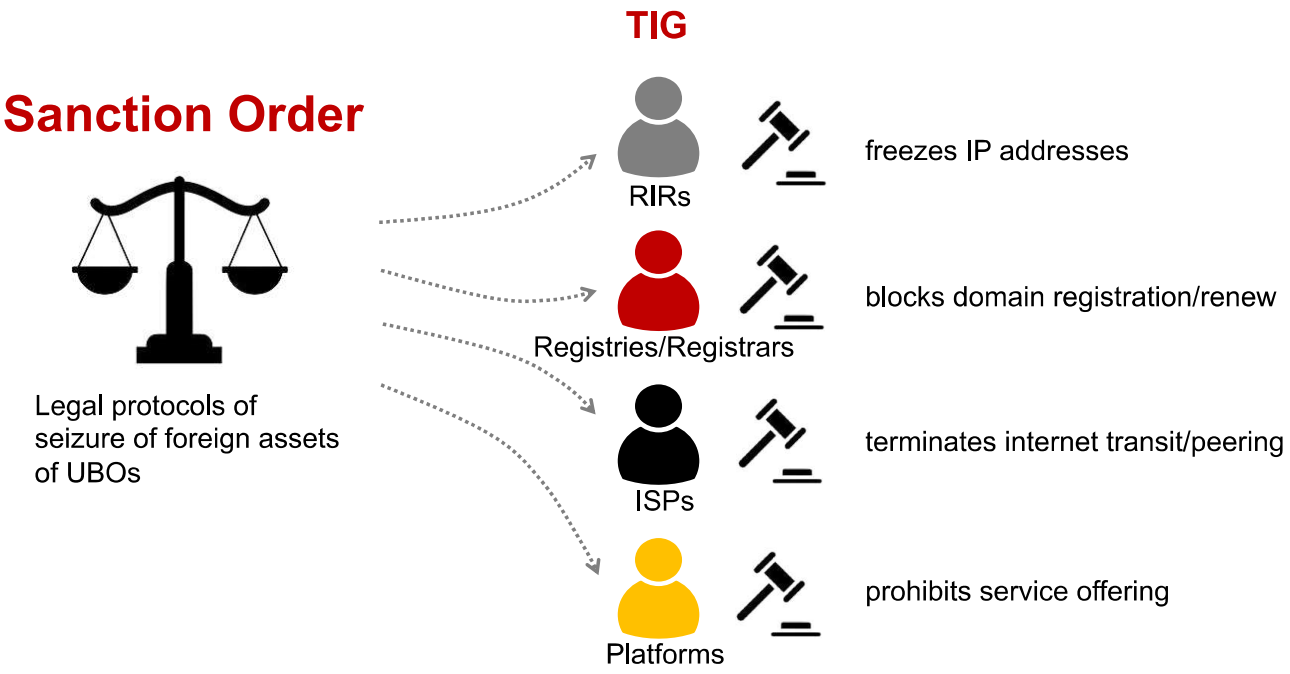
Self Regulation

- ICANN removes .su ccTLD since it doesn't exist in ISO3166-1 list

State Regulation

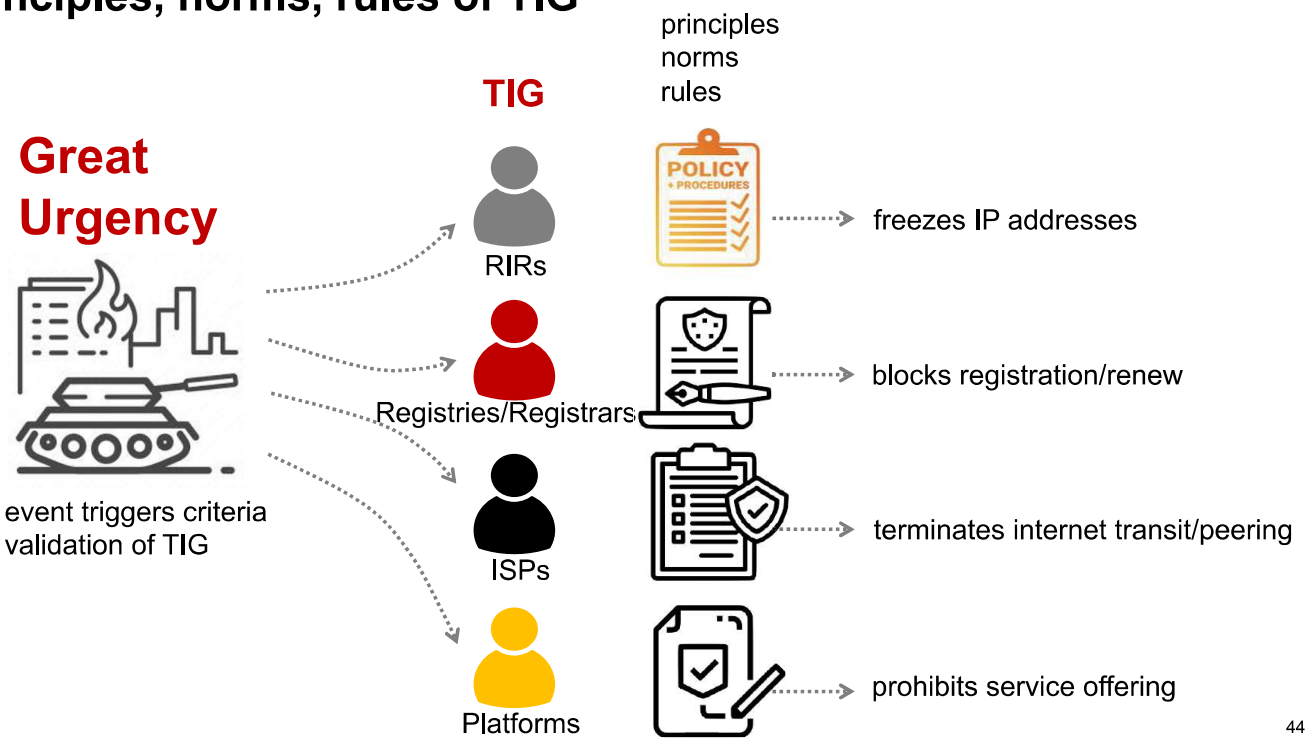
- RIPE NCC freezes IPv4 and IPv6 addresses hold by Russia UBOs that includes most state-owned ISPs.

Legal protocols for economic sanctions



43

Principles, norms, rules of TIG



44

Multistakeholder imposition of internet sanctions

2022/03/10

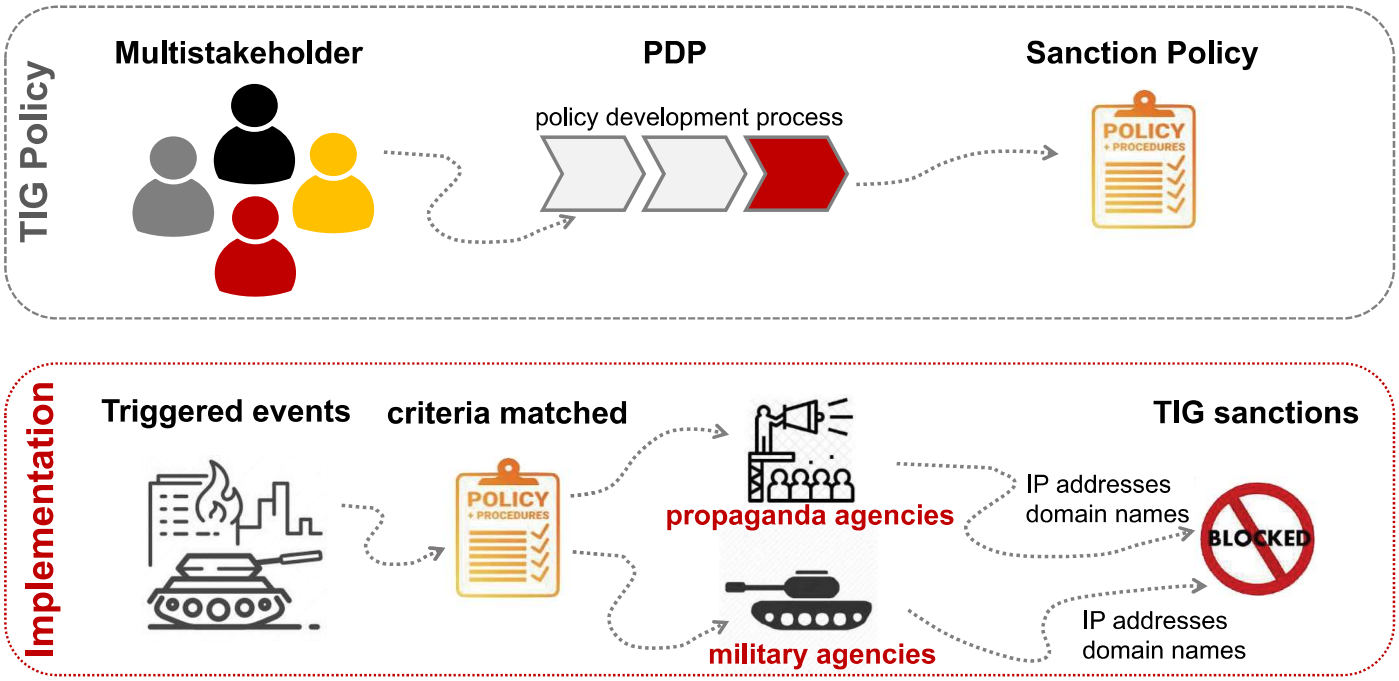




- **Military and propaganda agencies** and their information infrastructure are **potential targets of sanctions**.
- It is the time for the formation of a **new multistakeholder mechanism**. Using the mechanism to decide IP and domains sanctioned, lay the groundwork for timely decisions of similar gravity and urgency in the future.

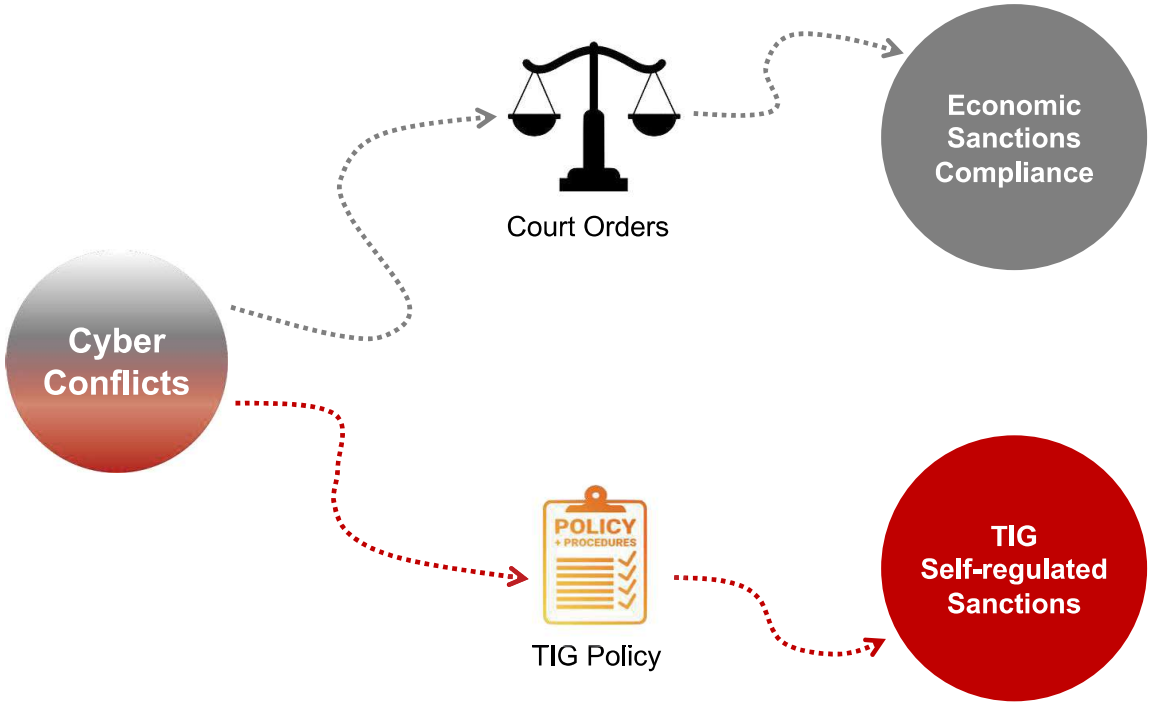
45

Conceptual model of TIG sanctions



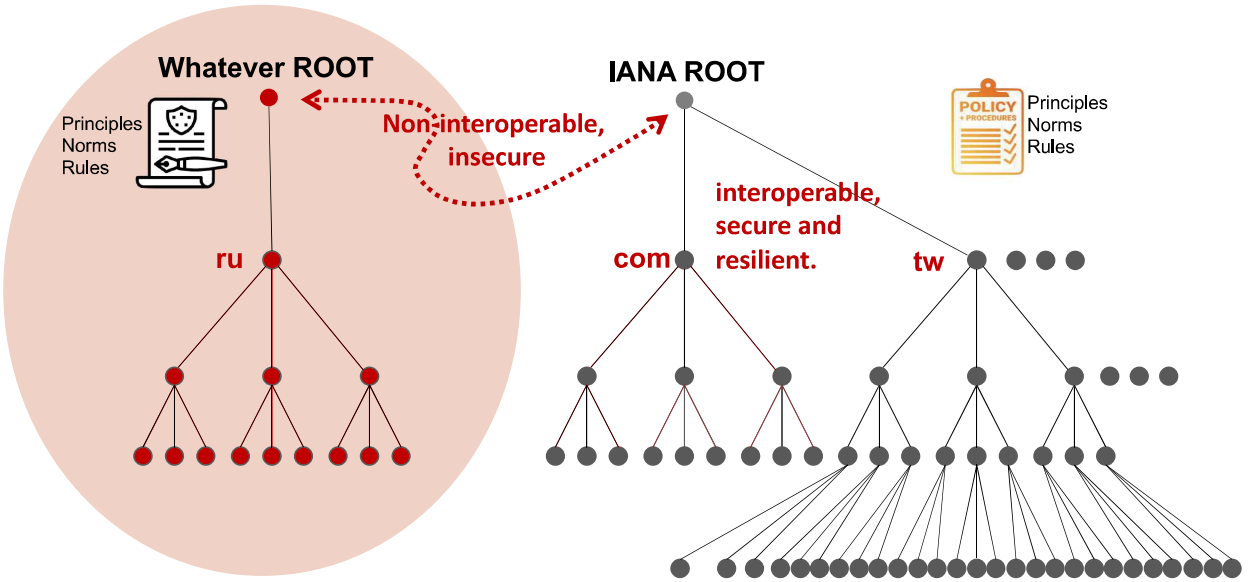
46

Future cyber conflicts



47

Issue: internet fragmentation



48

Key takeaways

- Resilience redefined
  - Designing the worst-case scenario and taking corresponding measures
  - Cybersecurity plan for reinforcement operations and for recovery operations can be totally opposite.
- Repurpose chokepoints: dual-use design
- Data priority scheme
  - There should be a data priority scheme along with a restriction on internet capacity.
- Internet fragmentation
  - Connecting internet is political & economic decision, not a technical decision
  - Connecting internet only if risk/value justified
  - Evolution is the nature of all innovation

49



50

附錄二：「2022 網路治理研習營」課程簡報（僅提供講師授權公開部分）

數位人權：全球網路自由度和政策趨勢

陳文生 / NII產業發展協進會顧問
TWIGF常務監事



簡報大綱

1. 人權與數位人權
2. 全球網路自由度
3. 全球相關政策趨勢
4. 我國網路自由度
5. 其他民主國家案例
6. 結語

美國4.28發布《未來網路宣言》，我國和60多國簽署



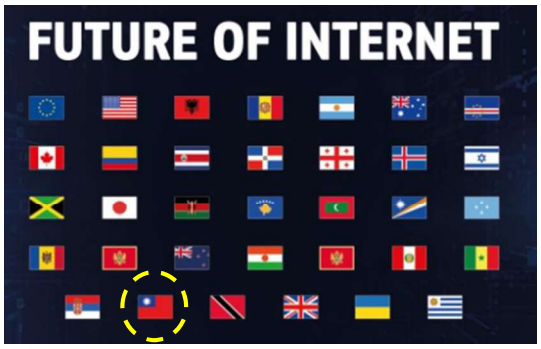
歐盟於Twitter：

Today, the & together with global partners launch the vision for an Internet that is:

- open
- free
- global
- interoperable
- reliable
- secure

宣言的 5 大承諾：

- 保護所有人的人權和基本自由
- 推動訊息自由流通的全球網路
- 推動包容性且可負擔的連線，讓所有人從數位經濟獲益
- 加強對全球數位生態系統的信任，包含透過保護隱私
- 保護和強化以 multistakeholder 方式治理網路



3

1 人權與數位人權



人權

憲法第二章 人民之權利義務 (第七條-第二十四條)

第七條	中華民國人民，無分男女，宗教，種族，階級，黨派，在法律上一律平等。
第八條	人民身體之自由應予保障。除現行犯之逮捕由法律另定外，非經司法或警察機關依法定程序，不得逮捕拘禁。非由法院依法定程序，不得審問處罰。非依法定程序之逮捕，拘禁，審問，處罰，得拒絕之。.....
第九條	人民除現役軍人外，不受軍事審判。
第十條	人民有居住及遷徙之自由。
第十一條	人民有言論，講學，著作及出版之自由。
第十二條	人民有秘密通訊之自由。
第十三條	人民有信仰宗教之自由。
第十四條	人民有集會及結社之自由。
第十五條	人民之生存權，工作權及財產權，應予保障。

5

人權

憲法第二章 人民之權利義務 (第七條-第二十四條)

第十六條	人民有請願，訴願及訴訟之權。
第十七條	人民有選舉，罷免，創制及複決之權。
第十八條	人民有應考試服公職之權。
第十九條	人民有依法律納稅之義務。
第二十條	人民有依法律服兵役之義務。
第二十一條	人民有受國民教育之權利與義務。
第二十二條	凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法之保障。
第二十三條	以上各條列舉之自由權利，除為防止妨礙他人自由，避免緊急危難，維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。
第二十四條	凡公務員違法侵害人民之自由或權利者，除依法律受懲戒外，應負刑事及民事責任。被害人民就其所受損害，並得依法律向國家請求賠償。

6

世界人權宣言及「核心人權公約」

- 《世界人權宣言》 **Universal Declaration of Human Rights**
  - 發布單位：聯合國大會
  - 發布日期：1948年12月10日通過
- **目前台灣已經通過施行法之核心人權公約**
  - ICCPR　公民與政治權利國際公約
  - ICESCR　經濟社會文化權利國際公約
  - CEDAW　消除對婦女一切形式歧視公約
  - CRC　兒童權利公約
  - CRPD　身心障礙者權利公約
- **尚未透過施行法國內法化之核心人權公約**
  - ICERD　消除一切形式種族歧視國際公約
  - ICMW　保護所有移徙工人及其家庭成員權利國際公約
  - ICPPED　保護所有人免遭強迫失蹤國際公約
  - CAT　禁止酷刑和其他殘忍、不人道或有辱人格的待遇或處罰公約

數位人權

APC (Association for Progressive Communications) 網際網路憲章

- 人人都能上網 (Internet access for all)
- 言論和結社自由 (Freedom of expression and association)
- 獲取知識 (Access to knowledge)
- 共享學習和創造—自由和開源軟體和技術開發 (Shared learning and creation – free and open source software and technology development)
- 隱私、監控和加密 (Privacy, surveillance and encryption)
- 網路治理 (Governance of the internet)
- 權利的認識、保護和實現 (Awareness, protection and realisation of rights)

APC Internet Rights Charter，https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter

主題一：人人能上網
Internet access for all

《世界人權宣言》第 26 條：教育應著眼於人格的充分發展和加強對人權和基本自由的尊重

1.1 重視網路存取發展和社會正義的影響，有助於創建更加平等的社會。
1.2 無論您身在何處，都有權訪問基礎設施網際網路作為全球公共基礎設施。
1.3 人們有權利獲取知识和技能，利用和塑造互联网，以满足自己的需求。
1.4 所有人都可以透過各種介面存取各式內容和應用程式的權利（包容性設計）(無障礙、少數族群語言...)
1.5 男性和女性的平等存取權 (equal access for men and women)。
1.6 負擔得起的網路存取權 (The right to affordable access)。
1.7 工作場所的存取權 (The right to access in the workplace)。
1.8 公共存取權 (The right to public access)。
1.9 存取和創建具有多元文化和語言多樣性的內容網站、線上工具和軟體。

9

主題 2：言論和結社自由
Freedom of expression and association

《世界人權宣言》第 18條：人人享有思想、良心和宗教自由的權利
《世界人權宣言》第 19條：人人享有見解和言論自由的權利；這項權利包括不受干涉地持有觀點的自由，以及不論國界通過任何媒體尋求、接收和傳遞信息和思想的自由。
《世界人權宣言》第 20條：人人享有和平集會和結社自由的權利。

2.1 言論自由的權利 (The right to freedom of expression)。
2.2 免於審查的權利 (The right to freedom from censorship)。
2.3 參與網路抗議的權利 (The right to engage in online protest)。

10

主題 3：獲取知識
Access to knowledge

《世界人權宣言》第 27 條：人人有權參與社區的文化生活、享受藝術並分享科學進步及其利益。

3.1 獲取知識的權利 (The right to access to knowledge)
3.2 資訊自由的權利 (The right to freedom of information)
3.3 獲得公共資助資訊的權利 The right to access to publicly-funded information)

11

主題四：共享學習和創造—免費和開源軟件和技術開發
Shared learning and creation – free and open source software and technology development

4.1 分享的權利 (The right to share)
4.2 自由開源軟件 (FOSS) 的權利 (The right to free and open source software)
4.3 開放技術標準的權利 (The right to open technological standards)
4.4 從匯流和多媒體內容中受益的權利 (The right to benefit from convergence and multi-media content)

12

主題 5：隱私、監控和加密
Privacy, surveillance and encryption

《世界人權宣言》第 12條：任何人的隱私、家庭、住宅或通信均不得受到任意干涉，其榮譽和名譽(honour and reputation)也不得受到攻擊。

5.1數據保護的權利(The right to data protection)
5.2不受監視的權利(The right to freedom from surveillance)
5.3 使用加密的權利(The right to use encryption)

13

主題 6：網際網路治理
Governance of the internet

6.1 對網際網路進行多邊民主監督的權利 (The right to multilateral democratic oversight of the internet)
6.2 透明度和可訪問性的權利 (The right to transparency and accessibility)
6.3 去中心化、協作和互操作網際網路的權利 (The right to a decentralised, collaborative and interoperable internet)
6.4 開放架構的權利 (The right to open architecture)
6.5 開放標準的權利 (The right to open standards)
6.6 網際網路中立性和端到端原則 (The right to internet neutrality and the end-to-end principle)
6.7 網際網路作為一個整體的權利 (The right to the internet as an integrated whole)

14

主題 7：權利的認識、保護和實現
Awareness, protection and realisation of rights

7.1權利保護權、意識權和受教育權 (The right to rights protection, awareness and education)

7.2權利受到侵犯時的追索權 (The right to recourse when rights are violated)

15

數位人權—澳洲 Digital Rights Watch

We believe that digital rights are human rights which see their expression online.



Privacy & Security

We believe in the fundamental right to privacy for all.

我們相信所有人的基本隱私權



Personal Information & Data Rights

We believe governments, corporations and organisations should uphold basic privacy rights.

我們認為政府、企業和組織應該維護基本的隱私權。



Power, Access & Technology

We advocate for increased transparency, accountability and oversight over the use of data.

我們提倡提高對數據使用的透明度、問責制和監督。



Journalism & Information Flows

We believe in the value of strong, effective & accountable journalism.

我們相信強大、有效和負責任的新聞的價值。

16

數位人權—國際網路人權組織Access Now

- Business and Human Rights (企業與人權)
- Content Governance (內容治理)
- Data Protection (資料保護)
- Digital Security (數位安全)
- Freedom of Expression (言論自由)
- Internet Shutdowns (網路中斷)

https://www.accessnow.org/blog/
https://www.rightscon.org/

17

2 全球網路自由度

Freedom on the Net 2021



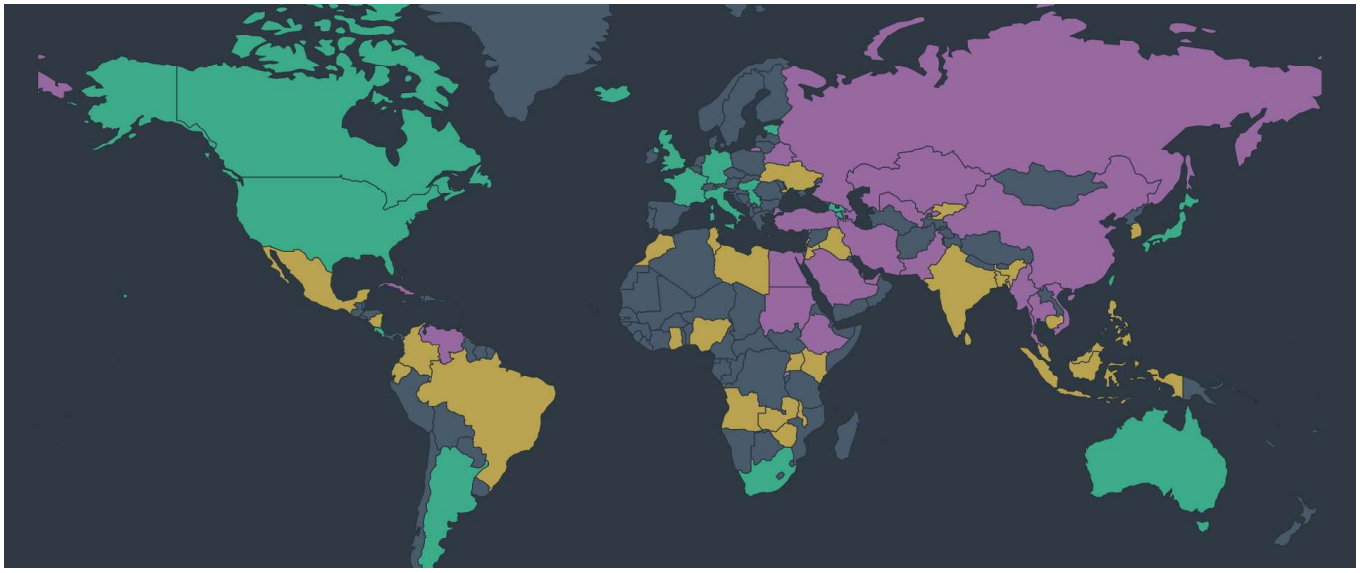
Freedom House

- 全球連續 11 年下滑
- 美國連續 5 年下滑
- 中國連續 7 年墊底

2021年

30%國家	44%國家	26%國家
NOT FREE	PARTLY FREE	FREE

評比全球70個國家＝88%上網人口



19

評比指標： 3 大類21子項共100分

A. 上網阻礙 (25分)

A1 網路連線、網速和網路品質，是否受限於基礎設施的不足？

A2 上網費是否貴到令人卻步，或是超出特定族群的可負擔範圍？

A3 政府是否為了限制上網，而對網路基礎設施進行技術性或法規面的控制？

A4 是否有法律、規範或經濟層面的因素，阻礙服務供應商的多樣化？

A5 服務供應商和數位科技的國家監管單位，是否採取自由、公平、獨立方式運作？

B. 內容限制 (35分)

B1 政府是否封鎖、過濾網路內容，尤其是受國際人權標準保護的議題？

B2 政府是否採取法律、行政或其他手段，迫使出版商、內容託管商或數位平臺刪除內容，尤其是受國際人權標準保護的內容？

B3 對網路和數位內容的限制，是否透明、符合比例原則、有獨立的上訴程序？

B4 網路記者、評論人、一般用戶是否進行自我審查？

B5 網路上的資訊來源是否被政府操控以利特定的政治利益？

B6 是否有經濟或法規等因素阻礙用戶發表網路內容？

B7 網路上的訊息是否多樣化且值得信賴？

B8 是否有阻礙用戶動員、組織社群和活動的情況，尤其是對政治和社會議題？

C. 侵犯用戶權利 (40分)

C1 憲法或法律是否保障言論自由、上網、媒體自由等，且由獨立司法系統執法？

C2 是否有將網路行為課以刑責的法律，尤其是受到國際人權標準保護的行為？

C3 是否有人民因為網路行為而受罰，尤其是受到國際人權標準保護的行為？

C4 政府對於匿名或加密通訊是否有所限制？

C5 政府是否有侵犯用戶隱私的網路監控活動？

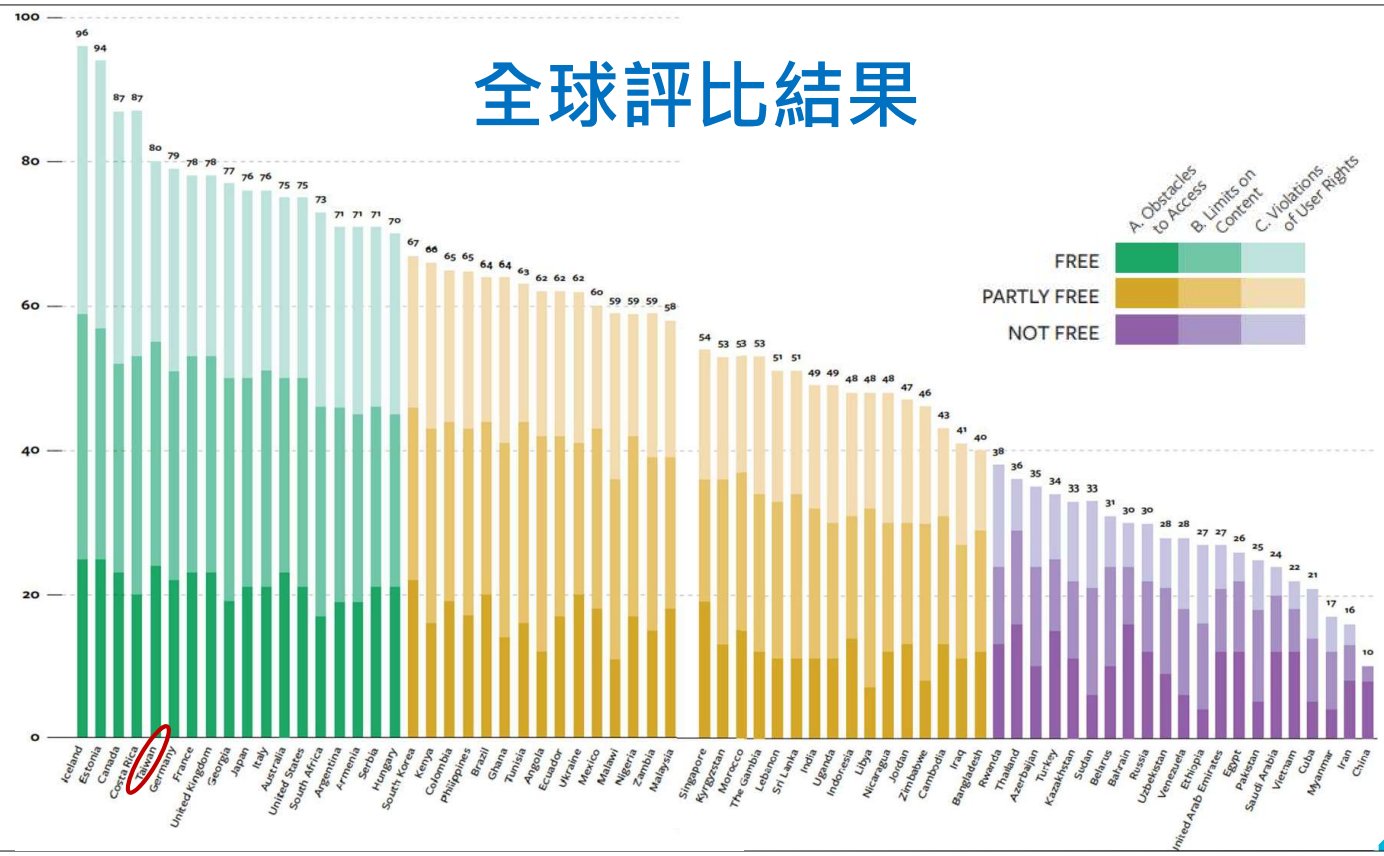
C6 業者處理用戶資料是否侵犯用戶隱私權？

C7 人民是否會因為網路行為而受到政府或其他單位法律外的恐嚇或身體暴力？

C8 網站、政府、民間單位、服務供應商及個別用戶，是否受到廣泛的駭侵及網攻？

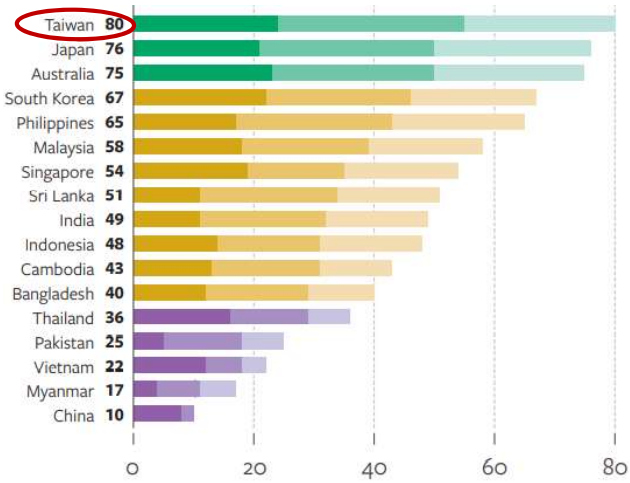
20

全球評比結果

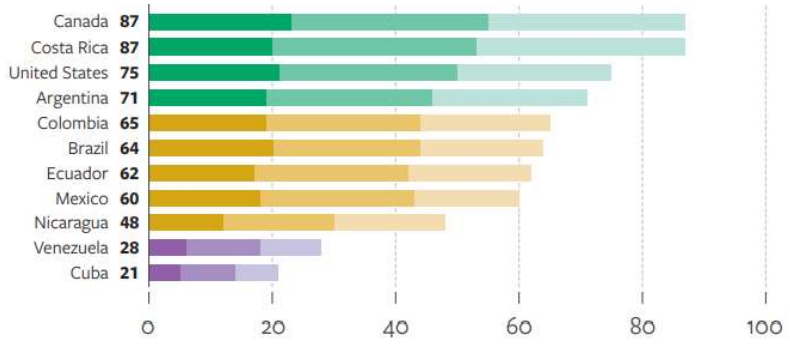


21

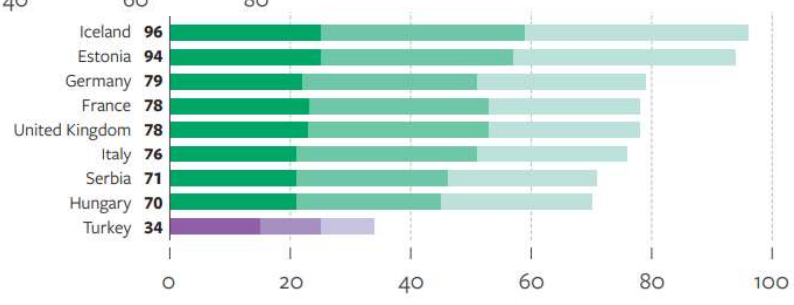
亞太地區



美洲地區



歐洲地區



22

3 全球相關政策趨勢

Freedom on the Net 2021



Freedom House

網路規範橫掃全球

- 48國（扣除重複）推出新規監管科技公司
  - 早期的網路規範由美國主導，但自由放任方式衍生各種網路濫用問題，於是各國政府開始監管數位領域



24國介入平臺內容管理，言論自由面臨風險

- **內容法規對人權的影響**
  - **民主國家**
    精心設計的平臺規範或可減輕線上危害，加強透明度和問責制
  - **威權國家**
    可能遭獨裁者濫用，以打壓人民對政治、社會和宗教的不同訴求
    - 中共當局將民間企業收歸國家權力之下，以更有效地消除異議言論、進行全面監控、操弄宣傳。如中國科技公司會因為沒有刪除嘲笑習近平的漫畫，或指控新疆集中營的言論而受罰



25

38國實施資料在地化、破壞加密，擴大政府監控疑慮

- **便於政府擴大監控的法規或措施**
  - 資料在地化（強制業者將用戶資料存於當地伺服器）
  - 禁止私人通訊採用加密
  - 將個資交給幾乎不受監督的執法機關
  - 以模糊的國安為由索取個資
  - 對資料跨境傳輸施加繁重的許可要求
- **疫情個資是否遭濫用值得關注**
  - 各國採用apps抗疫，但幾無防止濫用措施
    - 新加坡警方可取用TraceTogether app資料，引發民眾強烈抗議後，立法限制使用範圍
    - 澳洲情報與安全機構坦承，意外從該國的COVIDSafe app蒐集個資



26

21國擬捍衛市場競爭秩序，但可能淪為專制政權工具

- 競爭政策的不同目的
  - **民主國家**
    為了保護消費者的權益、防止個資遭濫用、促使不同產品可相互操作或無縫切換
  - **威權國家**
    可能出於政治動機。如中、俄兩國對民間企業採取嚴厲反壟斷措施，使其為政治利益服務，罔顧正當或法治程序

The News Lens 關鍵評論

2021/06/18, 經濟

中共加強對數十家互聯網公司「反壟斷」審查，個人數據應被視為「國家資產」

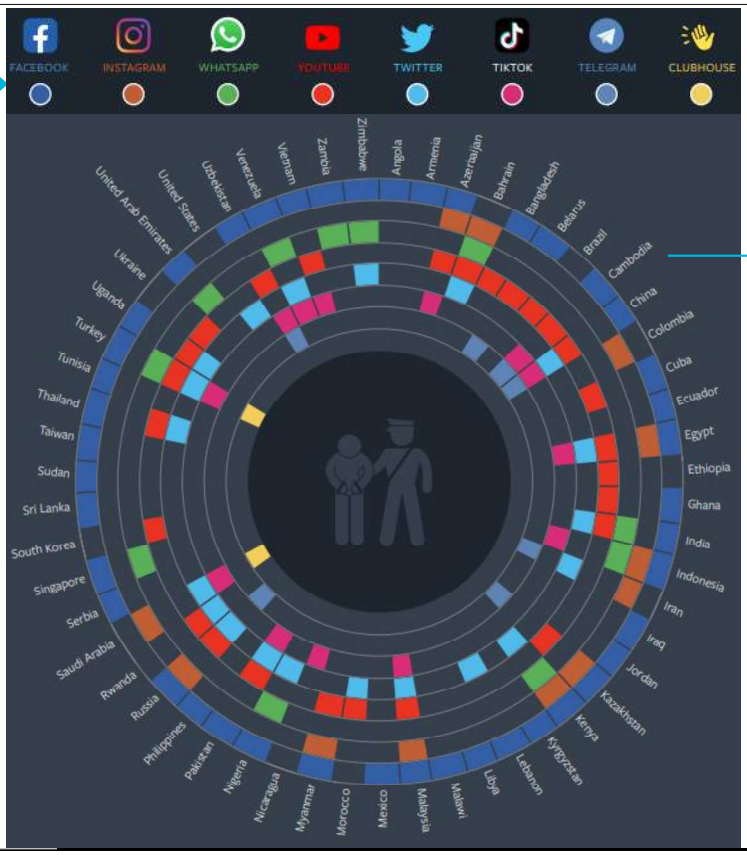
POLITICO REGISTER SIGN IN

EU negotiators agree new rules to rein in tech giants

'The Digital Markets Act puts an end to the ever-increasing dominance of Big Tech companies,' says lead MEP.



27



貼文惹罪、封網、監控……全球人權陷入危機

- 56國民眾因社群媒體上的貼文，而遭調查、逮捕或定罪
  - 如伊朗、泰國等，以煽動抗議、冒犯君王等為由，判處民眾死刑或數十年監禁
- 20國政府下令關閉網路；21國政府封鎖社群媒體和通訊平臺
  - 如印度、衣索比亞等國，且通常於抗議活動和選舉等政治動盪時期實施
- 45國政府使用間諜軟體進行監控
  - 墨西哥、匈牙利、印度等國疑似使用間諜軟體，對記者、人權維護者、政治異議份子等進行監聽或監控，有多人因此遭判刑和監禁

28

正向發展：著重透明度和正當程序的法規

- **歐盟提供「第三種方式」監管網路**
  - 中國的數位威權主義
  - 美國的傳統自由主義
  - 歐盟的「第三種方式」
    如《數位服務法》草案、《數位市場法》草案
    為科技產業制定積極的規則



- **其他國家亦有著重透明度的法規**
  - 臺灣《網際網路視聽服務法》草案：簡稱OTT TV專法（2021年暫緩，2022年重新推動），透過強制特定公司提供營運資料、易於使用的用戶投訴機制、闡明資料蒐集使用的服務條款等措施，提高串流影音平臺在我國的營運透明度
  - 美國《平臺問責制和消費者透明度法》草案：要求業者公布如何審核內容的詳細資訊、為用戶制定正當程序的保護措施、於4天內刪除法院判定的非法內容等

29

4

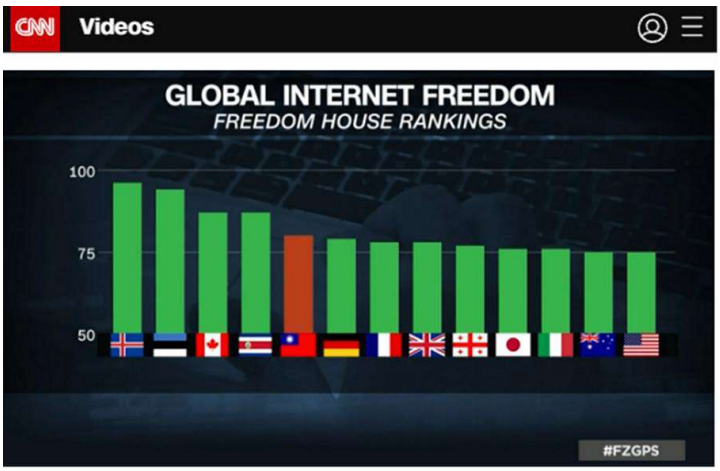
我國的網路自由度和相關政策

Freedom on the Net 2021



Freedom House

國際媒體的報導



CNN 節目Global Public Square：
臺灣的網路自由度排名超越德、美等民主國家



外交家雜誌：
中國和臺灣的網路自由度是天壤之別

31

全球第5名；亞太第1名

Taiwan **80** /100

FREE

A. Obstacles to Access	24 /25
B. Limits on Content	31 /35
C. Violations of User Rights	25 /40

獲肯定的項目

- 5項指標中4項滿分，凸顯網路普及率很高、資費可負擔、沒有顯著數位落差、有獨立監管單位、民眾可自由選擇 ISP

待改善的問題

- 供應商多樣化項目因被視為電信市場由特定業者主導，而小扣1分
- 雖有電信和廣播的獨立監管單位「通傳會」，但民眾對其獨立性有所疑慮

32

「上網阻礙」項目的評比結果 24/25

A1 網路連線、網速和網路品質，是否受限於基礎設施的不足？（6 / 6）

A2 上網費是否貴到令人卻步，或是超出特定族群的可負擔範圍？（3 / 3）

A3 政府是否為了限制上網而對網路基礎設施進行技術或法規面的控制？（6 / 6）

A4 是否有法律、規範或經濟層面的因素，阻礙服務供應商的多樣化？（5 / 6）

A5 服務供應商和數位科技的國家監管單位是否採自由、公平、獨立方式運作？（4 / 4）

全球第5名；亞太第1名

Taiwan **80** /100

FREE

A. Obstacles to Access	24 /25
B. Limits on Content	31 /35
C. Violations of User Rights	25 /40

獲肯定的項目

- 8項指標中5項滿分，代表沒有網路封鎖和審查、言論自由、訊息多樣化
- 《網際網路視聽服務管理法》草案規範OTT-TV業者的義務、《數位通訊傳播法》草案規定通傳業者的義務（惟人權團體認為此法將非法內容的裁定責任推卸給業者）

待改善的問題

- 網路內容責任的法律（如社維法、刑法誹謗罪、香港國安法、李明哲遭逮捕事件.....）可能導致民眾自我審查言論
- 臺灣兩大政黨和中共皆於臺灣的網路空間進行政治影響力的假訊息操弄（如中共付費國內媒體散播親共言論及介入社論審查）

「內容限制」項目的評比結果 31/35

B1 政府是否封鎖、過濾網路內容（或強制服務供應商執行），尤其是受國際人權標準保護者（如：新聞和言論自由，可討論政治、社會、文化、宗教、藝術等議題）？（6 / 6）

B2 政府是否採用法律、行政或其他手段，迫使出版商、內容託管商或數位平臺刪除內容，尤其是受國際人權標準保護的內容？（3 / 4）

B3 對網路和數位內容的限制，是否透明、符合比例原則、有獨立的上訴程序？（4 / 4）

B4 網路記者、評論人、一般用戶是否會進行自我審查？（3 / 4）

B5 網路上的資訊來源是否被政府操控以利特定的政治利益？（2 / 4）

B6 是否有經濟或法規等因素阻礙用戶發表網路內容（如：政府是否限制網路媒體的廣告 或投資、ISP是否落實網路中立、內容託管和平臺是否缺乏競爭）？（3 / 3）

B7 網路上的訊息是否多樣化且值得信賴？（4 / 4）

B8 是否有阻礙用戶動員、組織社群和活動的情況，尤其是對政治和社會議題？（6 / 6）

全球第5名；亞太第1名

Taiwan **80** /100

FREE

A. Obstacles to Access	24 /25
B. Limits on Content	31 /35
C. Violations of User Rights	25 /40

獲肯定的項目

- 8項指標中沒有滿分項目，但指出我國《憲法》保障言論等自由，且有獨立的司法系統

待改善的項目

- 多項法律將網路行為定為犯罪，且有受罰案例
- 未經法院核准的通訊監察，及索取通聯紀錄的案件增加
- 《科技偵查法》草案提高執法單位的監控能力，有侵犯人權的疑慮
- 缺乏個資法的獨立專責主管機關
- 疫情資料的蒐集使用缺乏合法性（如簡訊實聯制的資料遭指控用於犯罪偵查）和比例原則
- 常遭境外網路攻擊且有資料外洩問題

「侵犯用戶權益」項目的評比結果 25/40

C1 憲法或法律是否保障言論自由、上網、媒體自由等，且由獨立司法系統執法？（5 / 6）

C2 是否有將網路行為課以刑責的法律，尤其是受到國際人權標準保護的行為？（2 / 4）

C3 是否有人民因為網路行為而受罰，尤其是受到國際人權標準保護的行為？（4 / 6)

C4 政府對於匿名或加密通訊是否有所限制？（3 / 4）

C5 政府是否有侵犯用戶隱私權的網路監控活動？（3 / 6）

C6 業者監看和蒐集用戶資料是否侵犯用戶隱私權？（3 / 6）

C7 人民是否會因為網路行為而受到政府或其他單位法律外的恐嚇或身體暴力？（4 / 5）

C8 網站、政府和民間單位、服務供應商，以及個別用戶，是否受到廣泛的駭侵及網路攻擊？（1 / 3）

透明度報告（transparency report）

透明度報告是一個公司定期發布的一種聲明，披露各種與用戶數據、記錄或內容相關的請求的統計。透明度報告通常披露哪些實權政府在特定時間段請求或要求數據或記錄的頻次。這種企業透明度的形式使公眾得以辨別政府通過搜查令、法院傳票及其他方式得以訪問多少個人信息。部分透明度報告描述了遵守政府行動或版權規定刪除內容的頻率和數量。披露透明度報告還有助於人們了解網上討論之內容監管的適當範圍與權力。Google在2010年最先發布了一份透明度報告，Twitter則在2012年緊隨其後。其他公司在2013年的全球監視披露之後也開始發布透明度報告，並且發布的公司自那之後迅速增長。透明度報告目前由各個技術和通信公司發布，包括Google、微軟、威訊、AT&T、Twitter、蘋果公司、Dropbox、Meta、雅虎和CloudFlare。

1. 台灣網路透明度報告 – 台灣人權促進會，https://www.tahr.org.tw/issues/transparency-report
2. Google 資訊公開報告，https://transparencyreport.google.com/?hl=zh_TW
3. Meta Transparency Center， https://transparency.fb.com/data/content-restrictions/country/TW/

5

其他民主國家案例

Freedom on the Net 2021



Freedom House

全球第3名；美洲第1名

Canada

FREE

87 /100

A. Obstacles to Access	23 /25
B. Limits on Content	32 /35
C. Violations of User Rights	32 /40

- **隱私當局發現業者違法蒐集人臉資料**
  - 購物中心使用美商的人臉辨識軟體，在民眾不知情下蒐集臉資，違反《個人訊息保護和電子文件法》。隱私部門要求停止蒐集並刪除資料，且停止提供類似服務
- **盜版網站封鎖令上訴至最高法院**
  - 有電信業者對法院命令「全國主要ISP封鎖侵權節目的網站」，以捍衛言論自由為名，上訴至最高法院
- **《選舉現代化法案》違憲條款遭法院駁回**
  - 安大略省法院認為「將散播候選人的錯誤訊息定為刑事犯罪」，侵犯言論自由且違反憲法
- **《消費者隱私保護法》草案遭抨未考量人權**
  - 草案因提供企業使用個資的額外權限，而被批評未從人權角度立法
- **COVID-19 個資共享因訴訟而終止**
  - COVID-19 緊急命令授權跨部門（行政、執法、醫療）共享個資的措施，於人權團體提訴訟後停止實施
- **仇恨言論、誹謗等網路行為皆有法律規範**
  - 仇恨言論最高處2年監禁，其他如誹謗、鼓吹種族滅絕、威脅，最高處5年監禁。網路騷擾亦是違法行為

全球第6名；歐洲第3名

Germany 79 /100

FREE

A. Obstacles to Access	22 /25
B. Limits on Content	29 /35
C. Violations of User Rights	28 /40

法律授權情報單位擴權監聽，但無相關保障措施

- 聯邦情報局組織法修法，允許其監聽全球電信網路30% 傳輸容量；且監聽對象擴及無犯罪紀錄的人民，並可使用惡意軟體達成監聽目的。聯邦憲法法院等批評此法沒有同時提供有效的個人通訊保障措施

NetzDG修正案監管範圍擴及影音平臺

- 《網路執法法案》近來實施多項修正案，如業者須向警方提供嫌犯（指線上仇恨等內容的發布者）個資、法規適用範圍擴及影音分享平臺……

新《著作權法》過濾機制規定可能無效

- 大型平臺業者須設過濾機制，以封鎖涉嫌侵權的線上內容。但此條款可能無效，因為各黨派持反對意見，且歐盟最高法院尚未裁決《歐盟著作權指令》第17條的合法性（指平臺對使用者上傳內容是否侵權須負把關責任）

擬由DNS封鎖侵權網站引發通訊自由隱憂

- ISP和娛樂產業組織成立「網路著作權清算中心」，推動從DNS封鎖侵權網站，但引發從法律制度外限制通訊自由的隱憂

打擊假訊息的法規引發內容審查疑慮

- 為因應極端政黨操弄假訊息，立法部門以《國家媒體協定》取代《州際廣播協定》，但監管範圍從無線電廣播擴至新型媒體，且平均收視超過2萬次的媒體創作者（如YouTuber）須申請執照，引發內容審查等抨擊

41

全球第13名；美洲第3名

United States 75 /100

FREE

A. Obstacles to Access	21 /25
B. Limits on Content	29 /35
C. Violations of User Rights	25 /40

政府破壞使用科技進行集會結社的自由

- 執法單位加強監控種族不公的抗議活動，導致民眾發布訊息的寒蟬效應，且侵犯使用科技集會結社的自由

「緊急寬頻福利計畫」等政策解決上網阻礙

- 提供近 400 萬人網路服務和相關設備的折扣；另通過《基礎設施投資與就業法》，斥資650億美元興建高速寬頻網路

拜登撤微信禁令，但要評估敵國apps風險

- 川普以國安為由下令禁止下載中國抖音和微信，拜登撤除此令，但要求評估敵國apps的國安風險

川普防審查令遭撤，CDA第230條改革案不止

- 川普《防止線上審查》行政命令（旨在刪除《通信端正法》CDA第230條對中介機構免責的保護傘）遭拜登撤回，但至少9項改革230條的法案送交國會

川普帳號遭停權，引發社群媒體審查權質疑

- 川普因煽動暴力貼文而遭平臺停權，業者表示行使受《憲法》保護權利而執行平臺政策，但透明度等遭質疑

川普政府偷查記者通聯紀錄遭揭發

- 雖然政府索取個資通常是透過法院命令或搜查令，但爆出川普時期司法部偷查記者和政界人士等通聯紀錄

42

台灣人權促進會
Taiwan Association for Human Rights

關注議題
https://www.tahr.org.tw/issues

集會遊行與結社權	言論自由
移民、難民、無國籍	人身自由
居住權與反迫遷	憲政改革
隱私權	企業與人權
政府資訊公開	司法人權
人權教育	原住民權利
新冠肺炎（COVID-19）	國際公約與人權機制

其它(中國人權、性別平等、勞工、轉型正義、國際聲援...)

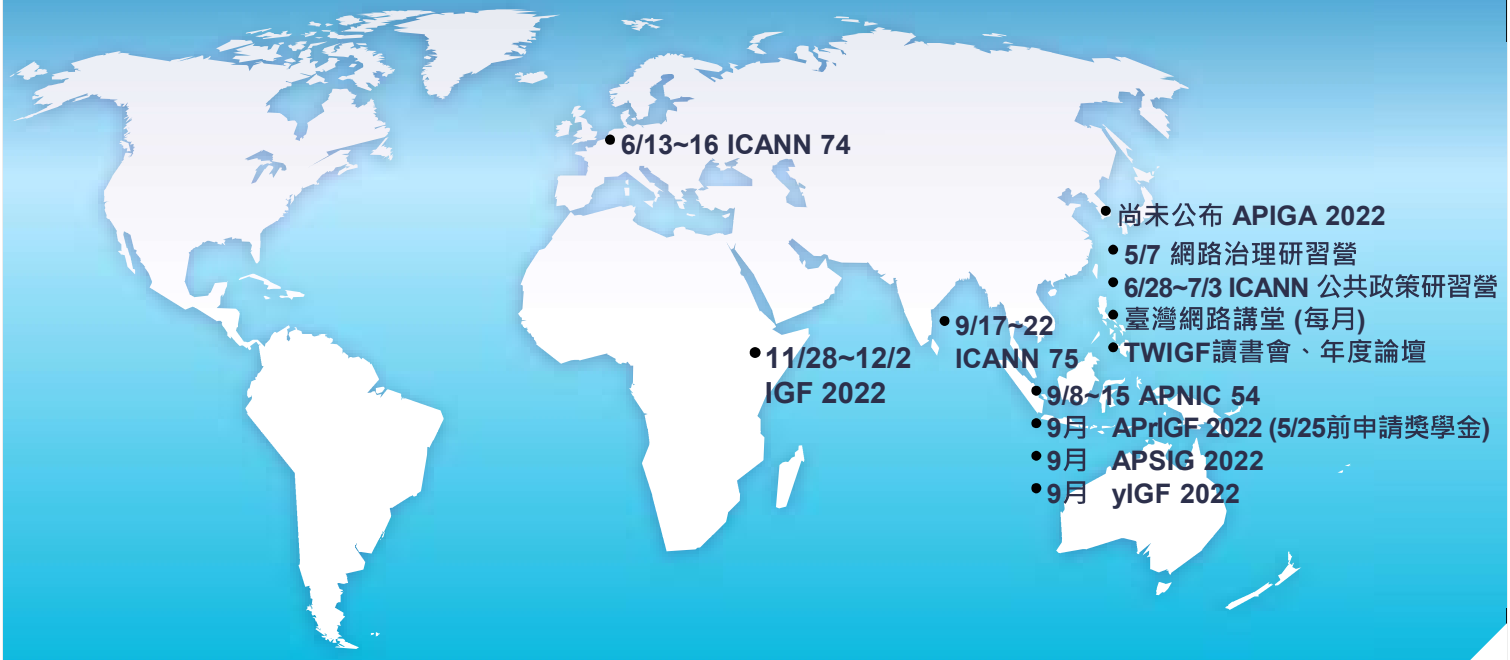
結語

6

網路自由有賴全民共同捍衛
網路治理需要大家共同參與



2022年網路治理參與機會



※ 可參考學員手冊--附件2

45

為何理想的數位世界如此重要？

我們如何在數位領域裡，適當和負責任地將數位人權理念推廣至全球各地，俾讓更多人享有數位人權。我們每一個人都有責任成為一個良好的數位公民，共同打造一個更理想的數位世界。

46

THANKS!

Any questions?





平台規範的時代來臨了？

從MUSK + Twitter談起

曾更瑩律師

2022網路治理研習營

May 7, 2022

四月時，發生了一件結合本人兩大興趣，併購&網路治理的大事

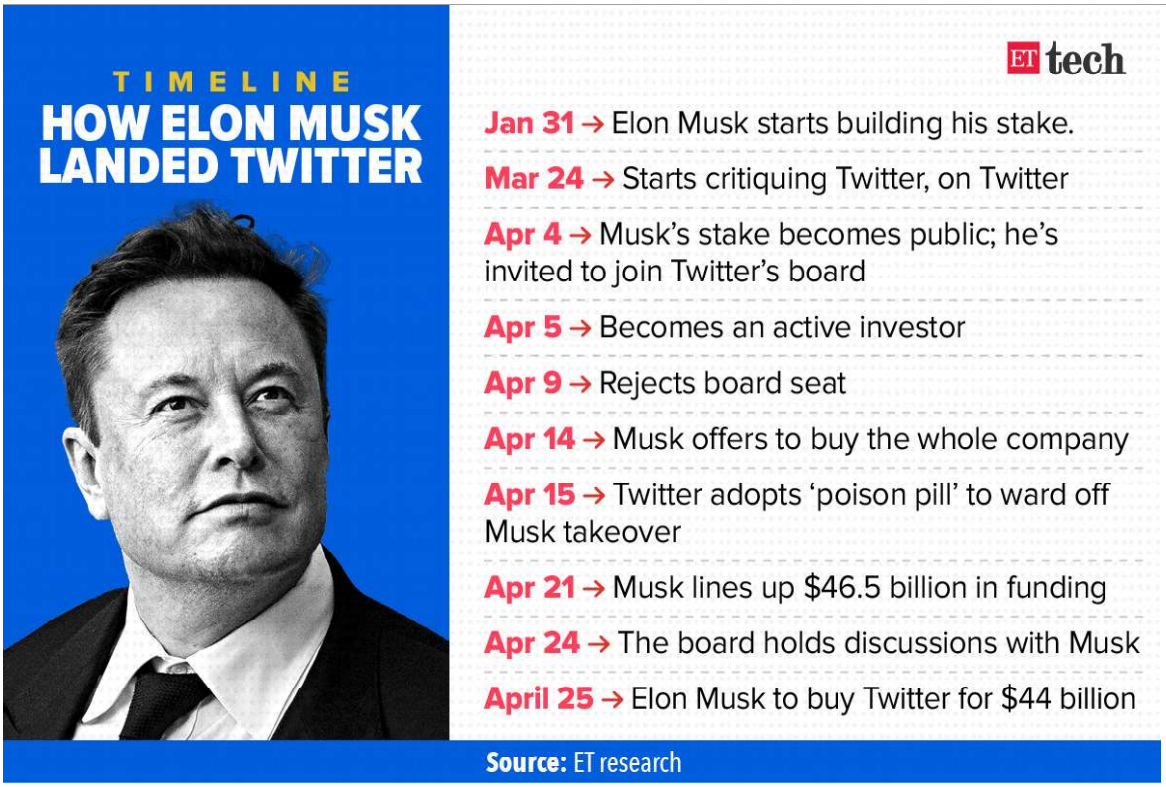


Elon Musk talks Twitter, Tesla and how his brain works — live at TED2022

YouTube • TED

Chris Anderson interviewed Musk on April 14, 2022





https://economictimes.indiatimes.com/tech/technology/timeline-how-elon-musks-twitter-takeover-unfolded/articleshow/91100011.cms



Musk 四月二十五日的推文

Musk 收購Twitter的宏願

- ❖Making the algorithms open source to increase trust
- ❖Defeating the spam bots
- ❖Authentcating all humans
- ❖Inclusvie arena for free speech
- ❖Political neutral

結果是：Twitter逃難潮（US）Facebook跳船潮（TW）

Musk + Twitter引發平台治理問題

European Council
Council of the European Union

About the institutions | Topics | Meetings | News and media | Research and publications | EN

Home > Press > Press releases

Council of the EU Press release 23 April 2022 02:17

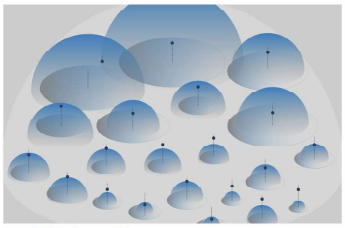
Digital Services Act: Council and European Parliament provisional agreement for making the internet a safer space for European citizens

An important step has been taken today with the provisional political agreement reached on the Digital Services Act (DSA) between the Council and the European Parliament.

In terms of ambition, the nature of the actors regulated and the innovative aspect of the supervision involved, **the DSA is a world first in the field of digital regulation.**

The DSA follows the principle that **what is illegal offline must also be illegal online.** It aims to protect the digital space against the spread of illegal content, and to ensure the protection of users' fundamental rights.

Infographic - Digital Services Act



See full infographic

Scope

The DSA will apply to all online intermediaries providing services in the EU.

The **obligations** introduced are **proportionate to the nature of the services concerned and tailored to the number of users**, meaning that **very large online platforms (VLOPs) and very large online search engines (VLOSEs) will be subject to more stringent requirements**. Services with more than 45 million monthly active users in the European Union will fall into the category of very large online platforms and very large search engines.

正當馬斯克等待Twitter回應他的offer之時，在歐盟的平行宇宙，正上演著DSA即將生效的老戲碼

但這次馬斯克收購Twitter打的主要是言論自由牌

Free speech absolutism

Someone you don’t like says something you don’t like --- the free speech defined by Musk.

但是Musk也說，free speech應該要在法律所規定的界線內，雖然他對於仇恨言論或是不當言論的判斷閃爍其詞

Content Moderation – Lossen or Tighten?

- ❑The draft Digital Servivce Act of EU (DSA) has been trying to impose more content moderation obligations on platforms since 2020
- ❑Notice/Awareness and Take Down – Basic Safeharbour Rule
  雖然DSA強調：
  - 主動採取行動不會喪失主張免責之資格
  - 平台沒有主動監控內容的義務
- ❑業者批評可能引發寒蟬效應

Online Platform的義務與責任

- Where an information society service is provided that consists of the storage of information provided by a recipient of the service the service provider shall NOT be liable for the information stored at the request of a recipient of the service **on condition that** the provider:
- (a) does NOT have **actual knowledge** of illegal activity or illegal content and, as regards claims for damages, is NOT aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (實際上不知情)
- (b) upon obtaining such knowledge or awareness, acts **expeditiously to remove or to disable** access to the illegal content. (知道後立即移除)

13

Additional Content Moderation Obligations

- Order to act against illegal content
- Order to provide information (users' personal information)
- Online platforms' obligation to report suspicions of criminal offences
- Online platforms will have to explain clearly why they have removed illegal content as well as give users the ability to appeal such takedowns. The DSA itself does not define what content is illegal, though, and leaves this up to individual countries.
- Large platforms will also have to introduce new strategies for dealing with misinformation during crises (a provision inspired by the recent invasion of Ukraine).

Risk Assesement

Onlne platforms shall analyse systemic risks they create and to carry out risk reduction analysis.

This analysis must be carried out every year and will enable continuous monitoring aimed at reducing risks associated with:

- dissemination of illegal content
- adverse effects on fundamental rights
- manipulation of services having an impact on democratic processes and public security
- adverse effects on gender-based violence, and on minors and serious consequences for the physical or mental health of users

然而**Musk** 和 EU 對於演算法的看法似乎有點雷同

Make Algorithm Open Source

No behind the scenes manipulation

- 馬斯克希望Twitter如何決定promote or demote a certain content應該公開透明
- 強調不論是利用演算法或人為方式，都不可以幕後操縱 Twitter平台上的內容
- Increase trust on Twitter is important!
- Defeat the spam bots or die trying!

Practical? 許多人紛紛評論

- 演算法即使公開，一般使用者也不可能理解
- 演算法電腦程式本身不重要，重要的是餵什麼資料給訓練演算法
- 演算法乃係平台的營業秘密，平台不可能公開
- 演算法一旦公開，內容農場、假訊息散布者等更容易帶風向、駭客入侵更容易

How about DSA?

- **Transparency on terms and conditions:** the tool used for content moderation (such as remove or demote illegal content) shall be disclosed to the user, including algorithmic decision-making and human view.
- **Assessment and audits**. VLOPs will be required to do annual assessment and audits of how their algorithms affect democracy, human rights, and the physical and mental health of minors and other users.
- **Dark patterns:** For online platforms and interfaces covered by the DSA, the co-legislators have agreed **to prohibit misleading interfaces known as 'dark patterns'** and practices aimed at misleading users.
- **Recommender Systems Transparency:** Requirements for the parameters of recommender systems have been introduced in order to improve information for users and any choices they make. **VLOPs and VLOSEs will have to offer users a system for recommending content that is not based on their profiling.**
- **Protecting minors online:** Platforms accessible to minors will have to put in place special protection measures to ensure their safety online **in particular when they are aware that a user is a minor. Platforms will be prohibited from presenting targeted advertising based on the use of minors' personal data as defined in EU law.**
- **Online advertisng transparency:** The main parameters used to determine the recipient to who the adverisement is displayed.
- **Inspection and disclosure:** The competent authorities in the EU countries have the power to conduct on-site inspection on VLOP and may order disclosure on the algorithm being used.

台灣即將制定數位通訊傳播服務法

- NCC在2021年底發布新聞稿公布數通法草案原則
- NCC說明，數通法草案參考DSA等國際相關法制規範，以數位通訊傳播中介服務提供者為規範對象，並以自律先行，強化規管對象之義務及資訊透明度，並加入他律、法律等公私協力概念與作為，以彰顯多方參與的網際網路治理（Internet Governance）精神；該草案共11章，規範要項包括：基本權利維護、數位通訊傳播中介服務提供者之免責要件、數位通訊傳播中介服務提供者之義務、線上平臺及指定線上平臺之義務、公私協力合作、專責機構之設立及相關罰則等。
- 數通法草案要求中介服務提供者提出透明度報告、通知及回應等相關義務。此外，為強化對使用者之保障，該草案要求線上平臺如移除使用者貼文，或對使用者處以停權等相關限制行為時，必須說明原因，並提供異議機制，以保障使用者權益。更重要的是，草案課予業者將資訊限制登載於共同資料庫的資訊透明義務。
- NCC原訂三月間發布草案搜集各界意見，六月送行政院

Musk 主張 Authentcating all humans

是實名化的意思嗎？

TED 主持人Anderson 提問: How come we can allow Twitter be owned by the

Richest Person

in the world?

Musk 幽默回答，那你怎麼不問問馬克祖柏克？他擁有Facebook 、IG、WhatsApp 三大平台，而且主管這些平台之營運
但，我不會去edit any tweets

法律是否允許線上平台被少數人收購？

- 今年三月二十四日，EU通過DSA的姐妹法案，Digital Market Act (DMA)，其中對於被認定為守門員(Gatekeeper)的核心線上平台(Core platform service)課以各種義務，確保公平競爭：
  例如不得任意將自不同服務所蒐集到的個資結合利用
- DMA對於大型線上平台之收購加以限制，需事前向結合主管機關申報，惟馬斯克現在所經營的事業無一屬於被規範的大型線上平台。
- DMA並沒有對於線上平台之所有權有特別規定

美國對於Twitter Deal在競爭法上的審查

- FTC 近期對於Musk在公開宣布收購Twitter前收購 Twitter 9%股權的行為展開調查，確認Musk是否漏未向FTC申報收購Twitter 9%股權。
- 如果 Musk前收購 Twitter 9%股權並非passive investment，Musk應向FTC申報，不過，Musk向SEC所提交的 filing說明他是被動的投資人

完成交易還是可能需要Anti-trust Filng

- 許多美國法學者發表評論，表示本件交易要完成，還是有可能要向美國競爭法主管機關提出anti-trust filing，並於申報期間經過，主管機關未提出異議後，始得進行交割。
- 若干學者認為，馬斯克的事業與Twitter並無競爭關係，即使需要提出結合申報，主管機關也不至於提出異議
- 拜登政府新推出的anti-trust政策比較著重於大型線上平台水平競爭之管理
- 也有學者認為馬斯克經營的Starlink提供網際網路接取服務，應該算是與Twitter有垂直競爭關係，但是如此一來，因為所有公司都有使用網際網路，都會跟提供網際網路接取服務的業者處於垂直競爭關係

平台的所有權是否應有特殊規範？

- 傳統媒體受有所有權限制
- 例如，台灣規定
  - 黨政軍不得涉入媒體
  - 廣播電台、無線電視不得有外資
  - 有線電視、衛星電視有外資比例限制
  - 新聞紙、無線電視或無線廣播事業之股東持股或與其相關企業共同持股達各該事業總股數百分之五十以上者，不得收購廣播電台或無線電視之股權
  - 媒體收購均受到主管機關嚴審、審查資金來源、防止大財團壟斷媒體（異業結合）、也防止過多媒體集中在同一集團手上（水平結合）
- 但是社群媒體或其他線上平台不受以上法規規範，主管機關依照公平交易法審核
- 按照DMA，平台收購一律受規管，平台可能無法收購另一個平台
- 是否有制定新規則之必要？

你是否贊成MUSK + Twitter ?

Thank you for listening.

Internet Policy

俄烏戰爭對網路治理規則的影響

Kenny Huang, Ph.D. 黃勝雄博士

2022 May 7

Internet Governance

網路治理軌跡

- 階段1：軍事發展 (1957-1970s)
  - DARPANet
- 階段2：學術研究 (1970-1990s)
  - TCP/IP
- 階段3：商業發展 (1990s-2000s)
  - WWW
- 階段4：大量媒介 (2000s-2010s)
  - WSIS
- 階段5: 所有人及所有物件 (2010s-2020s)
  - New internet complexity (IoT, AI, Big data..)

3

資訊社會發展

- 農業社會 (封建主義)
  - 要素： 土地與勞工
  - 君主制度
- 工業社會 (資本主義)
  - 要素: 土地、勞工、資本
  - 權力分散：行政權、司法權、立法權
  - 權力移轉：從皇宮移轉國會
- 資訊社會 (數據主義)
  - 要素: 土地、勞力、資本、數據
  - 權利分散: 決策權高度分散化
  - 權力移轉: 從政府治理模式移轉至多層及多方利害關係人治理模式

4

Internet 特性

- 技術架構
  - 植基於端點對端點原則(end-to-end)之分散網路組合的網路
- 資源
  - Protocols, names 及 numbers 盡乎無限資源 (IPv6), 無領土概念並可重複使用資源
- 法規
  - 在本國法、國際法之上的程式碼規範、 自律、及他律的混合型態

Protocols 及組織

Protocols

- 1969 RFC (Steve Crocker)
- 1971 @ (Roy Tomlinson)
- 1974 TCP/IP (Vint Cerf, Bob Kahn)
- 1982 SMTP (Jon Postel)
- 1985 DNS (Paul Mockapetris & Postel)
- 1991 HTML (Tim Berners-Lee)

組織

- 1975 IAB
- 1986 IETF
- 1989 IANA
- 1992 ISOC
- 1992 RIPE
- 1993 APNIC
- 1993 W3C
- 1998 ICANN
- 1999 TWNIC
- 2004 NRO
- 2005 IGF

DNS: 網路空間領域

- IP 位址
  - IPv4 : 32 bits, 43 億
  - IPv6 : 128bits, 無限
- 網域名稱
  - gTLD 通用頂級網域
  - ccTLD 國碼頂級網域
- 根伺服器 root server
  - 13 字元 (A-M)
  - 美國政府角色 : 授權頂級網域 zone file發布
  - 2016 年IANA 監理權移轉
    - Protocol : IETF
    - Number : RIRs
    - Names : ICANN 代管
- 管理
  - 1998年前: Jon Postel 管理 IANA, NSI 代管 root zone
  - 1998年後: root zone 改由美國政府委託 Versign 代管

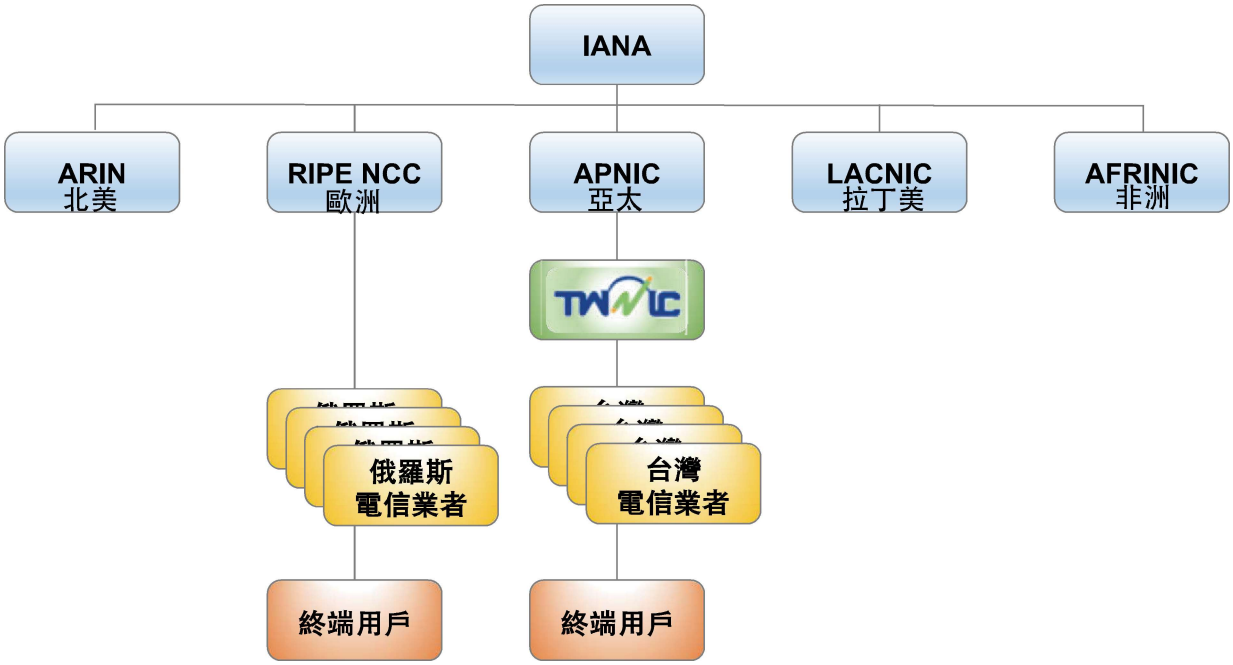
網路治理概念

- 1991 Tim Berners-Lee (WWW)
  - 我們設計的網路是研究一種規則，讓電腦可以相容地共同運作。就如同社會規範就是研究一種規則讓人們可以和諧地共同工作。
- 1992 Dave Clark (IETF)
  - 我們不相信國王、總裁、及投票。我們相信粗略共識、事實依據、及可執行的程式碼
- 1996 John Barlows 網路獨立宣言
  - 我來自網路空間，心靈所在之處。我代表未來向政府提出宣言，希望你讓我們獨自留在網路空間，在網路空間你並不受到歡迎，網路空間沒有你的管轄權。
- 1998 Lawrence Lessig (Code is the Law)
  - 我們必須了解在網路空間如何利用程式碼規範軟體行為, 我們可以經由設計、發展出我們認同價值的網路空間。或者我們放棄設計符合社會價值的網路空間。程式碼不會憑空產生，它只能透過我們設計才能產生。

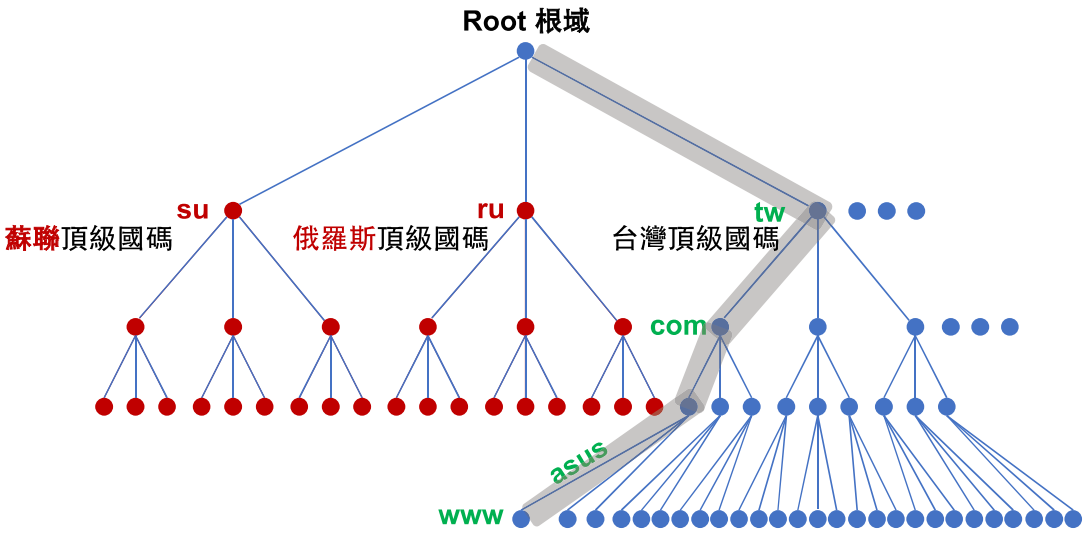
ICANN (1998)

- ICANNs mandate
  - Root Server
  - Domain names
  - IP addresses
- ICANN架構
  - 董事會
  - 支持組織 (supporting organizations)
    - gNSO, ccNSO, ASO
  - 諮詢委員會
    - GAC, ALAC, RSSAC, SSAC, TLG)
  - 究責機制
    - AoC Review, Reconsideration ..
- ICANN 運作原則
  - 安全與穩定 Security & stability
  - 由下而上政策制定機制
  - 多方利害關係人模式

IP位址發放結構



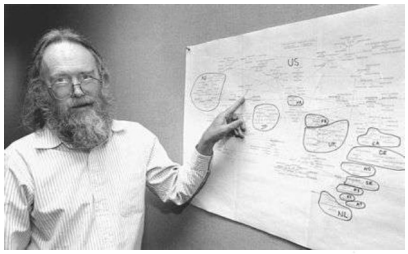
網域名稱結構

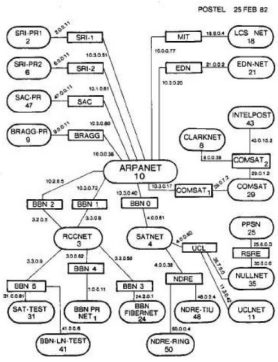


11

Jon Postel 與根伺服器管理機構

name		Operator 所有權人
A-Root		Verisign, Inc.
B-Root		Univ. of Sothern California, Information Sciences Inst.
C-Root		Cogent Communications
D-Root		Univ. of Maryland
E-Root		NASA Ames Research Renter
F-Root		Internet Systems Consortium （ISC）
G-Root		U.S. DoD Network Information Center
H-Root		U.S. Army Research laboratory
I-Root		Netnod
J-Root		Verisign, Inc.
K-Root		RIPE NCC
L-Root		ICANN
M-Root		WIDE project & JPRS





12

Jon Postel 變更根伺服器路徑



8 位根伺服器管理者(組織)

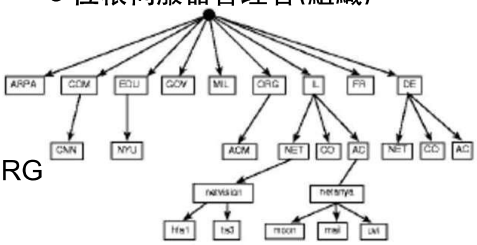


1998.01.28





IANA組織
DNSROOT.IANA.ORG



美國政府：
Postel 變更 root server 路徑沒有經過任何人授權同意。這次事件引起政府高度關注。美國強烈要求root server 路徑指向必須回復更動前的路徑指向。

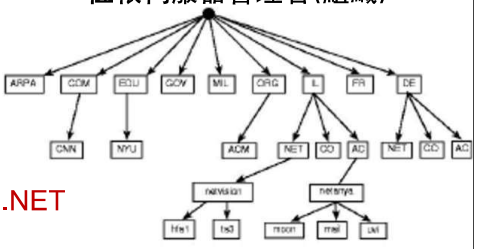
一週後, NTIA 公布改善網路域名及位址管理新計畫。
同年9月 ICANN 正式成立



4位根伺服器管理者(組織)

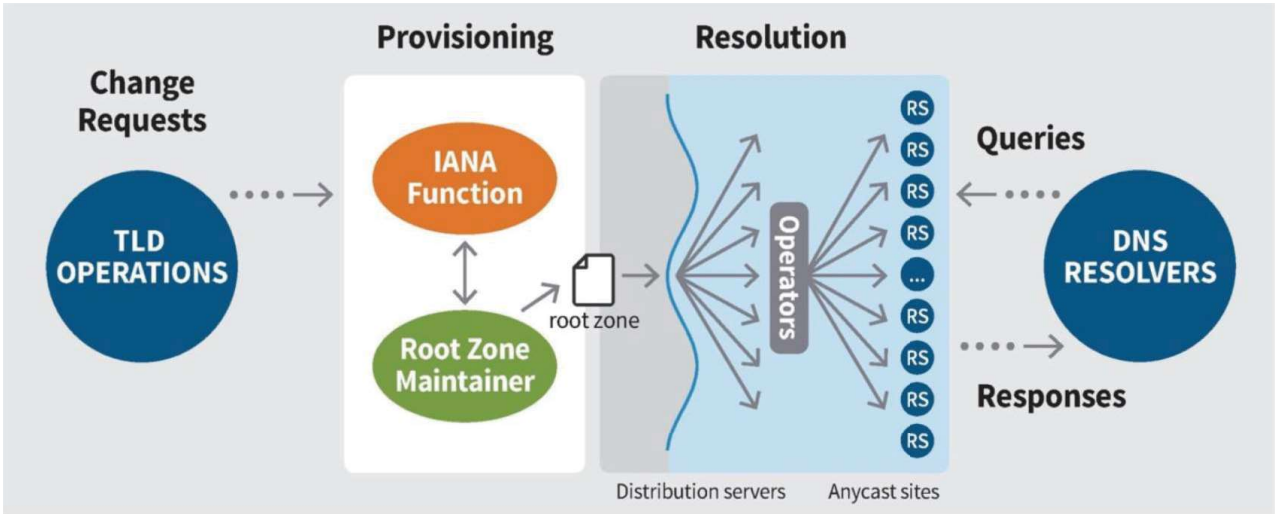


NSI 公司
A.ROOT-SERVERS.NET



13

網域名稱註冊與解析架構



14

網際空間主軸演化

Previous Decades
過去數十年主軸

Infrastructure

基礎建設

Last Decade
過去十年主軸

Technical Innovations

技術創新

Next Decade
未來十年主軸

Policy, Regulations & Governance

政策法規、治理

15

網路治理模式

多方利害關係人模式
Multistakeholder model

- ICANN
- 區域網路資訊中心 RIRs
- 網路標準機構 IETF
- ccTLDs, gTLDs, Registrars



多方利害關係人依其原則、規範、政策程序推動網際網路之發展與使用

有限介入模式
Limited intervention

- 英國調查權力法 (investigatory Powers Act)
- 美國 41條規則 (rule 41)
- 澳洲反加密法 (anti-encryption law)



網際主權模式
Cyber sovereignty

- 中國防火長城
- 俄羅斯網路獨立法
- 高密度網路審查國家



政府訂定網際空間範疇，實施控制措施以主張其網際空間管轄權

16

Cyber Jurisdiction Case: China Intranet



中國 Internet 非常類似企業 Intranet, 並且具下列優點

1. 中國可以強制網路審查權
2. 一旦面臨外部威脅，中國隨時可以切斷國際網路，並維持Internet局部接取功能
3. 國內訊務永遠不會離開國境

中國網路治理可跨越管轄權

- 一帶一路跨境基礎設施
- 中國電信、移動全球市場
- 華為、抖音、騰訊平台

17

Sanctions

18

Sanctions

- Definition
  - Political trade tools put in place against targeted countries with the aim of restoring international peace and security.
  - Change the behavior of the target country's regimes individuals or groups in a direction which will improve the situation of that country. Such as an arms embargo and a ban on the export on certain items could be aimed at supporting a peace process.
- Types of sanction
  - Country based sanction : embargos to the actual countries
  - List-based sanction: individuals such as terrorists, traffickers, corrupt leaders
  - Target-based sanction: individuals or organizations
- The most frequently applied sanctions
  - Sanctions on exporting arms and associated technical assistance, training, financing
  - A ban on exporting equipment that might be used for internal repression
  - Financial sanctions on individuals, government bodies and associated companies.
  - Travel ban on named individuals

19

Sanction regimes

- Financial sanctions
  - Prohibiting the transfer of funds to a sanctioned country
  - Freezing the assets of a government, companies, or residents
  - Prohibiting providing other financial services, such as insurance
- Sanction regimes
  - EU: uphold international security order; defending human rights and democracy
  - UN SC: threats to peace; security and stability; violations of human rights
  - US OFAC (Office of Foreign Assets Control)



46% Global GDP

20

Non-compliance to Sanctions

- It is a criminal offence to breach a sanction without authorization from the appropriate sanction regime
- Non-compliance to sanctions will be a serious threat to national security and foreign relations
- Breaching sanctions can face severe legal repercussions
  - Fines range up to millions of dollars
  - Prison sentences for the liable parties involved if the breach is considered to be taken place willfully.



21

Do sanctions work ?

- Sanctions are playing a growing role in modern geopolitics
- Short term sanctions have an effective outcomes
  - Evidence shows that the longer sanctions last the less likely they are to succeed

22

Sanctions and Internet Governance

ICANN and RIPE NCC

- 烏克蘭GAC代表請求 ICANN 實施俄羅斯的制裁. 關閉俄羅斯頂級網域名稱.ru, .рф, .su解析
- 關閉俄羅斯根伺服器



- 烏克蘭要求 RIPE NCC 取消核發給俄羅斯的所有IPv4與IPv6位址。



But





- ICANN移除 .su，說明因.su 已不在ISO3166-1, 不再符合 ccTLD 資格
- 依據註冊商授權合約第3.7.5.1條，烏克蘭無力付款續約可免除取消域名
- 三十多位ICANN現任前任董事及網路主導者共同發表網路治理制裁原則
- 歐洲代管.UA 烏克蘭頂級網域
- CENTR歐洲國家頂級網域管理局拒絕俄羅斯會員資格
- Godaddy 停止銷售.ru網域
- CA 不接受俄羅斯憑證更新

- 凍結俄羅斯最終受益人UBO之IP位址, 包含俄羅斯主導電信公司
- LINX 交換中心斷網
- GÉANT研究網路斷網
- COGENT國際轉訊斷網

25

網路治理制裁原則 Multistakeholder Imposition of Internet Sanctions

- 切斷國家與Internet連結的網路制裁不符合比例原則並且不適當
- 網路制裁有效性應該被評估
- 網路制裁必須精確，將無法預期結果可能性最小化
- 可將軍事與宣傳機構基礎設施視為網路制裁目標
- Internet 基於跨國特性及多方利害關係人治理架構，不適合執行網路制裁
- 政府嘗試操作網路治理機制實施網路制裁是不適當
- 部分適當有效且具體措施，網路治理社群於網路制裁審議過程可列入考量。
- 包含建立有效網域名稱與IP位址制裁清單，制裁清單可以列入限制接取之制裁方案，比照網路管理者阻擋垃圾郵件或惡意軟體方式執行。
- 建立多方利害關係人審議程序，制裁俄羅斯軍事及宣傳機構IP位址與網域名稱，並為未來面臨嚴重性急迫性決定奠定基礎。

26

外國資產控制辦公室網路制裁令



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

OFFICE OF FOREIGN ASSETS CONTROL

Russian Harmful Foreign Activities Sanctions Regulations
31 CFR part 587

GENERAL LICENSE NO. 25

Authorizing Transactions Related to Telecommunications and Certain Internet-Based Communications

(a) Except as provided in paragraph (c) of this general license, all transactions ordinarily incident and necessary to the receipt or transmission of telecommunications involving the Russian Federation that are prohibited by the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587 (RuHSR), are authorized.

(b) Except as provided in paragraph (c) of this general license, the exportation or reexportation, sale, or supply, directly or indirectly, from the United States or by U.S. persons, wherever located, to the Russian Federation of services, software, hardware, or technology incident to the exchange of communications over the internet, such as instant messaging, videoconferencing, chat and email, social networking, sharing of photos, movies, and documents, web browsing, blogging, web hosting, and domain name registration services, that is prohibited by the RuHSR, is authorized.

- 依據俄羅斯有害外國活動制裁法(RuHSR)，除通用許可規定外，禁止所有涉及俄羅斯發送或接收之電信服務。
- 除通用許可規定外，禁止美國或美國人直接或間接向俄羅斯出口、銷售、提供服務、提供軟體、硬體、及禁止提供網際網路交換涉及技術，例如即時軟體、視訊會議、聊天對話、電子郵件、社群網路、照片分享、電影、文件、網頁瀏覽、部落格、網站代管、網域名稱註冊服務等。

Internet Governance Regime and Sanctions

Internet Resources	Activity	Sanctioned ? US,EU,G7
IP addresses	new registration	yes
	in use	no
	transfer	yes
Domains	new registration	yes
	in use	no
	transfer	yes

Internet Governance Regime and Sanctions

Internet Resources	Sub element	Sanctioned ? US,EU,G7
IP addresses	RPKI RoA	?
	RPKI validation	?
	BGP	?
	Connectivity	yes
	Peering	yes
	Transit	yes
Domains	DNSSEC	?
	Email	?
	Resource records	?
	DNS	?
	Resolvers	?
	DANE	?
	Hosting	yes

29



30

附錄三：優秀學員參與 APrIGF 2022 會議摘要報告

國家通訊傳播委員會
「網路治理國際趨勢研析與人才培育」
委託研究採購案

APrIGF 2022 參與摘要報告

報告人：洪 O 廷（2022 網路治理研習營優秀學員）

中華民國 111 年 10 月

目　錄

目　錄 I

圖目錄 III

一、 會議資訊 1

二、 參加場次 3

三、 場次摘要 6

（一） S13. 從 COVID-19 到普選，該如何對抗造假資訊：多方利害關係人的數位素養 vs 立法與審查 6

（二） ARrIGF 開幕式 8

（三） S08. 朝向節能網路 –針對網路的永續性和能源效率，展開政策與策略制定的多方利害關係人對話 12

（四） S21. LEO 衛星叢集，是否能提供更好的網路接取與網路強韌性 18

（五） S02. 新冠疫情期間高等教育身心障礙學生的數位近用與網路接取 14

（六） S11. 回應後疫情時代的數位人權變動 18

（七） S03. 在網路治理議題上強化身障人士的發聲 18

（八） S19. 提升網路韌性，建立可本地存取的雲端服務 21

四、 參與心得 25

附件：APRIGF 2021 完整議程表 26

圖目錄

圖 1. 主持人與與談人會後合影 7

圖 2. OPENING PLENARY 會後合影 11

圖 3. S08 台灣數位部長唐鳳與談時的現場畫面 13

圖 4. S21 主講人呼籲大家一同深入瞭解 LEO 對於網路社群的影響 24

圖 5. S02 場次現場畫面 15

圖 6. S11 場次會議結束前的畫面 17

圖 7. S03 場次中學員公開發言分享自身經驗 20

圖 8. S19 場次畫面截圖 22

一、 會議資訊

2022 年 APrIGF（Asia Pacific Regional Internet Governance Forum，亞太區網路治理論壇）係採用混合型（hybrid）會議模式，於 9 月 12 至 14 日在新加坡君悅飯店舉辦，並同步以線上方式辦理。APrIGF 2022 的大會主題為「以人為本：展望一個具有包容性、永續性、被人們所信任的，由社群帶領的網際網路」(People at the Centre: Envisioning a community-led Internet that is inclusive, sustainable and trusted)，對照 APrIGF 2021 「邁向包容、永續及可信任的網路」(Towards an Inclusive, Sustainable, and Trusted Internet)，可見大會核心雖然並未改變，但更加地強調了「以人為本」的精神。今年度的討論主題如同去年，包括：包容、永續，以及信任共 3 類，惟經歷疫情的挑戰，人們逐漸回復正常生活的同時，APrIGF 2022 試問大家，是否該審思過去幾年疫情下科技對人們的影響、該如何讓公共福祉與以人為中心的決策流程重回檯面，取回人與人之間更加真實的連結。討論主題簡述如下：

- 包容（Inclusion）

「包容」關乎於採取行動促進網路的近用與公平性，不僅是聚焦在網路的接取，而更應該考量使用者是否具備使用網路的技能。多方利害關係人決策流程確保所有的聲音都能被公平地聽見。亞太地區因為自然環境、地勢的阻礙，讓所有人連上網路已經是一個難關，但 APrIGF 仍希望透過利害關係人們團結起來，確保「沒有人是落單的」(no one is left behind)，並支持人們取得可靠、可負擔的網路連線。APrIGF 歡迎各界針對此議題展開橫跨多個領域的討論。

- 永續（Sustainability）

網路及其相關應用的進化，促進了數位經濟的發展，以及科學、農業、健康與教育的實質進步。「永續」喚起各界深思技術及其創新對於全球的影響及成果。網路對環境有什麼影響？它的靈活性如何？網路相關技術如何幫助我們實現永續發展目標？APrIGF 鼓勵大家提出與永續發展相關的多元觀點，包括網路對於

社會經濟之影響。

- 信任（Trust）

「信任」乃是在安全及人民的基本自由與權利之間取得良好的平衡。網路的安全、穩定及靈活性攸關使用者能否在健全的數位環境中受益。利害關係人必須共同努力建立安全、可靠且值得信賴的網路空間，在不損害使用者安全、個人資料且相互尊重的情況下，實現網路的合理使用。為了維護網路的可信度，政府、企業、公民社會，以及其他利益關係人所扮演的角色及應負擔的責任為何？APrIGF 歡迎各界提出跨部門觀點，探討如何在具備適當安全考量的前提下，平衡網路使用者的需求與權利。

二、學員參加場次

日期	UTC 時間	臺灣時間（同新加坡時間）	議程主題	會議摘要
11 Sep (Sun)	06:00 – 08:30 (2.5 hours)	14:00 – 16:30 (2.5 hours)	Capacity Building Program for Fellows and Newcomers	
12 Sep (Mon)	01:30 – 02:30 (60 mins)	09:30 – 10:30 (60 mins)	S13. Combating Disinformation from COVID-19 to the General Election: Multistakeholder Digital Literacy vs Legislation & Censorship?	✔
	03:00 – 04:30 (90 mins)	11:00 – 12:30 (90 mins)	APrIGF 2022 Opening Plenary	✔
	05:30 – 06:30 (60 mins)	13:30 – 14:30 (60 mins)	S07. Online harassment as tools of exclusion: A discussion on Addressing Online Gender Based Violence Through Community Organised Helplines	
	07:00-08:00 (60 mins)	15:00-16:00 (60 mins)	S08. Towards an EcoInternet – A Multistakeholder Dialogue on Policy Making and Strategising for a Sustainable and Energy Efficient Internet	✔
	08:30-09:30 (60 mins)	16:30-17:30 (60 mins)	S10. Future of Work: Achieving a sustainable gig economy	
	09:30-10:30 (60 mins)	17:30-18:30 (60 mins)	Townhall Session	

日期	UTC 時間	臺灣時間 （同新加坡時間）	議程主題	會議摘要
13 Sep (Tue)	01:30-02:30 (60 mins)	09:30-10:30 (60 mins)	S02. Digital accessibility and connectivity for disabled students in higher education during COVID-19	✔
	03:00-04:30 (90 mins)	11:00-12:30 (90 mins)	APNIC Opening Ceremony and Keynotes	
	05:30-06:30 (60 mins)	13:30-14:30(60 mins)	S11. Responding to changing digital rights priorities in a post-pandemic world	✔
	07:00-08:00 (60 mins)	15:00-16:00 (60 mins)	APNIC Cooperation SIG and APrIGF	
	08:30-09:30 (60 mins)	16:30-17:30 (60 mins)	S14. Digital Resiliency of Civil Society in the context of shrinking Civic Space	
	09:30-10:30 (60 mins)	17:30-18:30 (60 mins)	Townhall Session	
	11:00-13:00 (120 mins)	19:00-21:00 (120 mins)	Welcome Social	
14 Sep (Wed)	01:30-02:30 (60 mins)	09:30-10:30 (60 mins)	S03. Strengthening the disability voice in Internet Governance	✔

日期	UTC 時間	臺灣時間 （同新加坡時間）	議程主題	會議摘要
	03:00-03:30 (30 mins)	11:00-11:30 (30 mins)	S19. Locally Accessible Cloud Service (LACS) for e-resilience	✔
	03:30-04:00 (30 mins)	11:30-12:00 (30 mins)	S21. LEO Satellite Constellations – Will They Bring Better Internet Access and a More Resilient Internet?	✔
	04:00-04:30 (30 mins)	12:00-12:30 (30 mins)	S25. Koo – Empowering Users and Building Cyber Resilience	
	06:00-06:30 (30 mins)	14:00-14:30 (30 mins)	S22. Measuring the Internet protocol parameters for reducing Internet poverty	
	07:00-07:30 (30 mins)	15:00-15:30 (30 mins)	S23. Child Online Safety: A .Kids conversation on creating a Child-centric Internet	
	07:30-08:00 (30 mins)	15:30-16:00 (30 mins)	S24. Assessing investments in surveillance and technology	
	08:30-10:00 (90 mins)	16:30-18:00 (90 mins)	APrIGF 2022 Closing Plenary	

*依日期/時間順序排列

三、 會議摘要

（一）S13. 從 COVID-19 到普選，該如何對抗造假資訊：多方利害關係人的數位素養 vs 立法與審查

會議名稱	S13. 從 COVID-19 到普選，該如何對抗造假資訊：多方利害關係人的數位素養 vs 立法與審查 S13. Combating Disinformation from COVID-19 to the General Election: Multistakeholder Digital Literacy vs Legislation & Censorship?
會議時間（UTC）	2022 年 9 月 12 日 01:30 – 02:30

摘要：

本場次是 APrIGF 2022 第一場會議，更早於 APrIGF 正式開幕。此會議由香港的 Tech for Good Asia 所申請，主持人為史丹佛大學的 Charles Mok 教授，Charles Mok 教授從探問「什麼是打擊造假資訊（disinformation）的最佳方法」起頭。

第一位與談人是 Meta 亞太區造假資訊政策負責人 Alice Budisatrijo 女士，Alice Budisatrijo 女士提及 Meta 在疫情期間對抗造假資訊的困難，一方面要在可靠資訊較為有限的情況下識別哪些消息是造假資訊，另一方面又要避免過度管制用戶，而不成比例地壓縮用戶表達意見的空間。Alice Budisatrijo 女士提及 Meta 透過三種作法對抗造假資訊，首先是「移除有害資訊」，例如針對疫情初期對於病毒的造假資訊；其次是透過與第三方事實查核機構合作，若是事實查核機構確認某些資訊是造假資訊，Meta 則會降低該則資訊的傳播；再者是在相關貼文下方提供專家意見的連結，例如關於疫情的貼文會被加註連結到公衛專家提供的資訊。

第二位與談人 Indriyatno Banyumurti 先生從 ICT Watch 組織在印尼的經驗觸及本次主題，他們在對抗造假資訊上則是採用教育群眾的取徑，例如製作動

畫、舉辦線上課程、虛實混合的工作坊，教育人們辨別造假資訊，此外他們也透過一系列的教育計畫一方面滿足當地人們的需求，另一方面也支持當地藝術家參與其中。

第三位與談人來自 Open Net 和高麗大學的 Kyung Sin PARK 教授提及近期南韓賠償近 140 位過去因為不實言論（false information）而入獄的政治犯，南韓耗費 40 年的時間認識到人們不應該僅因為不實言論而受到刑事懲罰。Kyung Sin PARK 教授強調正是因為人們有空間得以表達自己的意見，真理才能夠越辯越明。

第四位與談人是聯合國兒童基金會的 Rizky Ika Syafitri，Rizky Ika Syafitri 女士提及與印尼政府合作的經驗，該如何在疫情期間建立人們對於疫苗正確的認知，以及向假消息「學習」如何讓資訊變得有趣、吸引人，以培養人們的資訊素養，降低假消息的危害。與此同時，也要注意事實查核機構本身成為造假資訊的攻擊對象，如何保全人們對於事實查核機構的信賴也是值得關注的議題。



圖1. 主持人與與談人會後合影

（二）ARrIGF 2022 開幕式

會議名稱	APrIGF 2022 開幕式 APrIGF 2022 Opening Plenary
會議時間（UTC）	2022 年 9 月 12 日 03:00 - 04:30

摘要：

此次開幕式由 Cheryl Langdon-Orr 女士和 Anju Mangal 女士主持。首先由 Anju Mangal 女士向巴布亞紐幾內亞因地震受災的人民致意，同時感謝巴布亞紐幾內亞派部長級官員參與 APrIGF 2022，此外 Anju Mangal 女士也邀請會眾在短暫的會期中，設想那些無法參與、無法連上網路的人們，並幫助那些即便在會場，仍因為視力、聽力上的困難而需要幫忙的人們，處處凸顯此次「以人為本」的大會核心精神。

第一位致詞者為 Edmon Chung 執行長，Edmon Chung 為 DotAsia 執行長，同時也負責 APrIGF 秘書處營運。Edmon Chung 執行長不僅感謝新加坡再度協助 APrIGF 舉辦，也向贊助者和協力組織致謝，尤其是擔當共同舉辦之責的 APNIC。Edmon Chung 執行長也強調青年參與的重要性，特別是亞太區 yIGF 作為歷史最長的青年網路治理倡議，對於亞太區域社群的多元性與參與多有貢獻。

第二位致詞者為代表亞太區青年網路治理論壇（yIGF）的 Jenna Fung，致詞中提及 APrIGF 2022 會前 yIGF 舉辦的青年工作坊，25 位實體參與和 21 位線上參加者，橫跨 13 國家，論及演算法歧視、網路犯罪、元宇宙對於人們的衝擊等議題。「No one left behind」，yIGF 嘗試在不拋下任何一個人的前提下，促進對於網路的包容性、信任與永續發展的討論。

第三位致詞者 Paul Wilson 先生為 APNIC 的 Director General。Paul Wilson 先生提及此次 APrIGF 和 APNIC 的參加者組成多元性和扮演網路治理地區性連結的重要性。Paul Wilson 先生強調一方面要維持以人為本的精神，另一方面也要保持網路的可擴充、彈性、相容性和韌性。Paul Wilson 同時提及多方利害關

係人治理模型是網路能有今日發展的關鍵。

第四位致詞者是來自聯合國秘書長 Envoy on Technology 辦公室的 Amandeep Singh Gill。其提及 APrIGF 對於促進網路政策對話的重要性和多方利害關係人模型的有效運作。Amandeep Singh Gill 先生論及網路如何緊密地嵌合在人們日常的生活中，而如何建立開放、自由、安全的網路也是聯合國秘書長近期籌備的 Summit of the Future 中所要觸及的範疇。雖然聯合國運作是由成員國所領導的，但 Amandeep Singh Gill 先生也同意網路從設計之始就是依照多方利害關係人模型治理，因此也應該確保如此的運作機制和聯合國的運作模式相互連結。

第五位致詞者是新加坡通訊及新聞部部長 Janil Puthucheary 博士。Janil Puthucheary 博士提及網路改變人類社會的各種面向，例如降低了跨國合作的成本，但同時也使得某些未能近用網路的人形同被世界所拋下，網路的流動性也是治理層面上的一大難題，Janil Puthucheary 博士認為透過持續深化討論，才能帶領網路社群度過一次又一次的難關。

第六位致詞者是聯合國 IGF 秘書長 Chengetai Masango 先生。其提及過去兩年多來新冠疫情對於世界的影響，而網路則扮演了社會與經濟的驅動引擎，然而也使得沒有網路接取與近用可能的人們失去了享有基本權利與有尊嚴地活下去的機會。Chengetai Masango 先生期待未來的網路，不論在近用、可負擔、安全性與保密性都能更甚以往。Chengetai Masango 先生強調聯合國全力支持人們參與 IGFs 論壇以強韌網路與網路政策治理也感謝 APrIGF 扮演地區性的重要角色，創造人們能夠交流、產生交集的場域。

緊接著主持人 Anju Mangal 女士開展 APrIGF 2022 Opening Plenary 主題討論「People-centered Internet – How do we get it right?」。

第一位與談人是巴布亞紐幾內亞通訊及新聞部部長 Hon. Timothy Masiu 先生。Hon. Timothy Masiu 先生提及近期的地震提醒人們建立強韌網路，尤其在網路接取上的重要性。如巴布亞紐幾內亞正在建立數位基礎建設的步道上，不僅政府，也和資訊與通信科技（Information and Communication Technology，簡

稱 ICT）產業緊密合作，期望能在 2027 年建立全國跨地區的網路接取，特別是山區、偏遠地區和學校與醫療院所。

第二位與談人是來自有「東南亞的 Uber」之稱的運輸媒合與外送平臺 Grab 的 Ilaria Chan。Ilaria Chan 女士提及 Grab 最初嘗試解決人們在馬來西亞搭乘計程車時的安全疑慮，後來延伸到針對未能近用傳統金融體系的弱勢司機的微型金融，近期則是在新加坡針對疫情期間的小型攤販提供網路上架、針對人們微型保險需求提供服務。Ilaria Chan 女士認為即便在新加坡有極高的網路覆蓋率，仍然需要提升人們使用網路的技能，而「human-centered Internet」正是解決市井小民的日常問題。

第三位與談人是 Josh Tseng，來自新加坡非營利組織「Digital Accessibility Services」，Josh Tseng 提及自身有視力障礙，原先認為自己身為弱勢，無法改變社會的運作，直到在大學受到學校的啟發，發覺自己確實能有意義地參與政策的討論，促進身心障礙近用網路。

第四位與談人是來自亞洲互聯網聯盟/Meta 的 Sarim Aziz 先生。Sarim Aziz 先生談到新冠疫情加速亞太地區數位化的腳步，但同時，也使得人們在網路面前變得脆弱，想像在疫情高度警戒時期的封城中，若是缺乏網路，將會是如何地手足無措。Sarim Aziz 先生論及理想中 Metaverse 一方面提供前所未有的機會，但也應該像 TCP 當初制定一般，並非由特定公司、個人所擁有，而是一個普世、通用的標準。此外，其亦提及「Inclusive Internet Index」，由 Meta 所倡議，評價各個地區的網路可得性、可負擔性、可近用性（Readiness）和相關性（Relenvance），後者的可近用性談論人們是否有足夠的網路素養使用網路，相關性則是對當地人們、當地服務、當地社群而言，網路是否有扮演重要角色。

第五位與談人是 ICANN 的 Jia Rong Low，Jia Rong Low 先生提及 ICANN 在維護「網路道路」上的職責，雖然不若元宇宙等熱門議題吸引人，但是網路運作的重要基石，其中包含 IP、Domain Name 和網路協定，也是傳統上網路治理討論的範疇。Jia Rong Low 接著論及國際化域名議題，在決定納入各式語言進到域名系統中時，ICANN 需要和各個語言的當地社群討論哪些字、詞組

應該或不應該納入系統之中，其中，Jia Rong Low 先生也感謝亞太區的社群參與，使得此項浩大工程得以完成。



圖2. Opening Plenary 會後合影

（三）S08. 朝向節能網路 – 針對網路的永續性和能源效率，展開政策與策略制定的多方利害關係人對話

會議名稱	S08. 朝向節能網路 – 針對網路的永續性和能源效率，展開政策與策略制定的多方利害關係人對話 S08. Towards an EcoInternet - A Multistakeholder Dialogue on Policy Making and Strategising for a Sustainable and Energy Efficient Internet
會議時間（UTC）	2022 年 9 月 12 日 07:00 – 08:00

摘要：

本會議由 Dot Asia 執行長 Edmon Chang 主持。

第一位與談人是台灣新任數位部部長唐鳳，唐鳳提及台灣 2050 淨零碳排的目標和台灣在淨零碳排上會遇上因中小企業居多，有結構上量能較為不足的問題。此外，注意到資訊與通信科技（Information and Communication Technology，簡稱 ICT）產業本身的碳排固然重要，但也不能忽視 ICT 對於其他產業在邁向淨零碳排的幫助，例如利用 ICT 技術，使得傳統產業可以更有效率地追蹤生產過程中的碳排放。唐鳳也提及過去在駭客松活動中，有人提出讓用 App 結合加水站，每當人們在加水站加水時，就可以查看 App 得知自己避免了多少瓶裝水的消耗，透過這類「讓人們注意到自己的消費與碳排放、ESG 的關聯」的作法，使得人們的日常生活也能夠與社會共同目標緊密結合。

第二位與談人是來自南韓 Institute for Technology Assessment and Systems Analysis 和德國的 The Karlsruhe Institute of Technology 的 Jaewon Son。Jaewon 提及網路在碳排上最可見的影響莫非是此時此刻人們不一定要搭乘數千公里的飛機到新加坡，也能線上參與此場會議。此外，Jaewon 提到最簡單每個人都可以做的事情是取消不看的 Email 訂閱，因為 Email 訂閱不僅會頻繁地消耗傳輸所需的能源，也需要伺服器資源去儲存。

接著是由主持人 Edmon Chang 執行長介紹「骯髒、耗能」的網路，是否能

有不同的敘事模式，例如探討網路所帶來的效益，用以衡量其所產生的環境衝擊，而這正是 Dot Asia 的計畫「Internet Footprint vs. Physical Footprint」所想要關注的議題。在該計畫中，Edmon 提到他們發現比起實際傳輸的資訊量，維護網路傳輸量能本身更是耗能。而為了處理各國能源結構、網路使用人口等因素的不同，Dot Asia 也發起了一項關注經濟、能源、效率的先行研究，評比了亞洲六個國家的網路與能源消耗狀況，發現日本是最佳而香港是居於末位。

第三位與談人是原訂的主持人 Ellen Strickland，其簡短分享了紐西蘭在可再生能源上的努力，以國家為一個整體，推動 2030 年以前達成 90%再生能源，如此一來，即使機房、伺服器的節能進展有限，社會整體仍然能夠達成減緩氣候變遷衝擊目標。

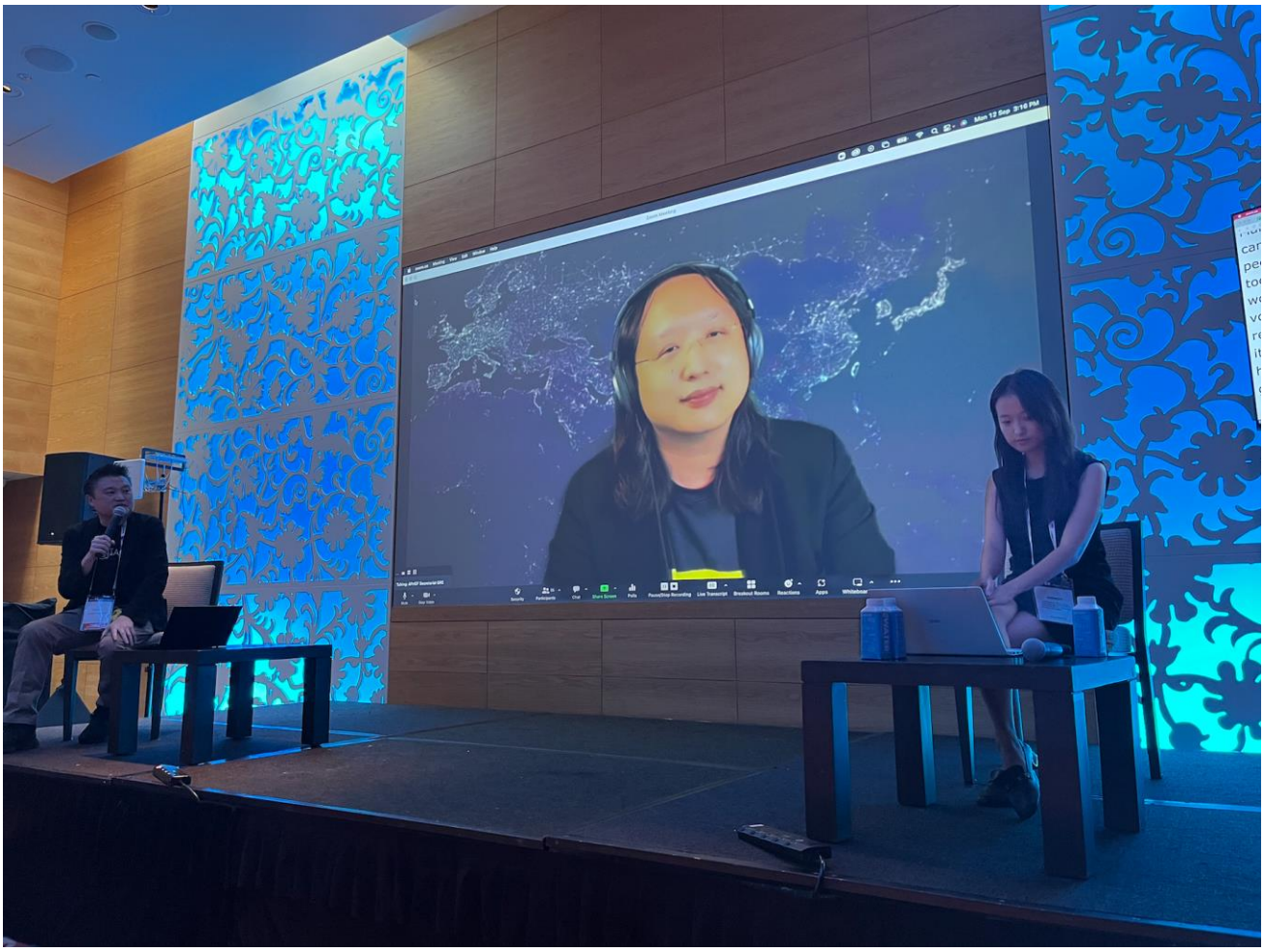


圖3. S08 台灣數位部長唐鳳與談時的現場畫面

（四）S02. 新冠疫情期間高等教育身心障礙學生的數位近用與網路接取

會議名稱	S02. 新冠疫情期間高等教育身心障礙學生的數位近用與網路接取 S02. Digital accessibility and connectivity for disabled students in higher education during COVID-19
會議時間（UTC）	2022 年 9 月 13 日 01:30 – 02:30

摘要：

本會議由 Sudha Bhuvaneshwari 博士主持，由來自各國的大學學者，討論高等教育中身心障礙學生在新冠疫情面對的挑戰。

第一位與談人是來自斯里蘭卡 General Sir John Kotelawela Defence 大學的 Nirosha Wedasinghe 博士，其提及在疫情初期，高等教育從實體切換到線上時，多數的教學內容仍然並非為數位教學而準備的，例如對於視覺障礙的學生而言，一張並未附帶語音說明的圖片，就會使得這樣的學生無法獲取其資訊；例如對於聽覺受損的學生而言，語音內容會是學習的一大障礙。Nirosha Wedasinghe 博士提及在她服務的學校，她們確實會慮及這些特殊需求的學生，然而更困難的是網路接取上的問題，對於居住在偏遠地區的學生而言，網路接取就是最直接而困難的問題，更甚者，即使不是在偏遠地區，也有都市學生難以接取 WiFi 或是當地 WiFi 並不足以支撐當地所有人的增加的上網需求。

第二位與談人是來自 Federation of Ceylon 的 H. K. MANIQUE GUNARATNE，其從政府的角度論及如何幫助身心障礙者和緩疫情對他們生活的衝擊，H. K. MANIQUE GUNARATNE 女士提及，身心障礙者一方面有交通、住宿的障礙，另一方面也因為他們來自草根階級，因此在過去以來，網路培訓相較於實體出席，較為容易執行，疫情期間也受惠於過去所建立的線上課程資源。然而場景換到高等教育的學生時，反而他們缺乏所需的裝置，例如視力受損的學生沒有可以以聲音輔助獲取視覺內容的電子裝置，甚者是他們也不知道如何使用這些裝置，此外這些裝置也相當昂貴，使得經濟資源不足的學生也無望取得，H. K. MANIQUE GUNARATNE 女士建議以補貼、有限期借用等方式，

由大學方協助身心障礙學生取得這些裝置。此外居住在外的學生無法取得家人的幫助，或是家人也沒有足夠的資訊素養協助。更甚者在疫情嚴重的時候，連續數個月的封城使得學生無法外出購買連網必須的 SIM 卡，連帶網路金融等服務也無法使用。

第三位與談人因為連線與環境音訊問題而難以確認其與談內容。主持人簡短總結其內容為：第三位與談人論及理工背景的學生，疫情期間使得他們無法到實驗室，無法有實際的軟體操作經驗，尤其考量到約 15%的人口有不同樣態的身心障礙，需要更多資源、資金協助他們的學習。



圖4. S02 場次現場畫面

（五）S11. 回應後疫情時代的數位人權變動

會議名稱	S11. 回應後疫情時代的數位人權變動 S11. Responding to changing digital rights priorities in a post-pandemic world
會議時間（UTC）	2022 年 9 月 14 日 05:30 – 06:30

摘要：

此會議由 Pavitra Ramanujam 女士主持，Pavitra Ramanujam 女士來自印度 Progressive Communications 協會，其提及 IGF 場域中，公民社會如何討論疫情的衝擊，私人企業與政府如何把握機會擴大科技的滲透與持續提升對於人們數位權利的掌握。

第一位與談人是來自 Nottingham Malaysia 大學的 Gayathry Venkiteswaran 教授，Gayathry Venkiteswaran 教授分享馬來西亞的經驗，在疫情下，一方面人們遇上公共衛生緊急事件，另一方面遇上政治上的動盪，馬來西亞經歷選舉與聯邦政府易位，綜合這些因素，馬來西亞錯失了針對數位權利改革的機會。Gayathry Venkiteswaran 教授認為馬來西亞政府持續加強對於網路上言論的控制與限制，其中種族、信仰、皇室/忠誠是馬來西亞最為敏感的議題，而要抗衡這樣的政治環境，Gayathry Venkiteswaran 教授認為持續關注表意自由、數位資訊的隱私和保護等數位人權是重中之重。

第二位與談人是來自泰國的 Darika Bamrungchok 代表 Thai Netizen Network 參與此次議程，Darika Bamrungchok 女士提及網路賦予人們快速動員與抗議的管道，但同樣科技發展也為政府提供了更多的監控、控制手段。Darika Bamrungchok 女士分享泰國在 2020-2021 的支持民主青年運動，政府透過四個互相支撐的支柱，建立起統治的生態系，首先是司法騷擾和起訴，泰國政府藉由電腦犯罪法、保護皇室形象的第 112 號等法律，監控與壓制網路內容；其次是網路和媒體審查，例如泰國政府會要求臉書下架詆毀泰國皇室的內容，或是

壓制獨立媒體在國內出版的可能性，雖然由此可見，政府雖然不再直接禁止人們瀏覽網站，但透過其他管道操縱網路上的內容；另外是資訊戰和數位監控，前者是散播消息、追蹤輿情，甚者瞄準倡議人士，後者則是泰國政府不再依賴傳統的閉路電視（Closed-Circuit Television，簡稱 CCTV），更甚者會使用間諜軟體來掌握人們的動向。

第三位與談人是來自韓國 Progressive Network Jinbonet 的 Byoung-il Oh。Byoung-il Oh 先生提及疫情期間在防疫與保障數位人權的兩難，作為非公衛專家，該如何確認公衛政策有達到國際人權上最小侵害的原則。南韓施行「Treat、Test、Trace」的 3T 政策以控制新冠疫情的傳播，快篩結果、甚至是信用卡、交通卡的資訊都被政府所搜集利用。Byoung-il Oh 先生認為南韓雖然在控制疫情上確實有些成果，但在人權保護上仍顯不足。

第四位與談人是來自 Timor Leste 的 Fernando Ximenes，Fernando Ximenes 先生提及談論 Timor Leste 的數位人權其實有些弔詭，畢竟有些當地人們甚至連網路都還沒有，更何談數位化。但不可否認外在的壓力仍然推著 Timor Leste 朝向數位化的腳步前進，數位化一方面賦予人們新的可能性，也形塑了這個社會，使得社會更被受管制和暴露在極權主義的風險下。



圖5. **S11 場次會議結束前的畫面**

（六）S03. 在網路治理議題上強化身障人士的發聲

會議名稱	S03. 在網路治理議題上強化身障人士的發聲 S03. Strengthening the disability voice in Internet Governance
會議時間（UTC）	2022 年 9 月 14 日 01:30 – 02:30

摘要：

本場次的主持是來自 ISOC Accessibility Standing Group 的 Gunela Astbrink，Gunela Astbrink 女士在開場時提及，雖然近年 IGF 等討論中，對於身障議題的重視仍顯不足，但值得欣慰的是關注度逐年提升，此次 APrIGF 中身障者的討論場次也是創下歷史新高，主持人邀請與談人們分享如何提升身障者的領導力，進而發揮更多的影響力。

第一位與談人是來自斯里蘭卡的 Manique Gunaratne 女士，代表 Employers Federation of Ceylon 參與此次討論，Manique Gunaratne 女士聚焦在身障者的領導力議題上，其認為身障者應該被賦能、佔據足夠的領導位置，如此一來才能為未來世代準備，扮演新生代的人生導師、提升身障者的網路近用、網路的包容性。Manique Gunaratne 女士認為如孟加拉給予身障者的領導力培訓課程就是一個很好的例子，為身障者族群種下種子，提升身障者在資金、資源分配上的話語權。

第二位與談人是來自孟加拉的 Vashkar Bhattacharjee，Vashkar Bhattacharjee 先生首先感謝 APrIGF 全體和主席 Anju 女士對於身障者的重視。Vashkar Bhattacharjee 先生認為可以從三個層次探討，分別是國家、區域、能力上，Vashkar Bhattacharjee 先生呼籲人們在國家層級上納入更多身障領導者，培育他們在能力上參與討論的可能，進而能將影響力帶到區域間，如 APrIGF 的討論之中。

第三位與談人是本次 APrIGF 主席 Anju Mangal，Anju Mangal 女士從 World Wide Web 基金會的經驗，以政策面的角度切入討論如何協助身障者近用網路，

尤其是有身心障礙的婦女、小孩、偏遠地區的居民。Anju Mangal 女士強調領導力的核心是服務社群，因此重點並不是自己、組織，而是實際存在的人們、社群和他們的需求。Anju Mangal 女士也提及，要發揮領導力納入身障族群的參與，例如 APrIGF 會場中，不僅要確保他們能夠進到會場、取得餐食，更要確保大家能夠認識他們，他們可以和其他人建立連結。Anju Mangal 女士也承認這樣的過程很困難，不僅是執行上費時費力，更不時會有人不請自來地指指點點他們應該如何做、哪裡應該做得更好，但 Anju Mangal 女士認為持續抱持著「以人為本」的精神，就能克服這些壓力繼續前行。

第四位與談人是來自巴基斯坦線上連線的 Muhammad Shabbir Awan，代表 ISOC Islamabad Chapter 參與討論。Muhammad Shabbir Awan 先生首先強調身障者的人數佔總人口 15% 的比例在未來因為天災人禍，數字是不降反升的，而促進身心障礙者的近用不單只是為了這 15%的人們，同時也會嘉惠於其餘的 85%的人們。

筆者在自由發言的階段中也公開回應第四位與談人的看法，分享自身在使用外語影音平臺時的經驗，日本近年的各家媒體陸續推出「Barrier-free」的影片，亦即為影音加上一般對話字幕和形容當下聲音的字幕，使得聽力受損的人們也能夠試圖透過文字瞭解當下影音想要傳達的情緒、劇情，而這樣的政策也嘉惠於像是筆者一樣的日語學習者，因為相對於直接聽取內容，有字幕的影音內容給予了日語沒有到母語等級，但也不至於完全聽不懂的人們一個緩衝空間，可以透過開關字幕慢慢提升外語能力，因此筆者也十分同意促進身障者的近用並不是單單為了身心障礙者，而是一個也能夠嘉惠於全體的政策。

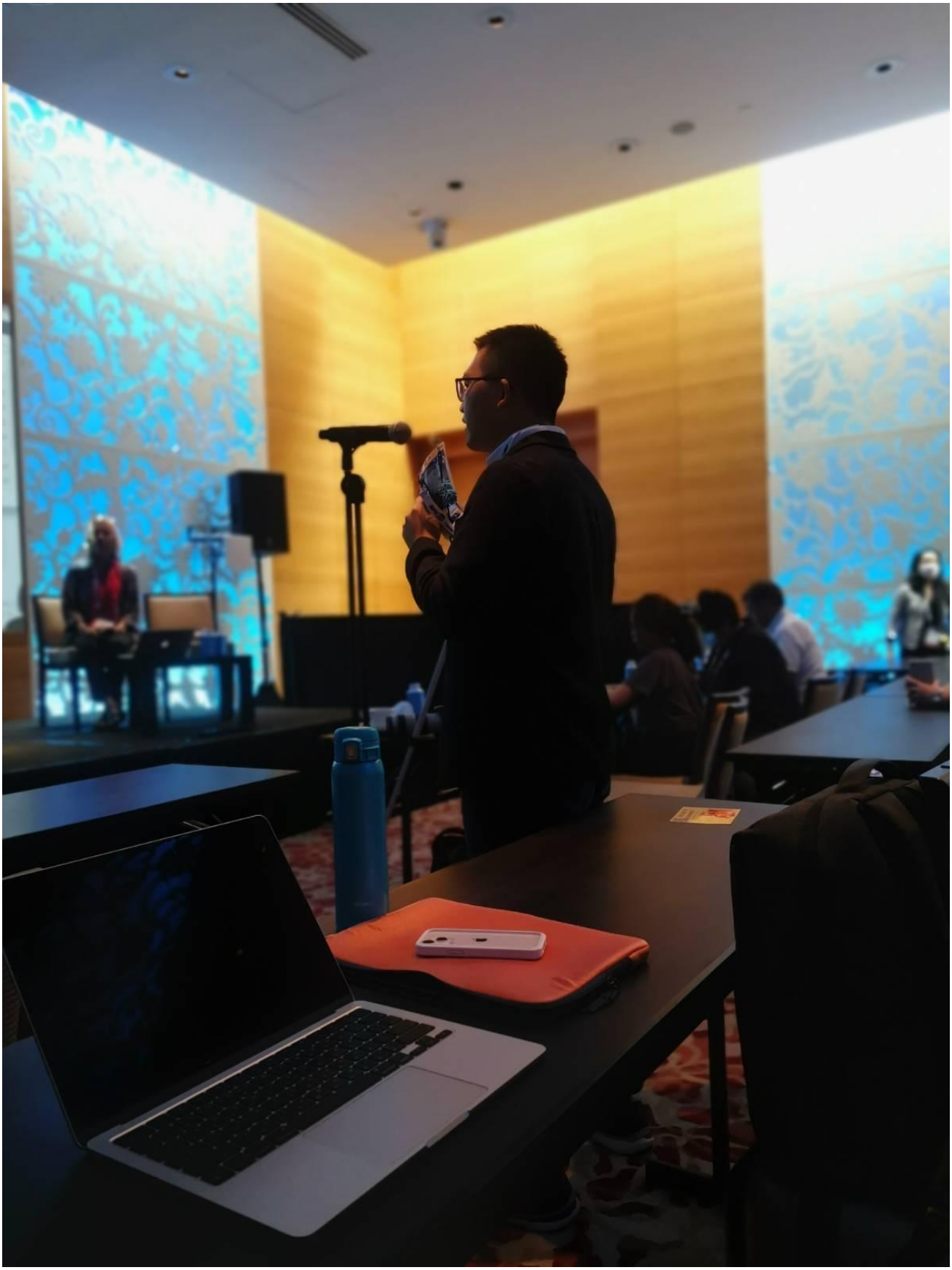


圖6. S03 場次中學員公開發言分享自身經驗

（七）S19. 提升網路韌性，建立可本地存取的雲端服務

會議名稱	S19. 提升網路韌性，建立可本地存取的雲端服務 S19. Locally Accessible Cloud Service (LACS) for e-resilience
會議時間（UTC）	2022 年 9 月 14 日 03:00 – 03:30

摘要：

本場次主講人為來自日本京都國際電氣通信基礎技術研究所（ATR）的 Toshikazu SAKANO。Toshikazu SAKANO 先生從 2011 年 311 日本東北大地震談起，世界各地不時都會有颱風、地震等天然災害的侵襲，而這類大規模自然災害也會導致電信基礎設備的毀損，例如纜線、網路交換器、機房等，此外也會有停電的風險存在，這些因素都會導致人們無法連上網路，嚴重影響人們的日常生活，而可本地存取的雲端服務（Locally Accessible Cloud Service，簡稱 LACS）的目的就是作為可攜帶的網路存取點，支援如受災地區等區域。

LACS 透過 WiFi 提供網路存取給附近的人們，包含的四個功能，有用戶註冊、重要資訊欄（公家機關使用）、公告欄、私人訊息，公告欄可以在不同組的 LACS 之間同步，進而使災害期間人們能夠協尋距離較遠的親朋好友，而一整套的 LACS 更會有太陽能充電板、電池供應電力，小型電腦、WiFi AP 和 Hub 提供網路接取。

承平時期，LACS 也可以提供人潮聚集的活動、網路發展較為緩慢的地區，當作臨時的網路接取點，

第二位講者是來自菲律賓 CVISNET 基金會的 Jeffrey N. Lianto，Jeffrey N. Lianto 先生提及菲律賓使用 LACS 於學校日常運作中的經驗，另外也提及 2019 年兩次的災害情境測試、疫情期間 2020/12-2021/2 線上學習系統、2021/9-2022/2 可行性測試，最後是 2022/12-2023/2 的測試計畫。

第三位講者是來自尼泊爾的 Ashirwad Tripathy，Ashirwad Tripathy 先生提及尼泊爾 2015 年經歷大地震後，開始反思該如何讓人們持續連上網路，剛好在

之前的 APrIGF 接觸到此議題，因此不僅能夠合作驗證 LACS 的有效性，也同時嘉惠於偏鄉地區教育機構的網路近用議題。



圖7. S19 場次畫面截圖

（八）S21. LEO 衛星叢集，是否能提供更好的網路接取與網路強韌性

會議名稱	S21. LEO 衛星叢集，是否能提供更好的網路接取與網路強韌性 S21. LEO Satellite Constellations - Will They Bring Better Internet Access and a More Resilient Internet?
會議時間（UTC）	2022 年 9 月 14 日 03:30 – 04:00

摘要：

本會議由來自美國的 Dan York 主講，其為 Internet Society LEO Satellite Internet Systems 計畫主持人。其首先提及「網路為所有人而存在」的核心信念，而基於這樣的信念，衍伸出的問題即是該如何讓沒有連上網路的人連上網路，其中一個近期最被關注的可能性即是低軌道衛星（Low Earth Orbit Satellite，簡稱 LEO），不同於地球同步衛星的低頻寬，LEO 不僅有高頻寬，更有低延遲的優勢，確實擴展了衛星網路許多應用的可能性，也因此如 Starlink 和 Amazon 都發射許多 LEO 到太空中。

第二位講者是 Dan York 的工作夥伴 Raj，承接 Dan York 提出的問題「LEO 對網路整體而言是好事嗎？」，LEO 好處，諸如提供偏遠地方網路接取、提供離島地區、自然災害受災地區確實是顯而易見的。然而短期內能夠實際運作的僅有 Starlink，Amazon 可能等到 2024、2025 才有機會正式營運，這導致了市場競爭上的問題，缺乏競爭外加衛星發射成本先天上就較高，也會使得價格居高不下，影響人們的可負擔性。另外，政策性的因素，例如主講人 Dan York 提到 LEO 營運商可能需要到超過 200 個國家或經濟體處理頻譜的申請、政府干預、區域的限制等，也是 LEO 在擔起網路骨幹之一的重擔前，需要面對的問題。

最後，主講人 Dan York 提及在科技上的議題，像是安全性、隱私性、開放協定、系統相容性、太空垃圾，也是相當令人擔憂。

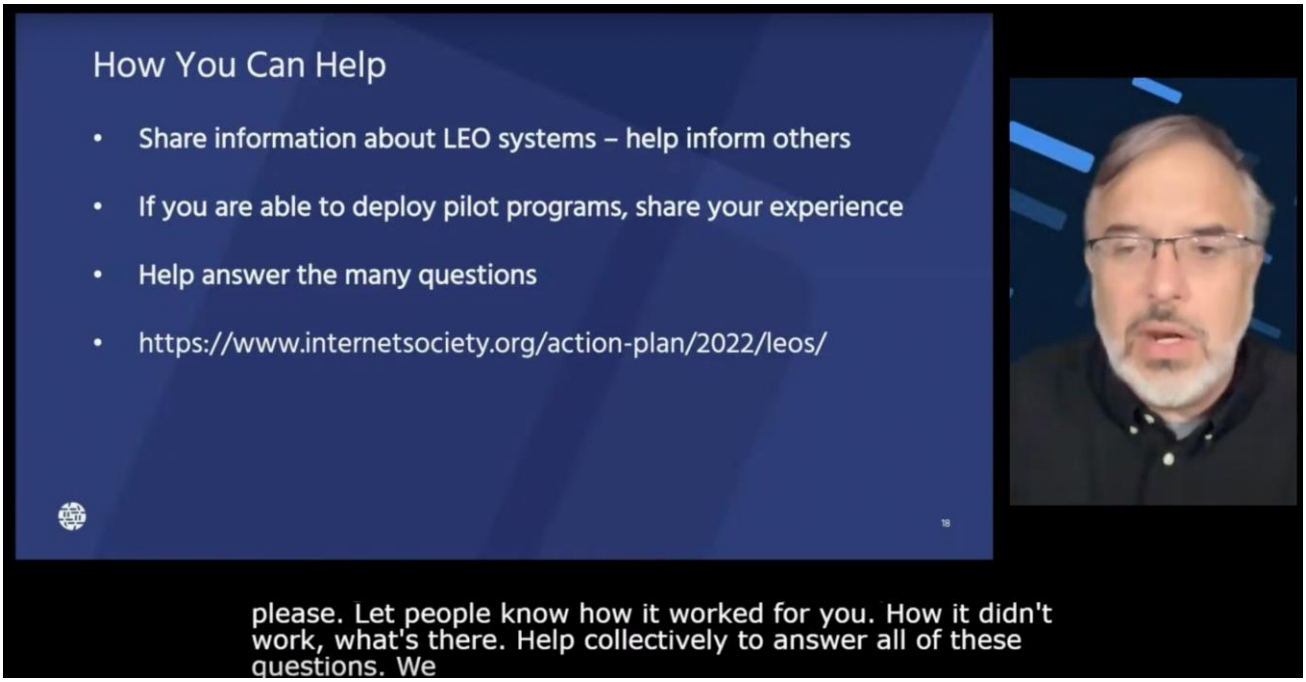


圖8. S21 主講人呼籲大家一同深入瞭解 LEO 對於網路社群的影響

四、 參與心得

「rights that people have offline must also be protected online」，網路治理社群不僅承接了聯合國人權理事會的標語，更在每一次的網路治理論壇之中實踐之。過去的我曾經以為這些不過都是口號，喊喊口號誰不會，但真正走到會場中，看著視障人士獲得人們的協助，一步一步地走到台上，不卑不亢地向眾人宣示他們的存在、看著不良於行的人們，拄著拐杖一緩一緩地走到麥克風前，侃侃而談自身的經驗，我才體認到，權利是靠爭取而來的，而網路治理社群提供絕佳的場域讓人們針對數位世界中的權利與價值腦力激盪。

在所有議程中，雖說有幾個講題很值得探討，例如對於身障學生在疫情時期的網路接取與近用、災害期間如何保持網路不中斷，但整場議程中最令我印象深刻的是「Townhill」，該議程並不討論特定主題，而是邀請所有人分享自己整天的所見所聞，進而提供草稿編撰委員會素材撰寫「APrIGF 共識文件」，整個過程既緩慢又無趣，對比之下，議程廳外逐漸散場、歡談的聲音略顯吵雜，但這樣的磨合共識的過程，我認為正是共識決決策模式能夠持續運作下去的基石。APrIGF 或是其他國家、區域 IGF 產出的文件不具有任何形式上的法律效力、拘束力、甚至是「公信力」，畢竟這些集會既不是政府舉辦的也不是聲譽良好的大企業主導的，但參與過其中的人、ICANN 大概就會知道，一份文件中的字裡行間，蘊含著的是一個又一個付出自己的時間、精力、甚至是昂貴的旅行支出的無名小卒們，透過不同意見的交流，進而交織出「共識」，或許是個「沒有共識的共識」，但至少可以知道就某個議題，大家無法達成共識。

共識決是網路治理社群的理想，也某種程度是現實，但這樣的理想現實的一面是決策相當緩慢、甚至無法做成決定，然而即使如此，在各個國家、地區的網路治理社群互相連結，持續澆灌出大家都能勉強接受的共識，或許就會是對現下的人類社群而言，最適合的答案了。非常感謝國家通訊傳播委員會和財團法人中華民國國家資訊基本建設產業發展協進會提供我此次機會一睹網路治理社群最真實且動態的面貌，期待未來能有夠多機會參與其中。

附件：APrIGF 2022 完整議程表

11 September (Sun) Day 0		12 September (Mon) Day 1		13 September (Tue) Day 2		14 September (Wed) Day 3	
14:00-16:30 SGT 06:00-8:30 UTC	Capacity Building Program for Fellows and Newcomers		S06. Empowering New Voices in Internet Governance Spaces		S15. Toward Trusted Design: User Protections for a Better Web for All		S03. Strengthening the disability voice in Internet Governance
		09:30-10:30 SGT 01:30-02:30 UTC	S13. Combating Disinformation from COVID-19 to the General Election: Multistakeholder Digital Literacy vs Legislation & Censorship?	09:30-10:30 SGT 01:30-02:30 UTC	S02. Digital accessibility and connectivity for disabled students in higher education during COVID-19	09:30-10:30 SGT 01:30-02:30 UTC	S09. Social Media Regulation during Elections: Expanding or Limiting Digital Democracy?
		10:30-11:00 SGT 02:30-03:00 UTC	Break	10:30-11:00 SGT 02:30-03:00 UTC	Break	10:30-11:00 SGT 02:30-03:00 UTC	Break
		11:00-12:30 SGT 03:00-04:30 UTC	APrIGF 2022 Opening Plenary	11:00-12:30 SGT 03:00-04:30 UTC	APNIC Opening Ceremony and Keynotes	11:00-12:30 SGT 03:00-04:30 UTC	Showcases S19. Locally Accessible Cloud Service (LACS) for e-resilience S21. LEO Satellite Constellations – Will They Bring Better Internet Access and a More Resilient Internet? S25. Koo – Empowering Users and Building Cyber Resilience

							IGF Secretariat Workshop: Internet governance within the system of United Nations: is IGF on a good path to adapt, innovate and reform?
		12:30-13:30 SGT 04:30-05:30 UTC	Lunch Break	12:30-13:30 SGT 04:30-05:30 UTC	Lunch Break	12:30-13:30 SGT 04:30-05:30 UTC	Lunch Break
			S07. Online harassment as tools of exclusion: A discussion on Addressing Online Gender Based Violence Through Community Organised Helplines		**S16. Protecting the Healthcare Sector from Cyber Harm**		**IG Futures (Summary Session by APrIGF-APSIG Fellows)**
		13:30-14:30 SGT 05:30-06:30 UTC	**S17. Advancing data justice in (post-)pandemic data governance: perspectives from Southeast Asia**	13:30-14:30 SGT 05:30-06:30 UTC	**S11. Responding to changing digital rights priorities in a post-pandemic world**	13:30-14:30 SGT 05:30-06:30 UTC	**Showcases** **S20. Here's How Your Genital and Physical Affects Your Digital Lives** **S22. Measuring the Internet protocol parameters for reducing Internet poverty**

		16:00-16:30 SGT 08:00-08:30 UTC	Break	16:00-16:30 SGT 08:00-08:30 UTC	Break	16:00-16:30 SGT 08:00-08:30 UTC	Break
		16:30-17:30 SGT 08:30-09:30 UTC	**S04. Inclusion of persons with disabilities in the ICT Job Sector**	16:30-17:30 SGT 08:30-09:30 UTC	**S01. Connecting the Unconnected – Efforts from Private Sector and Policy Lessons from the APAC**	16:30-18:00 SGT 08:30-10:00 UTC	**APrIGF 2022 Closing Plenary**
			S10. Future of Work: Achieving a sustainable gig economy		**S14. Digital Resiliency of Civil Society in the context of shrinking Civic Space**		
		17:30-18:30 SGT 09:30-10:30 UTC	**Townhall Session**	17:30-18:30 SGT 09:30-10:30 UTC	**Townhall Session**		
				19:00-21:00 SGT 11:00-13:00 UTC	**Welcome Social**		

來源：https://ap.rigf.asia/news/2022-program-schedule/

附錄四：實習學員參與網路治理會議摘要報告

國家通訊傳播委員會
「網路治理國際趨勢研析與人才培育」
委託研究採購案

實習學員參與網路治理會議摘要報告

報告人：2022 網路治理研習營實習學員
（江○毅、李○毅、韋○祥、徐○為）

中華民國 111 年 10 月

目錄

一、 實習規劃 1

二、 實習內容 1

三、 實習記錄 3

四、 實習心得交流 36

圖目錄

圖 1.EuroDIG 討論議題公開徵求結果統計 4

圖 2.EuroDIG 2022 Day 0 / Pre-event 議程 4

圖 3.EuroDIG 2022 Day 1-2 議程 5

表目錄

表 1.實習學員分工表 2

表 2.實習學員參與 EURODIG 2022 場次表 6

表 3.實習學員所參與網路治理相關會議場次 24

一、實習規劃

網路治理研習營辦理目標為協助國內社會各界人士與青年學子獲得網路治理知識，掌握當前重要治理議題發展，充分了解多方利害關係人參與網路治理精神，進而培養參與國內外網路治理政策討論的能力。培訓課程在課後除選出一名優秀學員外，對參與完整課程之學員進行實習意願調查，並協助前往實習。

本會安排實習學員參加國外及國內之網路治理會議，並請學員撰寫會議摘要，於實習最末舉辦線上交流會，請學員分享參與會議的收穫。實習時數約 12 小時，提供每人新臺幣 2 千元的實習津貼。

二、實習內容

本屆 21 位結業學員（不含公務人員）當中，有 20 位表達同意參加實習學員甄選的意願。評選小組共選出 4 名實習學員，分別為江◯毅（高雄醫學大學牙醫學系）、李◯毅（國立陽明交通大學科技法律研究所）、韋◯祥（國立陽明交通大學資工系）、以及徐◯為（淡江大學教育心理與諮商研究所）。

執行團隊在 6 月安排 4 名學員線上參加歐洲網路治理論壇（European Dialogue on Internet Governance，EuroDIG）。團隊先從議程中挑選出合適的會議主題提供給 4 名實習學員選擇，每人各參與 2 場次的會議；7 月至 8 月則提供國內外將辦理之網路治理會議資訊予學員參考，請學員自行選擇 1 場次參加（實體或線上皆可），會後撰寫會議摘要。

在實習尾聲，執行團隊於 8 月 31 日召開一場實習學員的線上交流會，讓大家分享參與會議的收穫。會中學員除了分享實習心得外，也提出對於本實習活動的建議。計畫成員林郁敏資深經理也在交流會中與大家介紹 2022 年國內外的網路治理會議辦理情況以及所討論的議題重點。

實習學員參與會議分工表詳表 1，其所交付的會議摘要會陸續刊載於研習營活動網站（https://igcamp.tw/）及網路治理觀測站網站（https://igwatch.tw/）。

表1.　實習學員分工表

姓名	參與場次
江◯毅	• Focus Area 1, Subtopic 1: The European vision of digital sovereignty: From principles to action.（EuroDIG） • Focus Area 4, WS 6: The Declaration for the Future of the Internet.（EuroDIG） • 元宇宙的新維度治理框架（臺灣網路講堂）
李◯毅	• Focus Area 1, Subtopic 2: Digital Sovereignty impact on the Internet infrastructure.（EuroDIG） • Focus Area 4, Subtopic 1: Responding to disinformation in times of COVID-19 and geopolitical conflict.（EuroDIG） • Beyond the Encrypted Content Debate.（IGF-USA 2022）
韋◯祥	• Focus Area 1, WS 3: International Connectivity: European Data-Gateway Platforms and the Global Gateway（EuroDIG） • Focus Area 4, Subtopic 2: Sovereignty and the Internet: a risk of fragmentation（EuroDIG） • 「公共空間的人工智慧應用與隱私隱憂」專題講座
徐◯為	• Focus Area 1, Subtopic 3: Digital sovereignty - is Europe going in the right direction to keep Internet infrastructure secure and open?（EuroDIG） • Focus Area 3, Subtopic 1: Regulating emerging technologies: artificial intelligence and data governance.（EuroDIG） • 自拜登數位資產政策，一探臺灣數位金融之機會與挑戰（臺灣網路講堂）

三、實習記錄

（一） 歐洲網路治理論壇（European Dialogue on Internet Governance，EuroDIG）

1. 會議資訊

歐洲網路治理論壇（European Dialogue on Internet Governance，EuroDIG）於2008 年創立，主要目標是促進歐洲人積極參與網路治理多方利害關係人對話，分享專業知識與最佳做法，針對不同的當代議題，一方面彙集各國見解，一方面尋求共識，進而型塑歐洲對於網路治理的展望與方向。

2022 年 EuroDIG 係採用混合型（hybrid）會議模式於 6 月 20 至 22 日在義大利的里雅斯特(Trieste Italy)同步以線上方式舉辦，大會主題為「Set the sails right」。

EuroDIG 從 2021 年 11 月 1 日開始公開徵求討論議題，直至 2022 年 1 月 3 日共計收到 79 份提案，議題類別包含連網與素養、網路治理生態系統發展、人權、創新與經濟、媒體與內容、安全與犯罪、技術與維運、跨領域/其他等共 8 類，各議題類別的提案數量如下圖 4 所示。當中除了無法歸類的「跨領域/其他」外，最熱絡的討論議題類別為獲得 13 份提案的「創新與經濟」，及 12 份提案的「安全與犯罪」。

此外，「網路治理生態系統發展」亦有 9 份提案，包含 2 份來自英國數位、文化、媒體暨體育部（Department for Digital, Culture, Media & Sport, DCMS）的提案，建議討論促進全球網路的多語化；及聯合國 WSIS 將於 2025 年決議是否持續舉辦 IGF 及採用多方利害關係人方式。「連網與素養」則有 8 份提案，包括 1 份由葡萄牙國家通訊管理局(Autoridade Nacional de Comunicações, ANACOM）的提案，建議討論歐盟的數位十年（The Digital Decade）、歐洲資料門戶（The European Data-Gateway）和全球門戶（Global Gateway）等計畫。

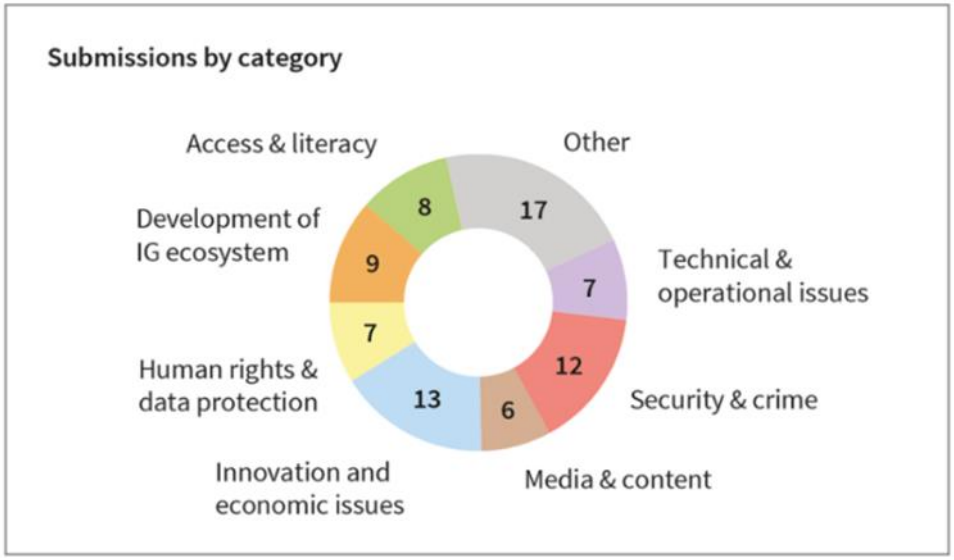


圖1. EuroDIG 討論議題公開徵求結果統計

2. 會議議程

EuroDIG 2022 會議從 6 月 20 至 22 日共 3 天，超過 30 場次的會議，三天議程請詳圖 2 及圖 3。

Day 0 / 20 June 2022 – Pre-event

10:00 – 11:00	Pre 1: How to put 'Katowice IGF Messages' into practice?
11:15 – 12:45	Pre 9: Multilingualism on the Internet
11:15 – 12:45	Pre 3: DNS Abuse – the consequences of definitions
13:00 – 14:30	Pre 5: Assessing Internet Universality ROAM-X indicators to advance digital transformation in Europe
13:00 – 14:30	Pre 2: Dynamic Coalition (IGF) on Data Driven Health Technologies – Building an onboarding toolkit together
14:45 – 16:15	Pre 4: NRI and Youth Assembly – Update on the global processes and how to participate?
14:45 – 16:15	Pre 8: Open Forum: The road ahead for ICT sustainability in Europe and beyond
16:30 – 18:00	Pre 6: Internet governance within the system of the United Nations: is IGF on a good path to adapt, innovate and reform?
16:30 – 18:00	Pre 7: A celebration of youth voices in Internet Governance

圖2. EuroDIG 2022 Day 0 / Pre-event 議程

Day 1 / 21 June 2022

10:00 – 10:30	Welcome
10:30 – 11:15	Focus Area 1, Subtopic 1: The European vision of digital sovereignty: From principles to action
10:30 – 11:30	Focus Area 2, WS 1: From commitments to action: Assessing the effectiveness of pan-European policies and regulations for the green digital transformation
11:30 – 12:15	Focus Area 1, Subtopic 2: Digital Sovereignty impact on the Internet infrastructure.
12:15 – 13:15	Focus Area 2, WS 2: How can collaborative standards development support the European cybersecurity agenda?
12:30 – 13:15	Focus Area 1, Subtopic 3: Digital sovereignty – is Europe going in the right direction to keep Internet infrastructure secure and open?
13:15 – 14:15	BigStage
14:15 – 14:45	Keynote
14:45 – 15:30	Focus Area 2, Subtopic 1: A new European regulatory regime: What are the Dos and Don'ts?
14:45 – 15:45	Focus Area 1, WS 4: Hot topic discussion (canceled)
15:45 – 16:30	Focus Area 2, Subtopic 2: How to Enable Rapid Cybersecurity Standards Implementation for Impact
16:30 – 17:30	Focus Area 1, WS 3: International Connectivity: European Data-Gateway Platforms and the Global Gateway
16:45 – 17:30	Focus Area 2, Subtopic 3: International Cooperation on Criminal Justice in Cyberspace: Where we are and where are we heading to?
17:30 – 18:00	Agreeing on the Messages for Focus Area 2
17:30 – 18:00	Agreeing on the Messages for Focus Area 1
18:00 – 18:30	Keynote – Set the sails right?
20:00	Social evening 2022

Day 2 / 22 June 2022

10:00 – 10:30	Keynote
10:30 – 11:15	Focus Area 3, Subtopic 1: Regulating emerging technologies: artificial intelligence and data governance
10:30 – 11:30	Focus Area 4, WS 5: Hot topic discussion (canceled)
11:30 – 12:15	Focus Area 3, Subtopic 2: The multi-stakeholder model: from its origins to its future
12:15 – 13:15	Focus Area 4, WS 6: The Declaration for the Future of the Internet
12:30 – 13:15	Focus Area 3, Subtopic 3: Upcoming digital identity initiatives impacting your live
13:15 – 14:15	BigStage
14:15 – 14:45	YOUthDIG messages
14:45 – 15:55	Focus Area 4, Subtopic 2: Sovereignty and the Internet: a risk of fragmentation
14:45 – 15:45	Focus Area 3, WS 7: Cross border e-Identification
16:20 – 17:30	Focus Area 4, Subtopic 1: Responding to disinformation in times of COVID-19 and geopolitical conflict
16:30 – 17:30	Focus Area 3, WS 8: Delay Tolerant Networks – Building Interplanetary Internet
17:30 – 18:00	Agreeing on the Messages for Focus Area 4
17:30 – 18:00	Agreeing on the Messages for Focus Area 3
18:00 – 18:30	Wrap-up

圖3. EuroDIG 2022 Day 1-2 議程

3. 參加場次

團隊先從 6 月 21 日-22 日的場次議程中挑選出合適的會議主題提供給 4 名實習學員，請學員每人挑選 2 場次參與（詳表 2）。以線上同步參與為主。

表2.　實習學員參與 2022 EuroDIG 場次表

日期	CEST 時間	臺灣時間	摘要撰寫	會議名稱
21 Jun（Tue）	10:30 – 11:15	16:35 – 17:15	江◯毅	Focus Area 1, Subtopic 1: The European vision of digital sovereignty: From principles to action
	11:30 – 12:15	17:30 – 18:15	李◯毅	Focus Area 1, Subtopic 2: Digital Sovereignty impact on the Internet infrastructure.
	12:30 – 13:15	18:30 – 19:15	徐◯為	Focus Area 1, Subtopic 3: Digital sovereignty – is Europe going in the right direction to keep Internet infrastructure secure and open?
	16:30 – 17:30	22:30 – 23:30	韋◯祥	Focus Area 1, WS 3: International Connectivity: European Data-Gateway Platforms and the Global Gateway
22 Jun（Wed）	10:30 – 11:15	16:30 – 17:15	徐◯為	Focus Area 3, Subtopic 1: Regulating emerging technologies: artificial intelligence and data governance
	12:15 – 13:15	18:15 – 19:15	江◯毅	Focus Area 4, WS 6: The Declaration for the Future of the Internet
	14:45 – 15:55	20:15 – 21:55	韋◯祥	Focus Area 4, Subtopic 2: Sovereignty and the Internet: a risk of fragmentation
	16:20 – 17:30	22:20 – 23:30	李◯毅	Focus Area 4, Subtopic 1: Responding to disinformation in times of COVID-19 and geopolitical conflict

*依照場次日期及時間排序

4. 場次摘要

(1) 歐洲數位主權願景：從原則到行動

會議名稱	歐洲數位主權願景：從原則到行動 The European vision of digital sovereignty: From principles to action
會議時間（CEST）	2022 年 6 月 21 日 10:30 – 11:15
摘要撰寫	2022 網路治理研習營 實習學員：江◯毅

摘要：

本環節做為本次 EuroDIG 正式會議期間的第一場對談，由國際多利益相關方組織網際網路與政策網絡管理的聯合創始人兼副執行董事 Paul Fehlinger 主持，邀集執行副總裁兼歐盟執委會競爭事務專員 Werner Stengg 、義大利國家創新基金總裁 Francesca Bria 、歐洲數位基礎設施、隱私和安全總監 Alberto Di Felice 及 Access Now 組織歐洲政策總監 Fanny Hidvegi，共同討論歐洲數位主權狀況，並反思歐洲是否朝著正確方向前進，以保持網際網路的安全和開放。

Werner Stengg 表示，他認為數位主權是給與歐洲公民、企業、政府對於數位轉型的控制權，他並提到歐盟執委會已經開始著手許多達成此一目標的行動，其中一個核心理念是民主價值，因此在進行這些行動時，歐盟執委會希望是由民選的組織團體來處理規則制訂而不是私人企業，希望能形塑一個更強大、獨立、廣泛接受意見、有活躍參加者、堅持自身價值的整體；對於目前歐洲在數位主權議題上是否朝著正確方向，他認為應該重新思考甚麼是「方向」，以形成更強而有力的人本數位政策，目前歐盟有已成為一套體系的眾多法案，綜合這些人本視野、策略方向、創新領航的法制架構，他認為歐洲有在對的方向。

Francesca Bria 認為科技與數位主權也意味著政治與經濟主權，是多個不同面向的綜合體，數位主權做為一個社群應該能夠設定技術發展方向，來達到社會、環境的永續性；她提到目前對未來數位社會有兩個占優勢地位的模型，其

一主要建基於矽谷的科技巨擘模型（Big tech model），帶有美國作家 Shoshana Zuboff 描述的監視資本主義（Surveillance capitalism）色彩。其二是以中國等數位威權為代表的大政府模型（Big state model）。她期待歐盟走第三條路 – 大民主模型（Big Democracy model），一種根據憲法架構保障數位隱私權、資訊自決權，強調民主、法治、公民參與的路線，在形成數位主權的概念時以民主為核心，透過包含歐盟數位服務法案（Digital Service Act）、數位市場法案（Digital Market Act）、數據法案（Data Act）、數據治理法案（Data Governance Act）、人工智慧法案（Artificial Intelligence Act）以及 GDPR 在內的眾多法案，形成一個遠比現存科技公司規範更好的系統，一個更民主自由的經濟系統，更保護基本人權的數位未來，以成為一個供全世界參考的典範。她認為這次的疫情中，歐洲在疫苗技術移轉給非洲及南方世界上展現了領導力，而現在歐盟正在透過數位主權議題創造更多的民主，因此她認為歐洲在此議題上有朝著正確方向。

Alberto Di Felice 引述官方定義表示，數位主權是考慮到全球市場中存在的最先進技術的同時，在公、私兩部門建立和維持關鍵科技的技術和專業科學知識的能力。他認為使用主權（Sovereignty）這個詞進行討論並不適切，因為對它內涵的理解存在普遍的歧異；過去一、二十年來，時常聽到由於歐洲對數位主權的意識起步太晚，因此受到美國大公司支配的相關論述，然而其實歐盟一直有規範，因此他認為更準確地說，歐洲並不是沒有數位主權，只是現在發現規則不太夠用，而他認為不同的政治體制都會面臨此議題，換言之，他的觀點是，數位主權不是地緣政治的問題，也不是矽谷與歐洲的對立，而是在討論社會及資本主義的未來應該怎麼發展，所以，應該更民主多方的討論，建立新的規則，幾年後再回來檢視規範是否漸趨完整。就商業的角度來說，若希望歐洲公司可以在數位化過程中得利，在這個單一市場中仍有許多障礙。關注太多地緣政治，對大多數公司並沒有助益，應該包含全球視野，確保在數位化的立法過程中，不會建立一個惡名昭彰的牆，傷害歐洲的公司及其發展能力。Alberto Di Felice 表示他觀察到普遍存在的保護主義，而他認為這會傷害商業發展，因此就他的觀點而言，目前歐洲在數位主權議題上，並沒有朝正確方向發展。

Fanny Hidvegi 表示，她認為歐洲數位主權的意涵是歐洲有能力設定自己的數位發展方向，而不是以利潤和監控為導向，這首先包括確保內部基本權利的法治和民主，其次以歐洲人民為中心透過外部關係來推廣這些價值觀。她提及因為來自匈牙利的背景，她希望將討論帶到數位主權框架的部分，檢視使用主權（Sovereignty）論述的個體，這是國族主義、保護主義時常使用的詞彙，包含許多面向，如：數據保護、數據串流、網路安全、國家安全，從法國總統大選的例子可以看出，數位主權、數據的價值被當作一種政治商品，她表示即便清楚知道政治現實中有數據交換的討論，她仍認為人權考量不該成為談判籌碼，因此，她認為討論應該建立在基本權利架構上而不是數位主權上；接著她提及，除了民族主義的觀點，主權論述也被使用在政府監控，例如惡名昭彰的歐盟外部邊境安全局人工智慧邊境管制計畫。她提醒需銘記在心的是，歐盟執委會不是獨立的權威單位，也沒有太大的實權敦促各政府落實法案，因此給了某些政府濫權的可能，Access Now 作為服務全球的組織不得不說，既然實際上歐美在此議題上仍有待改善，因此並沒有立場告訴全世界的其他國家，民主應該長成甚麼樣子。最後，她認為以現有的以及正在形成立法或調整的法案而言，在很小的數位世界中，歐盟的發展在對的路上，但在更廣闊的民主規則的法律議題上，她並不樂觀。

(2) 數位主權對於網路基礎建設的衝擊

會議名稱	數位主權對於網路基礎建設的衝擊 Digital Sovereignty impact on the Internet infrastructure.
會議時間（CEST）	2022 年 6 月 21 日 11:30 – 12:15
摘要撰寫	2022 網路治理研習營 實習學員：李◯毅

摘要：

EuroDIG 2022 年的會議共聚焦在四個主題，第一個主題為「歐洲數位主權之發展是否朝著使網路更安全及開放之正確道路前進」，本文要介紹的是本主

題的一個子議程，題目是「數位主權對於網路基礎建設的衝擊」。

本場次的主持人為ICANN董事Avri Doria，講者分別是ISOC的成員Callum Voge、法國IGF的Lucien Castex，以及Namex的顧問Innocenzo Genna。

Avri Doria開場時首先提到數位主權是多邊的（multilateralness），所以數位主權的概念要如何與ICANN的多方利害關係人模型相容，是蠻值得探討的議題；本場次還將提到歐盟DNS、NIS2及其他的問題，並探討歐盟這些立法究竟會對ICANN行之有年的多方利害關係人模型帶來什麼衝擊？數位主權（Digital Sovereignty）究竟指什麼？這些問題都會在本場次進行探討。

Innocenzo Genna提到歐盟數位主權的框架是奠基在民主以及人權，與俄羅斯及中國等有相當大的差異，因此雙方間常會有政策上的辯論及衝突，這些衝突往往政治意味濃厚。由於中國政府的數位主權概念是認為政府得以針對網路世界進行介入管制，因而歐美的雲端服務及電信服務難以進入中國市場。假如未來越來越多國家像中俄一樣干預網路自由，則會造成市場的損害。

Lucien Castex認為，由於COVID－19，使得全世界都面臨數位轉型的問題，國家利益與人權該如何平衡，也是數位主權核心討論的重點。

Callum Voge提到「數位主權」這個詞其實相當不精確，這也是為何歐盟的文件中並不常見到「數位主權」四個字。但當我們談到數位主權，其實有兩個涵義，第一個是提高彈性（Resilience），使數位經濟不容易受到某產業或某國家之威脅並減少對其依賴，但烏俄戰爭似乎加劇了這種情形，烏克蘭希望ICANN收回.ru的ccTLD，會讓政策制定者覺得網路是脆弱且缺乏彈性的；第二個是應用面之競爭，大部分社交媒體、搜尋引擎經營者非歐盟成員，歐盟要如何監管亦成為問題。此外，Voge亦提到NIS2的草案，將使歐盟內有多個司法管轄區，全球網際網路被切成碎片化的管轄範圍，這顯然與網路治理的理念相悖，強制執行及司法互助等執行面的問題，都還有賴後續的政策制訂。

(3) 數位主權—歐洲正在確保網路基礎設施的安全和開放是否朝著正確方向前進？

會議名稱	數位主權—歐洲正在確保網路基礎設施的安全和開放是否朝著正確方向前進？ Digital sovereignty - is Europe going in the right direction to keep Internet infrastructure secure and open?
會議時間（CEST）	2022 年 6 月 21 日 12:30 – 13:15
摘要撰寫	2022 網路治理研習營 實習學員：徐◯為

摘要：

本場次的主持人為 David Frautschy。與談人包括布魯塞爾歐洲政策中心的 Andrea Garcia Rodriguez、科學民意調查的 Florence G'Sell、大學生 JohannesThumfart 以及捷克工業和貿易部長的顧問 Jaromir Novak。隨著世界各國越來越多地使用「數位主權」的概念，並推出一系列政策來控制網路的運作，但這對於網路的發展是有害？還是有益的呢？都是值得探討的議題。

主持人 David Frautschy 先提到網路無國界，但在網路治理上世界各國政府正將地理邊界的概念加於網路世界上，這對於網路基礎建設的影響是什麼？又會如何影響網路的運行？以上述問題為開場，展開一連串的討論。

布魯塞爾歐洲政策中心的 Andrea Garcia Rodriguez 率先發表針對全球化背景之下，如何進行網路治理以及歐洲應該採取什麼策略來因應網路安全與網路開放性的想法。第一，填補各方需求與知識缺口。歐洲公共行政部門、國家層面、地區層面、政府層面、學術界以及私人網路隱私安全的不同需求，學術界需要能夠提供研究見解，以便將其用於政策。政策制定者應幫助學者推動研究方向。第二，公共部門和私營部門攜手建設基礎設施，使基礎建設更普及。要能連上網路，基礎設施是必備條件，歐洲各地區網路建設與使用狀況之間存有差異，有些地區有光纖與 5G 覆蓋；有些地區則還停留在網速較慢的限制下，

基礎建設的普及與均等是重要的。同時 Andrea Garcia Rodriguez 表示在數位主權的議題上，各國政府將地域國界的概念複製到網路虛擬世界上是一種非常危險的網路空間治理方式。

Andrea Garcia Rodriguez 進一步提出「我們需要建立哪些保障措施來保護網路自由？」的議題。他指出我們看到了越來越複雜的網路威脅形勢，尤其是中國大陸與俄羅斯，加強對網路空間的監控是有目共睹，實施嚴格的控制，以避免網路活動產生負面影響。

學生代表 Johannes Thumfart 從何謂數位人權談起，內容中有各方意見對於數位人權議題的看法，同時提到科技人權、數據人權等人權議題。其中也提到歐洲數位人權的雙重關切（Double concern）議題，並回顧歐洲過去幾年來關於數位人權的行動：縮小投資缺口、使歐盟工業和技術能力適應競爭環境等，並舉法國總統目前實施的法案：籌碼法案、數位市場法、數位服務法、數據治理法、數據法為例討論其對經濟影響。也討論到歐盟美國數據傳輸和法律確定性問題，像是避風港（2000）、愛國者法案（2001）、斯諾登的啟示（2013）等隱私保密強化的思考案例。

科學民意調查 Florence G'Sell 表示，歐洲過度監管網路技術發展的做法正在傷害中小型企業，這會導致中小型企業失去與中國、美國等大型國家競爭的籌碼。同時認為歐洲數位主權的核心問題為歐洲數位產業和整個產業，主要是出口導向。促進數位主權可能包括任何形式的經濟保護主義。

捷克工業和貿易部長的顧問 Jaromir Novak 同意 Florence G'Sell 的觀點，網路空間的監管在兩三年內一團糟。現在有太多立法在歐盟層面獲得批准，對於想要與大型科技公司競爭的小公司來說，這可能真的是有害的。我們應該專注於減少障礙及監管，提升技術創新研發，因為它肯定會改變未來的網路。

本會議探討世界各地對「數位主權」一詞的不同理解，並將該詞在歐洲的使用置於全球範圍內，討論將尋求確定與這個新術語相關的網路最大機會和威脅。各參與者在會議中熱烈討論與數位主權相關議題，包括世界各國如何以不

同的方式使用「數位主權」一詞、歐洲主要參與者如何使用數位主權術語、數位主權政策會如何損害網路基礎設施，又如何避免、地理邊界的劃定如何影響全球網際網路？等問題，而這次討論結果並無法取得共識，值得後續持續探討。

(4) 跨國連線：歐洲資料閘道平臺及全球門戶計劃

會議名稱	跨國連線：歐洲資料閘道平臺及全球門戶計劃 International Connectivity: European Data-Gateway Platforms and the Global Gateway
會議時間（CEST）	2022 年 6 月 21 日 16:30 – 17:30
摘要撰寫	2022 網路治理研習營 實習學員：韋◯祥

摘要：

- 主持人：Tomas Lamanauskas, Managing Partner of Envision Associates
- 與談人：Delphine Bernet-Travert, David Ringrose, Filipe Batista, Valter Nordh, Eka Kubusidze

來自歐盟對外事務部（European External Action Service）的 David Ringrose 開場說到主權的概念是有選擇的自由，歐洲致力於支持發展開放自由的單一安全網路。在 BELLA 計畫中，2021 年 6 月與合作伙伴興建了 EllaLink 海纜，讓拉丁美洲得以與歐洲直接互聯，此計畫除了硬體投資外，也讓雙邊符合 GDPR 規範，是標準上的整合。

擔任獨立管制機關小組（Independent Regulators Group，IRG）秘書長的 Delphine Bernet-Travert 分享從政治傳播角度切入的觀點，他點出不同政治敘事用詞本身就代表不同立場，例如講到歐洲主權（Sovereignt）時並非意指陶片放逐法（Ostracism）的那種，而是引出歐洲堡壘（Fortress Europe）的概念，而這本身就帶有部分負面意象。

來自喬治亞經濟與永續發展部（Ministry of Economy and Sustainable

Development of Georgia）的 Eka Kubusidze 提到國內與周邊五個國家都有光纜連線，將發揮自身處於歐洲與亞洲之間的地理優勢，以歐盟觀點出發，並支持歐洲維持網路開放存取。

代表葡萄牙通訊管理局（ANACOM）的 Filipe Batista 講到歐洲支持數位保護（protective）的概念，因此能有主權及自治，但因為歐洲是開放市場，並不會成為數位保護主義（protectionist）。Filipe 拋出了兩個問題，首先歐洲雖然本身市場很大，但如果未參與其他數位市場，不太可能成為全球數位經濟的領頭羊；歐洲是第三大數位資料儲存國，如果想成為世界級的資料匯流中心，就必須保持與世界的連線，並保證可連線性的安全及冗余。

北歐研究教育網路（NORDUnet）執行長 Valter Nordh 提到合作是最重要的關鍵，學術社群及研究單位會互相合作，因此不太認同歐洲堡壘的概念，而是認為可以將歐洲視為一座島嶼，需要確保和世界上其他島互聯。網路連線性對學術社群是重要的，當網路品質達到一定水準，學術社群會開始以我們從未想到的方式使用網路，將提出創新的點子，而最後還是要走到社會大眾才能達到完整循環。

有與會者提到關於資料跨境移動的問題。以往伺服器都放置在一起，而現今運算伺服器與儲存叢集可能位於不同的國家，產生了很多資料跨國移動的需求，除了增加對骨幹網路的需求，也因而衍生一些法律上的問題。學術社群在意的是研究本身，不在意網路底層走過了哪些國家。

(5) 監管新興技術：人工智能和數據治理

會議名稱	監管新興技術：人工智能和數據治理 Regulating emerging technologies: artificial intelligence and data governance
會議時間（CEST）	2022 年 6 月 22 日 10:30 – 11:15

摘要撰寫	2022 網路治理研習營 實習學員：徐○為

摘要：

本場主持人為 Thomas Schneider，與談人包括法國里爾的 EDHEC 商學院副教授 Gianclaudio Malgieri、埃及國際專家 Golestan Radwan 及 For Humanity 的執行董事 Ryan。

在新興科技蓬勃發展的背景下，本會議旨在討論如何監管新興技術，但從監管原則的訂定到監管實踐，仍然是需要持續討論的關鍵問題。隨著人工智能（AI）和大數據的新興技術蓬勃發展，我們正在見證一場技術革命。進步和創新是社會乃至於我們生活方式的原動力，新科技正全面性影響著全人類的點點滴滴，改變著人類的生活方式與社會的運行規則。雖然新興科技帶來多面向的好處，但同時伴隨著複雜而緊迫的法律、倫理、政策和經濟等等問題，迄今為止具有高度不確定性。目前可以觀察到的是新興科技對人民享有的人權和基本自由以及民主演進的運作產生重大影響。因此，它們需要仔細分析並採取治理監督行動。

法國里爾的 EDHEC 商學院副教授 Gianclaudio Malgieri 表示，人工智能的發展重點是要能帶給社會大眾信任感且能被信賴。科技帶給人類便利，與此同時也產生隱私等資訊安全疑慮，人工智能也可能傷人於無形，甚至有可能對於人類的身體、心理、社會與經濟產生負面影響尤其是在社交媒體上人工智能具有一定的影響力，所以可能需要人工智能法案，同時也提出人工智能法案實施的政治風險等,所以人類對人工智能設計和開發的監督是極重要且要慎重考慮。

埃及國際專家 Golestan Radwan 在發展人工智能與新興技術監管提出兩點看法。一、跨區域對話的重要性。網路無遠弗屆，但不同國家與地區有不同的網路基礎建設，網路發展步調也不同，因此我們需要區域偕同努力，不同地區需要坐下來一起討論關於新興技術的看法，人工智能是一項非常跨界的技術，我們不能違背不同國家的法規或指導方針，從而阻礙創新。要在鼓勵創新進步

的同時最小化風險。二、彼此互相尊重差異。讓我們不要試圖將我們自己的價值觀和自己這樣做的方式強加於他人。如果人工智能法案現在必須成為全球所有人工智能監管的基礎，是相當危險的，可能會疏遠世界其他地方的人，而將一些地區排除在外，這是我們所不樂見的情況。

For Humanity 的執行董事 Ryan Carrier 表示在設計人工智能監管制度時，要充分考量人類風險的性質，例如道德、偏見、隱私、信任等等，以及從設計監管制度一直到監管增修等等，需要充分考量每個環節的所有風險，並進一步提出以人為本的監管方法，Ryan 呼籲和要求需要多樣化的投入及多方利益相關者的反饋，且要廣納多元性別、弱勢族群等需求，融入思想的多樣性、生活經驗多樣性。在人工智能出現異常狀態時的風險也必須慎重考量，在監管同時也要設計當 AI 出現功能障礙或者出現異常時的解決方案。

主持人 Thomas Schneider 最後提出總結：我們試圖監管什麼？什麼屬於監管範疇？什麼不屬於監管範疇？我們如何衡量與定義我們試圖監管的事物的概念？是我們要深思的與討論的內容，我們希望歐洲委員會產生的公約，可以具差異性能權衡各方意見、區域差異、發展狀況等，來因地制宜的訂定監管措施。

(6) 未來網際網路宣言

會議名稱	未來網際網路宣言 The Declaration for the Future of the Internet
會議時間（CEST）	2022 年 6 月 22 日 12:15 – 13:15
摘要撰寫	2022 網路治理研習營 實習學員：江◯毅

摘要：

本場次討論的是在 2022 年 4 月 28 日，美國與歐盟執委會等 60 國共同簽署並發布的「未來網際網路宣言」（The Declaration for the Future of the Internet），文件中重申將促進一個開放、自由、全球化、可互通性、可靠和安全的網際網

路，並包含五個主要原則，包括保護及促進所有人之人權、基本自由、推動全球化的網際網路、增進包容與可負擔的網路近用、促進數位生態系中的信任以及加強多方利害關係人網路治理。

第一位與談者是網路治理論壇（IGFInternet Governance Forum） 多方利害關係人諮詢小組（MAGMultistakeholder Advisory Group）主席 Paul Mitchell，他表示 IGF 從創立之初就以多方利害關係人治理模式為基礎關注公共議題，目的與「未來網際網路宣言」中希望加強的核心民主價值及普世人權一致。網路使用者的數量相對於 2000 年代初期的 4 億，現在已經成長到超過 50 億，過去將近三年的時間中，因為疫情的影響，更加展示了網際網路的價值，卻也帶給生活在絕對線下世界（absolutely off-world）的弱勢邊緣群體不成比例的影響，如何與這些人連結並確保他們的網路可近性也是「未來網路宣言」的目標；現在，IGF 有 24 個充滿活力的議題小組，擴張到包含 152 個國家、區域、次區域及青年網路治理論壇，帶來了很多的關注，未來，IGF 在網路治理的議題上將繼續擔任先鋒，與來自世界各地的多方利害關係人共同合作、腦力激盪，透過論壇思考網路安全、性別、網路架構的政策等議題，並支持「未來網路宣言」。

第二位與談者為英國電腦學會（British Computer SocietyBCS）資訊安全專家小組 Information Security Specialist Group（ISSG）主席 Steve Sands ，他表示:「未來網際網路宣言」的重要性在於重申並文字化已經過長久討論及關於如何形塑一個更開放全球網路環境的原則；歐盟執委會正在規畫今（2022）年稍晚舉行高層級的政治會議，邀集所有利害關係人，由來自不同社群的成員討論該如何實踐宣言中的五項原則，此會議著眼於盡可能拓展參與此討論的國家數量，提升可以公開實踐這些要件的利害關係角色數量，而最重要的是確保在過程中能有充分的時間跟空間具體討論實踐方案。

第三位與談人是進步通訊協會（Association for Progressiive CommunicationsAPC）執行董事 Anriette Esterhuysen，她認為：「未來網際網路宣言」在保障公眾性的部分差強人意。形成該宣言的過程中，多方利害關係人

治理模式中由下而上發展的精神未被落實,也因此本宣言失去真正透過多國間、跨政府的溝通來獲得國際廣泛支持的機會，對於歐洲國家而言，由於有很澈底的被諮詢，他們在很多面向上更願意支持此宣言，然而對於印度、巴西、南非及其他南方國家（Global South）來說，本宣言更像是一個已完成的產品，只能被動選擇是否接受，並不真的有機會可以參與這個宣言的形成，因此他們更傾向不接受此宣言。

Anriette Esterhuysen 認為，在形成國際合作的共識時，有兩種可能的工作途徑：其一，一個更由下而上的、考量多方利害關係人、更多國家實質參與議程設定的方法，風險是可能只能達成更少實質內容的共識，但這樣才能形成一個所謂的更全球性的共識；其二，類似美國與歐盟執委會本次形成「未來網路宣言」的工作模式，可能可以獲得實質內涵可觀的文件，但文件內容可能更難獲得廣泛支持；他並表示其實認為兩者皆有重要性，但更務實地看，如果此宣言真的想要更廣泛的社群支持，應該重新檢視凝聚共識的過程，用更開放、跨國、由下而上的方式，以爭取更多的合作空間。

第四位與談人是來自 University of Aarhus 的 Kleinwächter，他呼應了 Anriette 女士的觀點，他認為「未來網際網路宣言」有很好的企圖，重申了網際網路開放性、包容性、非碎片化、透明、自由這些重要的原則，但就程序及實行的過程而言，有三個缺點：第一是矛盾、缺乏操作流程、與現存其他全球宣言脫節；矛盾指的是，宣言中提到支持強而有力的多方利害關係人治理模式，但這個宣言的形成過程中多方利害關係人或多或少被排除在外，因此讓宣言的公信力下降；其二，此宣言有好的原則，但缺乏國家、區域、乃至全球的層級上,該如何重新檢視這些原則的流程;其三,聯合國有數位合作路徑圖(Roadmap on Digital Cooperation)，國際上也另外有自由線上聯盟（Freedom Online Coalition，FOC)，本宣言最後有提到這些，但這個宣言與他們的關聯性，是平行的、可替代的、競爭性的哪一種關係並沒有闡明，因此讓人疑惑既然有這些現存倡議或合作方案，本宣言可以帶來什麼更近一步的行動？

第五位來自瑞士政府的 Jorge Cancio，分享了尚未參與「未來網際網路宣言」的國家觀點，他由三個面向解釋為何瑞士並未簽署此宣言，包含瑞士並非歐盟成員，該國強而有力的共識決策傳統，以及做為一個已經是開放、自由、安全、單一、互用性、值得信任網際網路忠實的支持者，瑞士政府並不清楚參與本宣言的實際意義為何。首先，由於非歐盟成員，因此並未參與歐盟執委會討論此宣言的過程；同時，瑞士是一個小但對國際高度依存的國家，有很強的由下而上決策模式的傳統，試著在決定所有決策過程中，包含聽見、諮詢所有利害關係人，因此通常需經歷一個很長且困難的過程；最後，作為聯合國總部的地主國，瑞士跟聯合國有很強的連結，也對聯合國、IGF、EURODIG 都強力支持，也對高層級專家小組樂觀其成，瑞士政府會盡最大努力去做到那些跟民主、人權相關的目標，對於參與宣言，則尊重國內的意見形成。

第六位與談者，來自義大利外交部的 Riccardo Villa 表示，義大利在 2021 年加入 Freedom Online Coalition，這展現義大利政府積極的確保義大利不僅展現也提供對跨國參與主動的貢獻，Riccardo 先生提到聯合國開放工作小組（Open-Ended Working Group，OEWG）有個倡議叫做 program of action on cyber，現在有 60 個共同締約國，義大利政府會繼續推動倡議，不僅對聯合國會員，透過兩國或國家群的方式，雖耗費很多時間、精力，但義大利堅定相信，確保一個穩定的平臺是政府應該採取的方式；最後，Riccardo 先生對前面 Steve Sands 先生提到的今（2022）年稍晚將舉行的高層級政治會議，Riccardo 先生希望更近一步，在會議中發展一些包含深化教育在內新的國家策略技巧。

最後一位與談者是英國政府的代表 Nigel Hickson，他表示就英國思考未來網際網路，參與及思維的演進而言，這個宣言來的正是時候，程序確實如前面的講者所言並非那麼由下而上，但畢竟這是政治宣言，所以流程尚有討論空間，但目前的國際形勢而言，有其重要性，俄國在入侵烏克蘭前即表示過他們會加強 ITU 對網路治理的角色來取代 ICANN 的工作，及其他目前在做這部分的實體，他們會有效率的推動這種高到低的治理控制，為此，透過宣言重新確保自

由、開放等原則是重要的。

綜上所述，大部分與談者認為內涵是好的，但過程有待改善，主要是多方利害關係治理模式沒有被落實，很多國家沒有參與簽署，但好消息是也有許多國家正準備簽署，且針對這些問題及不足的解決方案也正在著手進行。Steve Sands 提到預計今年將有個高層級的論壇，處理如何著手相關後續，這件事情令人期待，應該從過去的發展記取經驗，凝聚更多國家的共識，或許要整合過去有的 FOI（Freedom of information，資訊公開）、UN 協議等眾多的網路相關倡議，也或許如前面提到的可以更少的原則來確保更廣泛的支持。

(7) 主權及網際網路：網路分裂的風險

會議名稱	主權及網際網路：網路分裂的風險 Sovereignty and the Internet: a risk of fragmentation
會議時間（CEST）	2022 年 6 月 22 日 14:45 – 15:55
摘要撰寫	2022 網路治理研習營 實習學員：韋◯祥

摘要：

- 主持人： Vittorio Bertola
- 與談人： Peter Koch, Jurgita Miseviciute, Esteve Sanz
- 團隊成員：ittorio Bertola, Giovanni De Gregorio, Luc Steinberg, Adam Peake, Samo Grasic, David Frautschy, Charles Martinet, Peter Koch, Irene Signorelli

這場會議由來自開源軟體供應商 Open-Xchange 的 Vittorio Bertola 擔任主持人，開場提到了網路分裂的概念是全球網路分裂為多個部分，彼此無法（或只能有限度的）互相通訊，這場重點將放在什麼是網路分裂、哪些倡議會導致網路分裂。在二、三十年前網路主要從歐美學術圈開始發展，後來普及為平民也能上網後才突然變為全球議題,世界各國都以非常不同的態度規範網路世界,像是網路的發源地美國對於網路相當開放、北韓至今還只有封閉網路、中國雖

然可以對外連線但有防火長城。我們都同意不希望網路是分裂的，重點是找出會導致分裂的倡議、釐清法規該有的界線。

來自德國網路資訊中心（DENIC）的 Peter Koch 代表技術社群，點出就算是針對大公司制定規範，且法律上提供小公司豁免權，也需要注意要求新創公司盡到法遵義務還是相當困難。對於網域名稱及電子信箱等許多產業，雖然通訊協定在設計初期都高度去中心化，但實務上都出現規模經濟、贏者全拿的局面，但如果法律制定不當，或許會比放任還糟。

接著是代表隱私技術公司的 Jurgita Miseviciute，講到他們 ProtonMail 的信箱加密技術讓人權倡議者、新聞工作者，或是身處於非民主國家的人民，得以不受言論審查安全的通訊。完全不控管的網路環境無法正常運作，但也不能過度規管，重要的是找到兩者之間的平衡點。適當的管制可以促進創新、提供更多樣性的選擇、符合數位主權的想像。適當規管以塑造更好環境的例子，在金融業、能源界、通訊業大家都有目共睹，為了打造對所有人來說更好的網路，現在也該是科技產業加入的時候了。

第三位與談人是來自歐盟執委會（European Commission）的 Esteve Sanz，提到如果人民們在上網時接收到顯著不同的訊息，那網路連結世界的功能就失效了，還可能會因此造成嚴重的地緣政治衝突，因此這不只是技術議題，而是歐盟在意的重要政治議題。講到網路分裂的本質，其實就算是中國的大內網也是用 TCP/IP 標準、DNS 協定，因此至少大家都在同一個技術框架底下。但觀察到特定國家正推動從通訊協定標準上重造輪子，讓根本的網路底層就是不相容的，讓使用者得要從兩種網路之間作出抉擇。

來自英國電信管理局（Ofcom）的 Connor Corbett 率先提問，如果當政治影響力出現在標準制定組織，讓某些技術標準與現存實作不同，要到多大程度才會威脅到網路分裂。 Esteve 先說到這顯然會是政治上的一大混亂，對於選擇了新標準的開發中國家，經濟上的混亂程度也不可忽視，因為架構上的不相容，需要大規模的汰換設備，在投資時就會讓全球市場發現這個警訊。

一位有在參與 YOUthDIG 的國際關係碩士生 Charles Martinez 問到，大家都提到維護全球網路在各方面的重要性，但也提到在歐洲希望數位空間需要被規管，那各位覺得數位主權是造成網路分裂的元兇嗎？或認為這是兩者之間的取捨，並非需要在意的議題？Esteve 覺得在歐盟討論數位主權時最好的方法是看目前怎麼做的，也就是研讀一系列的準則法規，而本意不是為了分裂網路、無視人權。歐洲的成員本來就相當多樣，各國對數位主權的想像都不同。

(8) COVID - 19 及地緣政治衝突之「假訊息」現象

會議名稱	COVID - 19 及地緣政治衝突之「假訊息」現象 Focus Area 4, Subtopic 1: Responding to disinformation in times of COVID - 19 and geopolitical conflict
會議時間（CEST）	2022 年 6 月 22 日 16:20 – 17:30
摘要撰寫	2022 網路治理研習營 實習學員：李◯毅

摘要：

本文要介紹的是第四個主題「紛亂的網路時代」的第一個子議程「COVID - 19 及地緣政治衝突之『假訊息』現象」。本場次的主持人為歐洲廣播聯盟（EBU）國際關係部負責人 Nicola Frank，他提及近年來出現許多以經濟利益為目的的假訊息，對民主政治決策過程造成強烈的威脅，而實際上也可以看見這些假訊息造成扭曲的公共辯論及群眾的兩極分化，因而如何面對此問題，成為非常重要的課題。再者，從烏俄戰爭可以看到，這些假訊息甚至被武器化了，社交媒體也不見得像其自稱的「中立」。

第一位講者是同時於奧地利因斯布魯克大學（University of Innsbruck）以及德國漢堡萊布尼茲媒體研究院（Leibniz Institute for Media Research）任職的 Matthias C. Kettemann 教授，他的講題是「戰時假訊息之公開與私人管理方法衝突」。其提到假訊息是自古皆存在的問題，只可緩解，但實際上無法解決，就算

解決了他也不會消失。以烏俄戰爭為例，在虛擬世界我們看到攻擊烏克蘭的假消息，在現實世界中我們看到俄羅斯攻擊烏克蘭的網路基礎設施。歐盟的數位服務法賦予平臺審查的義務，這是一個管制假訊息不錯的方式。

第二位講者是聯合國教科文組織、言論自由和記者安全計畫之專家（Associate Programme Specialist, Freedom of Expression and Safety of Journalists, UNESCO）的 Rachel Pollack，他的講題是「訊息流行病的大流行」。其提到媒體行業的商業模式面臨重大挑戰，廣告數量下降了 50%。此外，記者的安全問題也在加劇，過去五年中有 455 名記者在工作中喪生。經查有超過 100 萬則推特推文是針對 COVID - 19 的假訊息，亦可觀察到民眾對社交媒體及傳統媒體資訊的信任度持續下降。因此，聯合國教科文組織正在努力打擊假訊息，也得到了歐洲議會的支持，並在 9 個國家及 4 個區域培訓事實查核員及記者，也開設線上課程教授媒體素養課程。

第三位講者是歐洲議會媒體網路治理部的媒體小組負責人 Urska Umek，他的講題是「人權角度之觀點」。他認為限制媒體言論自由是有必要的，因為假訊息對於人權亦有重大影響。但限制媒體言論自由可能會違反歐洲人權公約，所以只能暫時縮小公約的適用範圍。

第四位講者是 EDMO 顧問 Giacomo Mazzone，他的講題是「戰爭期間的事實查核」，他提到歐盟幾年前要求平臺簽署維護平臺安全的自我承諾協議，賦予其審查恐怖主義言論的義務。因為人工審查有其限制，像是說英語的審查員可能無法處理俄語的言論，故德國之聲設計了一個可以自動識別不同語言的程式以過濾假訊息。

第五位講者是歐洲廣播聯盟（EBU）新聞委員會主席 Eric Scherer，他的講題是「公共媒體於危機時期打擊假訊息」。他發現訊息越來越民粹化，越能煽動群眾情緒的訊息越容易散播，造成整個歐洲日益嚴重的兩極分化。歐洲亦有出現許多仇視記者的聲音，認為新聞菁英主義及白人主導的新聞媒體製造假訊息。但其實多數假訊息都是透過臉書、Youtube 等平臺散布而非記者。記者們正面臨

非常嚴重的網路騷擾，尤其是女記者。故記者應該要以自身的優勢為基礎，更傾聽民眾的聲音，只有與民眾合作才是擺脫這一切危機的出路。

主持人 Nicola Frank 於總結時提到，歐盟只是提供一個監管的框架，平臺的自律才是最重要的。且不只是平臺，媒體作為公共服務的工具，也應該要落實媒體自律，才能降低假訊息對公民社會造成的危害。

（二） 其他網路治理會議

1. 會議資訊

本次安排學員的網路治理會議包含 2020 年由台灣網路資訊中心以實踐社會責任，秉持社群共有共治共享的網路概念來創立的「台灣網路講堂」（Taiwan School on Internet Governance, TWSIG），該講堂整合與促進國內網路社群針對不同網路治理公共政策議題之討論，與我國網路社群共同建構一個網路公共議題的推廣平臺。臺灣網路講堂平均每月約 1 場次之講座/演講辦理，本次有 2 名學員選擇參與講堂的場次。

此外，由交通部所委託 NII 產業發展協進會辦理的計畫中，規劃了一系列與 ICANN 相關議題、國際網路域名及資訊安全相關政策發展等相關推廣活動，本次也有學員選擇該系列議題推廣活動作為實習參與。另有 1 名學員選擇線上參與於華盛頓特區所舉辦的 IGF-USA。

2. 參與場次

表3.　實習學員參與網路治理相關會議場次

負責學員	日期/時間	題目
江◯毅	7 月 12 日 14:00 –16:00	元宇宙的新維度治理框架（台灣網路講堂）
李◯毅	7 月 21 日 11:00 –12:15	通訊加密議題之辯論（IGF-USA 2022）

	（CEST）	
韋○祥	7 月 12 日 14:00 –16:00	「公共空間的人工智慧應用與隱私隱憂」專題講座
徐○為	8 月 29 日 14:00 –16:00	自拜登數位資產政策，一探臺灣數位金融之機會與挑戰（台灣網路講堂）

*按照時間排序

3. 場次摘要

(1) 元宇宙的新維度治理框架

會議主題	元宇宙的新維度治理框架
主辦單位	臺灣網路講堂
會議時間	2022 年 7 月 12 日 14:00 - 16:00
摘要撰寫	2022 網路治理研習營 實習學員：江○毅

- 主持人：李建良所長（中央研究院法律學研究所）
- 與談人（按照姓名排序）：李紀寬助理教授（清華大學科技法律研究所）、高崎鈞理事長（台灣區塊鏈愛好者協會）、曹筱玥系主任（國立臺北科技大學設計互動學系）、陳家駿理事長（台灣資訊智慧財產權協會）

摘要：

本場講座主持人中央研究院法律學研究所李建良所長表示，這波元宇宙的討論風潮從臉書母公司更名為 Meta 開始，但虛實整合的相關技術發展許久，其中涉及的商機、潛在風險、法律問題都值得探討，不論規範方式是平臺自治還是平臺外部的法律，始終將面臨法制跟科技的碰撞，而這當中的關鍵是法律人需要知道實際狀況是甚麼，才能因應制定並適用合適的規範。

台灣資訊智慧財產權協會陳家駿理事長指出，雖然作為一個執業 42 年的律師，他始終對新興法律議題很有興趣，接著他從許多不同面相提供了元宇宙中，

可能會面臨的法律適用議題，其中多數篇幅關於虛擬替身 Avatar 以及 NFT，包含：Avatar 是否代表真人、元宇宙中來自他人 Avatar 的騷擾是否應該適用妨害電腦使用罪、為了做出高度擬真 Avatar 而蒐集的眾多生物特徵是否屬於個人隱私的範疇， NFT 相關的則有：NFT 的法律性質是證券還是物品、將藝文作品內容上傳變成 256 位元代碼的 NFT 是否涉及公開和重製、將藝文作品轉換為 NFT 是否有侵犯商標權或著作權等。

陳理事長認為目前尚未有全面整合線上線下生活的網站，對於元宇宙到底是甚麼，大家都還在瞎子摸象，並且相關技術與應用是新興時代的產物，或許不需要現在就急著立法跟指定專責單位，可以先適用現存法律，若有無法處理的再立新法，從這個角度來說，法條上怎麼界定構成要件以滿足罪刑法定，是目前需要處理的部分。

台灣區塊鏈愛好者協會高崎鈞理事長探討了元宇宙中的定義議題、元宇宙的規則制定、區塊鍊的性質；從最基本的如何定義原宇宙，往下延伸到怎麼定義元宇宙中的人格、定義財產交割等；元宇宙的規則及架構有不同的可能性，有中心化及去中心化等不同架構，其中一個重要的概念是，當前各數位平臺使用不同的帳號密碼，在元宇宙中則會希望一組就可以通用；高理事長也提到了以去中心化的架構而言，在沒有中間人的情況下，法院想要查扣或阻止交易發生，基本上無法達成，但透過現在智能合約的強制執行概念，若將法律或需要履行的規則寫進區塊鏈就可以達成；而區塊鏈能去中心資料治理，並具有數據的互操作性，適合跨境、跨領域、跨產業以及跨平臺的使用，但區塊鏈不能處理鏈下資產，也尚不能進行複雜運算，更無法積極防偽，因此高度仰賴區塊鍊的去中心化架構也有其限制；高理事長表示，中心化、去中心化其實相生相剋，若中心化夠公開透明並提供足夠保障，未必一定要使用去中心化的架構。

清華大學科技法律研究所李紀寬助理教授主要分享了元宇宙的法律治理、規範及監理議題，李教授提到，雖然距離完全的虛實整合還有一段落差，但現況下有一部份已經存在，重要的是平臺提供方當前多以定型化契約規範使用者間，但未來虛實整合的程度越來越高，同樣的法律議題，會不會因為環境改變而需要調整，是否可能使某些風險增大、侵害增加？並進一步造成新的法益侵害，例如：Avatar 在元宇宙裡，靠其他人的 Avatar 很近，在其耳邊講話，是否構成性騷擾？偷偷照相是否侵害肖像權？會不會因為元宇宙的普及讓過去及現

在政府沒有規範的情形，未來政府需要著手規範？關於元宇宙與人才培育，李教授則期待業界、法律界可以給學生更多合作的機會。

國立台北科技大學設計互動學系曹筱玥系主任則透過影片介紹了該系同學將服裝設計與 3D 科技融合的作品，以及學校與旅遊觀光合作的虛擬藍眼淚觀光，提供了沉浸式感受。曹主任表示元宇宙技術中，體感設備、觸覺跟嗅覺回饋是目前的努力方向，遊戲音樂的應用程式及智慧醫療也都是發展趨勢，這也顯示未來體驗經濟，別於現在高度講求實體商品的經濟模式，密室逃脫、劇本殺等線上體驗活動，更有共創性需求的經濟活動將會越來越普及。

講座最後的問答時間，高崎鈞理事長表示，在區塊鍊的架構下，礦工作為節點是不是可以信任的，會影響智能合約是否可以被視為中立、可被信任的機制，而去中心化與中心化其實是程度差異，如君主專制與君主立憲，是集權程度的差異，但並非全然，法治需要視實際狀態中會遇到甚麼問題調整，中心化管理未必是壞事，去中心化也不必然是烏托邦，有些科技的狀況可能會很快就被技術調整修正，因此也不需要積極的介入規範。

曹筱玥系主任表示，體驗經濟的發展是她與學生的互動中所觀察得知，曹主任認為過去世代的娛樂或許是唱歌、吃大餐，而現今世代的娛樂則會希望跟社群連結，親身體驗是重要的，也因此甚至發展出可以吃的 NFT ，這些都是未來的重要發展趨勢。

(2) 通訊加密議題之辯論

會議名稱	通訊加密議題之辯論 Beyond the Encrypted Content Debate
主辦單位	IGF-USA
會議時間（CEST）	2022 年 7 月 21 日 11:00 am –12:15pm
摘要撰寫	2022 網路治理研習營 實習學員：李◯毅

摘要：

2022 年 7 月 21 日於華盛頓特區舉辦的 IGF-USA。本文要介紹的是上午的第二場大會演講「通訊加密議題之辯論（Beyond the Encrypted Content Debate）」。

本場次的主持人是政客公司（Politico）的記者 Eric Geller，與談人分別是民主與科技中心（Center for Democracy and Technology）技術長 Mallory Knodel、美國國家兒童失蹤與受虐兒童援助中心（National Center for Missing & Exploited Children, NCMEC）資深副主席暨法務長 Yiota Soura、美國聯邦調查局（Federal Bereau of Investigation, FBI）科技政策辦公室助理主任 Darrin Jones、網際網路協會（Internet Society）政策倡議主席 John Morris。

主持人 Geller 開場就提到，通訊加密是近期非常重要的議題。舉例而言，政府到底有沒有權利破解嫌疑人的手機訊息進行取證，隱私權與犯罪偵查間到底該如何權衡，是很困難的問題。

首先發言的 John Morris 認為，資料加密這個議題已經討論多年，但更需要的是從民間來的專業意見，Yiota Soura 也認同 John 的看法，並認為這個議題不應該僅僅是被傳媒關注而曇花一現。Geller 回應，美國最高法院近來也針對健保資料庫的隱私問題做討論，有些州立法規定，不須經病人同意即可儲存病歷資料並加以使用，而資安管控不佳使這些個資極易外流，因此更應該升高大眾對於資料加密及個資保護議題的認識。Mallory Knodel 認為弱勢族群及青少年對於資安的認識不足，常常將密碼外洩給陌生人，造成不可挽回的損害，因此必須加強大眾對於資料保護的認識。

當主題來到是否應讓 FBI 解密人民私下之通訊資料以獲取個資，於 FBI 任職的 Darrin Jones 提出了三個重點：第一，FBI 從來都沒有想要請科技公司為其開後門藉以獲得人民之通訊資料及個資，亦未請求任何可以直接獲取資料的權利；第二，FBI 傾向採取「設備端通訊監察」，也就是說 FBI 可以在通訊尚未加密前之發出端或已解密後之收取端，紀錄未加密或已解密之通訊內容；第三，最直接的下策即為直接扣押該設備，解鎖該設備並獲取資料。

Mallory Knodel 認為，民主國家應該要建立透明且可問責的制度以使大眾信賴，然而根據 Edward Snowden 於 2013 做出的全球監控揭露報告（Global surveillance disclosures）的結果卻事與願違，大部分國家會採取非民主方式獲取

個資或監視人民，這是十分令人擔憂。

John Morris 引用英國國會議員 Ian Levy 於 2022 年 7 月 21 日發表的論文「平臺對兒童安全的思考（Thoughts on Child Safety on Commodity Platforms）」，指出通訊監察最適當的方法還是「設備端通訊監察」，這在技術上是較容易被克服且能確保科技業者不需為執法機關開後門。John Morris 認為這些大的科技公司有時候並不是很贊同 FBI 的指令，因為這些公司需要對自己的客戶負責，客戶使用該軟體是基於信賴該軟體會保障個人隱私，倘若 FBI 會要求該公司提供客戶之通訊資料，則容易使客戶喪失信心，進而造成客戶流失，因此 FBI 也很難憾動科技巨頭們。Mallory Knodel 回應，在沒有通訊設備的年代人們以口頭或書面方式傳遞訊息，是最有隱私的方式；然而到了在數位時代，使用這些科技設備（如電話、傳訊 APP ）時就應該要明白這些訊息不可能被完美保護，因為其仍大可使用傳統方式通訊，若欲使用科技方式通訊則就要具有訊息可能流出的認知。 Darrin Jones 亦指出，美國憲法第四修正案賦予政府搜索扣押之權利，亦即個人隱私權在滿足特定要件下必須讓步，因此主張「絕對不可讓步的隱私權」是不可理喻的。

接著議題轉到了兒童色情的預防，Yiota Soura 指出雖然法律的執行面是個大哉問，但其實最困難的點在於犯罪的發現，如果過度以商業面考量科技公司客戶的隱私需求，則難以解決兒童色情之問題。據統計每年約有高達二千萬的兒童色情案件，但在這資訊「充分加密」的年代，這些案件都極難被執法者發覺，也不知從何辦起。因此這些大公司，如 Google、Dropbox 等，應該要在維護客戶隱私權及打擊兒童色情間，找出合理的平衡點。Darrin Jones 回應，他覺得客戶追求隱私是合理的，但不應要求「絕對」的隱私，就像在收 e-mail 時我們會期待科技公司可以幫我們篩選並過濾掉垃圾信件，這也是限縮自身的隱私權才有辦法做到。因此若要追求安全，就不可能享有絕對的隱私保護。

最後有人提問是否應該要以保護孩童為由監控他們的手機？Mallory Knodel 提及自己擔任學校老師的經歷，他發現青少年極度保護自己的秘密，他們不希望自己與另一半的傳訊被父母或任何人發現，因此我們還是要尊重孩子的意願不輕易窺探他們訊息內容。

Darrin Jones 最後總結，他認為這世界不是完美的，也不可能找出一個完美的制度。但是，我們應該讓科技來牽動我們的核心人權價值嗎？或是，我們是

否應該讓核心人權價值引導身為國民的我們，是值得深思的。

(3) 公共空間的人工智慧應用與隱私隱憂

會議主題	公共空間的人工智慧應用與隱私隱憂
主辦單位	交通部
會議時間	2022 年 08 月 11 日 14:00 - 16:00
摘要撰寫	2022 網路治理研習營 實習學員：韋○祥

在美國槍擊事件頻傳的推波助瀾下，不少政府、學校及家長團體開始思考是否需要更強化監控技術的應用。許多業者推出 AI 相關應用試圖解決問題，例如紐約打算在地鐵出入口加裝自動化檢測器，透過 AI 利用外觀形狀判斷，不用架設 X 光掃描器或是打開背包。人工智慧不僅被用於監控，在商業上也有許多的運用，如讓店員知道貴賓走進店裡，進而提供優惠或客製化服務等。

主持人梁理旋副執行長提到科技本身是中性的，端看執行者想法差異會導致不同的結果，因為大家對科技的不了解，很可能會得出 AI 會破壞隱私、是邪惡工具的結論。為了平衡兩邊觀點，因此本場次特別邀請了來自業界及學界的講者，分別從 AI 的實際應用與法律及隱私層面的隱憂切入。

演講一：公共空間之人工智慧應用

講者：張義明總處長（凌群電腦 資安巨資暨智慧城市技術研發處）

凌群電腦張義明總處長以自身在業界二十多年的經驗切入，介紹訓練資料的重要性、公共空間中 AI 實際應用場景、警方如何利用科技輔以執法。在實際談應用之前，他提出最重要的三個議題是資料的來源、合法性、正確性。以微軟推出的 Tay 聊天機器人為例，在 2016 年推出後不到一天，就被網路群眾訓練到出現種族歧視等偏激言論，由此可看出即使 AI 模型本身沒問題，但資

料來源不正確，也會導致 AI 出錯。

張總處長以蘇花改作為 AI 實際運用的案例做說明。對於部分路段只有單線道的蘇花改，以往可能需要先由人工計數車流量、根據公式計算紅綠燈時長，現在 AI 利用監視器影像辨識完不同車種的流量後，可以透過演算法自動調整最佳紅綠燈秒數，分散車流以提高總體疏運速度。外國也有發展出音頻分析技術，在各個路燈上的麥克風收到槍聲後，利用三角定位判斷開槍地點並通報警方，不過臺灣管制槍枝、比較少槍擊案，放鞭炮又會產生誤判，因此除了技術外有很多前置問題要排除。

進到問答環節時主持人先點出一個擔憂，演講中提到人臉辨識等各種影像分析技術，讓監視器像中國天網一般。張總處長解釋中國天網是無時無刻在識別並將辨識結果與真實身份做整合，警員隨時可調閱；臺灣的做法會確定因公需求才能使用，並建立完整機制進行稽核，避免濫用或誤用，且需要時才會把影像匯入軟體，因此本質上還是有所不同。

也有聽眾問到各家廠商販售 AI 產品時，是否會審視客戶的用途正當性。張總處長表示以凌群電腦為例，在收到需求時除了考量技術可行性也會討論適法性，特別是根據長期合作經驗，警方比廠商更在意是否符合現行法規框架、事後可以如何稽核避免誤用。

演講二：AI 監控的爭議與法律規範挑戰

講者：李建良所長（中央研究院 法律學研究所）

下半場的專題講座則由中研院法律所的李建良所長先就公共空間的定義討論起，接著討論何謂侵犯合理的隱私期待，最後講到未來歐盟法律走向。

對於定義空間屬性，戲院及工廠等「非請莫入」的場所算是私人空間，員警可以隨時出入的地點則是公共空間。在一個大家都看得到的公共空間，與隱私本身互相矛盾，可以探討如何算是合理的隱私期待。作為房東當然不能進入房客家中，請了保母也不該在家中用監視器侵犯隱私，老闆查看員工的公司信箱也是有爭議的行為。

行車記錄器的本質也是在監控，如果要探討錄製內容是否為個人資料、有沒有侵犯他人隱私，可以考慮拍攝到的內容是否可辨識出個人。法規明訂路邊監視器是為了防止犯罪，只能設在較容易引發犯罪的地方，如果用來作為主動取締交通違規的資料來源，可能就會產生爭議。

歐盟人工智慧法所涵蓋的層面非常廣，例如原則上禁止為了犯罪偵防目的，遠端進行人臉辨識，只有拯救人質等重大犯罪才能例外使用。也因為 AI 時代的資料串聯非常可怕，因此需要限定使用目的。在搜集資料時要盡到標示告知義務，例如在賣場設置隱藏式監視器，需要讓員工知道裝設位置。最後提到以上種種議題，最終都還是自由與安全之間的辯證及反思，AI 的反應速度與便利性提高，同時提升正確性與安全性，但是否會因此犧牲某部分的自由，或是喪失資料的自主性，都是需要再思考及討論的地方。

聽眾提問到如何針對監控目的，定義幾個可依循的合理原則。李所長以法律角度，拆分為形式性原則及實質性原則兩類。以公部門來說，由於監控會侵害到人民的隱私，進行任何監控都需要有相關的法律依據、必要性，要做目的外利用時也得有相應的理由、依據、必要性，才能夠通過層層審查避免誤用。

(4) 自拜登數位資產政策，一探臺灣數位金融之機會與挑戰

會議主題	自拜登數位資產政策，一探臺灣數位金融之機會與挑戰
主辦單位	臺灣網路講堂
會議時間	2022 年 08 月 29 日 14:00 - 16:00
摘要撰寫	2022 網路治理研習營 實習學員：徐◯為

- 主持人：洪思竹 前所長（海洋大學海洋法律研究所）
- 與談人：楊岳平 副教授（臺灣大學法律學院）、李秉錡 檢察官（新北地檢

署）、Eugene Lim（Head of Private Wealth, Matrixport）

摘要：

NII 產業發展協進會梁理旋副執行長簡單說明本活動緣於因美國總統拜登三月所簽屬的發展數位資產行政命令對於美國各部門、消費者、投資者、宏觀經濟深具影響，要求各部門對金融監管、犯罪偵查、環境、能源、國家安全等層面來制定數位資產行動計劃，由此可見美國政府非常重視數位資產未來發展，面對著全球金融系統數位化浪潮，本場活動邀請國內不同利害關係人，探討臺灣在數位資產發展規劃中所面臨的困境、可能的契機，及如何透過公私協力運作方式，共同在技術架構設計、金融穩定、支付系統、法規環境、人權保障、普惠金融及國家安全等各方面作出必要調整，建構符合最大公共利益的數位金融應用環境。

接著由本座談會的主持人海洋大學海洋法律研究所前所長洪思竹開場介紹三位與談人，首先是國立臺灣大學法律學院楊岳平副教授，畢業於美國博士，關注科技金融相關議題，為我們分享學術觀點；第二位講師為新北市地檢署李秉錡檢察官，在金融犯罪與洗錢防制上有豐富實務經驗，為大家分享實務界觀點；第三位講師則是來自新加坡加密貨幣 Matrixport 公司的 Eugene Lim，分享業界觀點。共同探討在數位金融資產上，臺灣所面臨的機會與挑戰。

臺灣大學法律學院楊岳平副教授分享從金融監管視角看國內外數位資產與監管架構的看法，分成三大面向探討數位資產金融監管議題：數位資產發行層面、數位資產交易層面以及數位資產業者。

數位資產發行層面上，依照是否吸收資金來做分類，例如比特幣的發行不涉及吸收資產，故在監管上相較於有吸收資金的數位金融商品難。有吸收資金的數位金融商品需要找到認購者來購買，不同數位資產發行名目不同：1.承諾返還本金、2.承諾未來分配利潤（分潤型）、3.承諾未來可換取特定商品或服務（功能型）、4.現時換取特定資產或權利。前二者與傳統金融業務較類似，有較高金融監管疑慮；後二者與商品交易或兌換較類似，理論上應惟一般消費者

保護問題，但虛擬通貨價值波動而產生投資人保護議題。

數位資產發行與金融監管上，大致分三種模式：適用既有法規（例美國、英國）、制定特別規範（例歐盟、泰國、馬來西亞）、全面禁止（例中國）。

數位資產交易層面上，大多發生詐欺等資訊不實、操縱市場、內線交易、資訊未充分揭露，而導致不公平不健全交易行為，進而衍生政府監管議題。監管上大致分為兩部分：適用既有法制、另訂特別規範。

數位資產業者監管層面上，以交易平臺為例，大致有使用與開戶規則、使用者資產保管、業者利益衝突之辨識與管理、業者營運活動透明性、交易市場健全性、價格發現機制、技術問題、清算/結算機制等八大面向，監管方式大約有三種方式：回歸既有法規、客戶資產監管、交易平臺監管。

綜上所述，各國對於數位資產的監管態度是逐漸增強監管力道。臺灣目前針對數位資產監管上以不變應萬變方式處理，較屬於弱監管的環境。最後楊教授提出臺灣在數位資產監管上中長期發展目標，在發行面：適用簡易發行申報規範；在交易面：引入基本的反詐欺規範；在業者面：引入客戶資產託管報戶規範與交易市場健全規範。並提出正在發展中的數位監管議題：數位資產信用交易、數位資產期貨、數位資產選擇權、數位資產 ETF 等供大家進一步思考。

新北地檢署李秉錡檢察官則從犯罪偵防角度談數位資產監管。他先分享生動的情境案例，包括虛擬貨幣之非託管錢包、虛擬貨幣之智能合約濫用、虛擬貨幣之 NFT 濫用、虛擬貨幣混幣器洗錢等，從實務的案例視角闡述虛擬貨幣衍生出的監管議題與監管難處。金融監督管理委員會《虛擬通貨平臺及交易業務事業防制洗錢及打擊資恐辦法》規管對象以在國內設立登記者為限，未落地於臺灣及自然人幣商皆不在監管範圍內，不列入納管對象。金管會長期以來較擅長監管體制健全穩定的金融機構，對於新興的金融監管問題還有很大進步的空間。

考量金管會現有監管量能，要針對虛擬貨幣等新興金融監管議題進行監管有一定的難度，如果監管辦法訂出來將虛擬業者全面登記納管，但沒有充足監

管量能與足夠的執法人員，可能減損政府威信。目前困境在於自然人幣商和外國幣商沒有作洗錢防制，李檢察官建議可參考當鋪業的監管模式全面納管虛擬資產業者，並由虛擬產業洗錢防制主管機關訂定子法規範在臺流通金額達一定資產規模要在臺灣設立公司，要求業者出具聲明書備查，由主管機關公告備查名單，並由金管會實質監管，參考保險業之會計師專案查核明定經營條件，實際審查內控制度。任何業者只要未履行洗錢防制就給於行政罰，再討論刑責，而玩家向未備查與未審查者交易，處行政罰。

以上是李檢察官的分享，目前如何監管還在討論階段，但全面納管以維護金融市場的穩定發展是政府未來的方向。

新加坡加密貨幣 Matrixport 公司的 Eugene Lim 引用拜登數位資產政策行政命令中的原則：Same business, Same risks, Same rules 做為開場。從自己跨國公司產業界中的觀察提出：因臺灣金融監管制度，使有些臺灣人自己發展出的創新數位金融商品，不易在自己臺灣境內上市，而轉往境外其他地方上市。也迫使臺灣的許多投資者需要在海外進行投資，才能交易數位金融商品。Eugene Lim 從跨國公司產業界的視角提出，臺灣可考慮不繼續使用傳統監管模式，以增加臺灣數位金融市場的活絡與多元性，發展出更具彈性的監管模式，讓臺灣有機會透數位金融資產與科技優勢，發展出更具國際競爭力的臺灣金融科技產業生態。

最後三位與談人對於美國發表數位資產政策，對臺灣數位金融的影響，皆表示直接影響不會太大。因美國有其獨特背景，金融監管較為碎裂，一個銀行就有三四個監管機構。而臺灣全歸於金管會，所以臺灣較沒有金融監管協調問題。但美國的政策監管內容對臺灣具有一定參考價值。間接影響上，美國政策影響著美元幣值的大小，而國際上美元為強勢貨幣，許多商品以美元計價，如果討論美元對臺灣影響就有不少影響層面可進一步探討。

四、 實習心得

（一） 江○毅

在線上交流會議中，聽到了不同實習伙伴的分享，伙伴們各自分享了自己實習過程中的所見，以及自己完成實習作業的方法。我個人的方法是先大致聽完會議，紀錄其中幾個關鍵字，接著從頭再聽一次錄影，大致打出逐字稿，國外會議的部分先用原文，再轉換成中文，接著國內外的逐字稿再去蕪存菁，整理出摘要。

伙伴們的作法似乎大同小異，只是或許不會整理逐字稿，而會直接整理摘要再調整，或者邊打摘要邊查找專有名詞，兩種作法都有值得學習的地方。提到查找專有名詞的伙伴提到，透過這個過程，學習到了產官學界及不同領域的許多用語，這也是我很喜歡這個機會的原因。

交流會議我們也討論了對實習的建議，其中我有共鳴的部分是希望可以有機會更認識 NII 的組織運作，我認為或許也可以有導師制度帶領實習同學，指導實習作業的完成；另外我個人希望可以有更多伙伴們互相交流的機會，可能以每個會議結束就有半個小時的交流，也或許可以彼此先校稿再交給 NII，讓伙伴能夠互相學習。

最後我們也討論到對數位中介服務法的想法，我認為此次修法並沒有太多有下而上的討論，跟我在網路治理研習營中學習到的多方利害關係人治理模式有很大的落差;伙伴們提到或許可以先處理有急迫性，且尚未有法律可以適用的部分，而不要追求一步到位、包山包海，這樣的觀點我也十分贊同。

這次實習的機會讓我學習到國內外對網路治理的討論及運作，也結識了不同背景同樣關注這個議題的伙伴，今天的交流會則是讓我聽到伙伴們實習的不同作法及觀點，實在受益良多，謝謝主辦單位及伙伴們。

（二） 李○毅

本次交流會議主要可分為三大部分，首先請實習學員分享參與會議的經驗，及國內外網路治理會議參與心得，接下來再由 NII 郝敏介紹今年 9~12 月國內外的網路治理會議相關活動及參加辦法，最後則是由每位實習學員分享自己對於研習課程和實習活動的建議。

大家共同皆有參加的活動是 EuroDIG 且大家不約而同皆有提到英文的困難，而我所選擇的第三場會議是 IGF-USA 中的場次，也是一場全英文的座談會我深深感覺到在這兩次的講座中我的英文聽力有蠻顯著的進步。我在 IGF-USA 選擇的大會演講是與平臺治理相關。我認為平臺治理其實就是「隱私權」及「其他基本權」兩個位於天秤兩端的權利該如何權衡的問題，實在非常複雜，相信未來臺灣也會針對數位中介服務法展開更多的討論！

關於未來實習活動的建議，如同我在交流會議中所提到的，由於講座通常只有一小時左右，其中又有好幾位與談人，常常每一位能分配到的時間只有十分鐘左右，因此很難藉由聽這些演講學習到很深入的知識，如果未來的實習能夠配合閱讀一些較深入的文獻，相信會對於網路治理的議題會有更深刻的見解，而不會只是像走馬看花般聽聽演講而已。至於實習要增加到 NII 參訪，我覺得見仁見智，我自己是比較希望能藉由實習更深入了解網路治理的相關知識，所以目前聽演講寫摘要的實習方式我已經覺得很不錯，如果能有機會更進一步閱讀更困難的文獻我相信會更有幫助。

（三） 韋○祥

很高興這次能被選為實習學員，參與國內外會議並負責撰寫 3 份摘要報告，在濃縮統整成會議記錄的過程中學到了很多。也因為需要撰寫報告，讓自己更為專注在會議的整體內容，在腦內精煉的過程中最大化參與的收穫。

對於撰寫報告的心得，可以分成座談會、專題演講兩類。座談會的部分，可能是因為題目涉及層面較廣，感覺與談人各講各的，最後比較沒有一個結論，會議摘要只能寫得出每個人的看法，但缺少一個整體性的概觀。專題演講的架構較為完整，上下半場之間雖然有互相呼應，但連貫性相對較低，感受到不同形式各有優缺點，摘要撰寫也各有難處。

在報告的撰寫上，我採取的方法是會議中先完整聽過一遍、邊聽邊快速記下重點；在會議結束後從摘錄的重點文字中回憶、整理整場的重點；確定了撰寫的重點架構後，再次觀看錄影回放確認講者意思，也補充遺漏的重要細節；最後順過一次文字，將口語內容轉化為適合書面閱讀的文字版本，並調整成符合習慣的中文句構。

這次交流會議中有一位實習學員提到了可以考慮規劃 NII 辦公環境參訪，

也勾起我之前被同儕問到的記憶,我們都知道網路治理相當重要、值得投注心力,但對於未來就業的幫助則較少公開資訊,因此會覺得認識未來可能的研究方向、工作內容會更有幫助,也較能鼓勵還在猶疑的學員們更深入參與網路治理的研究。

（四） 徐○為

1.國內外網路治理會議參與心得

此次見習收穫良多,感謝 NII 給我實習機會,讓我有機會去參與國內外網路治理的會議。這是我第一次參與歐洲網路治理對話論壇,全英文又帶有不同口音,對於較少參與國際會議的我來說有一定的英語門檻，感謝 Google 翻譯與 Youtube 的輔助字幕，來補足自身不足。

此次會議經驗提升了我的國際觀，並看到多方利害關係人團體在國際場合中的精采對話，我發現國際場合禮儀很重要，觀點與立場可以不同，但大家都可以心平氣和的來互動交流與探討如何解決問題，來做意見發表陳述，反觀某地方的立法院，一言不合就上演激烈攻防戰形成強烈反差。

深感知識儲備量一定要足夠，因為每位與談人的背景相當多元，橫跨各國家公、私部門、產、官、學界與學生等等，有時要聽懂他們的論述內容，確實要花費不少精力專注聆聽，並且使用翻譯工具與多方檢索相關資料，補充自己的相關知識，以確保能正確無誤的聽懂並理解各方利害關係人所談論的內容，我覺得對於相關背景知識不足的我來說是蠻挑戰的一件事。

最後延續著知識儲備來談，我希望參加的會議是網路治理與心理健康的議題，這樣更能結合自身專業背景來做延伸。

2.研習課程和實習活動建議

原本我以為實習是可以實際走訪 NII 去參訪與學習，所以第一點建議是希望未來在安排實習上可以讓我們實際去 NII 參訪實習。第二是增加培訓課程,在我們參與會議前可能可以提供我們參會的相關培訓，例如會議摘要撰寫、參會要特別注意觀察什麼等等，也希望可以提供實習培養計畫讓我們做學習參考。

第三是希望實習活動能盡量濃縮成一天，零碎碎片化的時間，雖然總和不超過 12 小時，但感覺有點點難排。不過這點要看大家有沒有共感，還是只是我個

人的感受。

第四是依照專業分發參與的會議，延續會議心得的內容，例如我的專業是心理健康，就可以選擇較為相關的網路治理議題，例如網路霸凌、網路性別歧視、網路成癮預防、網路社群媒體對使用者心理健康影響等等，這樣更能結合自身專業背景來做延伸。