110 年委託研究報告

「網路治理國際議題觀測與人才培育」

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 110 年 12 月

110 年委託研究報告

PG11004-0139

「網路治理國際議題觀測與人才培育」
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

許嘉雯、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 110 年 12 月

目　次

附　錄

表　次

圖　次

提　要

關鍵詞：網路治理、網路安全法、5G、網路自由度、人才培育

一、研究緣起

「數位國家‧創新經濟發展方案（2021-2025）」（下稱 DIGI+方案 2.0），推動數位轉型使臺灣航向 119 年智慧國家新典範，通傳會為 DIGI+方案 2.0 數位基盤分組的配合辦理強化網際網路治理能量措施作為推動方向，期在觀測國際網路政策議題，同時孕育我國網路治理能量，增加多方利害關係人共同對話，使各項關鍵議題都能受到充分討論，藉由奠定我國網路治理之基礎，增加我國數位經濟發展實力。

二、研究方法及過程

本計畫透過觀測國際網路治理議題及培育我國網路治理多元專業人才等方式，推動網路治理與國際同步，促使未來關鍵議題得增加國內多方社群對話機會，同時透過跨國學習，促進網路治理的國際交流與合作。

本計畫依委託辦理工作，如期完成如下所列的所有履約項目：

- 國際網路治理議題觀測：包括亞太網路資訊中心（APNIC）國際會議、歐洲網路資訊中心（RIPE NCC）國際會議、亞太地區網路治理論壇（APrIGF）、歐洲網路治理論壇（EuroDIG），以及聯合國網路治理論壇（IGF）所討論的議題。
- 通訊傳播政策案例研析：主題分別為英國《網路安全法》草案、5G 網路的治理議題初探，以及全球網路自由度及政策趨勢。
- 大專校園講座：分別於成功大學（南部）、陽明交通大學（北部）及東華大學（東部）舉辦，各場次時數皆達 2 小時，且出席人數超過 50 人。

- 人才培訓課程：「2021 網路治理研習營」課程達 8 小時，共計 21 人結訓，並從中選拔 5 位優秀學員線上參與 APrIGF 2021 國際會議，及交付線上參與摘要報告。
- 課程影片製播：將「2021 網路治理研習營」全日課程錄影剪輯成 2 小時影片，並從中製成 2 支 5 分鐘以上的精華短片，另與網紅合作製播 1 支 12 分鐘的 5G 議題精華短片。3 支精華短片皆附字幕、影片標題包含網路治理相關關鍵字、提供影片點閱流量分析；且 4 支影片皆上傳至 YouTube。
- 國際會議參與：線上參與 EuroDIG 2021，並提供重要議題報告。

三、重要發現

（一）英國《網路安全法》草案

雖然英國各界對於《網路安全法》草案出現「立法過度」和「立法不足」的兩極評價，但歷經多起網路恐怖攻擊和歧視等重大事件的英國社會，對於立法規範網路平臺已具高度共識，歧見的部分僅是執行方向和細節。

（二）5G 網路的治理議題初探

我國的 5G 安全防護策略方向，在因應地緣政治的美中對抗選擇上，和民主國家站在同一陣營。另一方面，我國亦面臨偏鄉 5G 建設推行不易的挑戰，但隨著 5G 覆蓋距離屢創新高，未來或可解決建置成本過高的問題。

（三）全球網路自由度及政策趨勢

《2021 網路自由度報告》以具體數字——48 國祭出新規監管科技公司，凸顯國家強化網路監管成為全球的常態，惟各國政府的監管方式是各行其是，當中歐盟著重透明度和正當程序的「第三種」監管方式值得肯定，且臺灣的《網際網路視聽服務法》草案（雖然已暫緩推動）也具同樣精神。

四、主要建議事項

（一）英國《網路安全法》草案

1. 立即可行之建議：觀察國際發展趨勢並進行國內政策溝通

目前國內各界對於涉及言論自由的網路規範仍是看法分歧，因此，推動相關法規需更加審慎，通傳會可多研析和比較歐盟、英、澳、美等國法案，並了解其社會情境，避免不合國情的引用；同時透過公正客觀的研究調查及充分的利害關係人溝通，了解國內對於內容治理的社會共識，以強化相關政策或立法的正當性和支持度。

2. 中長期建議：建立市場競爭制度，且將媒體素養列為重要施政項目

英國人權團體等主張從市場競爭制度建立業者問責，因為當市場有充足的競爭時，平臺業者就須積極回應言論自由和隱私等訴求，而且市場競爭的事前（ex ante）規範較不會引發社會爭議。因此，此項建議亦值得我國研議（通傳會、公平會、數位發展部）。

此外，英國《網路安全法》草案將強化推動媒體素養入法，如草案獲得通過，象徵法律認可媒體素養對於促進網路安全的價值。我國教育部推動「媒體素養教育行動方案」，以提升學生和國人的媒體素養；另各部會也依其職掌領域進行相關計畫。建議將媒體素養列為重要長期施政項目，並納入各部會的相關活動，且邀請民間響應，以發揮最大的宣導效益。

（二）5G 網路的治理議題初探

1. 立即可行之建議：響應節能減碳、追蹤 5G 健康研究、了解歐美資安宣導

在 5G 的環保議題方面，行政院已指示環保署修改《溫室氣體減量及管理法》，納入「2050 年淨零排放」目標。因此，建議通傳會將節能列為 5G 基地臺架設許可的審核項目、建設偏鄉 5G 網路補助案的加碼補助項目，或訂定 5G 網路頻段使用的碳足跡規範。

而對於 5G 引發的健康疑慮，我國預計 2023 年第二波釋照增加 37 ~ 40GHz「至高頻」，但國內電磁波安全相關研究似無高頻段的部分。因此，建議通傳會追蹤國際 5G 高頻段的健康影響研究，同時也請環保署了解歐盟對非游離輻射電磁波規範的檢視結果，以為國人的電磁波安全嚴格把關，並作為電磁波知識宣導的參考。

此外，關於 5G 的資安問題，我國整體資安防護已具法律基礎和配套制度，例如：通傳會將修訂「5G 資通安全維護計畫」稽核計畫及標準作業程序，以及提升民眾的資安意識。正如「布拉格提案」呼籲「5G 安全是所有利害關係人的共同責任」，我國可參考歐美自 2004 年起舉辦的全國性／國際性認知宣導活動，以增進民眾的資安防護能力。

2. 中長期建議：成立個資保護專責機關，防止 5G 的個資濫用和監控

我國自 2012 年實施《個人資料保護法》，面對 5G 時代的新挑戰，例如：企業和政府可能濫用資料以進行更精準的廣告投放、監控或政治操弄，有賴加速設立獨立的個資保護專責機關，釐清不同型態的個資蒐集和使用風險，並透過修改個資法以為不同資料量身訂做適用的規範，以真正落實個資保護，同時也增進民眾對於數位發展的信賴。

（三）全球網路自由度及政策趨勢

1. 立即可行之建議：檢討防疫資料的使用、於國際分享普及上網等成果、研析歐美內容規範新發展

《2021 網路自由度報告》指出，各國普遍缺乏防止疫情資料濫用的措施，我國也被認為疫情資料的蒐集使用缺乏合法性和比例原則，因此，建議通傳會分享星、澳、加等國的相關案例和我國的評比得分，讓中央流行疫情指揮中心了解國際觀點，促進我國檢討防疫資料的使用。

另一方面，我國於網路連線項目幾近滿分，顯示通傳會的數位基礎建設、電信法規鬆綁等措施可供他國參考。另報告也讚揚我國以創新工具打

擊假訊息，通傳會作為「抑假」統籌機關且與平臺合作因應，亦可和國際分享我國的對抗假訊息經驗。

此外，歐美各國的內容規範新發展，也值得通傳會研析其正反面評價。如德國《國家媒體協定》將監管範圍從無線電廣播擴及新型媒體，且網紅須申請執照；美國《通信端正法》（CDA）第 230 條的諸多修正提案中，被視為較著重透明度和正當程序的《平臺問責制和消費者透明度法》草案；加、德電信業者對於從域名系統（DNS）封鎖侵權網站採取相反做法等。

2. 中長期建議：持續推動透明開放的治理政策，以利人民數位福祉及提升國際聲譽

我國首度被納入全球網路自由度評比即獲得全球第 5 名的殊榮，除了凸顯國人得以享有全球最自由的數位環境及其帶來的數位福祉外，還獲得 CNN 電視、外交家雜誌（The Diplomat）等國際媒體的主動宣傳，提升我國的國際聲譽。為此，推動透明且開放的網路治理政策，是我國須持續努力的工作，並可參考《2021 網路自由度報告》提出的優良網路法規要素。

（四）大專校園講座辦理

1. 立即可行之建議

本年度受到 COVID-19 疫情影響，中央因應各級警戒對於集會活動人數有不同的管制上限，甚至在三級警戒期間幾乎全國大專院校皆改採線上教學，學生無須到校上課，以致於本工作項必須暫時停擺。考量未來疫情可能成為常態，且大專院校學生已逐漸適應線上教學模式，建議未來可放寬校園講座辦理形式，除了實體講座之外，亦可包含線上方式，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，授課對象也可不限於單一學校或科系，將可擴大辦理效益。

（五）人才培訓課程辦理

1. 立即可行之建議

同樣受到全球疫情影響，本年度研習營未能提供實際出國參與國際會議之誘因，以致於報名研習營的人數明顯低於前幾年。未來倘若國際間的網路治理會議得以重返實體，建議仍可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。

本年度的研習營為 1 日的線上活動，部分學員反映課程太過緊湊，且缺乏充分時間進行問答。建議通傳會未來可考量提高課程辦理經費，將研習營天數拉長為 1.5～2 天，實作上可考量先辦理 0.5～1 天的線上課程，再辦理 1 天實體（或依實際情況調整為線上）課程，惟需留意應預留充足的招生及評選時間。

（六）課程影片製播

1. 立即可行之建議

本年度執行單位以有限預算自行剪輯的 2 支短片，雖透過 YouTube 廣告加強推廣提高觀看次數，但相較於以數倍預算與網紅合作的短片，依然是望塵莫及，這也凸顯出推廣的「通路策略」之重要性。透過慎選調性符合本計畫且形象正面的合作夥伴，可善用其既有的通路（頻道訂閱者），快速鎖定目標受眾。未來通傳會若提高影片製播預算，可考量增加與網紅合作的影片數量，或是嘗試與 1～2 位網紅（特別是「知識型」網紅）合作，應更能擴大推廣版圖；推廣的管道也可不限於 YouTube，而是選用合作對象點閱率較高的平臺。

（七）國際會議 EuroDIG 參與

1. 立即可行之建議

歐盟致力成為全球網路規範的領導者，EuroDIG 諸多討論亦是我國當前關切的議題，因此，未來應持續參與，以了解重要議題的發展和歐洲觀點。例如：本次會議探討的《數位服務法》（DSA）、5G 風險、媒體素養、內容和平臺治理、從技術層處理非法內容、加密等議題之結論，皆有我國可參考之處。以 DSA 為例，會議建議 DSA 應該處理刪除非法內容的條款，可能造成寒蟬效應的問題；以及應提升法規的明確性，如：清楚說明盡職調查等責任、法規的適用地區和域外效力等。

Abstract

Through organizing campus lectures and training courses, as well as making video clips, this project aims to cultivate diversified professional talents and promote multi-stakeholders policy dialogue of Internet governance in Taiwan. In the meantime, analyzing communication policy issues and participating in international virtual forums were to understand the trends of communication policy, 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 draft Online Safety Bill

- In comparison with the highly consensus of the British society to regulate online platforms, the public opinion on internet regulations concerned with freedom of speech is diverse in Taiwan. Accordingly, the development of relevant policies needs to be more prudent. It is suggested to strengthen the legitimacy and support of relevant policies through the comparative analysis on platform regulations which include their social context of different western democracies, objective opinion polls, and sufficient multi-stakeholder communication. In the medium and long term, the accountability of online service providers can be established through new ex-ante regulatory such as the EU's Digital Markets Act (DMA). Moreover, media literacy should be regarded as a strategic priority and the power of public-private cooperation for its promotion could maximize the effectiveness of advocacy.

2. Policy issues analysis: the governance issues of 5G networks

- The strategic direction of 5G security of Taiwan in response to the geopolitical conflict between US and China is in line with the western democracies. Further, the challenge of extreme-cost for deploying 5G networks in rural areas might be solved by its coverage distance repeatedly hits new highs. Other policy recommendations for 5G governance issues are to include energy-efficiency as a standard for license granting of 5G base station to help Taiwan achieve Net Zero by 2050; to track international 5G health impact studies and WHO related reports to strictly control the safety of Radiofrequency Electromagnetic Fields for the people in Taiwan; and to set up an independent data protection authority to prevent data abuse and online surveillance in the 5G era.

3. Policy issues analysis: global Internet freedom and policy trends

- The annual report of "Freedom on the Net 2021" highlights the global norms have shifted dramatically toward greater government regulation on the digital sphere with its' study result that a total of 48 countries initiated legal or administrative action against technology companies. The approaches of governments to regulate the digital sphere, however, are extremely different. Taiwan enters this report for the first time with a fifth -place ranking globally and the first in Asia. Accordingly, we could share policies of meaningful internet access and the experience of combating disinformation campaigns with international community, and should promote transparent and open governance policies continually to benefit our own digital welfare and enhance international reputation of Taiwan. In addition, policies and regulations such as the disproportionate usage of

COVID-19 personal data and disproportionate criminal penalties for disinformation and defamation are suggested to be reviewed and improved.

4. Campus lectures in universities

- Three campus lectures were held this year and efforts in the youth education on Internet governance should be keeping on. Giving that pandemics are the new normal from now on, and the college students are 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 and five of them were awarded grants for online participation in APrIGF 2021. In the post-pandemic era, the international conferences may be hosted as physical meetings as before. Rewards for traveling abroad to participate onsite are needed to attract more talents to sign up for the training courses. In addition, 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) is also recommended, so that participants would have more time for learning and experience sharing.

6. Video clips production and publication

- Three video clips were produced and published online. The one cooperated with YouTuber got 13k views and about a hundred positive message from

the audience, while the other two edited from the video of the training courses got less than 600 views each even with ordering advertising service. 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 online this year is EuroDIG 2021. Giving that the European Union is committed to be the global leader in Internet regulation, and many discussions at EuroDIG are also issues of concern in Taiwan, it is suggested to participate EuroDIG continually to understand the development of emerging issues and European perspectives. For this year, the conclusions of discussion issues such as the Digital Service Ac (DSA), 5G risks, media literacy, content and platform governance, content moderation on the Internet infrastructure level, and encryption also provide policy implications for Taiwan's authority. Taking DSA as an example, it recommended that DSA should tackle specific issues such as enhancing clarity of due diligence obligations, of its geographical application and extraterritorial effects, and of content moderation provisions in the DSA that could potentially have 'chilling effects'.

第一章　計畫簡介

第一節 緣起與目標

一、計畫緣起

面對數位科技、數位經濟模式快速演變，通訊傳播事業導入運用物聯網、大數據、AI 等新興科技對網際網路生態所造成廣泛深遠影響同時，也帶給我國網路治理新興課題與挑戰。

為能有效建立開放、包容、信任、創新的數位社會、鼓勵數位轉型與奠基我國的數位經濟環境，通傳會將掌握通訊傳播有關之網路治理議題動向，促使我國數位政策思維與國際同步；同時，在網際網路治理模式的國際影響日深下，我國應增進國內網路治理議題討論之能量，廣泛納入多方利害關係人討論機制，進而強化我國數位政策能量，藉由前瞻觀點因應數位轉型所帶來之挑戰，完善我國數位經濟發展環境。

「數位國家・創新經濟發展方案(2021-2025)」(下稱 DIGI+方案 2.0)，推動數位轉型使臺灣航向 119 年智慧國家新典範，通傳會為 DIGI+方案 2.0 數位基盤分組的主責機關，配合辦理強化網際網路治理能量措施作為推動方向，期在觀測國際網路政策議題，同時孕育我國網路治理能量，增加多方利害關係人共同對話，使各項關鍵議題都能受到充分討論，藉由奠定我國網路治理之基礎，增加我國數位經濟發展實力。

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議題及培育我國網路治理多元專業人才等方式，推動網路治理與國際同步，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：國際議題觀測及我國現況分析、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。

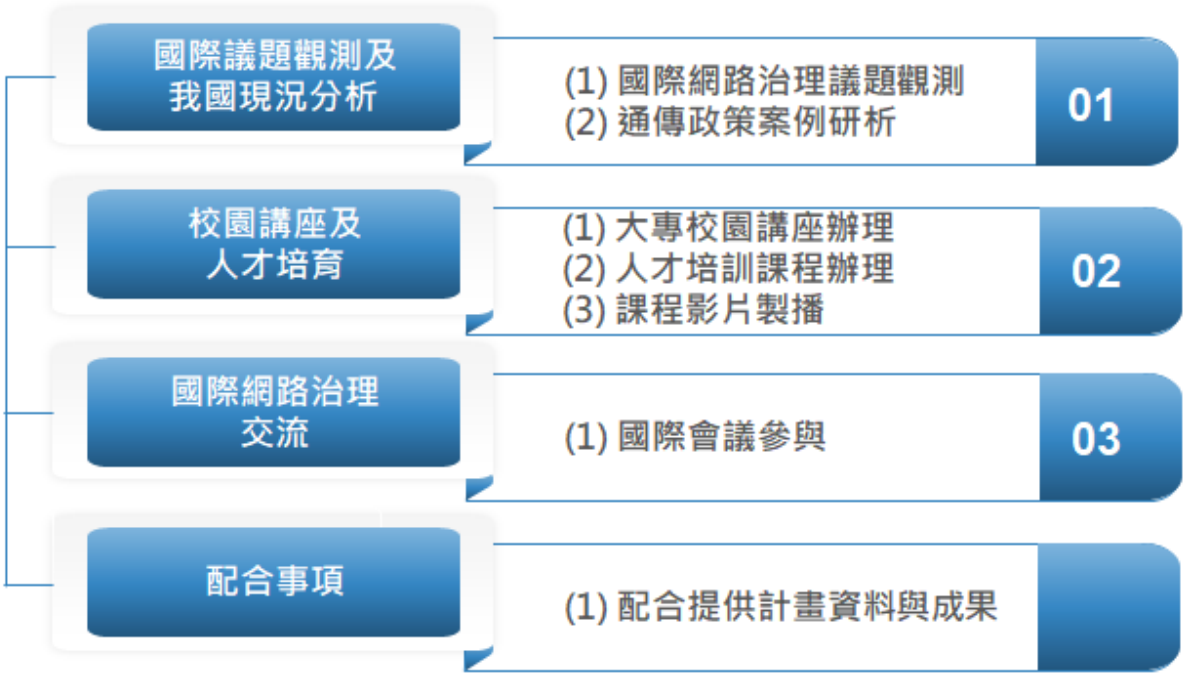


圖 1-1　計畫架構圖

第三節 執行時程及進度

本計畫執行時程為 110 年 4 月 16 日至 110 年 11 月 24 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 7 月 13 日依本案契約第十五條第（四）款約定，向通傳會提出契約變更申請，將本案規劃之人才培訓課程「2021 網路治理研習營」由實體活動變更為線上舉行。下表 1-1 為契約變更後之計畫時程表，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

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
(一)國際議題觀測及我國現況分析									
1. 國際網路治理議題觀測							觀測報告		
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		安排聯繫		場次 2、3		
2. 人才培訓課程辦理	籌備招募				開課 核發獎學金	優秀學員 APrIGF			
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		RIPE 82	EuroDIG			APrIGF APNIC 52		RIPE 83	IGF
專案管理（每月工作報告）									
報告與審查					期中報告	修訂		期末報告	修訂

表 1-2　計畫查核項目與履約期限

查核項目	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 場次大專院校分享 •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：國際議題觀測及我國現況分析、校園講座及人才培育，以及國際網路治理交流 3 大項工作。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 國際網路治理議題觀測

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，以及歐洲網路資訊中心（Réseaux IP Européens Network Coordination Center, RIPE NCC）國際會議。

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。本計畫執行期間所舉辦的上述國際會議概況如表 2-1 所示。

表 2-1 2021 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 52	9 月 8~16 日 線上會議	• 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 82	5 月 17~21 日 線上會議	
	RIPE 83	11 月 22~26 日 線上會議	
網路治理論壇	EuroDIG 2021	6 月 28~30 日 線上會議	• 大會主題：邁向歐洲的數位十年 • 議題類別：連網與素養、網路治理生態系統發展、人權與資料保護、創新與經濟、媒體與內容、安全與犯罪、技術與維運、跨領域/其他議題
	APrIGF 2021	9 月 27~30 日 線上和實地會議	• 大會主題：邁向包容、永續及可信賴的網路 • 議題類別：包容、永續、可信賴

屬性	會議名稱	日期與型式	大會主題與議題類別
	IGF 2021	12 月 6~10 日 線上和實地會議	• 大會主題：網路團結 • 議題類別：經濟與社會包容及人權；普及服務和有意義的連網；新興規範：市場結構、內容、資料、用戶權益；環境永續和氣候變遷；包容性的網路治理生態體系與數位合作；信任、安全與穩定

第二節 區域網路註冊中心之國際會議

APNIC 與 RIPE NCC 為全球五大區域網路註冊中心（Regional Internet Registries, 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），並為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，且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。

本年度計畫執行期間所舉辦的會議包括 APNIC 52 及 RIPE 82 和 83，討論議題簡述如後。

一、APNIC 52

APNIC 會議以會議形式(如：各種特別興趣小組 Special Interest Groups, 簡稱 SIG）或主題（如：IPv6）為名。APNIC 52 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：臺、日、中等國的網路資訊中心（如：TWNIC）分享其維運管理政策。
2. 合作 SIG 論壇：討論網路服務供應商（ISPs）和資料中心如何因應節能和環境永續。
3. 路由安全 SIG 論壇：分享路由安全的相關工具。
4. 政策 SIG（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（Domain Name System, DNS）和資源公鑰基礎建設（Resource Public Key Infrastructure, RPKI）政策，並通過「刪除資源要求證明文件的重複條款」等網路資源管理流程細節提案。
5. 技術場次：討論停電導致服務中斷、惡意機器人網路攻擊等問題。
6. IPv6（Internet Protocol version 6，第 6 版網際網路協定）部署：討論 IP 封包的分割問題。
7. APNIC - FIRST（Forum of Incident Response and Security Teams，資安事件應變小組論壇）安全會議：分享網路攻擊等資安事件處理經驗。

二、RIPE 82 和 83

RIPE 會議以會議形式（如：全體會議、合作會議）或工作小組的主題（如：DNS、IPv6）為名，也因此每一次會議的議題類別大致相同。RIPE 82 的主要討論議題和子題如下：

1. 反濫用：分享如何保護使用者免於惡意軟體等 DNS 濫用威脅。
2. DNS：討論當前網路發展的驅動力為應用程式而非 DNS。
3. 位址政策：討論 RIPE 資料庫是否刪除登記 IPv4 配置的規定。
4. IPv6：討論資通訊設備的 IPv6 規定。
5. IoT（Internet of Thing，物聯網）：分享促進 IoT 安全、如何偵測網路上的 IoT 設備等計畫成果。
6. 合作會議：歐洲國家頂級域名註冊管理機構委員會（Council of European National Top-Level Domain Registries, CENTR）提出對歐盟《數位服務法》（Digital Services Act, DSA）的建議，包括提供明確的 DNS 技術輔助功能的例外責任、提供明確的非法內容定義、於要求 DNS 業者協助前盡可能先從內容來源端處理問題。
7. 全體會議：討論如何兼顧加密保護隱私和執法偵查的需求、歐盟修正《網路與資訊系統安全指令》（Directive on Security of Network and Information Systems，簡稱 NIS2 Directive）。

RIPE 83 的主要討論議題和子題則包括：

1. 反濫用：分享不同類型網路資源被接管後的濫用活動及因應之道。
2. DNS：介紹技術議題如 PROXY v2 協定、RSA 加密演算法的驗證等。
3. 位址政策：介紹資料庫規範、IPv6 政策目標檢討等 RIPE 目前討論中的議題。

4. IPv6：討論如何建立可讓不相容設備都整併的 IPv6-only 網路。
5. IoT：分享使用者收到 IoT 惡意程式通知後的行為研究、影響 IoT 的政策進展。
6. 合作會議：介紹 NIS2 指令對根域名伺服器（root name server）的影響及立法進展、IGF 2021。
7. 全體會議：介紹並討論 DNS 的開放性及其壟斷和監管等問題

第三節 國際網路治理論壇

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（參閱上表 2-1），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。此外，亦有大會主辦單位規劃的全體會議、焦點會議、高層會議等其他型式的會議。各論壇的討論議題簡述如下。

一、APrIGF

APrIGF 2021 大會主題為「邁向包容、永續及可信賴的網路」，議題類別即為大會主題所列的包容、永續、可信賴，全體會議和座談共有 16 場，且多數座談由東南亞國家申辦。討論主題依據 3 個議題類別彙整如下：

1. 包容：疫情期間的網路重要性、協助兒童在疫情中學習、疫情對網路治理學校的影響、數位化引領的包容性成長、藉由實施 ROAM 原則 [1]促進亞太網路自由、亞洲數位權力的司法和法規發展（從人權角度看馬來西亞、印度、印尼的司法判決和法規案例）、APrIGF 的多方利害關係人主義和多元化。
2. 永續：數位化對氣候變遷的影響。
3. 可信賴：亞太地區監控武器化、疫情追蹤技術的隱私和監控問題、馬尼拉中介者責任原則（Manila Principles on Intermediary Liability）於亞太地區的挑戰、建立數位資訊素養、阻止仇恨言論和國家威權主義及平臺演算法審查、AI 能否有效監控網路危害、網路開放互通的重要性、改善全球路由安全。

1 ROAM（Rights, Openness, Accessibility, Multistakeholder participation）原則為聯合國教科文組織（UNESCO）於 2015 年提出，係指推動網路普及化的原則為人權、開放、連網、多方利害關係人參與。

二、EurDIG 2021

EuroDIG 2021 大會主題為「邁向歐洲的數位十年」，焦點會議和座談共有 22 場，討論主題依據其 8 個議題類別彙整如下：

1. 連網與素養：心理健康與數位成癮對人際互動的影響、教育內容取得的近期研究、研究內容和敏感資料的國際取得性。
2. 網路治理生態系統發展：歐盟《數位服務法》的機會與挑戰（2 場）、歐洲於數位相互依賴的角色。
3. 人權與資料保護：與 AI 相關的資料保護新發展、演算法偏見、因為 COVID-19 轉為線上行為（線上支付、虛擬會議、網路銀行等）的隱私影響。
4. 創新與經濟：5G 使用者觀點、歐洲和其他地區的數位生態系統競爭（指網路平臺壟斷的問題）。
5. 媒體與內容：歐盟著作權指令的實施（包含平臺使用新聞的分潤問題）、如何打造可信賴的歐洲媒體和公共領域、以媒體素養消除迷信、邁向法規框架的平臺自律和共管。
6. 安全與犯罪：歐盟 NIS2（修正《網路與資訊系統安全指令》）和網路安全議程。
7. 技術與維運：量子科技的優勢與挑戰、基礎建設層的內容管理。
8. 跨領域／其他：綠色網路治理－－在歐洲實現環境永續的數位轉型、資料主權和可信賴的網路識別（指疫苗接種資料）、加密和隱私及安全能否共存、耐延遲網路（Delay-Tolerant Network, DTN）的技術與應用。

三、IGF 2021

IGF 2021 大會主題為「網路團結」，會議型式眾多，以下彙整高層會議和國會會議（前者由 IGF 的「多方利害關係人諮詢小組（Multistakeholder Advisory Group)」主辦，後者由「各國議會聯盟 (Inter-Parliamentary Union)」等單位主辦；兩者合計共 10 場）、座談（所有人皆可提案申辦，共 83 場），以及開放論壇（限政府單位和國際組織申辦，共 31 場）的討論主題，並根據 6 個議題類別彙整。

表 2-2　IGF 2021 討論議題和主題

議題類別	高層和國會會議	座談	開放論壇
1.經濟與社會包容及人權	•AI 治理——自動化決策和以人為本的方法 •隱私權及合法使用個資 •平臺服務如何促進後疫情時代的全球經濟復甦和永續發展 •數位平臺於建設永續和包容社會的角色 •如何促進數位科技包容且多元的創新和投資及企業社會責任 •為未來工作建立公平的就業條件和能力	•AI 能否減輕仇恨言論 •打造包容性的數位經濟 •立法保護兒少安全 •以多方方式設計 AI 政策 •發展公平的數位健康藍圖（醫療公平性政策） •人權盡職調查的關係人角色 •AI 與人權是否本質上不相容 •金融科技是否為包容性經濟 •如何維護資料正義（如：邊緣化族群的資料代表性和權益） •建立數位常規的工具——追蹤科技公司服務條款的資料檔案	•從人權角度分享司法部門運用 AI 案例和挑戰（巴西網路資訊中心 NIC.br 主辦） •運用 AI 促進消費者保護（波蘭消費者保護暨競爭署主辦） •介紹非洲聯盟建立架構讓非洲國家不同的數位 ID 系統可互通（德國國際合作協會主辦） •網路平臺和政府如何保障女性線上參與權（聯合國意見及言論自由特別報告員主辦） •AI 人權影響評估的挑戰（歐盟基本權利局主辦） •透過數位包容強化民主

議題類別	高層和國會會議	座談	開放論壇
		• 如何做好 AI 的人權影響評估 • 如何將加泰隆尼亞（Catalonia）數位權力和責任憲章推廣到全球 • 推動殘疾人士上網 • 以多方模式處理 AI 道德挑戰 • 以多方方式促進媒體資訊素養 • IGF 數位人權討論如何支持 UN 數位合作藍圖和永續發展目標 • 電子商務如何影響綠色消費 • 企業和政府落實兒少數位權益 • 藉由數位素養防止弱勢族群的數位落差 • 運用國際勞工組織（ILO）的「確保合宜工作框架」因應數位平臺勞動力的挑戰 • 藉政府企業關係落實尊重人權 • 病毒接觸追蹤 apps（和人權）矛盾	（加拿大全球事務部主辦） • 介紹落實線上自由聯盟 Freedom Online Coalition（34 國政府組成）聯合聲明案例（芬蘭外交部主辦） • 展示 Globalpolicy.ai 政策發展資源網站（國際人權組織——歐洲理事會 Council of Europe 主辦） • 如何發展並訂定 AI 國際治理規範（中國大陸國家互聯網信息辦公室主辦）

議題類別	高層和國會會議	座談	開放論壇
		• 運用人權法規引導內容治理 • 重新解讀數位時代的國際言論自由保障 • 制定新《數位人權和責任法案》 • 兼顧成人內容傳遞許可與安全	
2.普及服務和有意義的連網（指使用者有合適的設備和能力，可持續且快速連至符合其需求的內容和服務）	• 投資於數位成長和賦能能力——跨國和跨洲際的綜效	• 消除連網的障礙 • 有意義連網的能力建構 • 開發中與低開發國家數位包容 • 網路普及的創新策略 • 開發中國家的數位轉型挑戰 • 將有意義連網納入數位包容政策 • 因應疫情的經驗分享（如：日本的遠距教學案例） • 建立數位基礎建設機制（建設方法、融資等） • 推動在地數位素養計畫（有在地內容和制度） • 有意義連網的概念與挑戰 • 南亞國家網路和言論自	• 有意義連網的關鍵要素（英國聯邦電信組織 Commonwealth Telecommunications Organisation 主辦） • 數位包容和能力建構（非洲聯盟委員會主辦） • 政府如何確保人人公平上網及兒少安全上網（經濟合作發展組織 OECD 主辦） • 推動有意義的連網（ICANN 主辦） • 介紹非洲網路能力建構計畫成果(全球網路專業論壇主辦）

議題類別	高層和國會會議	座談	開放論壇
		由問題	
3.新興規範：市場結構、內容、資料、用戶權益	•網路平臺於兼顧言論自由和打擊有害內容的角色 •推動包容和多元商業發展的治理模式(如降低科技巨頭市場集中度的風險)	•可信賴的資料跨境流通挑戰 •社群媒體之外的內容治理問題 •建立國際資料治理框架（包含資料跨境流通） •政府和科技巨頭於資料和內容治理的衝突 •平臺的反托拉斯規範全球概況 •平臺經濟對中小企業的改變 •開發中國家的數位平臺規範 •社群媒體的企業帳戶網購規範 •新反壟斷法規對中小企業影響 •建立數位經濟信任的消費者觀點 •追求數位自治的風險（網路分裂對全球貿易的影響） •分享波蘭的線上遊戲產業發展 •國家如何實施全球的人	•介紹瑞士的數位自決網路 Digital Self-Determination Network（瑞士外交部主辦，意指兼顧資料保護和使用的方案） •重新尋求資料跨境流通的全球共識（日本總務省主辦） •建立區域性資料跨境流通政策框架的好處和挑戰（德國國際合作協會主辦） •強化網路公司透明度（聯合國教科文組織 UNESCO 主辦）

議題類別	高層和國會會議	座談	開放論壇
		權制度和數位政策標準	
4.環境永續和氣候變遷	•打造永續的智慧城市	•推動數位世界減碳 •如何管理電子廢棄物以達到循環經濟 •數位化對氣候變遷的影響 •運用數位基礎建設促進永續的在地觀光業和大自然保護 •運用大數據和 AI 促進環境永續	——
5.包容性的網路治理生態體系與數位合作	——	•內容治理的多方倡議（如：「基督城呼籲」行動、FB 獨立監督委員會、全球反恐網路論壇） •國際網路治理的未來想像（為 2025 年 WSIS+20 會議蒐集意見） •運用公私夥伴關係推動數位能力（分享非洲案例） •透過開源軟體支持政府數位主權（意指「數位化政府」）目標 •從青年角度探討數位合作過程 •促進開發和使用開源軟	•提升多方利害關係人能力以加速政府數位轉型的非洲案例(德國聯邦經濟合作與發展部主辦） •缺乏網路本質和開放性等定義對網路監管的衝擊（網際網路協會 ISOC 主辦） •2022 年全球資訊社會高峰會 WSIS 的主題和形式（國際電信聯盟 ITU 主辦） •未來的網路架構願景及如何確保全球網路互通（英國數位、文化、媒體暨體育部主辦）

議題類別	高層和國會會議	座談	開放論壇
		體的包容性 •透過網路取得安全藥品的權益 •開發中國家合作推動數位轉型（運用其潛力、資料治理角色） •促進公民社會有意義的參與網路治理（共享決策權而非只是參與出席） •促進青年參與網路治理政策決策過程 •賦予青年參與網路治理決策過程	•青年 IGF 社群對於數位合作的參與（歐盟執委會主辦） •強化全球數位能力發展（聯合國秘書長科技特使辦公室主辦） •推動開放網路的挑戰（歐盟執委會主辦） •阿拉伯地區的數位合作（聯合國西亞經濟社會委員會主辦）
6.信任、安全與穩定	——	•IoT 的供應鏈治理和安全 •如何將國際關係中的中立原則運用於網路國際規範 •解決加密的政策衝突 •網路關鍵基礎建設的攻擊問題 •技術快速發展對數位產品安全的治理挑戰 •線上教育的資安挑戰及影響 •如何促進聯合國體系下的網路空間問責制和新	•多方合作對抗線上恐怖和極端主義（紐西蘭政府主辦） •介紹網路安全能力建構的知識網站（全球網路專業論壇 The Global Forum on Cyber Expertise 主辦） •COVID-19 時代的網路風險管理及國際合作（以色列國家網路安全局主辦） •分享巴西.br 域名衝突的行政解決措施（巴西網路指導委員會 CGI.br 主辦）

議題類別	高層和國會會議	座談	開放論壇
		規範發展 • 民主和線上投票的挑戰及創新 • 透過集體行動保護醫療保健系統安全 • DNS 隱私技術的現況分享 • 青年探討 IoT 安全和 AI 濫用 • 介紹和討論 IoT 的一種安全協議（INXU protocol） • 確保網路韌性及其核心價值（因應數位主權和立法監管興起、部分國家封鎖和控制網路） • 解決網路性別暴力和虐待 • 劃定政府網路間諜活動的界線 • 非洲的網路外交和數位轉型 • 從資安角度打擊假訊息	• 關鍵資訊基礎建設為全球公共利益（全球網路空間穩定委員會 The Global Commission on the Stability of Cyberspace 主辦）

資料來源：IGF 2021；本計畫彙整

第四節 彙整分析

為能更清楚呈現本（2021）年度國際網路治理會議的討論議題趨勢，本計畫採用 IGF 2021 的 6 大議題類別，並從各類別下的各場會議主題歸納出 19 個關鍵字，之後再將其他網路治理會議的討論主題依關鍵字進行重新歸類和次數統計。原則上，除了少數會議因探討不同主題之間的關係而採重複計算外（例如：「如何做好 AI 的人權影響評估」座談，歸類於「AI 治理」及「數位人權」），多數會議是 1 個場次歸類於 1 個最具代表性的關鍵字。重新歸類和統計的結果如下表 2-3 所示，當中最熱門的議題（次數最多）前 5 名依序為：

- 數位人權（包含保護人權、自由民主、監控封鎖、個資隱私等）：30 次
- 有意義連網／數位包容／數位落差／能力建構[2]：21 次
- 內容治理／平臺責任（包含新聞媒體分潤）：20 次
- 基礎建設／關鍵網路資源（包含相關網路技術）：20 次
- AI 治理：14 次

如就地區來看，APrIGF 最熱門的議題為「數位人權」和「有意義連網／數位包容／數位落差／能力建構」。EuroDIG 為「內容治理／平臺責任」，其次為「數位人權」和「基礎建設／關鍵網路資源」（主要為 5G、量子網路、低延遲網路等技術議題）。聯合國 IGF 則和 APrIGF 一樣，為「數位人權」和「有意義連網／數位包容／數位落差／能力建構」。至於屬於區域網路註冊中心（RIRs）的 APNIC 和 RIPE 會議，討論最多的自然是「基礎建設／關鍵網路資源」議題。

2 由於「有意義連網」（根據 IGF 會議資料係指使用者有合適的設備和能力，可持續且快速連至符合其需求的內容和服務）、「數位落差」、「數位包容」、「能力建構」等詞彙包含重疊且尚未明確區隔的概念，故將這些關鍵字並列。

表 2-3　2021 年國際網路治理會議討論議題

議題類別（IGF 分類）	關鍵字（摘自 IGF 各類別下的討論主題）	總次數	APNIC 52	RIPE 82 & 83	APrIGF 2021	EuroDIG 2021	IGF 2021
1.經濟與社會包容及人權	**AI 治理**	**14**	0	0	1	2	11
	包容性成長*	10	0	0	0	0	10
	數位人權（包含保護人權、自由民主、監控封鎖、個資隱私等）	**30**	0	1	**5**	**3**	**21**
	COVID-19（討論個資隱私、經濟復甦、數位落差和包容等議題）	9	0	0	3	2	4
2.普及服務和有意義的連網	網路建設	3	0	0	0	0	3
	有意義連網／數位包容／數位落差／能力建構	**21**	0	0	**4**	2	**15**
	數位轉型**	5	0	0	0	0	5
3.新興規範：市場結構、內容、資料、用戶權益	**內容治理／平臺責任（包含新聞媒體分潤）**	**20**	0	1	2	**6**	11
	媒體／資訊素養	4	0	0	1	2	1
	市場集中／壟斷	3	0	0	0	1	3
	資料治理／資料跨境流通	6	0	0	0	0	6
	消費者保護	3	0	0	0	0	3
4.環境永續和氣候變遷	環境永續／減碳／氣候變遷	9	1	0	1	0	7
5.包容性的網路治理生態體系與數位合作	數位合作／國際規範	9	0	0	0	1	8
	網路治理發展和參與	6	0	0	1	0	5
	網路分裂／開放互通	7	0	1	1	0	5
6.信任、安全與穩定	數位產品和 IoT 安全	6	0	2	0	0	4
	基礎建設／關鍵網路資源（包含相關網路技術）	**20**	4	8	1	**3**	4
	資訊安全（包含兒少安全、國家發動網攻）	12	2	2	0	1	7

資料來源：本計畫彙整

*「包容性成長」指的是透過強化機會平等和消除參與障礙的政策，促進共享繁榮（World

Bank, 2018）。此處強調社會和經濟面的包容性成長，且包括受到數位化影響的勞動權益和未來工作議題。

**「數位轉型」於政府部門和公共行政方面，係指使用數位科技、工具和應用程式（從流程數位化到區塊鏈和 AI），為政府的運作、和公民社會的互動，以及所提供的公眾服務，帶來新的方式（Council of Europe, 2021）。

本計畫擇定的 3 個通傳政策案例研析主題分別為「英國《網路安全法》草案」、「5G 網路的治理議題初探」，以及「全球網路自由度及政策趨勢」，分屬表 2-3 關鍵字所列的「內容治理／平臺責任」、「基礎建設／關鍵網路資源」，以及「數位人權」議題，且皆為前 5 名的熱門議題。各篇案例研析請詳本報告接續之第三章至第五章。

參考文獻

- APrIGF 2021. Program Schedule. https://aprigf.org.np/program-schedule/
- APNIC 52. Schedule. https://conference.apnic.net/52/program/schedule/#/day/1
- Council of Europe (2021). Study on the impact of digital transformation on democracy and good governance. https://rm.coe.int/study-on-the-impact-of-digital-transformation-on-democracy-and-good-go/1680a3b9f9
- EuroDIG 2021. Consolidated programme 2021 . https://eurodigwiki.org/wiki/Consolidated_programme_2021
- IGF 2021. Draft Schedule. https://www.intgovforum.org/en/content/igf-2021-schedule
- IGF 2021. Issue Areas. https://www.intgovforum.org/en/content/igf-2021-issue-areas
- RIPE 82. Meeting Plan. https://ripe82.ripe.net/programme/meeting-plan/
- UNESCO (2019). From Internet Universality to ROAM-X Indicators. https://en.unesco.org/themes/internet-universality-indicators/background
- World Bank (2018). Inclusive Growth: A Synthesis of Findings from Recent IEG Evaluations. https://ieg.worldbankgroup.org/evaluations/inclusive-growth

第三章 案例研析：英國《網路安全法》草案

第一節 前言

為了打擊網路非法內容和有害內容，保護民眾上網安全，英國數位、文化、媒體暨體育部（Department for Digital, Culture, Media & Sport, DCMS；以下簡稱數位部）於 2021 年 5 月 12 日發布《網路安全法》（Online Safety Bill）草案，要求網路服務提供者（以下簡稱網路業者或業者）承擔處理非法內容，以及保護言論自由和隱私等法律責任；大型業者還須進一步處理合法但有害（harmful）內容，並保護具民主重要性內容（content of democratic importance）和新聞內容（journalistic content）。

該草案並授權監管機關通訊管理局（Office of Communications, OFCOM）可對違法業者最高處全球年營業額 10%罰緩或中斷業務，甚至公司主管可能面臨刑責。英國數位部宣稱此法為「英國展現全球領導地位的開創性法規……帶來公平和問責的網路世界」（DCMS, 2021a）。該草案目前已送英國議會審議。媒體報導指出，由於英國執政黨在國會占多數，因此，只要大眾沒有強烈反對，草案很可能通過立法（Lomas, 2021）。

本章首先簡介英國政府推動此次立法之前的政策發展，其次彙整草案的立法目的與背景，並試圖了解當中是否有特殊的社會文化因素，接續再探討草案的規範重點，以及英國各界對草案的回應，進而從中找出可供我國借鏡之處。

第二節 政策發展

一、網路安全策略綠皮書（2017.10）

《網路安全法》草案的發展至少可追溯至 2017 年 10 月 11 日英國數位部發布的《網路安全策略綠皮書》（The Internet Safety Strategy Green Paper），當時主要是為了打擊霸凌、騷擾、酸民、色情等網路濫用行為，且策略上即主張業者應對使用者負責，並使用技術解決方案來避免有害內容，而政府的角色則在於支持使用者。

英國數位部並於綠皮書發布當日起，展開為期近 2 個月的意見徵詢，方式包括與各利害關係人的圓桌討論會議、焦點訪談，以及問卷調查（600 份）等，且於 2018 年 5 月發布《政府回應綠皮書意見徵詢》報告。報告指出，雖然許多公司聲稱於網路安全擁有良好紀錄，但他們如何執行的透明度不足，且與用戶體驗不一致，因為根據數位部的調查，70%英國人認為社群媒體公司對於防止其平臺上的非法或不道德行為仍然做得不夠；且 60%受訪者目睹網路上的不當或有害行為。也因此，數位部決定和內政部合作推出白皮書，並為未來的立法工作做準備（DCMS, 2018）。

二、網路危害白皮書（2019.04）

英國數位部和內政部於2019年4月8日發布《網路危害白皮書》(Online Harms White Paper），指出網路上充斥各種危害兒少安全和國家安全的內容，如兒少性虐待和教導自殘自殺的圖照影片、網路霸凌或威脅恐嚇的訊息、教唆恐怖攻擊的資料、顛覆民主的假訊息、違法交易槍枝刀械的資訊等。雖然目前也有相關法規和業者自律措施，但仍不足以保護民眾上網安全，加上大眾對網路危害的擔憂持續增加，並呼籲政府和業者採取進一步行動，因此，英國政府擬推動新的監管框架，透過適度和以風險為基礎的方法，針對提供用戶分享、互動、產生內容等服務的業者（包括社群媒體平臺、文件託管網站、公共論壇網站、訊息服務——不含私人訊息、搜尋引擎），建立其法定的注意義務（duty of care）[3]，以對其用戶安全承擔更多責任。違者將由指定的獨立監管機關處以巨額罰款，並追究高級管理人員的責任。此外，政府也擬訂定媒體素養策略等非法規性措施，協助所有使用者具備自我管理網路安全的意識和能力（DCMS & Home Office, 2019）。

英國數位部和內政部並於白皮書發布日起，展開為期近12週的公眾意見徵詢，包括舉辦100場和各利害關係人族群的交流會議(含國際會議），以及線上意見徵詢（共 18 個政策問題，選擇題和簡答題皆有，總計收到2,439份意見）；並於其他時間和受害者團體組織、心理健康組織、家長和兒少安全組織等團體座談交流，還舉辦一系列針對監管政策的主題研討會，及召開17次部長級會議等（DCMS & Home Office, 2020a）。

此兩個部會於2020年2月12日發布《政府初步回應白皮書意見徵詢》報告，同年 12 月 15 日再發布《政府最終回應白皮書意見徵詢》報告。最

3 法律暨政治論述網站 Verfassungsblog 刊登英國 Aston 大學資深講師 Dr. Edina Harbinja（2021）的專文分析指出，duty of care 源自健康和安全法規的義務。本報告採用「輔仁大學法律學院常用法學英文字彙表」之中文翻譯——注意義務。

終回應報告指出，公眾意見徵詢的結果顯示，英國迫切需要採取保護使用者的行動，適度的監管將可建立數位經濟的信心並促進數位經濟成長，且業者和使用者團體也樂見政府提供明確的監管規範。因此，政府將於 2021 年推出《網路安全法》草案，並指定通訊管理局（OFCOM）為監管機構（DCMS & Home Office, 2020b）。此外，報告還提前揭露草案的諸多規範重點，因內容同質性高，將於後續的草案章節一併介紹。

第三節 立法目的與背景

一、立法目的與原由

《網路安全法》草案係為通訊管理局（OFCOM）監管特定網路服務而制定條款。雖然草案沒有描述其立法目的，不過，數位部表示此法將可保護兒少網路安全、維護言論自由、促進民主政治辯論、抑制種族仇恨、打擊金融詐騙。數位部部長 Oliver Dowden 則宣稱此為全球開創性的法規，將迎來技術問責的新時代，以及公平和問責的網路世界（DCMS, 2021a）。

同樣的，草案也未載明立法原由或背景，但《政府最終回應白皮書意見徵詢》報告中，已說明促使政府採取強力監管行動的原由，主要包括：

- 英國成人上網率高達 90.8%（2019 年），每天平均上網時間超過 4 小時（2020 年）。但 75% 英國成人對於上網感到擔憂；且認為兒少上網好處大於風險的比例從 2015 年的 65%降為 2019 年的 55%。
- 非法的兒少性剝削和虐待（Child Sexual Exploitation and Abuse, CSEA）內容，威脅性日益升高。2019 年美國科技公司向美國國家失踪與受虐兒少中心提交的此類圖照和影片超過 6,900 萬件，年增率超過 50%；同年英國網路觀察基金會也發現超過 13.2 萬件此類資料，年增率為 26%；截至 2019 年 3 月，英國的虐待兒少圖像資料庫已有 830 萬張圖像，且英國國家犯罪署估計，至少 30 萬人對兒少構成性威脅。
- 恐怖組織利用網路煽動和聯繫恐怖攻擊行動，2017 年英國發生的 5 起恐攻事件皆有網路因素。雖然大型平臺亦有打擊線上恐怖主義的措施，例如：Twitter 在 2019 年 1 至 6 月關閉近 9.6 萬個宣傳恐怖主義和暴力極端主義的帳號，但恐怖分子及其支持者繼續利用各種網路平臺實現其目標。
- 大眾對於合法但可能有害的內容日益擔憂，如網路霸凌、虐待、倡導自殘、散播假訊息等內容。調查顯示，23%的 12-15 歲英國青少年曾經歷或

目睹網路霸凌、辱罵或威脅（2019 年）；80%英國多元性別者曾經歷反多元性別和網路虐待（2020 年）；2019 年英國的網路反猶太主義事件較前一年增加 50%。

- COVID-19 爆發更凸顯打擊非法和有害內容的必要性。研究發現，疫情期間 47%英國青少兒看過令自己後悔的內容；網路觀察基金會等單位光是 1 個月就阻止 880 萬次用戶嘗試連線兒少性虐待圖照和影片的網站；50%英國人在社群媒體看過疫情相關的假訊息和錯誤訊息，當中又以 5G 會傳播病毒或降低免疫系統的假訊息為最多。
- 白皮書還列出許多非法和有害內容的證據，例如：監獄罪犯將非法內容上傳至社群媒體、幫派利用社群媒體宣傳幫派文化和煽動暴力、危險鴉片類藥物於社群媒體上銷售、20%英國青少年曾遭網路霸凌、22.5%英國年輕人上網搜尋自殘和自殺資料、社群媒體及 AI 助長大眾輿論的操控，以及 61%英國人希望政府為打擊假訊息做得更多等。

二、社會情境

（一）民眾呼籲打擊網路恐怖主義

英國自 2005 年起，即飽受恐怖主義的攻擊。例如：2005 年倫敦地鐵爆炸事件、2007 年格拉斯哥機場攻擊事件、2013 年殺害英國士兵報復事件、2017 年西敏寺（國會大廈）汽車攻擊和曼徹斯特演唱會爆炸等 5 起恐攻事件，以及 2018 年再度發生西敏寺汽車攻擊事件等。

恐怖主義組織很早就會利用 Facebook、Twitter、Instagram、YouTube 等網路平臺進行戰績宣傳和招募新成員。2015 年起還開始使用加密的即時通訊軟件 Telegram，甚至還有躲避封鎖的迂迴策略。長期以來的恐攻事件已經造成英國民眾無數傷亡，因此，2017 年接連的恐攻和爆炸事件後，英國社會出現打擊網路恐怖主義的呼聲（Smith, 2017；Raian, 2019）。

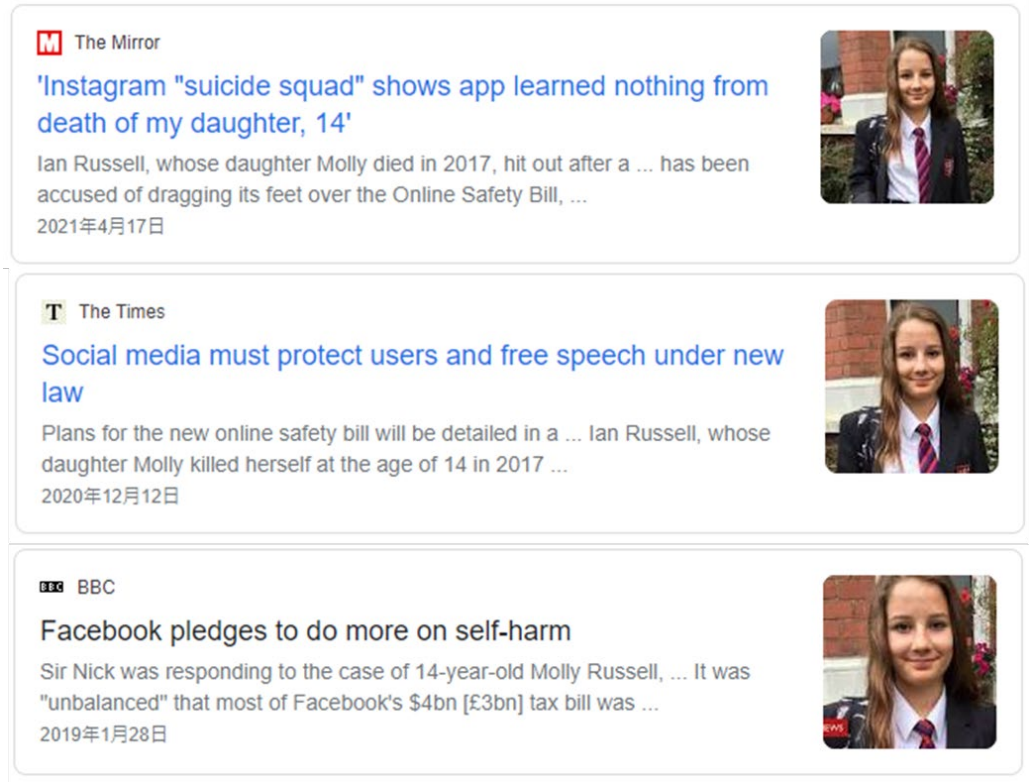
圖片來源：BBC News; Express

圖 3-1　恐怖主義組織利用網路進行宣傳和招募

（二）民眾強烈要求立法管制社群媒體

英國一名 14 歲少女 Molly Russell 因為瀏覽 Facebook 旗下 Instagram 大量憂鬱、自殘和自殺的圖文照片後，於 2017 年 11 月輕生身亡。此事件經英國媒體大肆報導後，在英國引發民眾強烈抗議，並要求立法管制社群媒體（Foster, 2020）。

Molly 的父親表示，政府允許社群媒體自我監管的時間已太長久，且他們持續朝向錯誤的方向發展，但這是攸關生死的問題，現在該是政府實施強力有效的網路法規時刻了（The Irish News, 2019）。英國全國防止虐待兒童協會（the National Society for the Prevention of Cruelty to Children, NSPCC）也發起「馴服野蠻西部網路」運動，推動社群媒體法規，並強調其調查顯示，英國（東南部）高達 9 成家長支持立法管制社群媒體（Evans, 2019）。



資料來源：Google 搜尋

圖 3-2　媒體多年持續報導 2017 年少女使用平臺而輕生事件

（三）英國首相和百萬民眾反制網路種族歧視

足球賽事風靡整個英國，不過，近年來少數族裔足球員在社群媒體遭到種族歧視的事件卻不斷上演，相關單位也為此接連發起抵制社群媒體行動，例如：2021 年 4 月英格蘭足球聯賽（English Football League, EFL）即展開三天的聯合抵制社群媒體行動（EFL, 2021）。

然而，這些抵制行動並沒有解決問題。2021 年 7 月 11 日英國於歐洲盃足球冠軍賽戰敗後，3 名非裔球員成為網路霸凌目標，社群媒體也因此備受各界譴責。英國首相強生表示，政府正推動《網路安全法》立法，迫使社群媒體對這種卑劣行為承擔責任和採取行動；同時最高可處長達 10 年的《足球禁令》（Football Banning Orders）也將修改為涵蓋網路種族主義，以禁止濫用網路者入場觀賽（Prime Minister's Office, 2021）。

此外，身兼英格蘭足球總會（English Football Association）主席的威廉王子也在 Twitter（2021）強調，種族主義虐待必須立刻停止，且霸凌者應為其行為付出代價。更有球迷自主發起請願活動，要求終身禁止種族主義者入場觀看足球賽，且已獲得超過百萬民眾連署支持(Change.Org, 2021)。

圖片來源：The Guardian; Change.Org

圖 3-3　英國首相及百萬民眾反制網路種族歧視

第四節 法案重點

《網路安全法》草案共計 141 條，篇幅為 145 頁，分成概述與重要定義、受監管供應商的注意義務、服務供應商的其他職責、OFCOM 的權力與職責、上訴與超級申訴、內閣大臣（部長）的監管職能、一般和最終條款等 7 大部分；以及豁免服務、恐怖主義罪刑、兒少性剝削和虐待罪刑、受監管的服務類別、進入和審查的權力共 5 個附件（DCMS, 2021b）。以下以主題呈現方式，簡介草案的規範重點。

一、受監管的服務、類別及豁免

(一) 受監管的服務

根據草案第 1 條至第 3 條，受此法監管的服務為「與英國有關」的「用戶對用戶服務」和「搜尋服務」。相關定義如下：

- 用戶對用戶服務（user-to-user service）：可讓用戶產生、上傳，或分享內容，且可能讓其他用戶看到這些內容的網路服務。
- 搜尋服務（search service）：一種搜尋引擎且不是用戶對用戶的網路服務。
- 與英國有關：指擁有大量英國用戶、英國形成其目標市場、英國個人能夠使用，或有合理理由相信該服務上的內容會對英國個人產生嚴重傷害的重大風險。

(二) 受監管服務的類別

前述受監管的「用戶對用戶服務」和「搜尋服務」，根據草案第 59 條和附件 4，可再分為如下所列的第 1 類、2A 類、2B 類，各類別的明確門檻條件將由內閣大臣（部長）考量風險和影響性等情況後訂定，OFCOM 則是進行相關研究並提供參考建議。

- 第 1 類用戶對用戶服務：門檻項目為用戶數量，及功能特性（數位部表

示，此類服務為「大型和最受歡迎的社群媒體網站」)。

- 2A 類搜尋服務：門檻項目為用戶數量，及內閣大臣認為相關的其他要素。
- 2B 類用戶對用戶服務：門檻項目為用戶數量、功能特性，以及內閣大臣認為相關的其他要素。

(三) 豁免的服務和內容

1. 豁免的服務（exempt service）

附件 1 的豁免服務不受此法規範，但內閣大臣（部長）有權力修改此項內容。目前所列的豁免服務包括：

- 所有服務項目中，「唯一」由用戶生成的內容為 email、SMS（Short Message Service，指透過電話號碼傳送的文字簡訊）、MMS（Multimedia Messaging Service，指透過電話號碼傳送的視訊通話），或一對一即時語音通話。
- 企業內部的網路服務。
- 功能有限的網路服務（只能對業者發布的內容發表或分享評論，或是給予喜好評價）。
- 公家單位的網路服務。

2. 豁免的內容

草案第 39 條和 18 條提及豁免內容，包括：

- 用戶生成內容（User-Generated Content, UGC）當中的 Email、SMS、MMS、對業者內容的評論與評價、一對一即時語音通訊（沒有附加文字訊息、影片或圖像）、付費廣告、新聞發布者的內容。
- 搜尋結果當中的付費廣告、公認新聞出版者的原文複製或連結。

二、受監管服務的業者義務

草案將受監管服務的業者義務分成「注意義務」(duties of care)和「其他義務」2 大類（表 3-1），「注意義務」包含處理非法內容等 8 項，可謂整部草案的核心；「其他義務」只有公布透明度報告和繳交年費 2 項。各項義務和其重點簡介如下。

表 3-1　受監管服務的業者義務

	義務 \ 服務類別	第1類 用戶對用戶服務	2A 類 搜尋服務	2B類 用戶對用戶服務
注意義務	1. 處理非法內容	O	O	O
	2. 處理有害內容	O 兒少+成人	△ 若兒少可觸及	△ 若兒少可觸及
	3. 保護言論自由和隱私	O	O	O
	4. 保護具民主重要性內容	O	X	X
	5. 保護新聞內容	O	X	X
	6. 風險評估	O	O	O
	7. 通報和改正	O	O	O
	8. 紀錄保存和檢視	O	O	O
其他	1. 公布透明度報告	O	O	O
	2. 繳交年費	全球年營收達一定門檻者；做為OFCOM執法經費		

◯代表具有法定的注意義務；△為特定情況才有義務；X 則代表沒有義務。

資料來源：本計畫製表

(一)注意義務

根據草案第 5 ~ 6 條和第 17 ~ 18 條，所有業者（第 1 類、2A 類及 2B 類）皆須履行的注意義務包括非法內容的風險評估、非法內容的處置、保護言論自由和隱私、通報和改正，以及紀錄保存和檢視。而所有可能被兒少觸及的服務（根據 137 條，兒少指 18 歲以下），其業者還須落實保護兒少網路安全的義務（包括處理有害兒少內容、進行兒少風險評估等）。此外，第 1 類用戶對用戶服務業者（指大型業者）還有額外的保護成人網路安全（包括處理有害成人的內容、進行成人風險評估等）、保護民主重要性內容，以及保護新聞內容的義務。

1. 處理非法內容

根據草案第 41 條，非法內容包括恐怖主義內容、兒少性剝削和虐待（CSEA)內容、優先非法內容(指內閣大臣／部長於規範中指定的罪刑)。雖然處理非法內容為所有業者的共同義務，但規範上仍略有不同。

- 用戶對用戶服務（第 1 類及 2B 類）的業者義務：採取適當步驟以減輕和有效管理其非法內容風險評估所識別出的危害個人風險。針對當中的優先非法內容，應儘量減少其存在、出現的時間長度及散佈，且經檢舉或發現時應迅速刪除；並於服務條款中說明如何落實此項義務（第 9 條)。
- 搜尋服務的業者義務：採取適當步驟以減輕和有效管理其非法內容風險評估所識別出的危害個人風險，並將搜尋結果出現「優先非法內容」和其他非法內容的風險最小化;且於公開聲明中說明如何落實此項義務(第 21 條)。

2. 處理有害內容

此項為第 1 類用戶對用戶服務的業者專屬義務。根據草案第 45 條和 46 條，對兒少或成人有害內容的定義幾乎完全相同，皆包括內閣大臣（部長）

指定的有害內容，及業者自行判斷的有害內容。內閣大臣（部長）指定的有害兒少內容，又分成「主要優先」和「優先」兩種，成人的部分則只有「優先」一種。至於業者自行判斷的有害內容，其定義為「業者有合理理由相信內容的性質將會（直接）或間接對具有普通情感的兒少／成人，產生嚴重不利身心影響的重大風險」。此處的「間接」是指，導致個人對目標兒少／成人做出或說出會對此人產生嚴重不利身心影響；或導致兒少／成人做出或可能做出對其身心產生嚴重不利影響的行為。

而在注意義務方面，處理兒少有害內容須採取適當步驟以減輕和有效管理其兒少風險評鑑所識別的不同年齡層的危害兒少風險，並降低這些危害的影響性；還要防止所有兒少透過其服務接觸到主要優先、優先和其他有害內容，並於服務條款中說明如何落實此項義務（第 10 條）；成人的有害內容則只須於服務條款中，說明如何處理對成人有害的優先內容，及成人風險評鑑所識別的其他對成年人有害的內容（第 11 條）。

至於兒少可觸及的 2B 類用戶對用戶服務及 2A 類搜尋服務，前者的義務和第 1 類用戶對用戶服務完全相同，後者則是大致相同，惟在處理有害內容的方式上，以降低風險的做法（將兒少透過搜尋結果接觸到的所有有害內容的風險最小化；第 22 條），取代前者的防止接觸。

3. 保護言論自由和隱私

根據草案第 12 條和 23 條，所有業者皆有保護「言論自由」和「隱私」的義務。保護「言論自由」係指法律範圍內的言論自由，「隱私」則指免受未經授權的隱私侵犯。第 1 類和 2B 類用戶對用戶服務的業者注意義務為，其安全政策和措施須「落實」保護用戶的言論自由權和隱私；而 2A 類搜尋服務的業者注意義務，則為安全政策和措施須「考量」保護用戶言論自由和隱私的重要性。此外，第 1 類用戶對用戶服務業者還須進一步進行影響性評估。

4. 保護具民主重要性內容

根據草案第 13 條，第 1 類用戶對用戶服務的業者須保護具民主重要性內容。此類內容包括：

- 新聞發布者的內容（將於下段「保護新聞內容」說明）。
- 受監管的內容（第 39 條）：泛指除了下列項目以外的用戶生成內容。
  - Email；
  - SMS 訊息（指透過電話號碼傳送的文字簡訊）；
  - MMS 訊息（指透過電話號碼傳送的視訊通話）；
  - 對業者內容的評論與評價；
  - 一對一即時語音通訊（沒有附加文字訊息、影片或圖像）；
  - 付費廣告；
  - 新聞發布者內容。
- 專門促進英國民主政治辯論的內容：草案無相關說明，但數位部新聞稿（DCMS, 2021a）舉例指出，主要社群媒體業者可能選擇禁止極端暴力畫面，但是當一個倡議團體使用這類內容以提高大眾認識特定團體的暴力行為時，基於保護民主辯論的考量，業者可在加註警語下保留這些內容。

至於業者的注意義務則在於確保決定如何處理此類內容時，尤其關於是否刪除或限制用戶訪問的決策，以及是否對生成、上傳或分享此類內容的用戶採取行動時（指警告用戶，或暫停、禁止用戶使用服務），都會考慮言論自由的重要性，且對各種政治觀點一視同仁。這些相關的處理原則和流程須於服務條款中加以說明。

5. 保護新聞內容

根據草案第 14 條，第 1 類用戶對用戶服務的業者，須保護新聞內容。此類內容包括：

- 新聞發布者的內容：由「公認的新聞發布者」直接在該服務上生成的內容或廣播的原版錄音，或用戶將前者內容的全文或連結上傳／分享到此服務上。「公認的新聞出版者」指擁有新聞廣播執照的實體，或是同時符合多項條件——如以新聞發布為主要目的且受編輯控制、受到標準守則約束、有英國營業地址、對其發布內容負有法律責任等的實體(第 40 條)。
- 為新聞目的生成的內容（草案無相關說明）。
- 和英國相關的內容：服務的英國用戶構成內容的目標市場，或大量英國用戶有（或可能有）興趣的內容。

而業者的注意義務則為確保決定如何處理此類內容時，尤其關於是否刪除或限制用戶訪問的決策，以及是否對生成、上傳或分享此類內容的用戶採取行動時（指警告用戶，或暫停、禁止用戶使用服務），會考慮言論自由的重要性；並應提供專門和快速的申訴程序，以及確保一旦申訴成功時的復原措施。這些相關的處理原則和流程須於服務條款中加以說明。

此外，雖然數位部新聞稿（DCMS, 2021a）提到，公民記者的新聞內容和專業記者一樣受到保護，不過，草案並未發現有相關的條文加以說明。

6. 風險評估

根據草案第 7~8 條及 19~20 條，所有業者對於既有的服務須在三個月內進行非法內容的風險評估，並於草案有相關重大更改時，或業者的服務營運有相關重大變更之前，及時更新風險評估。所有兒少可能觸及服務的有害內容風險評估，及第 1 類服務專屬的成人有害內容風險評估亦相同，惟一旦識別出非指定的有害內容，也就是內閣大臣（部長）指定的「主要優先」和（或）「優先」有害內容時，還須向 OFCOM 通報。

不同服務類別對於非法內容、有害兒少內容及有害成人內容(僅限第 1 類服務）的風險評估，雖然執行細節上略有差異，但執行重點不外乎為識

別、評估和了解個別用戶透過其服務遭遇各種非法／有害內容的風險程度及影響（尤其要將服務所使用的演算法納入考量）、對個人造成傷害的風險程度及影響、有利非法／有害內容傳播的服務功能之風險程度及影響、服務的設計和維運如何增加或降低所識別出的風險等。

7. 通報和改正

根據草案第 15 和 24 條，所有業者皆須提供用戶和受影響人士，易於操作的內容通報系統（包含違法內容、有害兒少和成人內容）及申訴程序，並明訂申訴程序的處理措施。申訴範圍則包含前述的問題內容、業者未落實注意義務、用戶生成或上傳分享的內容遭業者下架或限制訪問或暫停使用服務等處置。

8. 紀錄保存和檢視

根據草案第 16 和 25 條，所有業者皆須製作並保存風險評估的書面紀錄，以及為履行義務而採取措施的書面紀錄；並定期檢視其服務的義務履行情況，且當服務維運有重大改變時，須再次進行檢視。

(二)其他義務

1. 公布透明度報告

所有業者皆須交付並公布透明度年度報告，報告內容視屆時 OFCOM 的通知而定，可能包括推估多少用戶看到非法和有害內容、這些內容如何透過其服務散播、相關的服務條款／政策聲明如何落實、用戶舉報這些違反服務條款／政策聲明的系統和流程、識別和處理這些內容的系統和流程、進行這些內容風險評估的系統和流程等（第 49 條）。

2. 繳交年費

全球年營收達一定門檻的業者須繳年費，作為 OFCOM 執行此法的所需支出（第 52 條）。

三、OFCOM 的職責與權力

（一）OFCOM 的執法職責暨權力

1. 開立「運用技術告誡通知」

當 OFCOM 認為業者未履行處理非法內容的義務時（須有證據顯示網路上經常且持續可見恐怖主義或兒少性剝削和虐待的非法內容），OFCOM 可以開立「運用技術告誡通知」，要求業者使用經認可的技術（可單獨使用該技術或加上人工審核)來進行識別和迅速刪除非法內容。之後 OFCOM 再次評估且提供業者陳述機會後，如果認為業者沒有履行該通知，可再度開立「運用技術告誡通知」(use of technology warning notice)（第 63 ~ 66 條），或是直接寄發罰款通知（第 90 條）。而業者對於這些通知皆有向上級法院提起上訴的權利，上級法院將駁回上訴或撤銷 OFCOM 的通知（第 105 條）。

2. 行使權力：索取資訊、調查、約談和入內搜查

OFCOM 可以開立「資訊通知（information notice)」，要求業者提供 OFCOM 基於行使其促進網路安全職責的任何資訊，例如：為了評估業者注意義務的遵循狀況、決定年費的收取門檻、裁決罰款的金額、準備業者的「業務守則」、進行網路安全相關研究，或促進媒體素養等（第 70 條）。

OFCOM 還可以針對業者是否遵循各項義務、要求和通知，啟動調查和約談，且業者必須完全配合，但被約談者仍保有秘密通訊的權力（第 75 ~ 76 條)。此外，OFCOM 亦可直接行使入內搜查權，惟須確認搜查處為受監管服務的經營場所，且已提前 7 天通知業者將行使搜查權。而進入該場所後，OFCOM 可以檢查場所內的任何文件或設備，及觀察業者執行受監管的服務。如果直接行使搜查權遭拒，或需要緊急進入該場所時，則可向法院申請搜查令（第 77 條和附件 5）。

3.祭出懲處：罰鍰、業務中斷和刑責

OFCOM 可以針對沒有遵循注意義務及 OFCOM 通知或要求的業者，處以罰鍰或業務中斷。罰鍰金額由OFCOM決定，且上限可高達1,800萬英鎊，或全球年營業額10%，兩者以較高者為準（第 85～86 條）。業務中斷則是要向法院申請「服務限制令」（service restriction order），藉由其他相關業者的協助執行，中斷該違法服務的資金往來或廣告宣傳（第 91 條）。如果仍然無法防止該違法服務對英國民眾造成重大傷害，OFCOM 可向法院申請「網路接取限制令」（access restriction order），透過命令提供該服務網路接取的業者，阻斷英國用戶使用該服務（第 93 條）。

此外，針對前述索取資訊的「資訊通知」，相關人員若不遵守此通知的要求、在知情下提供假資訊，或是為了阻止 OFCOM 理解實情而提供加密文件，皆構成犯罪行為，並可透過簡易定罪程序（由法官直接定罪，不需經由陪審團的審判程序）處以罰金，或依起訴書定罪（第 72 條）。如果負責此通知的主管沒有採取合理措施防止上述犯罪行為的發生，同樣構成犯罪，並同樣可藉簡易定罪程序處以罰金，或依起訴書定罪，且處不超過 2 年刑責或（及）罰金（第 73 條）。又提供資訊相關人員的罪行如果經證明是在企業主管的同意或縱容下進行的，或可歸咎於主管的任何疏忽，則該主管及企業實體皆屬犯罪，並可因此受到起訴及懲罰（第 125 條）。

（二）OFCOM 的其他職責

1.訂定「業務守則」（codes of practice）

OFCOM 須為業者準備「業務守則」，針對如何處理恐怖主義和兒少性剝削和虐待的非法內容，以及遵循法規其他義務，提供建議措施。制訂守則或後續修訂時，必須諮詢內閣大臣（部長）、各方利害關係人代表（業者、用戶、兒童權益、受害者之代表），以及專家（網路安全相關的人權、公衛、新興科技、刑法、國安之專家）；並考慮守則內容對不同的受監管服務和受監管業者的適當性；還要確保守則和所追求的網路安全目標一致，例如：法律遵循和風險管理的系統和流程是有效的、服務條款是英國用戶（包含兒少）能夠了解的、該服務為兒童提供的保護標準比成人更高、以保護英國用戶免受傷害的角度來設計和評估服務（包含演算法的使用）等（第 29～31 條）。

2.建立服務類別登記

OFCOM 須建立並維護受監管服務的登記，分成第 1 類用戶對用戶服務、2A 類搜尋服務，以及 2B 類用戶對用戶服務。如前所述，各類別的明確門檻條件將由內閣大臣（部長）考量風險和影響性等情況後訂定，OFCOM 僅是進行相關研究並提供參考建議。登記項目則包括服務名稱、服務描述，以及業者名稱（第 59 條和附件 4）。如果業者對於被納入登記有所質疑，可向上級法院提起上訴，上級法院將駁回上訴或撤銷 OFCOM 登記（第 104 條）。

3.進行風險評估和提供指南

OFCOM 須針對各類受監管服務進行風險評估，以識別、評估和了解這些服務的傷害風險。進行評估時，要各別考慮非法內容對英國個人造成傷害的風險、兒少有害內容對英國不同年齡層兒少造成傷害的風險，以及成人有害內容對英國成人造成傷害的風險（第 61 條）。

OFCOM 還須為各類受監管服務建立風險剖析（profiles），並發布「風險評估指南」，以協助業者完成其風險評估的義務。風險剖析也是「風險評估指南」的一部分，且進行時需考量服務的特徵（包括服務特性、用戶族群、商業模式、治理，及其他系統和流程），以及風險評估所識別出的風險程度（第 61～62 條）。

4.推動媒體素養

OFCOM 推動媒體素養的職責其實於英國《通訊法》（Communications Act 2003）第 11 條已有規範，但草案要求 OFCOM 進一步強化此項職責，包括必須採取行動提高英國使用者的媒體素養，尤其要鼓勵受監管業者開發和使用可以提升媒體素養的技術和系統；必須執行、委託或鼓勵相關的教育活動；以及必須發布媒體素養措施和活動的評估指南（第 103 條）。

5.配合內閣大臣（部長）特定的指示

OFCOM 執行職責時，須考量內閣大臣（部長）發布的網路安全事務戰略優先事項聲明，並說明相關的回應措施（第 57 和 109 條）。此外，如果內閣大臣因為認為英國的公眾健康、安全，或國家安全受到威脅而向 OFCOM 發出指示時，OFCOM 須透過其推動媒體素養的職務，優先解決前述的特定威脅；或向指定的業者或全體業者發出公開聲明通知，規定業者在期限內，公開聲明如何因應該特定威脅（第 112 條）。

6.提供諮詢、研究和報告

OFCOM 須成立「不實和虛假訊息諮詢委員會」，以針對受監管業者如何處理此類訊息，以及 OFCOM 如何提升因應此類訊息的媒體素養，提供相關建議（第 98 條）。在研究方面，OFCOM 須掌握公眾對業者及其服務的輿論、研究受監管服務的用戶經驗，並了解用戶對於業者處理其申訴的看法（第 99 條）。OFCOM 還須發布「透明度報告」，從業者交付的「透明度報告」中，歸納並總結業者的透明度模式和趨勢，以及整體行業行為是否良好等（第 100 條）。

（三）域外適用

草案第 127～128 條特別說明此法的域外適用範圍和管轄權[4]。整體而言，此法提及的網路服務，包括於英國境內和境外提供的網路服務，且 OFCOM 的索取資訊權（第 70 條）也包括英國境外的資料；同樣的，約談權也擴及要求英國境外人士出席約談。

此外，對於違反 OFCOM 索取資訊要求的相關犯行及其懲處，亦適用於在英國境外進行的犯罪行為，包括提供資訊者的犯行（第 72 條）、負責該「資訊通知」主管的犯行（第 73 條），以及企業實體主管的犯行（第 125 條），且可在英國任何地方提起訴訟。

4 針對草案的域外適用，國際律師事務所 Herbert Smith Freehills（2021）表示，未來草案如何執行仍待觀察，但可注意它是否仿效歐盟《數位服務法》（DSA）草案，要求在境內指派 1 名法務代表。另一國際律師事務所 CMS（2021）則認為，OFCOM 可向法院申請「服務限制令」或「網路接取限制令」亦是因應域外管轄問題。

第五節 英國各界的反應

一、民間團體和國會肯定部分立法

加拿大兒童保護中心（The Canadian Centre for Child Protection, C3P）跨海肯定英國推動此項立法，並指出科技公司長期以來在沒有受到任何監管下運作，已經讓全世界的青少兒付出不小代價。如今英國政府透過立法要求科技公司對平臺內容負責，並將懲處違法者，是為保護兒少網路安全邁出勇敢的一步。C3P 還強調，打擊線上兒少性剝削和虐待內容有賴全球政府共同合作，現在各國應該採取類似行動以保護兒少網路安全（C3P, 2021）。

卡內基英國信託機構（Carnegie UK Trust）則是肯定英國數位部導入法定的注意義務，以系統性方式監管網路有害內容，也就是讓社群媒體設計和維運更安全的系統，而不是讓政府監管個別內容。它進一步說明指出，就如健康和安全的監管講求注意義務，業者對網路安全也應負起注意義務，以適當、基於風險的方式來維運系統，減少可預見的傷害；而且廣播電視的監管經驗顯示，熟練的監管者可以在上下文中，評估傷害且進行監管，並在維護言論自由之間取得平衡（Woods, 2021）。

英國上議院的通訊傳播與數位委員會也肯定草案為民眾創造更安全網路的立法目標，並讓英國有機會在以人權為基礎的網路法規上，引領世界（Communications and Digital Committee, 2021）。維權團體全球夥伴數位化（Global Partners Digital, GPD）則樂見草案將保護言論自由和隱私、提供下架內容便利申訴管道等促進用戶權益措施，做出明文規定（Earp, 2021）。

然而，不論是卡內基英國信託機構、上議院通訊傳播與數位委員會，或 GPD，同時也都提出對草案持反對或有所疑慮之處，這些意見將於後續段落中說明。

二、兒少保護團體盼更嚴格立法

英國全國防止虐待兒童協會（NSPCC）呼籲英國政府擴大立法，採取更多措施以阻止兒少造訪任何色情內容，且防止不當內容在不同平臺上傳播。NSPCC 表示，青少兒使用不同平臺來記錄和分享虐待行為，很容易從 Snapchat 轉到 WhatsApp，但目前草案沒有充分解決平臺之間迅速傳播的風險，因此，應該強制科技公司合作，提供系統性保護措施，並擴大立法範圍，以保護兒少免於受虐。兒少網路安全機構——網路觀察基金會（Internet Watch Foundation, IWF）也期盼政府能推出更嚴格的保護措施，以保障兒少上網的最大安全（E&T Magazine, 2021）。

三、維權團體等呼籲改革草案以保護言論自由和隱私

由英國和國際維權組織以及智庫(如Big Brother Watch、Global Partners Digital、Adam Smith Institute）共同組成的拯救線上言論聯盟（Save Online Speech Coalition)表示，有效且適當的管理網路的確相當不易，但草案可能創造一個西方世界最嚴苛的網路言論制度，因此，呼籲英國政府徹底修改此法以保護言論自由和隱私。修改重點包括：

- 勿將合法內容入法

強迫平臺審查合法但有害內容將帶來危害言論自由的風險。英國的言論已有廣泛的法律限制，線下的法律應該同樣適用於線上，但此法卻實施兩套言論制度，對線上的合法言論施加額外限制。因此，合法言論應完全從草案中刪除。

- 勿讓科技平臺充當言論警察

草案將授權甚至迫使（因為巨額罰款）大型科技公司對平臺進行大規模的監控和審查，充當網路言論的警察，將對言論自由產生嚴重的寒蟬效應。國家不應該支持科技公司原本就不利於隱私和言論自由的服務條款，也不該招募他們擔任國家言論警察。

- 保護網路私人通訊（勿將私人訊息入法）

政府也考慮審查私人通訊，可能會禁止加密，一旦成真將直接衝擊私人通訊的基本權利。網路私人通訊和匿名性對於民眾的安全和隱私，和保護世界各地的記者、維權人士和舉報人，都至關重要。侵蝕網路隱私的舉措將為更多專制政權樹立一個可怕的榜樣。因此，私人通訊不應屬於草案的範圍。

英國 Aston 大學資深助理教授 Edina Harbinja（2021）博士補充說明，由於草案的豁免服務僅限於email、即時訊息、一對一語音通話，是屬於該

服務唯一的用戶生成內容情況，因此，Facebook Messenger、Zoom 等平臺都將受到規範。

Harbinja 並表示，草案的規範形同鼓勵業者使用監看技術審查私人訊息以處理非法內容，而有害內容又充斥模糊定義，可能導致平臺對用戶內容進行過度嚴格的審核，這些都將危害個人的通訊隱私及言論自由。更令人擔憂的是，原本歐盟《電子商務指令》（E-commerce Directive）第 15 條禁止對用戶進行一般監控的規定可能會被撤銷，因為英國政府表示，英國已經脫離歐盟，英國立法不再有遵循歐盟法規的義務。

此外，還有議員和維權團體認為草案猶如「審查者的特許證」，它可能會阻止一般民眾發布合法的貼文，並將 OFCOM 變成言論自由的超級監管者。因此，他們也發起「合法言論皆能合法打字」(legal to say, legal to type)的反對活動（BBC News, 2021）。

英國上議院的通訊傳播與數位委員會也強調，草案處理有害內容的方式將威脅言論自由。委員會主席 Lord Gilbert 表示，如果政府認為某種尚未違法的內容會造成嚴重傷害，應該改由刑事犯罪來定義和定罪。例如：針對英格蘭足球員的種族歧視辱罵（目前並不違法），應立即運用法律力量來處置肇事者，這樣不但比較有效，而且也保護英國長期珍惜的言論自由價值（Communications and Digital Committee, 2021）。

四、公商組織呼籲國會莫讓立法破壞加密安全保障

上述維權團體提及的禁止加密問題，也受到網際網路協會（Internet Society, ISOC）、數位經濟聯盟（Coalition for a Digital Economy, COADEC）等三十多個公民團體和商業組織的高度關注。他們透過全球加密聯盟（The Global Encryption Coalition）表示，草案對英國公民和企業的安全威脅遠超過保護，因為點對點加密可以保護個人、商業和政府的資料傳輸安全，但未來業者可能為了遵循法規要求的對用戶內容負責而取消加密服務，導致英國失去最大的數位安全防護，進而讓犯罪份子有機可趁，損害英國公民、企業和國家的利益。因此，呼籲國會議員，莫讓此立法破壞保護安全的點對點加密（Wilton, 2021）。

ISOC 補充說明指出，加密技術可以保護交易安全、通訊機密性和人身安全，弱化或取消加密將使全民陷於安全風險中。尤其兒少的通訊一旦曝露給有心人士，可能將危害他們的人身安全（ISOC, 2021）。

而代表網路產業且會員包含 Facebook、Google 等科技巨頭的網路協會（Internet Association, IA），雖然尚未對草案發表聲明，不過，它於去年（2020）底英國數位部發布《政府最終回應白皮書意見徵詢》報告後曾表示，「涵蓋中介者責任的監管方法是實現網路益處的關鍵之一，政府回應中有許多有用的建議，但也有些可能導致意外的後果，例如：加密等重要問題即需更明確化，因為這攸關網路安全、隱私及如何保護言論自由。在政府訂定《網路安全法》時，我們將持續和它建設性地合作」（IA, 2020）。

五、各界擔憂責任模糊和嚴刑峻罰將導致過度審查

包括法律學者、律師、維權團體、上議院通訊傳播與數位委員會都認為草案缺乏清晰度，多種職責及其內涵含糊不清，恐將造成過度審查。以有害內容的定義為例，「業者有『合理理由相信』內容的性質將會（直接）或『間接』對具有『普通情感』的兒少／成人，產生『嚴重』不利『身心影響』的『重大風險』」，當中每個詞彙都被點名為語意不清。上議院通訊傳播與數位委員會表示，這將導致合法且善意的內容因為過度揣測其影響性而被審查，他們擔憂平臺將為了執行此項規範而嚴重干預用戶的言論自由（Communications and Digital Committee, 2021）。

而可能助長過度審查的，還有嚴刑峻罰。維權團體——開放權力組織（Open Rights Group）指出，雖然民眾強烈要求對發生濫用問題的社群媒體祭出重罰，但業者在無客觀標準下，要決定什麼是可接受和不可接受的內容，而且還要面臨巨額罰鍰和刑事責任的懲處風險，他們的解決方案就是大量刪除用戶內容，其中大部分是屬於完全合法的內容，最終不但沒有解決濫用問題，還導致所有人的言論自由遭到限制，英國也淪為專制國家（Burns, 2021a）。

此外，草案還將帶給企業沉重的成本負擔。英國律師事務所 Mishcon de Reya 的資料保護專家 Jon Baines 表示，草案要求科技公司對其運營方式進行大規模的改變，受監管的企業將面臨沉重的法遵和成本增加的挑戰，一旦代價太高，將會阻礙科技的商業發展和創新（Clarke, 2021）。

英國 Aston 大學資深助理教授 Edina Harbinja（2021）博士也指出，業者的負擔將無法估計，他們將被要求做出各種判斷，包括什麼是政治言論和新聞言論、哪些內容對用戶有害、傷害程度又有多大等，而且解決方案往往是侵犯個人的基本自由，因此，如果草案沒有大幅修改，一旦上路將是窒礙難行。

六、國會和媒體認為部分內容保護不足或有衝突

英國上議院通訊傳播與數位委員會雖然對於草案的強制刪除非法內容、避免兒童接觸有害內容、保護具民主重要性內容、保護新聞內容等規定表示支持，但也指出當中保護不足之處，包括刪除非法內容沒有限定完成時間、一般色情網站不在受監管服務的範圍內、民眾發起的政策和社會議題辯論不屬於受保護的民主重要性內容，以及公民新聞沒有明確定義無法受新聞內容條款的保護（Communications and Digital Committee, 2021）。

卡內基英國信託機構也提出草案沒有回應當下問題內容之處。它指出，雖然草案要求大型平臺對成人有害內容負責，但卻沒有妥善規範，也沒有反映大量存在且具危害性的種族主義內容及錯誤或虛假信息，政府應該闡明如何解決這些問題（Woods, 2021）。

科技新聞媒體 TechCrunch 則提及草案在內容注意義務方面的衝突。報導指出，保護具民主重要性內容和新聞內容使得內容審核更為複雜，甚至和處理有害內容的義務相互衝突。例如：極端主義團體試圖將他們的仇恨言論和辱罵偽裝成政治觀點、一些惡名昭彰的種族主義者也聲稱自己是公民記者（Lomas, 2021）。

七、各界擔憂政府權力過大和監管能力不足

卡內基英國信託機構表示，整個草案的運作方式令人擔憂。原則上行政部門和監管機構之間應該分權，但草案賦予數位部長太多權力，尤其是可以向 OFCOM 下達指令，要求其符合政府政策，這可能將包含政治上不中立的事情（Woods, 2021）。

科技政策暨產業顧問公司 Taso Advisory 也認為，草案為數位部長提供前所未有的權力來指導一個獨立的監管者，將會帶給企業嚴重的不確定性，因為規則可能會隨著一位政治人物的一時興起而改變。持相似看法的，還有維權團體Big Brother Watch。它表示，OFCOM只是名義上的獨立監管機構，其最高主管也是政治任命；而今草案還將賦予數位部長自由裁量權，OFCOM 的角色將淪為執行部長的命令，且所有行動都會冠以符合國家或國安利益為由。Big Brother Watch 並強調，任何言論自由權的限制都須符合英國法律，且透過完整的立法程序來決定，而不是將決定權交由這種有缺陷、政治化的監管體系（Dickson, 2021）。

另一個維權團體——開放權力組織指出，數位部長可以在任何時候片面決定什麼有害內容必須納入法規，且可因政治因素來做決定，然後號稱獨立監管機關的 OFCOM 就會下令業者執行新規定。政府還有權力封鎖在英國營運的服務，也就是當某服務上的輿論挑戰政府時，他們可以透過中斷服務來壓制異議，這是獨裁國家樂見的。此外，小型業者可能因為無法遵循嚴刑峻法而離開英國市場，反而鞏固了科技巨頭的市場力量（Burns, 2021b）。

法律學者 Edina Harbinja（2021）則是擔憂 OFCOM 能否承擔此重責大任。她表示，草案創造一個非常強大的網路監管機構 OFCOM，它擁有重要的執法任務和各種執法權力，將對企業和民眾的數位權利產生重大且持久影響。但 OFCOM 過去只有監管電信和廣播的經驗，且長期缺乏人力和技術能力，因此，未來它將如何監管網路安全事務令人疑慮。

第六節 結論與建議

一、結論

（一）草案評價兩極，但英國社會對立法規範網路平臺有高度共識

整體而言，英國各界對於草案的看法可分成「立法過度」和「立法不足」兩大類。一方面，維權團體、法律界、國會上議院等單位或專家，擔心草案迫使大型平臺業者充當網路警察，審查使用者的內容，且審查範圍包含定義模糊的合法但有害內容，以及沒有列入豁免服務的平臺私人訊息，加上違者將被處以嚴刑峻罰，這些因素可能導致業者過度審查，對言論自由帶來寒蟬效應，創造一個西方世界最嚴苛的網路言論制度。但另一方面，兒少保護團體呼籲擴大立法，以阻止兒少造訪任何色情內容；足球協會則擔心草案受到保護言論自由旗幟的弱化（Murgia, Bradshaw & Parker, 2021）；而上議院和公益團體等單位指出草案對於有害、具民主重要性、新聞等內容的保護不足之處，以及對種族主義和虛假訊息等內容沒有著墨等問題。

儘管如此，在歷經挾帶網路因素的多起恐怖攻擊、少女瀏覽大量自殺網路訊息而輕生身亡，以及引發英國首相親上火線和百萬民眾請願反制網路種族歧視等重大事件的英國社會，對於立法規範網路平臺已經形成高度共識 [5]，歧見的部分其實是執行方向和細節。此點除了從上述各界在批評草案的同時，大多也會提及他們認同之處得到驗證外，最顯著的還有維權團體等組織呼籲的是「改革」草案，而非「撤回」草案。

5 近期還有近 70 萬英國民眾向政府請願，要求規定申請社群媒體帳號時，要進行實名制的身分驗證。https://petition.parliament.uk/petitions/575833

（二）英國政策發展原本嚴謹且採多方模式，但最終在壓力下倉促提案

英國政府從 2017 年 10 月釋出《網路安全策略綠皮書》、2019 年 4 月發布《網路危害白皮書》，到 2021 年 5 月推出《網路安全法》草案並送英國議會審議，共計費時約 3 年半。數位部表示，英國信守多方利害關係人模式的網路治理，是確保網路自由開放和安全的最佳方式（DCMS & Home Office, 2020c)。因此，不論是綠皮書或白皮書階段，皆可見政府進行公眾意見徵詢，尤其白皮書階段的徵詢更是多元廣泛且頻繁，其型式的多元包括討論或交流會議、焦點訪談、問卷調查、政策研討會等；徵詢對象的廣泛涵蓋受害者團體組織、心理健康組織、家長和兒少安全組織等；次數的頻繁或數量之多可達100場利害關係人會議、17場部長級會議、超過2,400份徵詢意見等。

然而，受到 COVID-19 疫情影響以及輿論的壓力，數位部的提案時程似乎被迫提前進行，且嚴謹做法也未能堅持到最後。根據英國媒體報導，數位部曾於 2020 年 5 月表示，由於日以繼夜地處理病毒相關假訊息，以致無法於 2021 年底前，提交草案至議會，但此說法引發部分議員不滿（BBC News, 2020）。維權團體－－開放權力組織則提到「激烈的公眾言論正在給政府施加壓力.....自從綠皮書階段就參加無數次的討論會議，但看到草案時卻感到震驚」（Burns, 2021b）。CMS 法律事務所也指出，草案範圍超出《政府最終回應白皮書意見徵詢》報告，例如：業者對言論自由和民主內容的積極義務等規範都沒有在回應報告中（CMS, 2021）。由上顯示，數位部最終可能是在沒有充分進行公眾意見徵詢下倉促提案，這或許也是草案出現諸多定義不明條文，以及規範內容遭致眾多批評的一大主因。

二、建議事項

（一）立即可行之建議

1. 觀察國際發展趨勢並進行國內政策溝通

(1)平臺責任觀點逐漸轉為「問責」，但我國國情不同需更審慎因應

除了英國《網路安全法》草案外，同樣處於立法程序的歐盟《數位服務法》（Digital Services Act, DSA）草案和澳洲《網路安全法》（Online Safety Bill）草案，皆涉及網路業者對於網路內容的責任規範。此外，美國總統拜登就職前也曾表示贊成廢除保障網路業者對平臺內容免責的《通信端正法》（Communications Decency Act, CDA）第 230 條（Hamilton, 2021）。由此顯示，國際間對平臺責任的觀點，正由過去的「免責」逐漸轉變為「問責」。

我國通傳會亦研擬「新版」《數位通訊傳播法》，規範平臺業者責任。在平臺責任觀念逐漸轉變的國際趨勢下，此次科技巨頭或許不會如同 2018 年一樣，透過亞洲網路聯盟（Asia Internet Coalition, AIC）要求我國撤案重審[6]，就像它們也沒有反對英國推動《網路安全法》。不過，我國國情有別於歐美國家，以英國為例，相較於英國社會因為歷經重大事件而對立法規範網路平臺形成高度共識，雖然國內也曾發生因網路霸凌或假訊息而自殺身亡的憾事，但目前社會各界對於涉及言論自由的網路規範仍是看法分歧，且缺乏理性討論的空間，動輒以「數位威權」、「數位東廠」、「網路戒嚴」等負面語彙加以抨擊。因此，我國對於相關政策法規的推動恐需更加審慎，正如行政院政務委員羅秉成表示：「臺灣社會對此議題高度敏感……以臺灣各方面能力和政治生態來看，我們沒有超前的條件」（陳洧農，2021）。

6 成員包含 Google、Facebook、Twitter 等網路業者的亞洲網路聯盟（AIC）於 2018 年 12 月 12 日公開致函行政院，以危害言論自由和人權為由，要求行政院撤回《數位通訊傳播法》草案（吳家豪，2018）。

(2) 現階段可先進行國際案例深入研究和國內政策溝通

目前我國對平臺業者採取自律方式，但是網路上的公然侮辱、毀謗、霸凌、假訊息、危害國家安全和兒少安全、商業廣告等內容，已有既有法律或透過修法加以規範[7]（雖然亦衍生濫用法規問題，但此為另一課題）。這種做法不但是英國最近處理足球員遭網路霸凌的方式（擬將實體世界肇事者不得入場觀賽的《足球禁令》，修法擴及網路的肇事者），而且也是英國上議院對於此次草案的一項修正建議（嚴重的危害應由法律來定義犯罪，而非由業者自行審查有害內容並加以處置）。因此，現階段我國應該尚有時間，而且也需要針對如前所述的先進國家相關法案進行深入研究、綜合比較及追蹤立法進展。研究範圍除了草案條文外，也必須了解其政策發展過程、社會情境、各界看法，以掌握國際總體趨勢、釐清特殊國情規範，進而從中找出可供我國參酌之處。

此外，我國也需要透過公正客觀的研究調查，以及充分的多方利害關係人溝通，了解國內對於網路內容治理的民意動向和社會共識，以強化相關政策或立法的正當性、支持度，及儘可能符合最大公共利益。例如：英國的白皮書即指出 75% 英國成人對於上網感到擔憂、61%英國人希望政府為打擊假訊息做得更多……，且白皮書公布之後還進行多元且頻繁的公眾意見徵詢，這些政策發展措施值得我國學習，同時也可避免再度被亞洲網路聯盟（AIC）指責「臺灣政府與產業間缺乏持續性的實質溝通」（吳家豪，2018）。

7 根據理律法律事務所曾更瑩律師於 2020 網路治理研習營的專題講習資料。可參考本團隊執行通傳會「強化我國網路治理交流與人才培育」委託研究計畫之期末報告。

（二）中長期建議

1. 建立市場競爭制度

英國維權團體和上議院認為，從市場競爭制度來建立業者的問責，將是更好的方式，也比《網路安全法》更加重要。因為目前市場缺乏競爭，迫使民眾只能使用少數平臺；但如果是競爭激烈的市場，平臺業者就必須積極回應用戶對言論自由和隱私等訴求，凸顯促進競爭對維護數位人權的至關重要。因此，應該立法建立新的市場競爭事前（ex ante）規範，以在損害發生之前即展開預防措施，例如：政府有權針對具有市場主導地位的平臺進行有利於競爭的干預、確保消費者可以行使合法的選擇權(Burns, 2021; Communications and Digital Committee, 2021）。而此項能夠促進數位市場公平競爭、維護言論自由等人權，又相對不會引發社會爭議的事前規範方式，亦值得我國主管機關（依據立法院初審通過之相關組織法，涉及的行政部門包括通傳會、公平會、數位發展部[8]）著手進行研議，並可參酌歐盟《數位市場法》（Digital Market Act, DMA）草案之相關規範。

2. 將媒體素養列為重要且長期施政項目

英國《網路安全法》草案將 OFCOM 強化推動媒體素養的職責入法，雖然條文簡短，且對於如何執行或須達成什麼目標也幾乎沒有著墨，但如果草案獲得通過，形同法律認可媒體素養對於促進網路安全的價值。我國教育部自 108 年推動「媒體素養教育行動方案」，以提升各級學生和國人於獲取資訊、解讀資訊和分享資訊的能力（110 年度計畫目標）。另一方面，各部會也依其職掌領域推動提升媒體素養的相關工作，例如：通傳會

8 根據立法院 5 月 5 日初審通過的《國家通訊傳播委員會組織法》修正草案，及《數位發展部組織法草案》，前者第 3 條掌理事項之第七款「通訊傳播競爭秩序之維護」並沒有如其他條款增列「網際網路傳播」，而後者的附帶決議為「數位發展部在數位市場秩序維護上，應向相關部會(包含國家通訊傳播委員會、金融監督管理委員會、公平交易委員會等)積極提供法制及管理機制之建議」（立法院，2021）。因此，究竟何者為網路或數位市場秩序的事前規範主管機關，仍待釐清。

舉辦 110 年度「廣電媒體素養公民培力合作」活動、文化部 109 年度平面媒體兒少新聞識讀推廣計畫舉辦「媒體識讀工作坊」、衛福部等單位於 107 年舉辦「兒少權益與媒體識讀暨媒體素養桌遊培力工作坊」。隨著媒體素養的重要性日益在國際上獲得正式認可，建議教育部將媒體素養列為重要且長期施政項目，且於其「透過多元管道，培養全民素養」面向，納入上述各部會的宣導活動，除了可避免資源重複之外，也可盤點出尚未納入宣導的族群，並予以補強。此外，還可善用民間的力量，邀請民間單位響應宣導活動或提供宣導資源，尤其網路平臺業者可能樂於共襄盛舉，因為這也是他們展現善盡教育用戶和促進安全網路環境之責的良機。

參考文獻

- 立法院 (2021)。立法院第 10 屆第 3 會期司法及法制、交通委員會第 1 次聯席會議議事錄。https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=44859&pid=209244
- 行政院 (2020)。立法院第 10 屆第 1 會期行政院施政報告。https://www.ey.gov.tw/File/FF5849ABBA72E66F/f7aead47-25ba-4171-b002-a0066115750a?A=C
- 吳家豪 (2018)。AIC 發公開信 籲政院撤回數位通訊傳播法草案。新頭殼 Newtalk 轉載中央社，2018/12/12。https://newtalk.tw/news/view/2018-12-12/179729
- 教育部 (2021)。媒體素養教育資源網。https://mlearn.moe.gov.tw/CaseOfficer
- 通傳會 (2019)。108 年度廣電媒體專業素養培訓與公民培力推廣計畫。https://www.ncc.gov.tw/chinese/files/20060/5265_43217_200602_1.pdf
- 通傳會 (2021)。110 年度廣電媒體專業素養公民培力推廣，合作辦理申請。https://seminars.tca.org.tw/D18j01187.aspx
- 陳洧農 (2021)。【講座】羅秉成、蘇正平、劉昌德：「打假訊息」的台灣模式如何建立？如何延續？關鍵評論，2021/6/17。https://www.thenewslens.com/article/152354
- 諄筆群 (2021)。點教育》媒體素養教育首應導正年輕世代的使用觀念。新新聞，2021/2/8。https://www.storm.mg/article/3428873?page=1
- BBC News (2020). Online Harms bill: Warning over 'unacceptable' delay. 2020/6/29. https://www.bbc.com/news/technology-53222665

- BBC News (2021). Online Safety Bill ‘catastrophic for free speech‘. https://www.bbc.com/news/technology-57569336
- Burns, H. (2021a). Online Abuse: Why Management Liability isn’t the Answer. Open Rights Group. https://www.openrightsgroup.org/blog/online-abuse-why-management-liability-isnt-the-answer/
- Burns, H. (2021b). Why the online safety bill threatens our civil liberties. Politics. https://www.politics.co.uk/comment/2021/05/26/why-the-online-safety-bill-threatens-our-civil-liberties/
- C3P. (2021). Statement: Canadian Centre for Child Protection Supports UK’s Online Safety Bill. https://protectchildren.ca/en/press-and-media/news-releases/2021/uk-online-safety-bill
- Change.org. (2021). Ban racists for life from all football matches in England. https://www.change.org/p/football-association-and-oliver-dowden-sec-of-state-dcms-pm-boris-johnson-ban-racists-for-life-from-all-football-matches-in-england
- Clarke, L. (2021, May 13). The UK’s Online Safety Bill could drown internet services in red tape. TechMonitor. https://techmonitor.ai/regulation-compliance/uk-online-safety-bill-red-tape-boris-johnson
- CMS Law-Now (2021). UK's Online Safety Bill published. 2021/5/18. https://www.cms-lawnow.com/ealerts/2021/05/uks-online-safety-bill-published

- Communications and Digital Committee (2021). Communications and Digital Committee publishes report on freedom of expression online. 2021/7/22. https://committees.parliament.uk/committee/170/communications-and-digital-committee/news/156755/communications-and-digital-committee-publishes-report-on-freedom-of-expression-online/
- DCMS & Home Office (2019). Online Harms White Paper - Executive summary. GOV.UK, 2019/4/30. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper-executive-summary--2#contents
- DCMS & Home Office (2020a). Online Harms White Paper - Initial consultation response. GOV.UK, 2020/2/12. https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response#next-steps
- DCMS & Home Office (2020b). Online Harms White Paper: Full government response to the consultation. GOV.UK, 2020/12/15. https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response#part-7-conclusion-and-next-steps
- DCMS & Home Office (2020c). Consultation outcome Online Harms White Paper. GOV.UK, 2020/12/15. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper#contents
- DCMS (2018). Consultation outcome. Internet Safety Strategy green paper. GOV.UK, 2018/6/7. https://www.gov.uk/government/consultations/internet-safety-strategy-green-p

aper

- DCMS (2021a). Press lease. Landmark laws to keep children safe, stop racial hate and protect democracy online published. GOV.UK, 2021/5/12. https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published
- DCMS (2021b). Draft Online Safety Bill. GOV.UK, 2021/5/12. https://www.gov.uk/government/publications/draft-online-safety-bill
- Dickson, A. (2021). New UK internet law raises free speech concerns, say civil liberties campaigners. The Politico, 2021/6/29. https://www.politico.eu/article/uk-concerns-over-internet-free-speech-tech-regulation-power-grab/
- E&T Magazine (2021). Government urged to bolster Online Safety Bill to tackle sexual harassment in schools. https://eandt.theiet.org/content/articles/2021/06/government-urged-to-bolster-online-safety-bill-to-tackle-sexual-harassment-in-schools/#top
- Earp, M. (2021). UK online safety bill raises censorship concerns and questions on future of encryption. CPJ. https://cpj.org/2021/05/uk-online-safety-bill-raises-censorship-concerns-and-questions-on-future-of-encryption/
- EFL (2021). English football announces social media boycott. 2021/4/24. https://www.efl.com/news/2021/april/english-football-announces-social-media-boycott/
- Evans, K. (2019). 9 out of 10 parents back social network regulation. NSPCC, 2019/2/12.

https://www.nspcc.org.uk/about-us/news-opinion/2019/9-in-10-parents-back-social-network-regulation/

- Foster, P. Barker, A. & Parker, G. (2021). Tech platforms could face duty of impartiality in new UK online law. Financial Times, 2020/11/12. https://www.ft.com/content/8b93c8d4-7b6c-4158-bfad-0d4a2e2fdfd2
- Hamilton, I. A. (2021). Here's what could happen to Section 230 – the internet law Donald Trump hates – now the Democrats have both Houses. Business Insider, 2021/1/9. https://www.businessinsider.com/future-of-section-230-democrats-both-houses-2021-1
- Harbinja, E. (2021). The UK's Online Safety Bill: Safe, Harmful, Unworkable? VerfBlog, 2021/5/18. https://verfassungsblog.de/uk-osb/
- Herbert Smith Freehills LLP (2021). New Era For UK Online Regulation: Long-awaited UK Online Safety Bill Published. 2021/5/14. https://hsfnotes.com/tmt/2021/05/14/new-era-for-uk-online-regulation-long-awaited-uk-online-safety-bill-published/#page=1
- Hern, A. (2021). Online safety bill 'a recipe for censorship', say campaigners. The Guardian. https://www.theguardian.com/media/2021/may/12/uk-to-require-social-media-to-protect-democratically-important-content
- IA. (2020). Statement On The UK Government's Final Response To The Online Harms White Paper. 2020/12/15. https://uk.internetassociation.org/news/statement-on-the-final-online-harms-white-paper/

- ISOC (2021). Internet Society: UK Online Public Safety Bill is trying to legislate the impossible – a safe Internet without strong encryption. https://www.internetsociety.org/news/statements/2021/internet-society-uk-online-public-safety-bill-is-trying-to-legislate-the-impossible-a-safe-internet-without-strong-encryption/
- Lomas, N. (2021). UK publishes draft Online Safety Bill. TechCrunch. https://techcrunch.com/2021/05/12/uk-publishes-draft-online-safety-bill/
- Murgia, M.& Bradshaw, T. & Parker, G. (2021). Racist abuse of black footballers reignites debate over social media policing. Financial Times, 2021/7/14. https://www.ft.com/content/bd3c4025-130d-4825-85bd-b8230711d5f2
- O'Callaghan, C. (2021). A wrestle with an octopus - the Online Safety Bill. A step too far onto the toes of free speech, or not far enough? Lexology. https://www.lexology.com/library/detail.aspx?g=7a953d6d-a841-4940-b00f-b5191dc8d9fc
- Prime Minister‘s Office (2021). Government sets out action to stop online racist abuse in football. GOV.UK, 2021/7/15. https://www.gov.uk/government/news/government-sets-out-action-to-stop-online-racist-abuse-in-football
- Rajan, A. (2019). Tech giants write to ministers to spell out views on internet regulation. BBC News, 2019/2/28. https://www.bbc.com/news/entertainment-arts-47400140
- Smith, L. (2017). Messaging app Telegram centrepiece of IS social media strategy. BBC News, 2017/6/5. https://www.bbc.com/news/technology-39743252

- The Irish News. (2019). Molly Russell's father calls for regulation of social media. 2019/3/11. https://www.irishnews.com/magazine/technology/2019/03/11/news/molly-russell-s-father-calls-for-regulation-of-social-media-1570373/
- Twitter (2021). The Duke and Duchess of Cambridge. 2021/7/12. https://twitter.com/KensingtonRoyal/status/1414514323142107136
- Wilton, R. (2021). The Online Safety Bill puts the security of all citizens and communities at risk. The House, 2021/6/15. https://www.politicshome.com/members/article/draft-online-safety-bill-undermines-duty-of-care-to-constituents
- Woods, L., Perrin, W., & Walsh, M. (2021). The Draft Online Safety Bill: Carnegie UK Trust initial analysis. Carnegie UK Trust, 2021/6/15. https://www.carnegieuktrust.org.uk/blog/the-draft-online-safety-bill-carnegie-uk-trust-initial-analysis/

第四章 案例研析：5G 網路的治理議題初探

第一節 前言

隨著各國 5G 陸續商轉，全球正逐漸步入 5G 時代。根據瑞典電信設備大廠 Ericsson 於 2021 年 7 月發布的《愛立信行動趨勢報告》，目前全球已有 160 多家電信商推出 5G 服務，用戶數約 2.9 億，用戶滲透率最高的地區為東北亞，其次是北美；歐洲因為起步較晚，5G 布建速度落後於中、美、韓、日和部分阿拉伯國家。但整體而言，預估 2021 年底，全球 5G 行動用戶數將超過 5.8 億；2026 年底前將達 35 億，全球將有 6 成人口使用 5G。

臺灣愛立信公司表示，臺灣在這波 5G 科技浪潮中處於領先位置，自 2020 年推出 5G 商用網路以來，根據官方（通傳會）統計目前已有超過 270 萬的 5G 用戶，滲透率達 11%以上；且臺灣 5G 網路品質從速度到使用者體驗皆名列前茅，顯示臺灣的 5G 發展位於全球前段班（愛立信，2021）。

我國自 2019 年推動為期 4 年的「臺灣 5G 行動計畫」，打造適合 5G 創新運用發展的環境。5G 網路建設更是通傳會 2021 年的施政重點，期能於 2 年半內達成電波人口涵蓋率 85%目標（通傳會，2021a）。

而全球加速發展 5G 將帶來什麼治理挑戰，也逐漸獲得國際關注。例如：日內瓦網路平臺數位觀測站（Geneva Internet Platform Digital Watch Observatory，以下簡稱 GIP 數位觀測站）和歐洲議會科學與技術選項評估（Science and Technology Options Assessment, STOA）小組，都開始匯集 5G 相關的政策資料；近兩年的聯合國網路治理論壇（IGF）和歐洲網路治理論壇(EuroDIG)也各有座談場次討論 5G 的環保、人權和健康等議題。為此，本章節針對 5G 網路（Network）的治理議題廣泛蒐集資料，並分成地緣政治、資訊安全、數位人權、環境保護、健康疑慮等五個主題，介紹其治理議題，期能協助我國在擴大發揮 5G 正面效益的同時，也為降低 5G 的負面衝擊超前部署。

第二節 地緣政治

一、5G 成為政治戰場的原因和影響

（一）5G 從技術議題變成政治議題

知名政治風險諮詢公司歐亞集團（Eurasia Group, 2018）從兩個面向分析 5G 網路從一項基礎科技變成政治戰場的原因。首先，是 5G 網路在新一代的數位應用（如智慧城市、自駕車）扮演關鍵角色，使得 5G 的開發和布建比 4G 更加受到政治影響，且包括資通訊科技、製造業、汽車業，甚至是整個國家的產業，都想在新興的 5G 生態系統中奪取一席之地。另一方面，是近年來美中兩國的貿易和科技衝突不斷升高，美國對其經濟和國安日益擔憂，中國則是野心勃勃地發展其工業、科技和經濟，使得做為未來各項發展關鍵基礎設施的5G，每個議題都變得政治化，連以往枯燥的技術課題也成為關注焦點。例如：5G 網路標準的制定、供應鏈的位置、行動數據的保護、哪些公司在哪些國家興建 5G 網路等。在此國際局勢下，各國政府和相關產業對於何時及如何布建 5G 網路基礎設施的決策，將對美中和各國未來的數位發展以及全球權力的平衡，產生重大影響。

（二）排除華為 5G 的代價

不過，相較於未來影響，當下的立即衝擊引發更多關注。GIP 數位觀測站指出，美、中對抗顯示世界兩大強國將 5G 視為控制經濟和國安的關鍵。而全球 5G 生態系統分成兩大陣營，除了可能導致技術上的不相容（無法互通操作）之外，許多國家政府限制或禁止使用對其不利的外國供應商所生產的關鍵零組件，也會造成競爭降低、成本提高，進而對整體市場產生負面效應。綜合各方估計，美國單是國防部和太空總署禁止承包商使用華為等中企的技術，就需花費 120 億美元；歐盟布建 5G 如果排除華為設備需要額外投入 550 億歐元，且延誤 1 年半的時程；英國逐步淘汰華為設備也會增加 20 億英鎊的支出和 2～3 年的時程（GIP Digital Watch, 2021）。

GIP 數位觀測站並表示，中國大陸不但通訊設備市占率居全球之冠，且全球 5G 專利高達 36%亦為中企所持有。因此，儘管美國 AT&T、日本 NTT、法國 Orange 和我國中華電信等多家國際電信業者共同成立「開放性無線電接取網路聯盟」（Open Radio Access Network Alliance，簡稱 O-RAN 聯盟），提供各國華為 5G 設備之外的替代性選擇，但由於其開放網路架構中包含中企專利，所以，中企仍可從 O-RAN 聯盟銷售的 5G 設備中獲利。

二、美國 5G 淨網計畫和各國立場

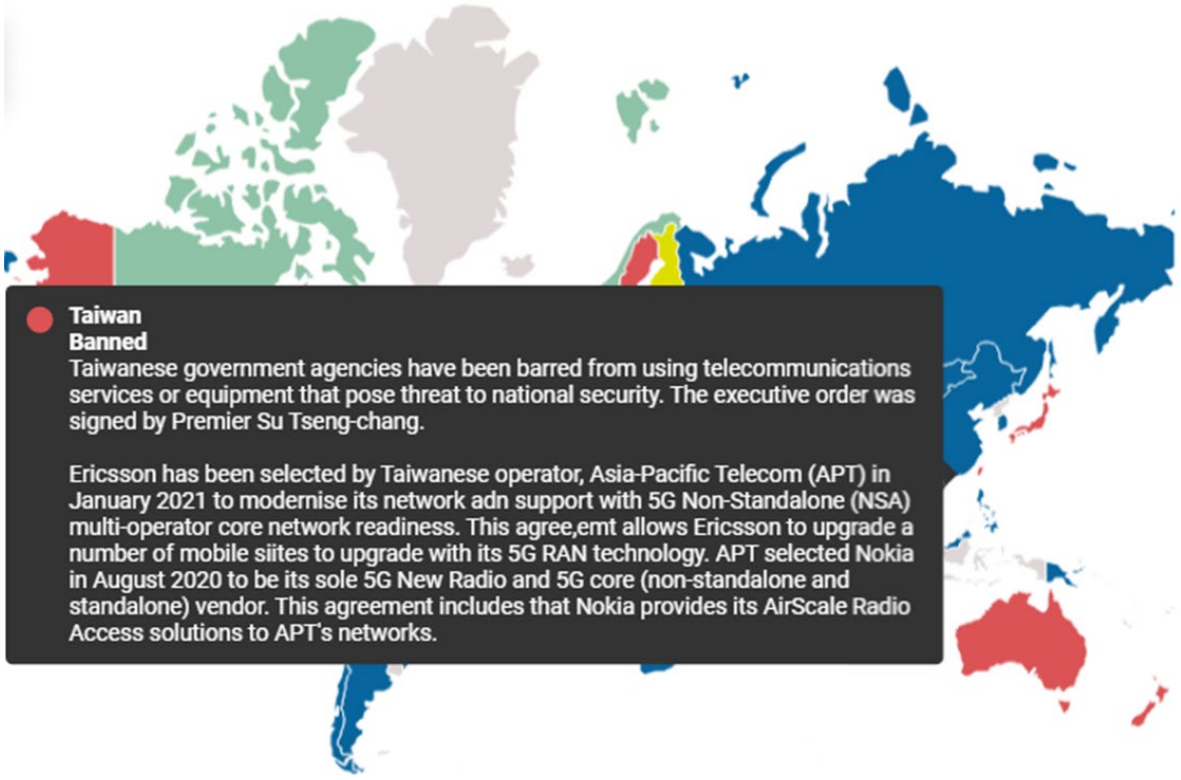
（一）5G 乾淨通道計畫

根據歐亞集團的觀察，中國大陸的 5G 發展策略為奪得全球先驅者的優勢，而美國的策略則是在阻擋中國大陸的同時，掃除民間企業的法規障礙。美國政府自 2018 年即以國安風險或威脅為由，陸續透過法案或行政命令對中國大陸的通訊設備供應商祭出限令，禁止美國政府機構採購或限制於美國商業市場流通。而當中與 5G 最直接相關者，即是美國國務院於 2020 年 4 月發布的「5G 乾淨通道計畫」（5G Clean Path），將 5G 乾淨網路定義為「在端對端的通訊路徑中，從傳輸、控制、運算到儲存上，都不使用來自不可信且必須遵守中國共產黨指令的業者所生產的設備」，並公布全球 27 家 5G 乾淨網路名單，且把華為與中興等中企列為拒絕往來戶（Eurasia Group, 2018；陳曉莉，2020）。

（二）淨網計畫和國際響應情況

美國於 2020 年 8 月進一步將「5G 乾淨通道計畫」擴大為「乾淨網路計畫」（Clean Network，簡稱淨網計畫），實施範圍包括營運商、應用程式商店、應用程式、雲端、電纜、通道等 6 個領域，受影響的中企也擴及至阿里巴巴、百度、騰訊、字節跳動等。美國並號召世界各國加入淨網計畫，截至2021年1月底，共計超過60個國家（代表全球三分之二以上GDP）加入，當中包括26個歐盟成員國、27個北約組織成員國，以及我國；還有 200 家電信業者也共襄盛舉，國內五大電信業者全部入列（GIP Digital Watch, 2021；He, 2021；陳曉莉，2020）。

除了加入美國的淨網計畫外，各國也紛紛基於安全考量，推出不同程度的華為 5G 設備禁令，例如：美、日、英、澳、瑞典和我國等，是完全禁用華為設備；德、法等國是鼓勵採用「非」華為設備；加、義、比等國為電信業者自動選擇「非」華為設備（GIP Digital Watch, 2021）。



資料來源：GIP Digital Watch

圖 4-1　各國規範華為 5G 設備情況之互動式地圖

（三）淨網計畫引發的抨擊

儘管淨網計畫獲得國際熱烈響應，不過，美國內部存有反對意見。例如：美國喬治亞理工學院網路治理計畫創辦人 Milton Mueller（2020）表示，淨網計畫是美國系統性的企圖分裂全球網路，迫使各國資訊服務業者將中國大陸企業排除在外，其背後目的其實是為了保持美國高科技產業的全球領先地位。此種美國經濟民族主義的思維忽視 WTO 電信設備和服務的自由貿易協定，也罔顧全球化數位經濟的商業利益和消費者利益。

三、5G 中製設備的國安疑慮

（一）西方國家的看法

美國聯邦通訊委員會代理主席 Jessica Rosenworcel 表示，不安全的網路設備可能破壞美國 5G 的未來，中共有能力在網路中植入惡意軟體或電腦病毒，以竊取美國的個資、智慧財產，或監控企業與政府部門（Mihalcik & Reardon, 2021）。前主席 Ajit Pai 在任時也指出，華為和中興是美國的國安威脅，已有充分證據證明它們和共軍的關係密切，且中共法律（指《國家情報法》）本來就規定中企具有和情報部門合作的義務（Chris, 2020）。

澳洲政府則是曾耗費 8 個月並實施 300 多項安全措施，試圖找到能夠安全使用華為設備的方法，以促進市場上供應商來源的多元化，但最後仍因無法消除風險而宣布禁止華為參與澳洲 5G 建設。澳洲情報單位表示，引進華為 5G 設備最大的風險，並不在於中共可藉此向澳洲進行竊聽等諜間活動，而是他們能夠關閉澳洲的 5G 網路系統，進而影響民生和經濟，癱瘓整個國家運作（天睿，2021）。無獨有偶，英國政府連續兩年對華為網路設備進行安全檢測的結果，亦皆顯示有影響國家安全的瑕疵（林妍溱，2020）。此外，瑞典政府亦基於國安理由禁止華為參與 5G 建設，且瑞典法院認證，此項規定有正當理由，並不違法（辜泳秝，2021）。

（二）中國大陸的反制

對於西方國家指控華為 5G 危害國家安全，中國大陸方面除了強力反駁這些指控缺乏具體證據，是不公平的推論之外，同時也採取報復行動。例如：2019 年禁止澳洲主要出口收入來源的煤炭進口，以及 2021 年 7 月藉由全球最大電信商——中國移動的 5G 設備招標案，重挫瑞典 Ericsson 於中國市場的營運，其得標占比從 2020 的 11% 降為 1.9%，且所有外商的得標占比也降為只有 5.4%（辜泳秝，2021；MoneyDJ，2021；邱立玲，2019）。

至於華為等中企在這波國際抵制潮下究竟受到多少衝擊，目前市場有

不同說法。有些市場分析認為，從全球商業合約數量來看，芬蘭 Nokia 已經躍居 5G 基地臺的龍頭，華為 5G 的勢力已走下坡；但也有分析指出，華為和中興積極布局中東和非洲市場，截至 2021 年第一季，華為仍以 27%的市占率穩坐全球通訊設備龍頭寶座，大幅領先市占率分別約 17%的 Nokia 和 Ericsson，且中興的市占率亦有約 10%，名列全球第 4 大廠（黃晶琳，2021；時報資訊，2021）。

第三節 資訊安全

第一節 新架構和 IoT 帶來新風險

歐盟網路安全局（European Union Agency for Cybersecurity, ENISA）和全球行動通訊系統協會（Groupe Speciale Mobile Association, GSMA）皆指出，5G 網路採用核心網路、網路切片、無線接取網路、網路功能虛擬化、軟體定義網路、多接取邊緣運算等新架構，雖然同時也設計許多內建的安全控制，如新的相互驗證功能，以限制當今 4G/3G/2G 的網路威脅，加強對個別消費者和行動網路的保護，但是新架構和新功能的採用也帶來潛在的新威脅（ENISA, 2020；GSMA, 2021）。

資安業者卡巴斯基更直言表示，5G 網路安全需要重大改進，以降低遭駭客攻擊的風險，這些安全問題源自兩個部分。首先，是 5G 網路架構去中心化的安全問題，過去網路架構硬體的流量接觸點較少，安全檢查和維護相對容易，但 5G 以軟體為主的動態系統擁有大量的流量接觸點，任何一小部分的不安全都可能危及網路的其他部分。另一方面，是連接到 5G 網路的設備安全問題，目前物聯網（Internet of Things, IoT）裝置沒有安全標準，許多裝置的生產製造缺乏安全性，數十億個 IoT 意味數十億個潛在的安全漏洞，智慧電視、門鎖、冰箱、喇叭，甚至魚缸溫度計等小型裝置都可能成為網路弱點，使得駭客攻擊更加猖獗（Kaspersky, 2021）。

歐盟執委會（European Commission, EC）也指出，IoT 和 5G 網路有安全疑慮。EC 表示，5G 網路是數位化經濟和社會的未來支柱，將帶來智慧醫療、智慧電網、智慧工廠、智慧交通等新產業和新服務，當中也涉及數十億個連網裝置連接到能源、運輸、銀行和健康等關鍵部門的系統，並承載巨量重要敏感資訊。然而，5G 網路的架構不集中、對天線的需求增加、對軟體的依賴性更高，還有智慧的邊緣運算能力，這些都為惡意者提供更多的網路攻擊切入點。因此，確保 5G 網路的安全和強韌至關重要（EC, 2021）。

第二節 風險類別和危害

（一）威脅種類

根據歐盟網路安全局於 2020 年 12 月發布的《5G 網路威脅樣貌》報告，2020 年全球 5G 網路因為尚在早期布建階段，所以，沒有發現針對 5G 基礎設施的攻擊事件。不過，5G 網路的威脅仍可分成 9 大類，包括惡意活動/濫用（如惡意程式、分散式阻斷服務攻擊、威脅供應鏈或服務商、攻擊軟硬體漏洞等）、竊聽/攔截/駭侵、實體攻擊（攻擊基礎設施、連網設備）、故意毀損、意外毀損、軟硬體故障、服務中斷、重大災害、利用/濫用法律。這些威脅可能來自網路罪犯、組織的內部人員、國家政府、駭客主義者、網路戰士、網路恐怖分子、企業，以及網路鬧事者（ENISA, 2020）。

（二）風險類別

歐盟執委會則是發布 5G 網路安全工具箱，將 5G 網路的風險分成下列 5 種情境的 9 項風險（EC, 2021）：

- 安全措施不足：網路配置錯誤；沒有存取控制；
- 5G 供應鏈：設施品質低劣；依賴單一國家的供應商；
- 主要威脅者的作案手法：政府藉 5G 供應鏈進行干預；透過組織犯罪濫用 5G 網路；
- 5G 網路和其他關鍵系統的相互依賴：嚴重破壞關鍵基礎設施或服務；破壞供電系統以中斷網路；
- 使用者裝置：入侵 IoT、手機或智慧裝置。

（三）安全危害

ENISA 和 EC 並未詳述上列威脅或風險可能產生的危害。不過，綜合國內資安專家看法，由於 5G 網路是現代化國家必備的關鍵基礎設施，水電燃氣等公共事業、製造業、健康醫療、交通運輸、金融服務等系統都將透過 5G 網路運作；加上萬物連網，即使是不起眼的路燈都可能遭到駭客劫持進而發動分散式阻斷服務（Distributed Denial of Service, DDoS）攻擊。因此，其危害程度也將從 4G 時代的竊取個資以販售牟利、攻擊系統以勒索贖金，擴大為嚴重侵犯人權（如對民眾進行 24 小時嚴密監控）、危害個人生命安全（如攻擊自駕車系統），甚至癱瘓整個國家和社會的運作，讓一國陷入嚴重的危機當中（黃彥棻，2020；雷喻翔，2021；李忠憲，2021）。

第三節 政策建議

（一）布拉格提案

歐盟、北大西洋公約組織，以及美、德、日、韓等 32 國於 2019 年 5 月共同發布「布拉格提案」(The Prague Proposals)，從政策、技術、經濟、資安隱私及強韌等四大面向，提出各國建設 5G 網路時的安全建言，當中也包括選擇供應商的重要考量。例如：

- 政策面：管理網路和連網服務的法律和政策，應以透明和公平為指導原則，並在充足監督和尊重法治下，兼顧全球經濟和互通性的規則；應考量第三國對供應商影響的總體風險，尤其第三國是否為網路安全、打擊網路犯罪或資料保護的國際協議締約國。
- 技術面：利害關係人應考量 5G 網路的技術變化（如邊緣運算、軟體定義網路）對於通訊管道整體安全的影響；供應商產品的風險評估應考量所有相關因素，包括適用的法律環境和供應商生態系統。
- 經濟面：多樣化的通訊設備市場和供應鏈，對於安全性和經濟彈性至關重要；供商應具有透明的所有權、合夥關係和公司治理結構。
- 資安隱私及強韌面：所有利害關係人應共同努力，促進國家關鍵基礎設施的網路、系統和連接設備的安全性和強韌。

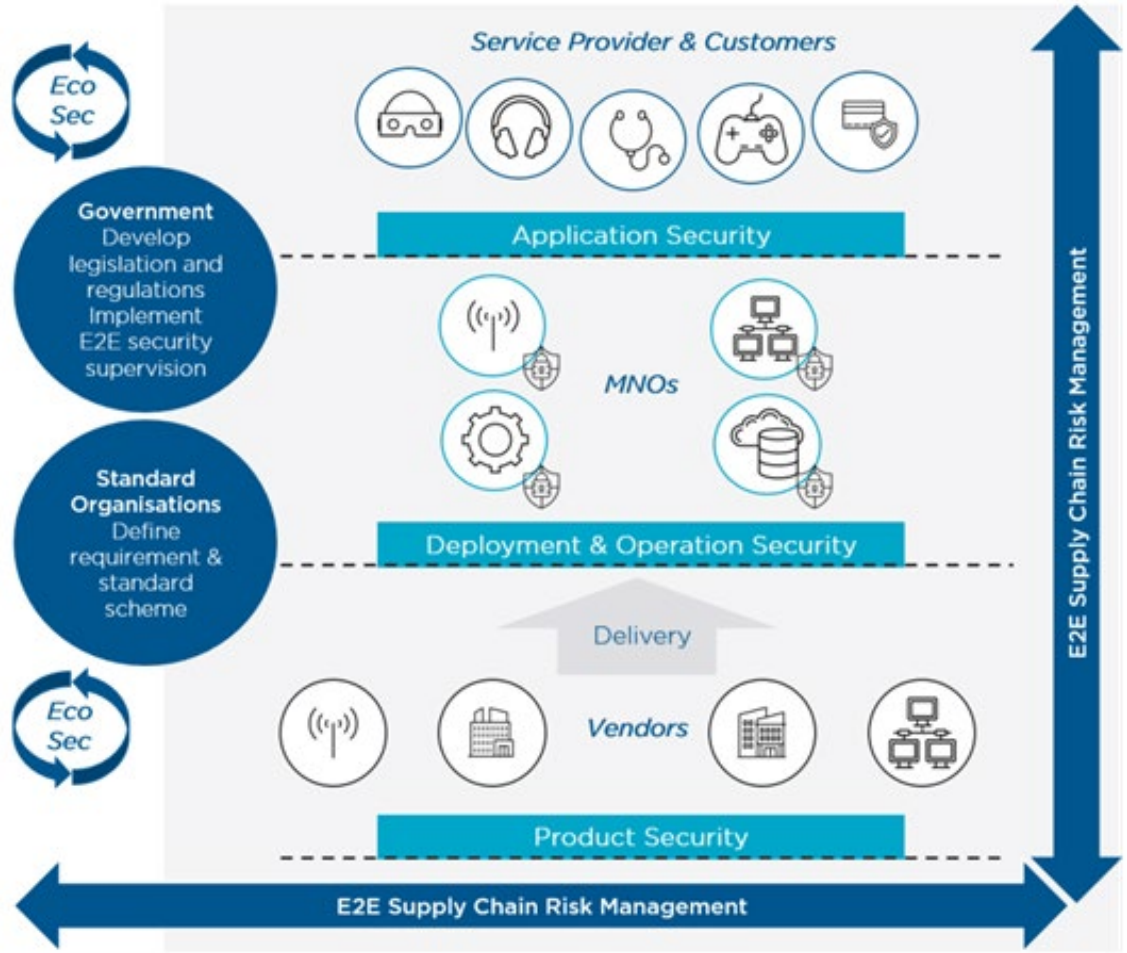
（二）歐盟 5G 網路安全工具箱

歐盟 5G 網路安全工具箱為其所歸類的前述 9 個風險，制定策略性和技術性的安全措施，並呼籲歐盟成員國加以落實，以確保整個歐洲布建安全的 5G 網路。策略性措施例如：加強國家當局角色（包含法規力量）、對營運商進行審查、針對高風險供應商採取限制/排除措施、確保供應商的多樣化、識別歐盟的關鍵資產並強化多元永續的 5G 生態系統、增強國家層面的抗災能力等。技術性措施則包括：確保落實網路架構的安全要求、評估

現有 5G 標準安全措施的實施情況、確保嚴格執行存取控制、提高虛擬化網路功能的安全性、增進實體安全、強化軟體的完整性和更新修補管理、透過健全的採購條件提高供應商流程的安全標準等（EC, 2021）。

（三）民間企業/組織建議

民間企業及工商組織從多方利害關係人的角度，對 5G 網路安全提出相關建議。例如：資安業者卡巴斯基建議網路供應商需重視軟體的保護以因應 5G 網路的獨特風險、政府訂定 IoT 安全等級標章並獎勵製造商提升產品安全、共同推動消費者的 IoT 安全認知教育（Kaspersky, 2021）。GSMA（2021）協會則直接強調「5G 網路安全是共同的責任」（參閱圖 4-2），例如：政府要制定規範並監管點對點（End-to-End, E2E）安全、標準組織要定義規格和標準、服務供應商和消費者應為 5G 應用的安全負責、行動網路營運商（Mobile Network Operators, MNOs）應為 5G 布建和維運的安全負責、製造商應為 5G 產品的安全負責。GSMA 強調，唯有所有利害關係人都履行其責任時，才能實現安全的 5G 網路。



圖片來源：GSMA

圖 4-2　5G 網路的利害關係人安全責任

第四節 數位人權

一、濫用個資與監控

（一）物聯網的巨量個資可能遭濫用

5G 網路將促進各式 IoT 服務。不過，Ericsson《5G 人權評估》報告指出，無所不在的 IoT 裝置將產生無數的個人資料，企業可能會在未經民眾同意下，積極尋求獲取特定且高度個人化的敏感資訊，以預測民眾的消費行為並將其貨幣化；而政府也可能在民眾不知情下，監控人民的行動（Ericsson, 2021）。

歐洲議會 STOA 小組的 5G 知識網站也指出，5G 技術將增加並徹底改變資料的產生和結合，科技公司將可透過智慧手錶等穿戴裝置挖掘民眾的健康資料，以及透過智慧住宅內的各種設備互連掌握民眾的生活習性。這些改變可能以新的方式挑戰資料保護，也代表未來需要強化個資和隱私相關法規（STOA, 2021）。

（二）5G 小型基地臺和標準有利於監控和斷網

Ericsson 和歐洲議會 STOA 小組皆表示，5G 高密度的小型基地臺（因為 5G 射頻波的範圍較小，需要密集架設小型基地臺）可以更精準地追踪個人位置，雖然這有助於追捕犯罪分子，但也可能遭到濫用，對個人隱私帶來風險，甚至危及個人自由。Ericsson 進一步指出，密集的小型基地臺也意味可以各別關閉 5G 網路，可能為政府提供更多可以鎖定特定群體的工具。例如：政府可能要求服務供應商關閉某公寓、某辦公大樓或某個少數民族居住地區的網路連線（Ericsson, 2021; STOA, 2021）。

美國哈佛大學甘迺迪學院研究員 Bruce Schneier（2020）從 5G 的標準和安全來看監控問題。他表示，儘管 5G 在加密、認證等安全層面較 4G 有所改善，但 5G 標準協定本身就存在安全漏洞，例如：5G 可以即時追蹤用

戶位置、切斷 5G 連線等安全漏洞皆已經被發布，而這些問題之所以沒有被解決，一方面是因為市場力量將成本置於安全之上，另一方面則是包括美國在內的各國政府希望在 5G 網路中保留監控的選項，以方便蒐集間諜活動情報和犯罪偵查所需的資料。

二、數位落差

推動通訊網路基礎建設的公民團體 Rhizomatica 擔憂 5G 反而可能擴大數位落差。其創辦人 Peter Bloom（2020）表示，5G 不再是以「人」為中心，而是在於促進萬「物」連網，以及高清的電視、遊戲和虛擬實境的應用；加上 5G 的頻譜取得和建置成本高昂，可能排擠投入鄉村建設的資金；而且 5G 因為傳輸距離短，也相對不適合用於大範圍卻只涵蓋少數人口的鄉村地區。因此，5G 恐怕不但不會縮小數位落差，而且還可能使情況惡化。

Ericsson《5G 人權評估》報告也同樣提出數位落差問題。報告指稱，5G 在不同國家之間，以及一國內部的不同地區布署不均，可能加劇數位落差的不平等現象（Ericsson, 2021）。

所幸，近期技術社群和產業界傳出可望突破技術限制的好消息。電機電子工程師學會（Institute of Electrical and Electronics Engineers, IEEE）於 2021 年 4 月的線上廣播節目提到，5G 的固定無線接取（Fixed Wireless Access, FWA）服務為縮減城市和鄉村數位落差的一種解決方案（IEEE Spectrum, 2021）。而 Nokia 和美商晶片大廠高通（Qualcomm）也在 2021 年 6 月共同宣布透過其 FWA 平臺，成功創下 5G 毫米波（24.25～52.6 GHz）延伸覆蓋 10 公里通訊距離的世界紀錄，象徵 5G 毫米波可以在鄉村和郊區提供極致容量，協助縮短數位落差（謝佳雯，2021）。

三、未來工作

Ericsson《5G 人權評估》報告指出，5G 將促使機器能夠執行更專精和更專業的工作，未來不只是工廠的藍領工作，還有某些白領工作，都可能受到影響，甚至被機械取代。另一方面，企業、政府和勞工也會面臨新技能短缺的問題（Ericsson, 2021）。

世界經濟論壇（World Economic Forum, WEF）《2020 未來工作報告》雖然沒有提到 5G 技術，但也指出「機器人革命」對未來工作的重大影響。WEF 表示，目前人類的工作有三分之一由機器代勞，由於 COVID-19 疫情加速企業的自動化步伐，因此，2025 年由機器處理的工作就會增加為二分之一。雖然過程中也會產生 9,700 萬個新工作，但被機器取代的工作數量也幾乎相同。此問題有賴政府提供技能培訓和更強大的社會安全網，以避免許多勞工深陷結構性失業的困境（BBC News, 2020）。

不過，芬蘭電信設備大廠 Nokia 科技長 Marcus Weldon（2020）有不同看法，他認為 5G 驅動的自動化將使工作變得更好，而非取代人類。Weldon 表示，雖然自動化的確會威脅某類工作，如重複性的文書工作將會永遠消失，但自動化也會協助人類拓展技能、提高生產力、創造新的工作職缺。這種人機共同演化將持續進行，且預估至 2030 年 70%職務將是這一類的「新領工作」（new-collar jobs）。

第五節 環境保護

一、5G 促進節能環保主張

聯合國 2020 年網路治理論壇（IGF）的其中一場座談－－「5G 時代的行動網路對環境影響」肯定 5G 發展對於節能環保的正面效益。包括技術社群、電信產業、公民團體等代表在內的與談人普遍認為，5G 網路的單位傳輸能源消耗比 4G 效率更高；且可透過使用再生能源進一步減碳；更重要的是，5G 網路結合 AI 等科技還能協助其他產業節能減碳，展現智慧農業、智慧建築、智慧能源和智慧製造（IGF, 2020）。

電信科技領域的國際顧問管理公司 Analysys Mason 於 2020 年發布的《綠色 5G：建立永續世界》報告，也強調 5G 有助於避免氣候變遷。報告指出，氣候危機已攸關人類存亡，而 5G 網路高容量、無所不在、低延遲的特性，正可以提升能源效率，減少二氧化碳排放，且其效益可從兩方面來看。首先，是行動通訊產業對於提升自身能源效益的努力，率先於 2016 年承諾致力推動聯合國永續發展目標，並訂於 2050 年實現淨零排放。所以，業者布建 5G 時會將能源效率納入重要考量，例如：基地臺採用智慧電源，這將使 5G 網路成為最具永續性的網路。另一方面，是效益更大的促進效應，也就是 5G 可以促進其他產業實現其永續目標。5G 結合雲端、AI 和邊緣運算等科技，可以支持最有效和最靈活的資源分配，降低能源消耗。例如：支持智慧能源管理、智慧交通管理、高效準時的供應鏈；並減少對辦公空間和商務旅行的需求（Gabriel et al., 2020）。

英國主要電信商 O2 則進一步預估 5G 可為英國減少的二氧化碳排放量。O2 於 2020 年《更綠色連網的未來》報告指出，超高速的 5G 結合智慧連網解決方案，預估至 2035 年之前，可為英國減碳 2.69 億噸，幾乎等同英格蘭 2018 年的碳排放總量，其中公用事業和家庭能源減碳最多，約占 67%；汽車業亦占 16%，製造業約 15%。O2 並強調，行動技術的進步將對

英國實現2050年淨零排放目標發揮關鍵作用，當中電信業更要率先以身作則，因此，O2 將淨零排放目標提前為 2025 年，並推動行動電信設施供應鏈減碳 30%（O2, 2020）。

二、5G 增加耗能汙染主張

由法國總統馬克宏創立的因應氣候變遷諮詢組織－－法國氣候最高委員會（Haut Conseil pour le Climat, HCC）於 2020 年底發布 5G 網路報告，示警 5G 網路將大幅增加能源消耗及碳排放，因為 5G 基礎建設需生產新設備並進行布建、5G 資料傳輸量和儲存量將大幅增加，且 5G 將帶動全新消費電子產品的生產製造並因此增加電子廢棄物汙染。

HCC 預估，5G 網路將使法國的能源消耗從目前的 16 TWh（兆瓦時）增加為 2030 年的 40TWh，增幅高達 2.5 倍；二氧化碳排放量從目前的 1 億 5,000 萬噸，額外增加 2,700 ~ 6,700 萬噸，增幅為 18 ~ 44%。HCC 並呼籲法國政府，將手機網路納入全國低碳策略，並於未來 26 GHz 頻段拍賣前，訂定 5G 網路頻段使用碳足跡目標的規範。

不過，法國政府和電信業者認為，這份報告忽略 5G 網路所帶來的正面效益，例如：促進其他產業（運輸、農業、交通、商業等）提升能源使用效率和落實遠距服務，可以間接減少能源消耗和碳排放。但 HCC 仍堅稱，目前無法預估 5G 網路所能產出的任何正面影響(趙偉婷，2021；駐法國代表處經濟組，2020）。

法國也有電信集團坦承 5G 將增加能源消耗。法國 Bouygues 電信的總裁 Olivier Roussat 表示，5G 網路的耗電量是 4G 的 3 倍；另一方面，雖然以傳輸同量數據所需的能源來看，5G 是低於 4G，但速度加快後，民眾使用的頻率也會增加。整體而言，5G 會使能源消耗大幅攀升(楊眉，2020)。

我國電信業者亦曾提出類似說法。台灣大哥大總經理林之晨表示，5G 基地臺的耗電量約為 4G 的 3 倍，而 5G 基地臺所需的密度也是 4G 的 3 倍，所以，1 條 5G 網路的整體耗電量為 4G 的 9 倍（歐祥義，2019）。

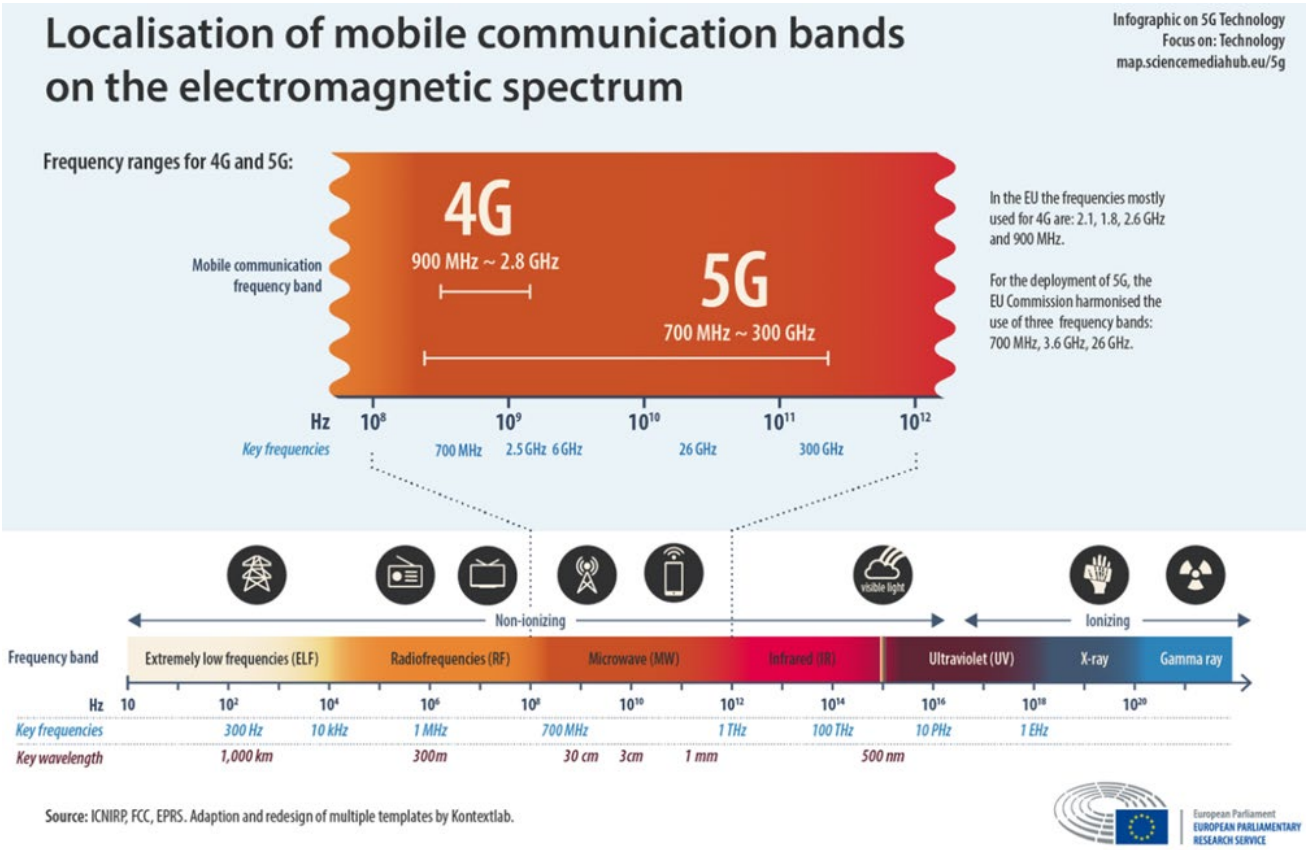
第六節 健康疑慮

一、專家請願和民眾抗議事件

5G 技術在臨床、門診和其他醫療事務的新應用，可望協助改善健康和照顧護理。然而 5G 技術是否會帶來新的健康威脅，持續引發爭辯，並且也是部分民眾抗議 5G 發展的主因。例如：2017 年超過 180 名科學家和醫生呼籲歐盟暫停推出 5G （至 2021 年 5 月參與連署的科學家和醫生增為 417 人）；2019 年有瑞士民眾走上街頭要求政府停建 5G，同年英國倫敦有人大量散發警惕 5G 危害的傳單，以及美國有小鎮的議會通過緊急法案，禁止在住宅區設置 5G 基地臺等事件。尤其 2020 年受到新冠肺炎（COVID-19）相關的網路謠言影響，諸如 5G 會削弱免疫系統以致容易染疫、5G 會傳播新冠病毒……，英、荷、比等 10 個歐洲國家，以及美、澳等西方先進國家，都傳出多起 5G 基地臺遭到民眾縱火破壞事件，英國甚至在一個月內有 77 座基地臺遭破壞（STOA, 2021; 5G Appeal, 2021；Nakashima, 2020；BBC 中文，2019；上報，2019）。

二、涉及健康議題的 5G 頻率

根據歐洲議會 STOA(2021)小組的 5G 知識資料，目前使用的 2G～4G 通訊系統大多於 6 GHz(十億赫茲)以下的頻率運作，如 4G 頻段範圍為 700 MHz(百萬赫茲)到 3GHz。但是 6 GHz 以下頻率無法有效發揮 5G 全部潛力，加上 5G 的射頻電磁場(Radiofrequency Electromagnetic Fields, 以下簡稱 RF EMF 或電磁波）傳輸方式也與 4G 略有不同，且 RF EMF 訊號密度也有差異，所以，5G 需要額外的頻段。目前歐盟確認的 5G 初期頻段（參閱圖 4-3)為 700 MHz、3.6 GHz、26 GHz，皆已遠高於「超高頻」(Ultra-High Frequencies，簡稱 UHF，頻段為 300MHz～3GHz）範圍，且跨越至「極高頻」(Super High Frequency，簡稱 SHF，頻段為 3～30GHz）。而研究人員已關注至 300 GHz 頻率，顯示未來 5G 可能使用 30～300 GHz 的「至高頻」（Extreme High Frequency, EHF）。有關 5G 頻率對健康影響的爭辯將於下段說明。



資料來源：STOA 網站

圖 4-3　5G 使用的頻段

三、對健康影響的爭辯

（一）無害論

主張 5G 不會影響健康者強調的是，目前沒有科學證據證明行動通訊在既定範圍內操作時，會對人類健康有害。歐盟執委會 2019 年委託的 5G 相關研究結論為「除了不顯著的熱效應外，迄今尚無證據顯示毫米波（24GHz 以上）對人類健康有害……且 5G 可能只會讓電磁波曝露量非常微幅地增加而已」（IDATE, 2019）。美國食品藥物管理局（Food and Drug Administration, FDA）2020 年相關報告也提出類似結論，認為「沒有科學證據證明曝露於手機的射頻能量會導致健康問題」。國際非游離輻射防護委員會（International Commission on Non-Ionizing Radiation Protection, ICNIRP）2020 年發布更新版 RF EMF 指南已將 5G 運作的頻率納入，並強調「沒有證據證明電磁波會導致癌症、電磁波過敏、不孕，或任何其他健康影響」。不過，這份指南也遭專家抨擊為沒有回應長期曝露的問題，且沒有納入人類和動物組織的非熱能效應或生物效應（STOA, 2021）。

（二）風險論

世界衛生組織（World Health Organization, WHO）和旗下的國際癌症研究署（International Agency for Research on Cancer, IARC）則從風險角度論事。雖然 WHO 早在 2014 年就表示「沒有證據顯示使用手機會危害健康」，但也因為沒有證據可以確認手機電磁波和癌症的關係，因此，WHO 和 IARC 把手機電磁波列入「2B 級致癌物（懷疑對人類致癌）」，惟咖啡和泡菜也同屬此一等級（BBC 中文，2019）。

歐洲議會 STOA 小組 2021 年委託的研究則認為，即使是 2G～4G 的低頻段都可能存在致癌及對生育和發育產生負面效應的風險，更何況是使用高頻段的 5G，且 5G 後期使用的高頻段可能趨近於雷達和微波，但目前有關高頻段對健康影響的研究並不充足。因此，建議修訂公眾和環境的射頻

曝露限制、於固定地點上網時避免使用無線方式，並進行 5G 對健康長期影響的評估，同時也要找到監測 5G 曝露的適當方法（Belpoggi, 2021）。

四、歐盟的看法

歐洲議會 STOA（2021）小組表示，歐盟 5G 初期頻段當中的 700 MHz 和 3.6 GHz，在使用和危害識別上與 2G～4G 相似，皆已針對致癌性和生育及發育影響進行流行病學和實驗研究調查；不過，包括德國電信公司 Telekom 等單位的數個文獻分析報告都顯示「既有研究對於電磁波是否影響人類健康並沒有一致的結論」，尤其 26 GHz 和更高頻率的研究不夠充足，因此，未來需要投入更多研究。STOA 小組並指出，歐盟的非游離電磁波曝露指南是依據 ICNIRP 指南訂定的，歐盟執委會衛生局已表示將根據既有的科學證據進行重新評估，且不排除審查曝露限制值的可能性。此外，WHO 預計 2022 年發布電磁波健康風險評估報告，亦值得關注。

第七節 結論與建議

一、結論

（一）我國 5G 安全策略和民主國家同一陣線

在「資安即國安」的戰略下，我國 4G 網路釋照即依據「行動寬頻業務管理規則」相關規定，禁止中製設備用於核心網路、傳輸骨幹及基地臺等重要設施，且 5G 網路亦比照辦理。因此，2019 年美國在台協會(American Institute in Taiwan, AIT）前處長酈英傑即表示，臺灣「率先」意識到中製電信設備的風險並禁用，值得其他國家效仿。而 2020 年美國也將我國和全球 60 多個國家同列為淨網計畫的「乾淨國家和地區」，且國內五大電信業者亦全是「乾淨的電信商」；同年，臺美雙方還發布「5G 安全共同宣言」，強化 5G 資安合作，且宣言所推動的防護措施亦呼應 32 個國家共同發布的「布拉格提案」（AIT, 2019；尚國強，2020；蘇文彬，2020；總統府，2018）。由此顯示，我國的 5G 安全防護在因應地緣政治的美中對抗的選擇上，以及相關的策略方向，皆和民主國家站在同一陣營，符合民主國家的潮流。

（二）5G 覆蓋距離屢創新高，可望縮減偏鄉的連線落差

正如國際間擔憂 5G 建設成本高昂等因素恐怕加深城鄉數位建設落差，通傳會「強化偏鄉地區 5G 寬頻服務與涵蓋——普及偏鄉寬頻接取環境計畫」也指出相同問題，且因為既有的「電信事業普及服務基金」額度有限，故透過政府補助部分經費的方式（不超過核定總工程經費的 50%），推動偏鄉 5G 網路建設，惟仍面臨補助經費對電信業者吸引力有限的挑戰（通傳會，2021b）。而此挑戰隨著 5G 毫米波的通訊覆蓋距離不斷刷新紀錄（目前為 10 公里），可望獲得紓解。如本章第四節所述，包括技術社群和產業界都看好此發展趨勢有助於縮減 5G 網路的連線落差。產業界龍頭並表示，5G 將能以具成本效益的方式，將寬頻服務擴展至鄉村和郊區。

（三）5G 促進節能環保或增加耗能污染，尚無統一定論

目前國際間對於 5G 網路究竟是促進節能環保，或是增加耗能汙染，並無統一定論。主張 5G 促進節能環保者認為，5G 結合智慧連網有助於其他產業提升能源使用效益；代表案例為英國電信商 O2 預估至 2035 年之前，5G 可為英國減碳 2.69 億噸，幾乎等同英格蘭 2018 年的碳排放總量。而主張 5G 不利節能環保者則強調，5G 網路的基礎建設各種設備和施工、資料傳輸儲存量將大增、換機潮增加電子廢棄物等因素，將大幅增加耗能及汙染；代表案例為法國氣候最高委員會（HCC）預估，5G 網路至 2030 年將使法國的能源消耗增加 2.5 倍，碳排放量增加 18～44%。

（四）5G 健康風險亦無國際共識，歐盟將檢視電磁波曝露限制值

有鑑於歐洲民眾對於 5G 健康風險有所疑慮，尤其是 5G 所使用的頻段範圍遠高於 4G，甚至未來還可能使用「至高頻」(30~300 GHz），歐盟執委會和歐洲議會等單位近年來持續委託執行相關研究，結果發現 5G 是否影響人類健康沒有一致結論，且很少有 26 GHz 和更高頻率的健康影響研究。另一方面，雖然歐盟非游離電磁波曝露指南的依據來源——國際非游離輻射防護委員會(ICNIRP)的 RF EMF 指南，於 2020 年發布的更新版本已將 5G 運作頻率納入，ICNIRP 並強調沒有證據證明電磁波會造成任何健康影響，惟這份指南也遭抨擊為沒有回應長期曝露的問題，且沒有納入人類和動物組織的非熱能效應或生物效應。也因此，歐洲議會 STOA 小組認為，未來需要投入更多研究，並透露歐盟執委會衛生局不排除審查非游離輻射電磁波曝露限制值的可能性。

二、建議事項

（一）立即可行之建議

1. 將節能列為 5G 基地臺架設許可等審核，響應 2050 年淨零碳排

在 2050 年達成淨零排放及各國著手研議碳關稅的國際趨勢下（全球已有 130 個國家宣布推動淨零排放，且歐盟預計 2026 年起徵收碳關稅），行政院已指示環保署積極修改《溫室氣體減量及管理法》，並納入「2050 年淨零排放」目標，同時還要研議碳定價（賴于榛，2021）。由此凸顯節能減碳可能成為所有產業的共同責任。其實部分國內電信業者已經有所行動，例如：遠傳電信和台達電子合作於 5G 基地臺使用節能系統、中華電信加入民間推動的「台灣淨零排放倡議」等。因此，建議通傳會可將節能列為 5G 基地臺架設許可的審核項目[9]，或建設偏鄉 5G 網路補助案的加碼補助項目，抑或是參考法國氣候最高委員會（HCC）建議的訂定 5G 網路頻段使用碳足跡規範，以鼓勵或要求所有電信業者能以節能方式布建和營運 5G 網路。

根據NCC今年6月和8月的統計資料，全臺4G基地臺約為10.5萬座，5G 基地臺約為 2 萬座；又台灣大哥大總經理林之晨表示「5G 基地臺所需的密度為 4G 的 3 倍」。由此來看，未來幾年電信業者仍需持續佈建 5G 基地臺，並申請架設許可。

2.追蹤國際 5G 健康影響研究、WHO 報告及歐盟電磁波規範檢視結果

通傳會於2020年進行首波5G釋照，釋出1800MHz、3.5GHz及28GHz三個頻段（1800MHz 無人得標），且預計 2023 年的第二波釋照可能增加37～40GHz 的「至高頻」（林淑惠，2021）。雖然國內亦有電磁波安全的相

9 根據通傳會 2021 年 6 月和 8 月的統計資料，全臺 4G 基地臺約為 10.5 萬座，5G 基地臺約為 2 萬座；又台灣大哥大總經理林之晨表示「5G 基地臺所需的密度為 4G 的 3 倍」。此外，「電信三雄」中華電信、台灣大哥大、遠傳電信於11月份的法說會上皆宣布「2022年的重點目標為力拚5G基地臺覆蓋率」。

關研究[10]，但似乎沒有著墨高頻段的部分。此外，我國的一般民眾環境電磁波曝露指引及基地臺電磁波管制標準亦是參考國際非游離輻射防護委員會（ICNIRP）的標準值而訂定。通傳會長期向民眾宣導行動通訊電磁波的正確觀念，一方面讓民眾了解目前基地臺電磁波致癌風險的證據不足，另一方面也教導民眾使用行動電話時如何減少電磁波的曝露[11]。因此，在當前國際間對於 5G 健康風險尚無共識的情況下，建議通傳會追蹤先進國家 5G 高頻段的健康影響研究，以及 WHO 預計於 2022 年發布的電磁波健康風險評估報告，同時也建議行政院環保署了解歐盟對非游離輻射電磁波規範的檢視結果，以為國人的電磁波安全嚴格把關，同時也作為未來持續和民眾宣導正確知識的參考。

3.了解歐美全國性資安認知宣導，做為我國提升民眾資安意識參考

我國提升資安向來不遺餘力，不但自 2019 年實施《資通安全管理法》，且推行中的第六期「國家資通安全發展方案（110 年 ~ 113 年）」對於 5G 網路的安全維護更有進一步規劃。例如：通傳會將修訂「5G 資通安全維護計畫」的稽核計畫及標準作業程序；行政院資安處和經濟部及通傳會（協辦）將制定我國 IoT 資安檢測驗證框架、優先策略及清單項目。由此顯示我國整體資安防護已具備法律基礎和配套制度（行政院資安處，2021）。

正如「布拉格提案」和 GSMA 協會等單位皆呼籲「5G 網路安全是所有利害關係人的共同責任」，我國第六期資安發展方案指出當前國人資安意識不足的問題，並責成通傳會提升民眾的資安意識。因此，建議可了解美國的全國資安認知月（National Cybersecurity Awareness Month）和歐盟的網路安全日（Safer Internet Day）等計畫，其長期（兩者皆從 2004 年舉辦迄今）透過全國性／國際性的認知宣導活動之實施策略、措施和具體成效，以做為我國推動民眾資安意識的參考。

10 例如：通傳會 108 年「基地臺電磁波安全研究之文獻回顧與探討」委託研究計畫。
11 資料來源：通傳會行動通訊電磁波網站之「電磁波科學園」手冊。

（二）中長期建議

1. 成立個資保護專責機關，防止 5G 時代的個資濫用和監控

5G 技術加上無所不在的 IoT 裝置，將改變資料的產生、結合和數量，可讓科技公司更精準地掌握民眾的習性和喜好，進而用於投放廣告獲利，其影響性不只在於侵犯個資和隱私，還可能被用於政治操弄，危害民主發展。因此，歐洲議會 STOA 小組提醒，個資保護工作將受新的挑戰，並需要強化相關法規，當中也包括各種 IoT 蒐集資料將被傳輸到不同國家的資料跨境傳輸問題。

我國自 2012 年開始實施《個人資料保護法》，並由各目的事業主關機關分散管理，而後由國家發展委員會成立「個人資料保護專案辦公室」，且作為個資法的法律主政機關，惟迄今尚未取得歐盟《一般資料保護規則》（GDPR）的適足性認定。面對 5G 時代個資保護的更多挑戰，有賴政府加速設立獨立的個資保護專責機關，釐清不同型態的個資蒐集和使用風險，並透過修改《個人資料保護法》為這些資料量身訂做適用的規範（包含跨境傳輸規範），以真正落實個資保護，同時也增進民眾對於數位發展的信賴。

參考文獻

- AIT (2019). 美國在台協會處長酈英傑「台灣網路治理論壇」致詞講稿。2019/7/5。https://www.ait.org.tw/zhtw/remarks-by-ait-director-w-brent-christensen-at-the-taiwan-internet-governance-forum-july-5-2019-zhtw/
- BBC 中文 (2019)。5G 致癌？網絡技術引發健康擔憂的真偽明辨。2019/8/19。https://www.bbc.com/zhongwen/trad/world-49277500
- Chris (2020)。撕破臉到底，美國 FCC 正式宣布華為、中興是「國安威脅」。Inside, 2020/7/1。https://www.inside.com.tw/article/20213-US-FCC-officially-designates-Huawei-ZTE-as-national-security-threats
- MoneyDJ (2021)。以牙還牙！美制裁華為，北京報復封殺愛立信、諾基亞。科技新報，2021/8/4。https://technews.tw/2021/08/04/beijing-revenge-blocked-ericsson-and-nokia/
- 上報 (2019)。憂 5G 輻射危害人體健康　瑞士千人抗議要求政府停建基地台。上報，2019/9/23。https://www.upmedia.mg/news_info.php?SerialNo=71877
- 天睿 (2021)。澳洲記者揭政府為何禁華為參與 5G 網絡。大紀元，2021/5/21。https://www.epochtimes.com/b5/21/5/21/n12964452.htm
- 台灣人權促進會(2021)。【聲明】先有個資保護專責機關，才有健全的數位發展。2021/5/6。https://www.tahr.org.tw/news/2940
- 行政院資安處 (2021)。國家資通安全發展方案(110 年至 113 年)。2021/2/23。https://nicst.ey.gov.tw/Page/296DE03FA832459B/e5eb620d-dae2-40ae-85d5-

264955863506

- 李忠憲 (2021)。5G 風險與國安。清流雙月刊 No.32，2021/3。http://mjib-ebook.com/MJIB/no32/index.html
- 尚國強(2020)。美推乾淨網路　將台灣列入「乾淨國家與地區」名單。上報，2020/8/12。https://www.upmedia.mg/news_info.php?SerialNo=93705
- 林妍溱 (2020)。英國發現華為設備有「影響國家安全」的瑕疵。iThome, 2020/10/5。https://www.ithome.com.tw/news/140350
- 林淑惠 (2021)。第二波 5G 釋照 擬增 37～40GHz 頻段。中時新聞網，2021/4/6。https://www.chinatimes.com/newspapers/20210406000180-260204?chdtv
- 邱立玲 (2019)。報復澳洲禁用華為 5G？中國大連封殺澳洲煤炭進口。Yahoo 新聞，2019/2/23。https://tw.stock.yahoo.com/news/報復澳洲禁用華為 5g-中國大連封殺澳洲煤炭進口-071330047.html
- 時報資訊 (2021)。《大陸產業》美歐聯手封殺下 華為通信市占仍冠全球。Yahoo，2021/6/19。https://tw.stock.yahoo.com/news/大陸產業-美歐聯手封殺下-華為通信市占仍冠全球-034758778.html
- 通傳會 (2021a)。通傳會今(3)日通過「補助 5G 網路建設作業要點」，將加速完備國家數位競爭力基礎，提供全民更優質的智慧生活。2021/3/3。https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=45793
- 通傳會 (2021b)。強化偏鄉地區 5G 寬頻服務與涵蓋-普及偏鄉寬頻接取環境計畫。https://www.ey.gov.tw/File/9C7508704746DE24
- 陳曉莉 (2020)。美國擴大乾淨網路計畫，將移除不可靠的中國程式。iThome, 2020/8/6。https://www.ithome.com.tw/news/139238

- 辜泳秝 (2020)。維持華為 5G 禁令 瑞典法院：基於國家安全無違法。中央社，2021/6/23。https://www.cna.com.tw/news/firstnews/202106230009.aspx
- 黃彥棻 (2020)。資安防禦新思維 專家：董事會也要懂資安。大紀元，2020/7/30。https://www.epochtimes.com.tw/n319242/資安防禦新思維-專家-董事會也要懂資安.html
- 黃晶琳 (2021)。華為 5G 勢力式微 諾基亞躍全球 5G 基地台龍頭。聯合新聞網，2021/6/29。https://udn.com/news/story/7240/5564228
- 愛立信 (2021)。愛立信：2021 年底 5G 用戶數將超過 5 億。2021/7/13。https://www.ericsson.com/zh-tw/press-releases/2/2021/7/20210713-ericssion-5g-users-will-exceed-500-million
- 新世代金融基金會(2021)。感謝唐鳳政委 呼應本基金會設立個資保護專責機構之呼籲。2020/7/31。http://www.appacus.org.tw/xmdoc/cont?xsmsid=0J092620032486508681&sid=0K213429246631744392
- 楊眉 (2020)。法國多個城市為何要叫停 5G 網絡？法廣 RFI，2020/9/25。https://www.rfi.fr/cn/生態/20200925-法國多個城市為何叫停 5g 網絡
- 雷喻翔 (2021)。智慧城市中的 5G 應用。清流雙月刊 No.32，2021/3。http://mjib-ebook.com/MJIB/no32/index.html
- 趙偉婷 (2021)。網路更快，環境更壞？法國官方警告：5G 時代恐增 45% 碳排。台達電子文教基金會，2021/2/22。https://www.delta-foundation.org.tw/blogdetail/3117
- 歐祥義 (2019)。《CEO 開講》林之晨：5G 網路應共用 政府須考量這個。自由時報，2019/9/2。https://ec.ltn.com.tw/article/breakingnews/2891363

- 駐法國代表處經濟組 (2020)。法國氣候最高委員會警示 5G 網路將大幅增高二氧化碳排放量指數。經貿透視，2020/12/31。https://www.trademag.org.tw/page/newsid1/?id=778003&iz=2
- 賴于榛 (2021)。蘇貞昌：積極修法納 2050 淨零碳排、研議碳定價。中央社，20201/8/30。https://www.cna.com.tw/news/firstnews/202108300341.aspx
- 總統府 (2018)。國家資通安全戰略報告-資安即國安。https://www.president.gov.tw/Page/317/969/國家資通安全戰略報告-資安即國安-
- 謝佳雯 (2021)。高通拚技術與合作夥伴創延伸範圍 5G 毫米波世界紀錄。聯合新聞網，2021/6/10。https://udn.com/news/story/7240/5522748
- 羅拉 (2020)。法國啟動拍賣 5G 頻率和阿米什模式。法廣 RFI，2020/9/29。https://www.rfi.fr/tw/法國/20200929-法國啟動拍賣 5g 頻率和阿米什模式
- 蘇文彬 (2020)。臺美發表 5G 安全共同宣言，要聯手從供應鏈把關 5G 網路安全。iThome, 2020/8/26。https://www.ithome.com.tw/news/139624
- 5G Appeal (2021). http://www.5gappeal.eu/about/
- BBC News (2020). Machines to 'do half of all work tasks by 2025‘. 2020/10/21. https://www.bbc.com/news/business-54622189
- Belpoggi, F. (2021). Health impact of 5G. European Parliament, 2021/7/22. https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)690012
- Bloom, P. (2020). The shift from connecting people to connecting things: Why 5G will not reduce the digital divide. APC, 2020/5/29. https://www.apc.org/en/news/shift-connecting-people-connecting-things-why-5

g-will-not-reduce-digital-divide

- EC (2021). EC (2021). The EU toolbox for 5G security (Factsheet). 2021/3/24. https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security
- ENISA (2020). ENISA Threat Landscape for 5G Networks Report. 2020/12/14. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks
- Ericsson (2021). 5G Human Rights Assessment. 2021/3/5. https://www.ericsson.com/en/blog/2021/3/5g-human-rights
- Eurasia Group (2018). Eurasia Group White Paper: The Geopolitics of 5G. 2018/11/15. https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf
- Gabriel, C., He, A. & Chern, A. (2020). Green 5G: Building a Sustainable World. https://www.analysysmason.com/research/content/white-papers/green-5g-sustainability-rma18-rdns0/
- GIP Digital Watch (2021). 5G and Digital Policy. https://dig.watch/trends/5g
- GSMA (2021). Securing the 5G Era. https://www.gsma.com/security/securing-the-5g-era/
- He, C. (2021). Trump Administration Rewrote US Approach to China Threat. The Epoch Times, 2021/1/25. https://www.theepochtimes.com/trump-administration-rewrote-us-approach-to-china-threat_3668729.html
- IGF (2020). WS #119 Mobile Internet Impact on the environment in 5G era.

https://www.intgovforum.org/multilingual/content/igf-2020-ws-119-mobile-internet-impact-on-the-environment-in-5g-era#undefined

- Kaspersky (2021). Is 5G Technology Dangerous? - Pros and Cons of 5G Network. https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons
- Mihalcik, C. & Reardon, M. (2021). FCC proposes more restrictions on Huawei, ZTE equipment. CNET, 2021/6/18. https://www.cnet.com/news/fcc-proposes-more-restrictions-on-huawei-zte-equipment/
- Nakashima, E. (2020). DHS to advise telecom firms on preventing 5G cell tower attacks linked to coronavirus conspiracy theories. The Washington Post, 2021/5/13. https://www.washingtonpost.com/national-security/dhs-to-advise-telecom-firms-on-preventing-5g-cell-tower-attacks-linked-to-coronavirus-conspiracy-theories/2020/05/13/6aa9eaa6-951f-11ea-82b4-c8db161ff6e5_story.html
- O2 (2020). O2 reveals vision for a greener, connected future: 5G to play key role in building a greener economy. 2020/8/12. https://news.o2.co.uk/press-release/o2-reveals-vision-for-a-greener-connected-future-5g-to-play-key-role-in-building-a-greener-economy/
- Schneier, B. (2020). China Isn't the Only Problem With 5G. Foreign Policy, 2020/1/10. https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/
- STOA (2021). Explore our 5G technology knowledge map. European Parliament, 2021/6/1. https://www.europarl.europa.eu/stoa/en/home/news/details/explore-our-5g-tech

nology-knowledge-map/20210601CDT05281

- The Prague Proposals (2019). https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/
- Weldon, M. (2020). 5G-powered automation will transform work for the better. Financial Times, 2020/10/14. https://www.ft.com/content/0dbdca77-0c5b-4717-be90-d2d01bc9c980
- Mueller, M. (2020). Trump and Pompeo: Stop the Internet, we want to get off. Internet Governance Project, 2020/8/7. https://www.internetgovernance.org/2020/08/07/trump-and-pompeo-stop-the-internet-we-want-to-get-off/

第五章 案例研析：全球網路自由度及政策趨勢

第一節 前言

長期研究追蹤全球自由程度的美國人權組織——自由之家（Freedom House），於 2021 年 9 月 21 日發布《2021 網路自由度報告》（Freedom on the Net 2021），指出全球網路自由度已經連續 11 年下滑，連美國的得分也是連續 5 年下降，且中國大陸連續 7 年墊底，尤其近來各國紛紛對科技巨頭祭出網路新規，反而遭部分政府濫用於打壓言論自由及取得個資。

不過，自由之家也表示，**首度被納入評比的我國，一舉奪下全球第 5 名**，僅次於冰島、愛沙尼亞、加拿大與哥斯大黎加（並列第 3 名），且**在亞太地區居冠，值得各國學習**（Freedom House, 2021；VOA 美國之音，2021）。

自由之家成立於 1941 年，為美國捍衛民主和人權的非營利組織，營運經費約 9 成來自美國政府贊助[12]。其《網路自由度報告》自 2009 年開始發布，研究結果經常獲得紐約時報、華盛頓郵報、經濟學人、衛報等國際媒體的報導，以及政治人物的引用。本（2021）年度報告是由荷蘭和美國政府，以及 Amazon、Google 等業者贊助，但報告也強調維持研究的獨立性。

《2021 網路自由度報告》評比全球 70 個國家、涵蓋全球 88%上網人口的網路自由程度。其國家挑選的主要考量包括該國的網路使用人口數、於地區或全球的定位、對網路保護或限制措施的特殊性；評比項目則分成上網阻礙、內容限制、侵犯用戶權利等 3 大類 21 項指標。由於**指標中有多項通傳會相關業務，加上我國首度被納入評比**，因此，本年度報告值得進一步探究，除了可以藉此掌握過去一年來的全球網路自由度及其相關的政策趨勢之外，還可以了解國際間從民主和人權角度，如何評價我國的網路政策，進而找出我國能夠貢獻或向國際社會學習的政策經驗。

12 資料來源為《自由之家 2020 財政年度經審核的財務報表》。https://freedomhouse.org/about-us/financials。

第二節 全球網路自由度概況

一、評比指標

《2021 網路自由度報告》從上網阻礙、內容限制、侵犯用戶權利等 3 大類 21 項指標（參閱下表 5-1），評比全球 70 個國家過去一年來（資料蒐集期間為 2020 年 6 月~2021 年 5 月）的網路自由程度。每項指標依重要性而有不同分數，所有指標加總為 100 分，得分高低象徵以下 3 種不同網路自由程度。

- 網路「自由」：70 分 ~100 分
- 網路「部分自由」：40 分 ~69 分
- 網路「不自由」：0 分 ~39 分

表 5-1 《2021 網路自由度報告》評比指標

類別	指標	分數
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？	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
	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？	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？	6
	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？	4
B 內容限制 35 分	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
	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？	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
	B4 網路記者、評論人、一般用戶是否會進行自我審查？	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？	4

類別	指標	分數
	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、內容託管商和平臺是否缺乏競爭）？	3
	B7 網路上的訊息是否多樣化且值得信賴？	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
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？	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？	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？	6
	C4 政府對於匿名或加密通訊是否有所限制？	4
	C5 政府是否有侵犯用戶隱私權的網路監控活動？	6
	C6 業者監看和蒐集用戶資料是否侵犯用戶隱私權？	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？	5
	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？	3

資料來源：Freedom House；本計畫彙整

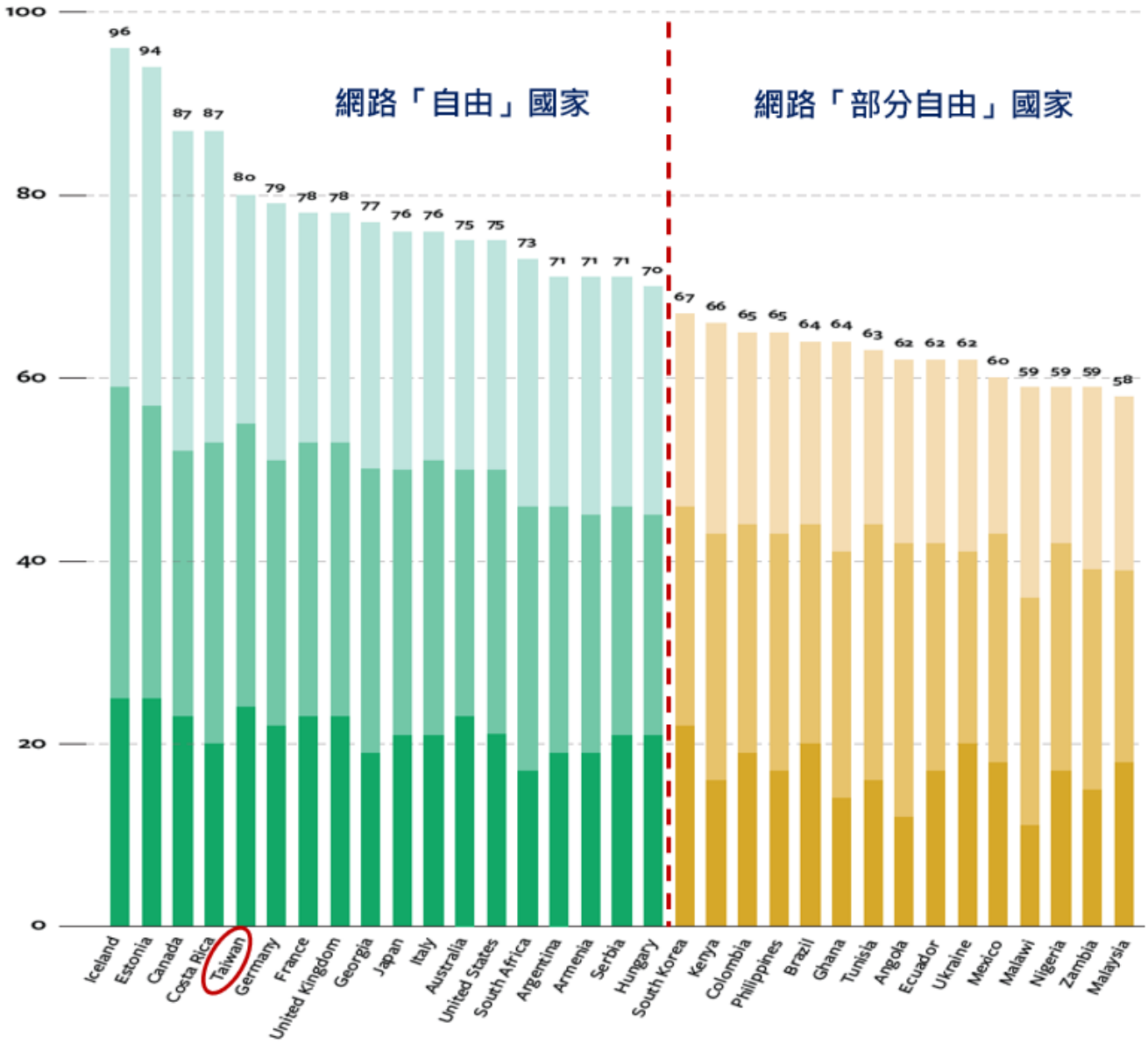
二、評比結果

自由之家的評比結果顯示，全球網路自由度連續第 11 年下滑，各國皆推出監管科技巨頭的法規或行政措施，且網路言論自由也受到空前的打壓（詳第三節「全球相關政策趨勢」）。所幸，包含我國在內的網路自由度名列前茅國家仍帶來希望的曙光。各國的排名和得分(前 33 名)如下圖 5-1 所示，全球評比結果的重點包括：

- 高達 30 個國家的網路人權環境惡化，降幅最大的國家為緬甸、白俄羅斯、烏干達。美國得分也是連續第 5 年下滑，中國大陸則是連續 7 年墊底。
- 網路「不自由」國家（21 國，占 30%）比網路「自由」國家（18 國占 25.7%）更多，其餘 31 國（44.3%）為網路「部分自由」國家。
- 全球網路「不自由」國家的前 5 名依序為中國大陸（10 分）、伊朗（16 分）、緬甸（17 分）、古巴（21 分）、越南（22 分）。
- 全球網路「自由」國家的前 5 名依序為冰島（96 分）、愛沙尼亞（94 分）、加拿大和哥斯大黎加（同為 87 分）、臺灣（80 分）。
- 上述國家為全球的網路自由帶來希望曙光。冰島和愛沙尼亞享有高連網率、對內容限制很少，且對數位人權提供強大的保護措施。哥斯大黎加是最早承認上網為基本權利的國家之一，且有強力法規保障言論自由，以及防止濫用和監控。**臺灣則擁有有意義且負擔得起的網路連線，還有獨立的司法制度保護言論自由，且透過創新法規和對數位科技的民主監督，因應中國大陸的不利影響**(詳第四節「我國網路自由度和相關政策規範」)。
- 亞太地區經濟和科技發展程度相對較佳的國家中，只有臺灣、日本（76 分）、澳洲（75 分）為網路「自由」國家；南韓（67 分）、新加

坡（54 分）則為網路「部分自由」國家。

- 歐洲地區除了冠亞軍的冰島和愛沙尼亞外，德國（79 分）、英國（78 分）、法國（78 分）、義大利（76 分）等國同樣為網路「自由」國家。
- 美洲地區除了第 3 名的加拿大和哥斯大黎加外，屬於網路「自由」國家還有美國（75 分）和阿根廷（71 分）。



資料來源：Freedom House；本計畫加註標示

圖 5-1　全球網路自由度排名（第 1 名~33 名）

第三節 全球相關政策趨勢

《2021 網路自由度報告》統計其所評比 70 個國家過去一年來與網路自由度相關的政策法規，本計畫據此重新歸納彙整為以下全球相關政策趨勢。

一、48 國祭新規監管科技公司，國家強化網路監管成為全球常態

過去一年來，有 48 國（包括歐美和我國等民主國家，以及中俄等極權國家）對科技公司的內容管理、資料管理或市場競爭，實施新的法律或行政規範（參見本節第三至第五點），國家控制科技巨頭和強化網路監管，顯然已經成為全球常態（global norms）。雖然當中有些措施是為了降低線上危害、控制資料濫用、終止操弄市場的行為，但許多新法規對民間企業施加過於廣泛的審查和資料蒐集要求，且用戶的網路活動普遍是由業者，以缺乏民主治理的保障措施（例如：透明度、司法監督和公共問責制）方式，加以管理和監控。於是網民的權益淪為主要犧牲品，言論自由受到前所未有的破壞，全球網路自由度也呈現連續第 11 年下降。

國家政府之所以強化網路監管的一大主因，是業者未能透過自律解決網路上的危害，以致產生權力移轉。許多國家的政策制定者都表示，需要從外國勢力、跨國公司，甚至是民間社會的手中，奪回對網路的控制權。

早期的網路規範由美國所主導，尤其是言論自由和自由市場方面。然而，美國對科技產業的自由放任方式，導致專制的操弄、資料濫用和廣泛的瀆職行為。而在缺乏以自由開放網路為全球共同願景的情況下，各國政府於是採用自己的方法來監管數位領域。

二、56 國對網路言論究責、20 國實施斷網，全球人權陷入危機

過去一年來，高達 56 國（大多為民主程度較低和極權國家，民主國家中只有美國、南韓和我國等少數者）的民眾因為網路言論而遭到逮捕或定罪，當中伊朗、泰國、埃及等國政府還以煽動抗議、冒犯君王、販賣人口（實情為分享鼓勵女性就業的影片）為由，裁處死刑或數十年監禁等特別惡劣的判決。此外，還有印度、衣索比亞等至少 20 國政府下令關閉網路，21 個國家封鎖社群媒體和通訊平臺，這些斷網或封鎖措施通常是在抗議活動和選舉等政治動盪時期實施的。

值得關注的還有監控科技的商業市場蓬勃發展。間諜軟體在全球大肆擴散，墨西哥、匈牙利、印度、摩洛哥等至少 45 個國家，疑似使用秘密公司的間諜軟體，對記者、人權捍衛者、政治異議分子等人士進行監聽或監控，甚至有多人因此遭到判刑和監禁，已經形成嚴重的人權危機。

所幸當中有一法國案例，可望對監控市場的濫用行為進行問責。法國政府於 2021 年 6 月對法國一家監控科技公司的 4 名高層主管，以參與酷刑和戰爭罪起訴，因為該公司過去出售給利比亞和埃及專制政權的監控工具被用於追蹤反對黨人士。

三、24 國介入平臺的內容管理，言論自由面臨風險

過去一年來，至少 24 國（包括歐美和我國等民主國家，以及中俄等極權國家）宣布規範平臺處理內容的新法規（草案）或措施，例如：要求刪除非法內容、懲處某些刪除形式、須任命法律代表來處理政府的規範，以及更嚴格的透明度和正當程序規定。還有些法規是免除法院命令即可刪除內容，或是強制使用 AI 刪除內容。

這些新法規對人權的影響因國家而異。在民主堅強的國家中，精心設計的平臺規範或可減輕線上危害，同時加強透明度和問責制。然而，類似的法律可能會被獨裁者濫用，以打壓人民對政治、社會和宗教的不同訴求。尤其是中國大陸，當局進一步將民間企業置於國家權力之下，以更有效的消除異議言論、進行全面監控，及操弄傳播，例如：當地科技公司會因為沒有刪除嘲笑習近平的漫畫、指控新疆集中營的言論等，而受到懲罰。

但另一方面，亦不能仰賴平臺來管理內容。儘管美國前總統川普的言論顯然助長美國國會大廈的暴動事件，不過，Facebook、Twitter 等平臺決定封鎖其帳號，也凸顯科技公司握有過大權力。一個充滿活力的民主需要法律和制度來防止權力集中於少數人手中，無論他是政府或民間企業。

四、38 國實施資料在地化、破壞加密等措施，擴大政府監控疑慮

過去一年來，至少 38 國（包括歐美和我國等民主國家，以及中緬等極權國家）推出影響科技公司管理用戶資料的法律或行政措施。越來越多的法律藉由強制平臺將用戶資料儲存在國內伺服器，以利政府監控。這些資料在地化措施使得安全標準薄弱國家的資料，更容易受到駭客攻擊，企業也難以提供更安全的跨國網路服務。其他會擴大監控和資料濫用風險的規範，還包括避免私人通訊採用加密、將個資交給幾乎不受監督的執法機關、以模糊的國安為由取得個資、對資料跨境傳輸施加繁重的許可要求等。

COVID-19 疫情相關個資是否遭到濫用的問題亦值得關注。各國持續採用追踪接觸者、管理疫苗接種、追蹤隔離合規等 apps，然而卻幾乎沒有防止濫用的保障措施。例如：新加坡政府於 2021 年 1 月證實該國 TraceTogether app 蒐集的資料可由執法機關取得，在引發公眾強烈抗議後，修法將資料取得限制在特定犯罪的調查。另外，澳洲情報與安全機構於 2020 年 11 月也坦承，他們意外從該國的 COVIDSafe app 蒐集個資。

所幸少數政府取消或終止過於廣泛的資料使用措施，例如：亞美尼亞政府停止從電信公司蒐集追蹤接觸者的位置和電話紀錄等資料，而且也銷毀儲存這些資料的硬體設備。

五、21 國擬捍衛市場競爭秩序，惟可能淪為專制政權的權力工具

過去一年來，至少 21 國（歐美民主國家和中俄等極權國家皆有）採取捍衛數位市場競爭秩序的行動。各國政府意識到，市場力量如果不加以控制，就會對用戶的權利構成威脅。因此，監管機構紛紛採用競爭政策，作為防止濫用用戶資料，以及為用戶提供更多選擇的工具。

一些國家與企業合作，使不同產品具有互操作性，並允許用戶在不同產品之間無縫切換。然而，競爭政策也可能出於政治動機，中國大陸和俄羅斯等專制政權採取嚴厲行動，幾乎不考慮正當程序或法治，反而讓民間企業為政治利益而服務。

隨著越來越多的政府建立監管數位市場的能力，他們必須遵守必要性、符合比例原則、程序透明，並保護人權，以確保國家和企業權力都對公眾負責。

六、歐盟提供「第三種方式」監管網路，臺美亦有著重透明度法規

儘管《2021 網路自由度報告》凸顯全球網路自由度下滑，數位人權和言論自由都受到空前威脅，但仍有正向發展值得一提。報告指出，歐盟的網路監管框架可能在中國大陸的數位威權主義及美國傳統的自由主義之間，提供「第三種方式」。歐盟《數位服務法》（DSA）和《數位市場法》（DMA）草案承諾為科技產業制定積極的規則。以 DSA 為例，它要求大型中介機構對其營運提出詳細報告，包括內容審核、推薦系統等演算法管理、線上廣告政策等，並且加強對正當程序的保護，諸如對用戶的內容審核結果通知、提供用戶申訴流程等。

此外，我國和美國也有 2 個法案因為著重於透明度和正當程序，而受到報告肯定。報告指出，我國的《網際網路視聽服務法》草案 [13]透過強制特定公司提供其營收和用戶數等營運資料、易於使用的用戶投訴機制、確保服務條款闡明資料的蒐集和使用等政策，提高串流影音平臺在我國營運的透明度。報告還說明，此法源自於擔心中國大陸的平臺在臺灣非法經營，並可能協助傳播來自北京的假訊息或其他操弄的內容。

美國的法案則是指美國兩大黨推動的《平臺問責制和消費者透明度法》（Platform Accountability and Consumer Transparency Act）[14]，此草案和改革《通信端正法》（Communications Decency Act, CDA）第 230 條 [15]有關，例如：要求業者公布其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，以及於 4 天內刪除法院判定的非法內容等。

13 通傳會主委陳耀祥 2021 年 9 月 30 日於立法院交通委員會上表示，暫緩推動《網際網路視聽服務法》，待《數位通訊傳播法》定案後，再考慮是否納管 OTT-TV 及如何納管。

14 雖然《2021 網路自由度報告》形容此法是美國公民社會積極推動下的兩黨法案，不過，經查詢美國國會網站，法案自 2021 年 3 月 17 日送交參議院後，迄 11 月中旬尚無任何進展（Congress.gov, 2021）。

15 第 230 條係指網路服務供應商不必為第三方使用者的內容承擔法律責任，而且對於善意的限制冒犯性內容，也可免於遭到起訴。

惟報告也提醒民主政策制定者，應該保持警惕，因為他們的法律也可能對網路自由產生負面影響。例如：德國 2018 年的《網路執法法案》（Network Enforcement Act，又稱 NetzDG）引入有問題的規範，要求業者在沒有法院命令的情況下，迅速刪除內容。雖然後來進行修法，但倒退的民主國家和專制政權一直在模仿和濫用原始法律，迫使社群媒體刪除同性戀和跨性別者的相關內容，以及調查性的新聞。同樣的，一些國家也引用歐盟 2018 年實施的 GDPR（一般資料保護規則），以阻止資料的跨境流通，或對政府的監控賦予豁免權。例如：中國大陸於 2021 年 11 月實施的《個人信息保護法》，雖然引用 GDPR 框架，但其適用對象只涵蓋企業、組織和個人，因而被專家批評為沒有限制政府的使用行為，尤其是監控系統的使用。

第四節 我國網路自由度和相關政策規範

《2021 網路自由度報告》臺灣篇指出，臺灣擁有亞洲地區最自由的網路環境。以下依 3 大評比類別綜述我國於該類的整體概況，並將各子項指標的得分、相關法規政策、是否涉及通傳會業務等項目，以表格加以說明。

一、上網阻礙

「上網阻礙」共有 5 項指標，合計 25 分，我國得 24 分，當中 4 項指標獲得滿分，凸顯我國的網路普及率很高、沒有顯著的數位落差、有獨立的監管單位、民眾亦可自由選擇網路服務供應商。只有在供應商多樣化項目，因為被視為電信市場由特定業者主導，而小扣 1 分。

這 5 項指標的得分、相關發展和法規政策，摘錄於下表 5-2，每項指標都提及通傳會的相關業務，包括網路普及和偏鄉建設、合理的上網資費、《電信管理法》鬆綁管制、通傳會為電信和廣播的獨立監管單位，惟報告也提到民眾對於通傳會的獨立性有所疑慮。

表 5-2 我國於「上網阻礙」項目的評比結果

指標 （得分 / 總分） 相關發展和法規政策	NCC 業務
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） 臺灣的網路普及率高達 9 成（網路行銷整合服務業者 HootSuite 資料）或 83%（TWNIC 資料），且用戶可透過多種方式上網。根據 NCC 統計，2019 年有 583 萬人使用固網，行動網路普及率為 114%，且全國有近 10,000 個免費 Wi-Fi 熱點。臺灣政府致力將行動服務升級為 4G 和 5G，主要電信業者已經開始提供 5G 服務。2021 年 7 月臺灣於 SpeedTest（國際知名測速網站）的全球行動和固網速度指數分別排名第 28 和第 30 名。	○
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） 臺灣沒有明顯的數位落差，只有在地區和年齡方面有些微差異；外來移民的上網	○

指標 （得分 / 總分） 相關發展和法規政策	NCC 業務
率更是從 2014 年的 72%，躍升為 2020 年的 96%；政府還成立愛部落（i-Tribe）計畫，為原住民社區增加無線寬頻網路，且提高當地民眾取得數位醫療服務和其他資訊的能力。此外，上網費尤其是行動網路費，是民眾可負擔的，且於《2021 包容性網路指數報告》（The Inclusive Internet Index 2021）的可負擔性排名第 47（報告由經濟學人發布，研究 100 個國家）。	
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） 臺灣政府沒有刻意限制網路連接，且臺灣的網路基礎設施和連接國際網路的海纜都是民間私有，4 個網路交換點——TWIX、TPIX、EBIX 和 TWNAP 皆由電信業者營運，網路海纜則大多由中華電信鋪設（但交通部持有 35%中華電信股份）。此外，2020 年 Google 和 Facebook 也提出興建連接美國和臺灣的海纜計畫。	○
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） 雖然臺灣的用戶可以自由選擇 ISP，且 2020 年 7 月實施的《電信管理法》鬆綁管制（如舊法下的第二類電信業者改為只需辦理登記，不必申請執照），不過，新法仍有外國人直接持股不得超過 49%等規定。此外，礙於舊法的市場進入門檻較高等因素，目前市場仍由特定業者主導，固網和行動市場以 5 大電信業者為主，且中華電信的市占率高達 68%[16]。	○
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） 負責監管電信和廣播服務的 NCC 是一個獨立的政府機關，但由於 NCC 的委員是由行政院院長提名經立法院同意，且主委和副主委亦由行政院院長指定，因此，臺灣民意基金會 2020 年 11 月發布的調查結果顯示，68%民眾對於 NCC 的獨立性有所疑慮。另外，關於 NCC 對多次違規的中天新聞臺於 2020 年底的換照申請予以駁回，無國界記者組織（Reporters Without Borders, RSF）認為 NCC 的決議不構成侵犯新聞自由。	○

16 經查證中華電信資料，68%實為寬頻固網的市占率，如就行動市場來看，市占率降為 37%。

指標 （得分 / 總分） 相關發展和法規政策	NCC 業務
其他監管數位科技的部會諸如公平貿易委員會，負責監管與電信服務相關的競爭法；還有數個不同部會共同監管《個人資料保護法》的實施（參見指標 C6）。此外，行政院資安處負責監管關鍵基礎設施安全的相關問題（參見指標 C8）。 而網路內容的監管單位則依資訊的性質而定（參見指標 B2 和 B3）。例如：與食品衛生相關的內容，由衛生福利部處理；兒少相關內容，由多個部會資助成立的 iWIN 網路內容防護機構負責。此外，預計 2022 年還將成立數位發展部，負責推動數位轉型和其他網路相關業務。	

資料來源：本計畫彙整

二、內容限制

「內容限制」共有 8 項指標，合計 35 分，我國得 31 分，當中 5 項指標獲得滿分，凸顯整體而言，臺灣沒有網路封鎖和審查，網路訊息和媒體相當多樣性，且民眾可以自由發布內容及辯論社會政治議題；而即使政府對於特定內容有所限制，亦是有法律依據。至於扣分的項目，主要是因為涉及網路內容責任的法律（甚至是中國大陸和香港的法律）可能會導致民眾的自我審查；以及不論是臺灣的兩大政黨或是中國大陸政府，都在臺灣的網路空間進行政治影響力的假訊息操弄。

此 8 項指標的得分、相關發展和法規政策，摘錄於下表 5-3，當中與通傳會業務相關者共有 6 項，包括臺灣公司不能提供中國大陸的 OTT-TV 服務、iWIN 網路內容防護機構請求刪除有害兒少內容、民眾對媒體的信任度下降、網路上充斥假訊息、對岸付費國內媒體散播親共言論及介入社論審查、ISP 須以非歧視方式提供網路服務，以及研議中的《數位通訊傳播法》規定通傳業者的義務和《網際網路視聽服務法》[17]針對 OTT-TV 進行監管。這 2 項草案所屬的指標——B3 之內容限制是否透明且符合比例原則.....，及 B6 之是否限制網路媒體的廣告或投資等，皆獲得滿分。惟報告也指出有人權團體認為《數位通訊傳播法》將非法內容的裁定責任推卸給業者。

表 5-3　我國於「內容限制」項目的評比結果

指標（得分/總分） 相關發展和法規政策	NCC 業務
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) 臺灣政府通常不會強迫服務供應商封鎖、過濾網站或社群媒體，但有特定法律授權限制網路內容（參見指標 B3）。根據 2020 年 9 月實施的新規定（更新《臺灣	○

17 同註 13。

指標（得分/總分） 相關發展和法規政策	NCC 業務
地區與大陸地區人民關係條例》），臺灣公司不能提供中國大陸的 OTT-TV 服務（網際網路視聽服務），尤其是愛奇藝或騰訊（參見指標 B6）。 教育部的網路守護天使是一款提供給家長和教育者的內容過濾軟體，2020 年的下載次數近 9.9 萬次。但台灣人權促進會發現，此軟體沒有明確的過濾標準，且會過濾臺灣廢除死刑推動聯盟、臺灣同志諮詢熱線協會等公民團體的網站。	
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） 多項法律禁止發布某些類型的內容，並允許刪除這些內容（參見指標 B3）。例如：政府於 2016 年期間引用《食品安全衛生管理法》要求刪除內容多達 153 次；《著作權法》要求中介機構刪除侵犯版權的第三方內容；《兒童及少年福利與權益保障法》要求內容託管商限制瀏覽被認為對兒少身心健康有害的內容，且 iWIN 於 2020 年也請業者刪除 1,184 件民眾投訴的有害內容。 此外，司法和警察單位也處理或要求內容刪除的案件。2021 年 2 月法院裁定一名被告應刪除其在 Google 上對某間醫療院所的評論，包含當中的錯誤訊息。又 2021 年 3 月警方強迫臺灣某色情平臺於調查期間暫時關閉該網站。 Google 報告指出，2020 年下半年臺灣政府提出 19 項內容刪除請求，當中有 11 項為選舉相關內容，此次 Google 的執行率為 59%。	○
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） 網路審查在臺灣並不常見，政府對內容的限制有法律依據。然而，民間社會認為政府單位請求刪除內容及其被執行的情況，缺乏透明度和監督機制（參見指標 B2）。多項法律包括《兒童及少年福利與權益保障法》、《食品安全衛生管理法》、《藥事法》、《消費者保護法》、《化粧品衛生安全管理法》、《傳染病防治法》等，禁止發布特定類型的內容。以《傳染病防治法》為例，它授權政府強制供應商阻止造訪或刪除販賣動物違禁品的網站。而舊版《化粧品衛生管理法》有關網路上	○

指標（得分/總分） 相關發展和法規政策	NCC 業務
的化妝品廣告須經事前審查的規定，則是已於 2017 年被大法官認定違憲。還有一個審理中的「被遺忘權」案件（某職棒隊前老闆要求 Google 刪除「聲稱」他有違法情事的資料），原本高等法院裁定我國《個人資料保護法》沒有保護「被遺忘權」，但最高法院於 2021 年 2 月判決發回重審。 此外，NCC 有 2 個研擬中的法案。《數位通訊傳播法》對數位通傳業者課以不同程度的義務，例如：規定業者須於服務條款中說明隱私和安全政策，及舉報不當內容的管道；草案還要求中介機構實施「通知和下架」機制，以在收到通知後立即刪除非法內容。惟草案也被人權團體批評為將非法內容的裁定責任推卸給業者。而《網際網路視聽服務法》則是針對 OTT[18]進行監管，此草案受到對愛奇藝等中國大陸 OTT 在臺灣服務疑慮的影響，因為它們沒有經 NCC 依據《臺灣地區與大陸地區人民關係條例》核准。草案還要求 OTT 業者提高透明度，尤其須於服務條款中說明隱私保護和網路安全政策、資料使用的訊息、用戶舉報問題的管道等。業者還須確保平臺上的內容不會危害國家安全、公共秩序或道德，或損害青少年的身心健康。至於什麼構成國家安全將由相關行政單位決定（參見指標 B6）。	
B4 網路記者、評論人、一般用戶是否會進行自我審查？（3/4） 涉及網路內容責任的法律如《社會秩序維護法》和刑事誹謗條款，可能會影響自我審查（參見指標 C2 和指標 C3）。另外，對於中國大陸和香港的法律恐懼亦是。例如：臺灣社會運動人士李明哲 2017 年過境澳門時遭到逮捕，之後中國大陸以其網路發文內容做為證據，判以「顛覆國家政權罪」及 5 年刑期，以致讓需要前往中國大陸的臺灣人，在網路上論及中國大陸相關問題時特別戒慎恐懼。還有香港於 2020 年 6 月實施的《國家安全法》，也可能鼓勵言論的自我審查，因為它的處	x

18根據歐盟電子通訊監管機構 BEREC 於 2016 年《OTT 服務報告》，OTT 服務的定義為「藉由網際網路向終端使用者提供的內容、服務或應用」。此項法案針對網路視聽服務進行規範，而非所有的 OTT（over-the-top），因此，簡稱 OTT 應更正為 OTT-TV 較為合適。

指標（得分/總分） 相關發展和法規政策	NCC 業務
罰範圍擴及中國大陸以外的言論。另外，一些公司、記者和用戶也會因為稱臺灣為國家而受到中國大陸官方和親共人士的強烈抨擊，他們並為此發表道歉文。	
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） 臺灣政府不會下令或試圖脅迫網路媒體以影響其報導，但政治的虛假訊息和網路影響操作是個重要議題。瑞典智庫民主多樣性（Variety of Democracy, V-Dem）2019年的研究發現，臺灣是外國政府散播假訊息攻擊的主要目標之一，使用的熱門話題包括兩岸統一、臺灣民主缺陷、詆毀政府因應 COVID-19 疫情、誹謗民進黨候選人等。臺灣民間團體——台灣民主實驗室 2020 年 10 月的報告指出，中國大陸的假訊息策略包括付費給臺灣媒體和網紅散播親中的言論。同年，美國網路安全公司 Recorded Future 也指出，中國大陸省級政府以 740～1,460 美元不等的月薪，在臺灣召募支持統一的網紅。路透社早於 2019 年即報導中國大陸當局付費給臺灣的新聞媒體至少有 5 家。同年，臺灣的國家安全局也指控中國大陸政府參與某些臺灣新聞媒體的社論審查。 此外，臺灣兩個主要政黨——民進黨和國民黨，都聲稱對方僱用評論員在網路上散播操弄的訊息。牛津大學網路研究所（Oxford Internet Institute）的報告指出，有受訪者聲稱競選活動和政黨會付費來散播網路訊息，但他們不確定這些是否為錯誤或故意誤導的內容。	○ （打擊假訊息）
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） 臺灣用戶發布網路內容不會受到嚴格的限制，且網路新聞媒體無需獲取執照即可發布新聞。服務供應商則受《電信管理法》規範，在網路品質、價格、條件和資訊方面，必須以非歧視方式提供服務（參見指標 A4）。 但臺灣對於來自中國大陸的投資或網路廣告，有所限制。根據《臺灣地區與大陸地區人民關係條例》，中國大陸實體直接持有媒體和其資產，須獲得臺灣政府核	○

指標（得分/總分） 相關發展和法規政策	NCC 業務
准；而中國共產黨的廣告則是完全禁止。 《網際網路視聽服務法》草案要求特定規模、營收、流量或市場影響力的 OTT 服務進行登記，否則將面臨 10～100 萬新臺幣罰款（參見指標 B3）。外商企業還需設立當地代表，並定期向 NCC 報告國內用戶數量、流量、營收等資訊。如果當地電信公司為來自中國大陸的非法 OTT 業者提供服務，將面臨巨額罰款。	
B7 網路上的訊息是否多樣化且值得信賴？（4/4） 臺灣的網路資訊和數位媒體生態系統反映不同的興趣、社群和語言。一些新的網路媒體促成這種多樣性。但媒體環境也存在政治兩極化和聳動的內容。臺灣媒體觀察基金會的研究發現，臺灣民眾認為 2019 年的媒體環境比 2014 年更不可靠及更不可信。LINE、Facebook、Instagram 和 PTT 論壇充斥假訊息，會削弱人們獲取可靠資訊的能力（參見指標 B5）。台灣民主實驗室 2020 年的民調發現，80%受訪者認為網路錯誤訊息是嚴重的威脅。此外，2021 年 5 月 COVID-19 疫情爆發後也出現許多關於疫苗的錯誤訊息，例如：疫苗可能導致老年人死亡。 所幸政府、科技產業和公民社會設計創新工具，來因應虛假和錯誤訊息的影響（參見指標 B5）。例如：科技政委唐鳳推動在每個部會部署「迷因工程」團隊，以幽默正確資訊快速回擊不實訊息；LINE 用戶可以將訊息轉傳給 Cofacts 機器人以進行事實查核，此平臺是由公民技術團體 g0v 透過群眾協作開發的。	○ （打擊假訊息）
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） 臺灣人民可以自由使用數位平臺和網路上的訊息，來辯論政治議題和動員社會。當前事件（例如：保護藻礁的全民公投）往往會在社群媒體上引發大量辯論。	✕

資料來源：本計畫彙整

三、侵犯用戶權益

「侵犯用戶權益」共有 8 項指標，合計 40 分，我國得 25 分。雖然沒有指標獲得滿分，但報告指出，臺灣的憲法保障言論自由、新聞自由，以及秘密通訊，並有獨立的司法系統，民眾也可以自由使用加密技術，且通常不會因為網路活動而遭受身體暴力或其他嚴重的威脅。

而得分較低的項目，主要在於有多項法律將網路行為定為犯罪且有民眾因此受罰的案例、未經法院核准的通訊監察案件及索取通聯紀錄案件越來越多、《科技偵查法》草案提高執法單位的監控通訊能力有侵犯人權的疑慮、缺乏《個人資料保護法》的獨立專責主管機關、疫情資料的蒐集使用缺乏合法性和比例原則、經常遭受境外網路攻擊且有資料外洩問題。

此 8 項指標的得分、相關發展和法規政策，摘錄於下表 5-4，當中提及與通傳會業務相關者共有 4 項，包括《金融時報》報導中共對旺旺中時媒體集團的新聞編採下指導棋、所有電信號碼（包括預付的 SIM 卡）銷售必須登記註冊、電信公司依《電信管理法》等須配合執行監察工作但沒有解密的法定義務、簡訊實聯制的資料遭指控用於犯罪偵查、《資通安全管理法》監督關鍵基礎設施（包含通訊傳播領域）供應商的網路安全及規定安全事件的通報應變機制。

表 5-4　我國於「侵犯用戶權益」項目的評比結果

指標（得分/總分） 相關發展和法規政策	NCC 業務
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） 臺灣的憲法保障言論自由和新聞自由，政府還將《公民與政治權利國際公約》（International Covenant on Civil and Political Rights）當中的保護言論自由和資訊取得納入國內法，且於 2005 年開始實施《政府資訊公開法》。 臺灣的司法是獨立的，它為言論提供相當大的保護（參見指標 C3）。然而，至少	×

指標（得分/總分） 相關發展和法規政策	NCC 業務
有一項法院裁決破壞強力的言論自由標準——2000 年大法官釋憲聲明誹謗罪並不違反憲法中對言論自由的保護（參見指標 C2）。	
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） 臺灣有多項法律將網路行為定為犯罪。以刑法為例，第 309 條規定公然侮辱罪處最高拘留兩個月或新臺幣 9,000 元罰金;140 條和 310 條分別為侮辱依法執行職務的公務員，以及誹謗罪的懲處。 在傳播不實和錯誤訊息方面，《社會秩序維護法》對於散布謠言（包含透過網路）以致破壞公共秩序者，處 3 日以下拘留或新臺幣 3 萬元以下罰鍰。《嚴重特殊傳染性肺炎防治及紓困振興特別條例》第 14 條規定，散播對他人和大眾造成損害的疫情謠言或不實訊息者，處 3 年以下有期徒刑或高額罰緩（新臺幣 300 萬元）。《公職人員選舉罷免法》第 104 條規定，散播對他人和大眾造成損害的選舉相關謠言或不實訊息者，處 5 年以下有期徒刑。《反滲透法》規定散播由敵對外國勢力所指示、委託或資助的選舉相關假訊息的刑事處罰。《災害防救法》則對於在知情下通報災害不實訊息者處新臺幣 30 萬元以上至 50 萬元以下罰金。還有《食品安全衛生管理法》規定，任何人不得故意散播和市場糧食價格或糧食生產計畫相關的謠言或錯誤訊息。	✕
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） 臺灣有網路使用者因為網路活動而受到調查或起訴，雖然案件很少遭致監禁或高額罰款等重大處罰，但近年來《社會秩序維護法》的案件增加，且過去一年來至少有 4 起散播假訊息的案件遭罰，案由如聲稱新北市因疫情而封城、放疫情假 2 週、延後開學至 3 月 1 日、政府正提供家庭財務補貼，罰款金額則從新臺幣 2 千元到 6 千元不等。其他案件如批評故宮博物院的政策、聲稱蔡內閣提供奢侈午餐	○

指標（得分/總分） 相關發展和法規政策	NCC 業務
和濫用公帑等，皆被法院駁回。而網紅涉嫌僱用網軍侮辱外交官並導致其自殺身亡的案件則仍在審理中[19]。 此外，至少有 2 位網路用戶因違反《嚴重特殊傳染性肺炎防治及紓困振興特別條例》而被判有罪並處以罰款，其中一個案例為故意發布錯誤訊息聲稱某人 COVID-19 檢測呈現陽性。 新聞媒體和記者也遭刑事誹謗指控。例如：2019 年 7 月旺旺中時媒體集團因為《金融時報》報導其新聞編採經常接受中國大陸政府的指示，而向《金融時報》及轉載該篇報導的中央通訊社之負責人及撰稿記者，提起刑事誹謗訴訟。另外，蘋果日報則是因為報導大同公司的人事鬥爭和財報問題而被提告誹謗，法院於 2021 年 4 月裁定蘋果日報無罪。	
C4 政府對於匿名或加密通訊是否有所限制？（3/4） 臺灣對於匿名通訊有些限制，因為臺灣有強制性的 SIM 卡註冊要求。電信相關法規要求服務提供商在銷售所有電信號碼（包括預付的 SIM 卡）時，須登記用戶的姓名和身分證號碼。NCC 在 2017 年強調，註冊有助於刑事和欺詐案件的調查及防範。 臺灣民眾可以自由使用加密技術。雖然《通訊保障及監察法》授權執法單位在獲得法院授權下，可以監聽有線和無線的電信通訊，且電信公司應確保其系統能配合執行監察工作，但電信公司沒有明確的法律義務解密訊息，或向執法單位提供解密的密鑰。 2020 年 9 月法務部公告《科技偵查法》草案，授權持有法院命令的執法單位透過	○

19 此案於 2021 年 11 月 12 日由臺北地方法院宣判該名網紅和網軍共 2 人侮辱公署罪，處有期徒刑 6 月，得易科罰金 18 萬元（資料來源：聯合報。卡神楊蕙如率網軍「黑」外交官 有罪！判侮辱公署 6 月最高刑。https://udn.com/news/story/7321/5885194?list_ch2_index）。

指標（得分/總分） 相關發展和法規政策	NCC 業務
實體、網路傳輸或植入惡意軟體等其他必要方式，存取包含加密通訊在內的用戶電子設備。	
C5 政府是否有侵犯用戶隱私權的網路監控活動？（3/6） 臺灣憲法明確保障秘密通訊，並要求監看人們通訊的執法機關須受到監督。司法院的釋憲也保護隱私權和資訊自主權。此外，《個人資料保護法》也規範政府機關和民間部門對於個資的蒐集、處理和使用（參見指標 C6）。然而，某些法律和執法過程卻破壞了隱私權。 《通訊保障及監察法》規定，調閱通訊內容須有法官核發的「通訊監察書」，且須為偵查最重本刑 3 年以上有期徒刑之罪。對於同類型犯罪，檢察官還可聲請「調取票」取得通聯紀錄。但在緊急情況下和特定重罪（如最輕本刑 10 年以上之罪），檢察官不需經由法院許可，即可通知執行機關進行監察。根據司法部門統計，2020 年的通訊監察案件約 56,000 件，索取通聯紀錄約 123,000 件，總計 90%以上案件沒有聲請法院核准。台灣人權促進會表示，缺乏司法審查的情況越來越常態化。不需司法監督即可下令監聽的，還有國家安全局在緊急情況下，可直接對在國內的外國或敵國勢力進行監聽，且無須披露其監聽活動。《刑事訴訟法》也有執法機關取得個資的規定，在持有法院核發的「搜索票」，或經當事人的自願同意下，可以取得通聯以外的個人資料。 法務部推出《科技偵查法》草案以提高執法單位的監控通訊能力，例如：檢察官可以在沒有搜索票下使用 GPS 等位置追踪工具進行為期兩個月的調查、警察可使用加裝攔截手機訊號設備的無人機進行長達 30 天的監視。雖然法務部表示，新型態的數位犯罪會透過通訊軟體聯繫，政府因此需要有新的應對權力。不過，民間團體批評草案條款將導致合法允許嚴重侵犯隱私權和其他人權。 而在使用間諜軟件技術方面，目前並不清楚政府是否允許，但加拿大的公民實驗室（Citizen Lab）2015 年報告將臺灣政府列為 FinFisher（間諜監控軟體）的可疑	x

指標（得分/總分） 相關發展和法規政策	NCC 業務
客戶。更早之前政府也被發現與目前已經解散的義大利公司 Hacking Team 論及購買間諜軟體。 另外，也有人擔心政府對社群媒體進行監控。國家安全局於 2018 年承認為了追踪中國大陸的不實訊息並確保國家安全，而監控社群媒體。其他政府單位也被發現購買監控和分析系統。	
C6 業者監看和蒐集用戶資料是否侵犯用戶隱私權？（3/6） 臺灣《個人資料保護法》規範個資的蒐集、處理和利用，以及跨境傳輸，但缺乏獨立專責的主管機關。 另外，《電信管理法》和《通訊保障及監察法》要求服務提供商和電信業者配合刑事調查執法和其他政府機關的監管要求（參見指標 C5）。還有某些具有調查權力的政府單位也直接向其他政府部門和民間企業索取個資，且無需先取得法院命令，或受到其他監督。例如：經濟部在 2017 至 2018 年間，向中華電信、Yahoo 臺灣分公司等其他業者和政府單位提出 1,112 份個資索取請求，且成功率達 100%。另刑事調查局在 2015 至 2016 年向 Facebook 提出 565 項個資索取請求，成功率為 52.9%。 COVID-19 疫情期間，政府也增加資料的蒐集和監測，但遭到民間團體和專家批評缺乏合法性及比例原則。2020 年 2 月頒布的《嚴重特殊傳染性肺炎防治及紓困振興特別條例》，賦予中央流行疫情指揮中心廣泛的權力執行接觸者追踪和公開個資。當月鑽石公主號遊輪發生集體感染事件，政府從電信公司取得超過 60 萬人的手機位置訊息，以進行接觸者追踪。政府並使用電子圍籬系統，透過手機定位資料，確保個人落實隔離。中央流行疫情指揮中心可以取得系統中的匯總資料，負責確認隔離的警察也可以取得個人的姓名、電話號碼和地址。2021 年 5 月政府還推出 1922 接觸追蹤系統（簡訊實聯制），該系統使用二維條碼（QR Code）追蹤用戶的位置。雖然 NCC 強調系統資料僅用於疫情調查，但有法官聲稱資料被用	○

指標（得分/總分） 相關發展和法規政策	NCC 業務
於鎖定嫌犯的行蹤。	
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） 臺灣用戶通常不會因為他們的網路活動而遭到身體暴力或其他嚴重的威脅，但是網路騷擾是個問題。例如：太魯閣號火車重大事故的乘客（因為被誤認是肇事者）、打破臺灣零確診紀錄的機師、報導臺灣隔離追蹤措施有隱私疑慮的外媒記者，以及 LGBT+（Lesbian 女同性戀者、Gay 男同性戀者、Bisexual 雙性戀者、Transgender 跨性別者）網路用戶等，都曾被網路騷擾或人肉搜索。此外，也發生罕見的暴力襲擊網紅事件。有民眾因為對影片內容不滿，而教唆襲擊網紅蔡阿嘎和其妻子。為此，行政院於 2021 年 4 月通過《跟蹤騷擾防制法》草案[20]，將處理包含網路騷擾在內的問題。	✕
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） 臺灣經常受到境外網路攻擊，尤其是來自北京。行政院資安處 2019 年曾表示，臺灣公部門每月平均遭受 3 千萬次網路攻擊，其中一半推測是來自中國大陸。2020 年 9 月有政府報告顯示，至少 10 個單位和 6 千個電子郵件帳號長期成為攻擊目標，且有 4 個中國大陸政府支持的駭客組織參與其中。美國國務院於 2020 年的人權相關報告亦指出，中國大陸政府對臺灣記者的電腦和手機進行網路攻擊。 資料外洩也是臺灣的資安問題。有國際資安公司於 2020 年 5 月指出，超過 2 千萬筆臺灣戶籍資料在暗網上流傳（出售）。 臺灣《資通安全管理法》監督關鍵基礎設施供應商的網路安全，並要求公務機關制定網路安全維護計畫，此法還規定發生安全事件時的通報應變機制。	○

資料來源：本計畫彙整

[20] 本草案已於 2021 年 11 月 19 日經立法院三讀通過。

第五節 其他國家案例：加、德、美

本節簡介網路自由度名列前茅的先進民主國家，其過去一年來的相關法規政策。雖然冰島、愛沙尼亞及哥斯大黎加，為全球網路自由度排名前3名的國家，但由於它們為人口稀少的小型國家（分別為37萬、133萬、509萬人），因此，案例首選設定為和哥斯大黎加同為全球第3名的加拿大（美洲第1名）。其次，則挑選歐洲「先進民主大國」中，網路自由度排名第1的德國（全球第6名、歐洲第3名）。另外，也加上網路發源地及孕育全球科技巨頭的美國（全球第12名、美洲第2名），做為參考案例。

一、加拿大

《2021 網路自由度報告》加拿大篇指出，雖然加拿大鄉村地區的網路基礎設施和電信服務不足，但對大多數人來說，網路連線是可靠且負擔得起，且人民享有強力的言論自由和新聞自由保護。以下為網路自由度報告所挑選的加拿大近一年來最主要的相關政策法規，並由本計畫從細項指標的資料摘錄重點，及補充法案或訴訟案件的最新進展。

- **盜版網站封鎖令上訴至最高法院**

  加拿大法院於 2019 年 11 月命令全國主要 ISP 封鎖侵權節目的網站，其中一家 ISP 業者 Teksavvy 於 2020 年 6 月向聯邦法院提起上訴，並於 2021 年 5 月遭到駁回。Teksavvy 基於捍衛言論自由等原因，於 2021 年 8 月再向最高法院提出上訴（Tremblay, 2021）。

- **《選舉現代化法案》違憲條款遭法院駁回**

  為了打擊假訊息和外國干預選舉，加拿大於 2019 年 6 月實施《選舉現代化法案》（Election Modernization Act），將散播政治候選人的錯誤訊息定為刑事犯罪。安大略省法院認為此舉侵犯言論自由且違反憲法，因此，於 2021 年 3 月裁決駁回相關條款。

- **《消費者隱私保護法》草案遭抨擊未考量人權**

  加拿大政府於 2020 年 11 月提出《消費者隱私保護法》（Consumer Privacy Protection Act, CPPA）草案，以加強保護個人線上隱私權，但同時也為企業提供使用個資的額外權限。草案因此遭到未從人權角度立法、沒有將隱私訂為一項人權等批評。草案推動迄今（2021 年 10 月底）仍無立法進展（Mcphail, 2021）。

- **COVID-19 個資共享因訴訟而終止**

  安大略省政府於 2020 年 4 月的 COVID-19 緊急命令授權行政部門和執法部門、醫療體系等危機處理人員共享個資。經人權組織提起訴訟後，安

大略省政府於 2020 年 8 月終止個資共享措施。此外，加拿大隱私專員辦公室（Office of the Privacy Commissioner, OPC）的 2020 年年度報告也強調，疫情期間需要提高隱私保護，並建議要改革隱私法規。

- **仇恨言論、威脅、誹謗等網路行為皆有法律規範**

  加拿大對於網路言論有所規範，仇恨言論最高可處 2 年監禁，其他如誹謗、鼓吹種族滅絕、威脅，最高可處 5 年監禁。此外，安大略法院在 2021 年 1 月的一件訴訟案中，確認「網路騷擾」為觸法行為，並將其定義為「持續發布誹謗內容，以騷擾、煩擾、調戲受害者」。

- **隱私當局發現業者違法蒐集人臉資料**

  加拿大的中央和地方隱私部門經長期聯合調查後，於 2021 年 2 月發布調查結果表示，大型購物中心使用美國 Clearview AI 公司的人臉辨識軟體，在民眾不知情或未經允許下，蒐集他們的人臉資料，違反 2018 年實施的《個人訊息保護和電子文件法》（Personal Information Protection and Electronic Documents Act, PIPEDA），並因此要求 Clearview AI 停止蒐集加國人民的人臉資料，且刪除之前蒐集的資料，同時也需停止在加拿大提供類似的軟體和服務（PIPEDA, 2021）。

二、德國

《2021 網路自由度報告》德國篇指出，德國的網路環境整體而言是自由的，媒體和民間社會經常公開討論網路監管相關問題，且有獨立的司法系統對行政和立法部門的監管措施進行監督。不過，受到政黨涉及網路假訊息的報導影響，德國的網路自由度略有下降，且情報單位擴大網路監控權力的新立法，也引發隱私問題。以下為網路自由度報告所挑選的德國近一年來最主要的相關政策法規，並由本計畫從細項指標的資料摘錄重點。

•NetzDG 修正案要求提供嫌犯個資，且監管範圍擴及影音分享平臺

規範社群平臺移除非法內容的《網路執法法案》（NetzDG），自 2018 年上路來已陸續實施多項修正案。如 2021 年 4 月實施的網路平臺須向聯邦刑事警察局提供發布線上仇恨等罪行的個人用戶資料。此修正案一度曾因部分內容可能違憲而遭總統拒絕簽署，之後修改資料揭露流程規範，使得向警察局傳輸資料變成合法化後，才得以正式生效。此外，2021 年 6 月實施的修正案還將 NetzDG 適用範圍擴及影音分享平臺，但同時也提供用戶對於刪除內容的上訴管道。

•新版《著作權法》已上路，但設置過濾機制規定可能無效

配合 2019 年版《歐盟著作權指令》（EU Copyright Directive）的規定，德國於 2021 年 6 月實施新版《著作權法》（Copyright Act），內容包括大型平臺業者必須設置過濾機制，以封鎖涉嫌侵權的線上內容。但設置過濾機制可能無效，因為不論是執政黨或其他黨派多持反對意見，且歐盟最高法院對於《歐盟著作權指令》第 17 條（指平臺業者對使用者上傳內容是否侵權須負把關責任）的合法性，也尚未做出裁決。

•業者推動從 DNS 封鎖侵權網站，帶來法外限制通訊自由的隱憂

在德國營運的網路供應商（經查詢為德國電信 Telekom、來自英國的 Vodafone 電信、來自西班牙的 Telefónica 電信等）和娛樂產業組織於 2021

年 3 月成立網路著作權清算中心（The Clearing House for Copyright on the Internet, 德文簡稱 CUII），以推動從域名系統（DNS）封鎖侵權的網站。此項倡議正由聯邦網路局（Federal Network Agency，德文簡稱 BnetzA）針對是否違反網路中立原則進行評估。聯邦卡特爾辦公室（The Federal Cartel Office, 德文簡稱 BkartA）也密切關注此案發展，但遭質疑無關其監管職責。此外，此倡議還引發從法律制度外限制通訊自由的疑慮。

•極端政黨增加操弄假訊息，但法規解決方案引發內容審查疑慮

德國網路媒體 Netzpolitik 於 2021 年 3 月揭露一場假訊息宣傳活動，指稱散播德國氣候變遷、COVID-19 和難民陰謀論的一個波蘭網站，與德國的右翼民粹主義政黨——德國另類選擇黨（Alternative for Germany, 德文簡稱 AfD）有關，且促進其政治利益；這也是德國的內容操弄增加的一大主因。然而，立法者推出的打擊假訊息法規解決方案，卻引發內容審查、破壞媒體選擇權等抨擊。2020 年 11 月生效、取代德國《州際廣播協定》（Interstate Broadcasting Treaty）的《國家媒體協定》（The State Treaty on Media，德文簡稱 MStV），將監管範圍從無線電廣播擴大至新型媒體，規定平均收視超過 2 萬人次的媒體創作者（如：YouTuber）須申請執照、聚合第三方內容的平臺業者（如：Google、Facebook）演算法須符合透明度及非歧視性等。此外，它還要求實施自律的業者必須懲罰發布不實訊息的累犯。

•法律授權情報單位擴權監聽，但未同時提供通訊隱私的有效保障

德國於 2021 年 6 月實施修訂版的聯邦情報局（Federal Intelligence Service，德文簡稱 BND）組織法，允許其監聽高達全球電信網路 30%的傳輸容量；且監聽對象擴及沒有犯罪紀錄的人民，並可使用惡意軟體達成監聽目的；還可以蒐集處理各種通訊資料，從而能夠監控人民的通訊行為、金融交易資料、行蹤資料等。包括德國聯邦憲法法院、資料保護部門、法律專家等，皆批評此法沒有同時提供有效的個人通訊保護措施。德國《基本法》（Basic

Law）第 10 條保障人民的通訊隱私，不論是實體或網路的通訊。也因此，非政府組織已經展開反對此次修法的陳情行動。

三、美國

《2021 網路自由度報告》美國篇指出，雖然美國的網路蓬勃發展，網路內容多樣化且基本上不受國家審查，但 2020 年 11 月總統大選的假訊息和陰謀論內容大肆傳播，已威脅美國的民主核心。2020 年還有多起政府監控、騷擾種族不公抗議活動的案件，以致美國的網路自由度下滑。以下為網路自由度報告所挑選的美國近一年來最主要的相關政策法規，並由本計畫從細項指標資料摘錄重點，及補充法案的最新進展。

- **「緊急寬頻福利計畫」和《基礎設施投資與就業法》解決上網阻礙**

  美國國會於 2020 年 12 月通過「緊急寬頻福利計畫」（The Emergency Broadband Benefit, EBB），此為 COVID-19 援助計畫的一部分，為近 400 萬人提供網路服務和相關設備的折扣。美國的網路基礎設施容易受到惡劣氣候破壞，上網費用也瀕臨可負擔的危機，數位落差問題更是因為疫情的持續而更加顯著。因此，拜登總統於 2021 年 4 月提出《基礎設施投資與就業法案》（Infrastructure Investment and Jobs Act），當中即包括延長 EBB 計畫，並將斥資 650 億美元大舉興建高速寬頻網路。此法案已於 11 月獲得美國國會通過，且經拜登簽署生效（The White House, 2021）。

- **拜登撤銷川普的禁用微信行政命令，但下令評估敵國 apps 風險**

  拜登總統於 2021 年 6 月撤銷前總統川普的禁用微信行政命令，這是川普於 2020 年 8 月以威脅國家安全為由，所發布的禁止下載來自中國大陸的社群媒體——抖音和微信的行政命令。隨後美國商務部也宣布將這 2 項服務從美國 apps 商店下架，但禁令遭到數個地方法院基於言論自由考量而阻擋實施。不過，拜登同時也指示商務部，評估和敵國（foreign adversary）有關的 apps（指由敵國所持有、控制或管理的 apps）是否有潛在的國安風險及侵犯用戶隱私的疑慮。

- **拜登撤銷川普《防止線上審查》行政命令，但改革 CDA 第 230 條提案不止**

  拜登總統於 2021 年 5 月撤銷前總統川普的《防止線上審查》（Preventing Online Censorship）行政命令，此命令旨在刪除《通信端正法》（CDA）第 230 條對中介機構的免責保護傘，並指稱「社群媒體故意審查保守派的觀點，導致政治偏見」。但紐約大學 2021 年 2 月的研究結果認為「聲稱反對保守派的本身，就是一種沒有可靠證據的假訊息」，部分公民團體和產學界人士也批評此行政命令危害言論自由。自 2021 年 1 月起，至少有 9 項改革 CDA 第 230 條的法案提交至國會。

- **川普因煽動暴力而遭社群媒體停權，但社群媒體的審查權力亦引發質疑**

  美國 2020 年的網路內容充斥和 11 月總統大選相關的假訊息、陰謀論，以及誤導性和煽動性言論，包括前總統川普也對其支持者發布煽動性貼文，並直接導致 2021 年 1 月 6 日的國會大廈暴力攻擊事件。Twitter、Facebook、Instagram、Reddit、Snapchat 等社群媒體因此紛紛暫停或永久禁止川普的帳號，並表示他們是行使受《憲法》保護的權利來制定和執行平臺政策，進而刪除違反其政策的內容和帳號。不過，有關社群媒體執行服務條款的透明度、內容審核的標準、演算法的公平客觀性等問題，都引發強烈質疑。

- **政府加強監控種族不公抗議活動，破壞使用數位科技進行集會結社的自由**

  2020 年 5 月發生非裔男子遭白人警察壓頸致死案後，美國民眾經常透過社群媒體組織種族不公的抗議活動。雖然美國對於個人運用數位工具組織或動員公民活動，沒有法規限制，但政府卻加強對社群媒體和通訊平臺的監控（例如：地方執法人員沒收抗議民眾的電子設備並讀取私人訊息），甚至還有騷擾和恐嚇行為（例如：聯邦調查局特務對 1 名在 Twitter 玩笑自稱是地方抗議活動領導者的民眾和其母親進行盤查）。執法單位的這些行動導致民眾對於發布抗議活動相關訊息的寒蟬效應，而且也侵犯人們使用數位科技進行集會結社的自由。

•美國缺乏強力的聯邦資料保護法，川普政府偷查記者通聯紀錄遭揭發

2021 年 5 月至 6 月媒體接連報導川普時期的司法部，於進行政府資訊外洩的調查時，秘密獲取記者、政界人士和其家人的通聯紀錄，引發大眾強烈反彈。隨後司法部宣布不再秘密蒐集記者的紀錄，還有議員提出《保護記者免於國家過度壓迫法案》（Protect Reporters from Excessive State Suppression Act）。整體而言，美國的私人企業或公部門對於資料使用幾乎沒有受到法律限制。ISP 和內容託管商會大量蒐集用戶的網路活動、通訊和喜好等資料，政府也會請求索取這些資料，但通常是透過傳票、法院命令或搜查令。美國缺乏強力的聯邦資料保護法，目前大多數的資料隱私立法都是在州或地方層級，2020 年至少有 30 個州考慮制定隱私相關法案。

•美國持續受到網路攻擊威脅

美國於 2020 年 12 月發現堪稱近年規模最大、手法最複雜的網路攻擊事件。知名資訊科技公司 SolarWinds 被俄羅斯政府支持的駭客入侵，以作為滲透到美國聯邦政府機構、民間企業、智庫和公民組織系統的工具，該公司的軟體更新已被 1 萬 8 千多名客戶安裝，拜登政府因此於 2021 年 4 月對俄羅斯實施制裁。隨後於 2021 年 5 月又發生重大網路攻擊事件，疑似由俄羅斯支持的駭客，對美國最大燃油管線業者之一的「殖民管線」（Colonial Pipeline）公司，進行勒索軟體攻擊，導致美國東岸的燃料供應中斷。此次拜登總統發布行政命令以強化聯邦政府的資訊安全網絡（network）。此外，美國聯邦政府也於 2021 年 3 月揭露美國公私部門受來自中國大陸政府的 3 萬多起網路攻擊。

第六節 結論與建議

一、結論

(一) 報告以具體數字驗證治理觀念轉變及國家強化網路監管成為全球常態

《2021 網路自由度報告》以具體數字，也就是過去一年來有 48 國（占調查國家的近 7 成）祭出新規監管科技公司，驗證近來平臺責任觀念轉變的說法。正如報告所述，過去全球對於網路規範的態度是由美國主導，傾向讓科技產業自由發展，但卻導致各種網路危害和濫用行為層出不窮，且業者的自律機制顯然無法解決問題，於是各國政府開始轉為強化監管網路，並成為全球常態。惟在缺乏以網路自由開放作為共同願景下，各國政府監管數位領域是各行其是。

(二) 歐盟第三種監管方式及我國政策獲肯定，可為全球網路自由帶來希望

承上述的治理觀念轉變，身為人權團體的自由之家也有條件的認同政府監管措施。例如：報告認為「在民主堅強的國家中，精心設計的平臺規範或可減輕線上危害，同時加強透明度和問責制」。此外，報告也肯定歐盟著重透明度和正當程序的「第三種」網路監管方式，並認為我國《網際網路視聽服務法》草案（雖然通傳會已表示暫緩推動）也具同樣精神，而且還讚揚包含我國在內的排名前 5 名國家，為下滑的全球網路自由帶來希望。惟報告也提出警語，類似的法規會遭到獨裁者濫用於監控或打壓人民，甚至連民主國家都可能採用過於廣泛的審查和資料蒐集要求，以致全球言論自由和數位人權陷於空前的危機。

(三) 報告呈現全球趨勢並評比各國政策，可作為檢視施政和研究索引的工具

自由之家的全球網路自由度研究計畫已經持續進行 10 餘年，且研究結果經常獲得國際各大媒體的報導。《2021 網路自由度報告》更是由美國政府和荷蘭政府等單位贊助，且動員全球超過 80 位研究人員才得以完成。因此，報告可謂具有相當的可信度和品質。再就報告的內容而言，除了包括

全球和各國的網路自由度評比結果外，還針對評比的21項指標介紹過去一年來該國的相關政策或法規。因此，未來可將每年一度的報告作為了解全球網路規範趨勢、檢視我國的施政成效，以及檢索各國政策或法規案例的工具。

二、建議事項

(一) 立即可行之建議

1. 與指揮中心分享國際正反案例，促進我國檢討改善防疫資料的使用

《2021 網路自由度報告》指出，各國普遍沒有防止疫情資料遭到濫用的措施，新加坡的執法單位、澳洲的情報機關等，都坦承可從國家 COVID-19 疫情追蹤 apps，取得民眾個資。不過，加拿大政府已經終止行政和執法部門及醫療單位等機構，共享個資；亞美尼亞政府更是停止從電信公司蒐集追蹤接觸者的資料。我國在報告中得分較低的項目，包括被認為疫情資料的蒐集使用缺乏合法性和比例原則，當中也提及通傳會為了「簡訊實聯制」疑似遭用於警方辦案而出面澄清等事件。正如加拿大隱私專員辦公室（OPC）強調疫情期間需要提高隱私保護，我國也應研議和檢討改善相關法規和措施，通傳會可從作為電信事業主管機關和負責推動我國網路治理符合國際潮流之業務角度，藉由分享上述國家案例和我國得分，讓防疫決策最高機關——中央流行疫情指揮中心了解國際上的不同見解與做法。

2. 於國際會議分享我國普及上網成果和打擊假訊息經驗

我國於《2021 網路自由度報告》的網路連線類別幾乎得到滿分。報告形容我國提供有意義且負擔得起的網路連線、沒有顯著的數位落差、政府致力將行動服務升級為 4G 和 5G、民眾亦可自由選擇網路服務供應商。由此顯示，通傳會所推動的數位基礎建設及縮短偏鄉數位落差、電信法規鬆綁及電信批發價格管理等措施，值得提供給其他國家參考。此外，報告也讚揚我國的公私部門以創新工具打擊假訊息，通傳會作為抑制假訊息散播的「抑假」統籌機關 [21]，並與社群平臺合作即時處理假訊息，亦可將相關措施分享給國際社會。至於分享的場合，主要可透過主動申辦 APrIGF 的

[21] 參考資料來源：行政院「2019 防制假訊息政策簡介」。

座談會議。此外，適逢歐洲議會「外國勢力干預歐盟民主程序（含假訊息）特別委員會」專程於 11 月初訪臺，並表示要將臺灣經驗帶回歐洲，或許未來我國也有機會受邀於 EuroDIG 擔任講者，分享我國的對抗假訊息政策。

3. 研析德國監管擴及影音平臺、美國 CDA 修正提案、DNS 處理違法內容

根據《2021 網路自由度報告》，德國《網路執法法案》近期實施的修正案已將適用範圍擴及影音平臺；以打擊假訊息為立法宗旨之一的《國家媒體協定》也將監管範圍從無線電廣播擴及新型媒體，並規定平均收視超過 2 萬次的媒體創作者（如：YouTuber）須申請執照等。上述法規及其可能造成的內容審查等問題，或可供通傳會參考。當然，涉及平臺對於第三方內容是否免責的美國 CDA 第 230 條修正案，也需掌握其立法進展。報告指出，今年（2021）以來至少有 9 項改革案提交國會，而當中較佳的是著重透明度和正當程序的《平臺問責制和消費者透明度法》草案。

此外，從 DNS 處理非法內容的問題亦值得研析。加拿大發生法院對 ISP 的侵權網站封鎖令，被業者基於維護言論自由而上訴至最高法院的案例；但德國卻是 ISP 聯合娛樂產業推動從 DNS 封鎖侵權網站，並帶來法外限制通訊自由的隱憂；而歐洲國家頂級域名註冊管理機構委員會（CENTR）於 RIPE 82 會議則主張應該從內容層而非 DNS 處理內容問題；英國通訊管理局（OFCOM）網路技術官員於 EuroDIG 2021 表示，以 DNS 阻斷產生不符合比例原則的問題。我國曾於 2019 年封鎖宣傳中國大陸惠臺措施的 www.31t.tw 網站，且據報載通傳會也考慮從「網路層措施防制假訊息擴張」（楊綿傑，2020），因此，相關的國際案例、倡議和討論，可供通傳會作為參考。

(二) 中長期建議

1. 持續推動透明開放的治理政策，以利人民數位福祉及提升國際聲譽

我國首度被納入全球網路自由度評比即獲得全球第 5 名的殊榮，是多

年來包含政府在內的多方利害關係人共同努力的成果，除了讓國人得以享有全球最自由行列的數位環境和其帶來的數位福祉外，此番成果還獲得國際媒體的主動宣傳。例如：美國之音、自由亞洲電臺、印度時報等媒體皆以「臺灣網路自由度高居全球第五」為題，報導全球的評比結果；美國 CNN 電視「全球公共廣場」（Global Public Square）節目也指出「臺灣網路自由度超越德、美等民主國家」；美國時事雜誌外交家（The Diplomat）更是報導「中國大陸和臺灣的網路自由度是天壤之別」（Cook & Funk, 2021）。

為此，推動透明且開放的網路治理政策，是我國須持續努力的工作，並可參考**《2021 網路自由度報告》提出的 5 個優良網路法規要素，包括：依企業的類型和規模量身制定義務；要求業者對於內容審核、資料使用、廣告業務須有透明度；對於第三方內容應有強力的中介機構安全港保護條款；確保正當程序和申訴管道的暢通；強韌的加密和隱私標準。**

此外，外交家雜誌在前述所指報導提到一個問題——我國某些法律對於誹謗和散播假訊息的處罰過重（亦為自由度報告中得分較低項目），且易被執法機關濫用，即使最終被獨立的司法機關駁回，但可能已經造成傷害；值得我國省思。或許通傳會可從《數位通訊傳播法》的內容規範介接其他部會，以及罰則等項目，推動相關法規的檢討與修正。

參考文獻

- VOA 美國之音 (2021)。互聯網自由度排名中國連續七年墊底台灣全球第五。https://www.voachinese.com/a/freedom-of-the-net-report-20210921/6236898.html
- 黃有容 (2021)。「數位通傳法」立法歷時多年 NCC 盼年底提新草案。聯合新聞網，2021/9/30。https://udn.com/news/story/7314/5783539
- 葉志良 (2021)。娛樂前哨站 OTT 數位浪潮。臺北產經，2021/4/21。https://www.taipeiecon.taipei/article_cont.aspx?MmmID=1201&MSid=1071501505364212011
- CNN (2021). Global Public Square. https://edition.cnn.com/videos/tv/2021/09/26/gps-0926-taiwan-china-democracy.cnn
- Congress.gov (2021). https://www.congress.gov/bill/117th-congress/senate-bill/797/text
- Cook, S. & Funk, A. (2021). On Internet Freedom, China and Taiwan Are Worlds Apart. The Diplomat, 2021/10/12. https://thediplomat.com/2021/10/on-internet-freedom-china-and-taiwan-are-worlds-apart/
- Freedom House (2021 a). Freedom on the Net 2021: The Global Drive to Control Big Tech. https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech
- Freedom House (2021 b). Freedom on the Net 2021: Country Report. https://freedomhouse.org/countries/freedom-net/scores?sort=desc&order=Total%20Score%20and%20Status
- Mcphail, B. (2021). Bill C-11 was the gift that needed returning. The Hill

Times, 2021/10/27.
https://www.hilltimes.com/2021/10/27/bill-c-11-was-the-gift-that-needed-returning/324436

- PIPEDA (2021). Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta.
https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

- The White House (2021). Remarks by President Biden on the Bipartisan Infrastructure Law. 2021/11/16.
https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/11/16/remarks-by-president-biden-on-the-bipartisan-infrastructure-law/

- Tremblay, A. (2021). TekSavvy to appeal Supreme Court over landmark website-blocking order. MobileSyrup, 2021/8/26.
https://mobilesyrup.com/2021/08/26/teksavvy-to-appeal-supreme-court-over-landmark-website-blocking-order/

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，於南部、北部及東部大專校園共辦理 3 場次、各 2 小時、且出席人數達 50 人以上的網路治理講座（參閱表 6-1），藉以讓更多大專青年對網路治理產生興趣，並了解網路治理攸關所有網路使用者的權益，進而願意關心並參與網路治理的議題討論。宣講場合則於特定課程，或整個系所的固定集會活動，且系所橫跨文科與理科，出席者涵蓋大學生與研究生。

表 6-1 大專校園講座辦理總表

場次	時間	學校	系所 / 活動名稱	講題與講者	人數
1	5/13（四） 13:30～15:30	成功大學（南部）	成大電機研究所及電腦與通訊研究所碩士班	網路治理的源頭與數位主權的爭議 吳國維／NII 董事	135
2	10/12（二） 19:00～21:00	陽明交通大學新竹光復校區（北部）	科技法律學院	網路治理：數位主權是否真實 吳國維／NII 董事	54 人，另計線上人數 60 人
3	10/25（一） 10:00～12:00	東華大學（東部）	法律學系	公私協力還是國際政治角力？談全球網路治理在國際主權理論下的美麗與哀愁 蔡志宏／臺北士林地方法院 庭長	74

第二節 成功大學場次

一、活動訊息

- 系所：成大電機研究所、成大電腦與通訊研究所。
- 場合：專題討論課程。
- 時間：110 年 5 月 13 日（四）13:30～15:30。
- 地點：成大電機系地下一樓，迅慧講堂。
- 人數：135 人。
- 講題：網路治理的源頭與數位主權的爭議。
- 講師：吳國維／NII 產業發展協進會董事。

二、演講內容摘要

（一）網路龍頭的壟斷議題

講者首先從「壟斷」的議題談起，對於美國幾家科技巨頭稱霸於網路世界，歐盟嘗試用壟斷法來提告，然而，壟斷有其定義，例如：網站的普及率必須達到多廣，否則難以認定其具備壟斷之事實，再加上這些科技巨頭多有龐大的律師團撐腰，要控告他們壟斷並非易事。

再以澳洲國會前陣子通過的「新聞媒體議價法」為例，這個案例的起因，是澳洲的公平交易委員會，提告 Google 與 Facebook 壟斷。講者提醒聽眾留意，「廣告」的形式有許多種，但在這個案例當中，澳洲特別強調「網路」廣告，所以在談壟斷時，清楚定義範疇相當重要。在網路世界裡，若要處理這類網路治理的議題，就必須透過大家的協作。

（二）IETF 對 Google DNS 的看法

關於技術面的網路治理議題，講者以 DNS 8.8.8.8 為例，這是 Google 提供的 DNS 伺服器，其可攔截傳統的 DNS 解析功能，轉為在 Google 的系統裡解析，最高的處理流量甚至可以達到網路整體流量的三分之一。然而，IETF（Internet Engineering Task Force，網際網路工程任務組）指控 Google 的此項服務可說是一種駭客行為，因為其從中阻斷 IETF 訂出的 DNS 解析程序，這個議題在技術圈也討論了大約五年的時間。

很多政府認為網路衍生出許多傳統的政治及法律無法解決的爭議，所以在國際會議上，常會指責 IETF 創造出網路。對此，IETF 的前主管 Leslie Daigle 回應：創造網路之目的，是為了要讓世界平面化，不需要再有國界的限制。大約從 2016 年開始，國際間陸續有人建議各國在網路上是否應該要有自己的國界，定義出法律的管轄權；長期投入網路治理的喬治亞理工學院 Milton Mueller 教授對此表示不予認同，他認為透過 IP 與 domain

name，世界就是一個平面，沒有國界。

（三）網路的運作及 RIR 爭議

任何設備連上網路，都必須要有 IP 位址，並找到 DNS 解析器，一般使用者並不會關心如何申請 IP 位址，因為手機業者都已經設定好了，其後端的 DNS 就會幫使用者進行解析。在臺灣，電信公司的 IP 來源有兩種，一種是向我國的「台灣網路資訊中心」（TWNIC）申請，另一種是直接向亞太地區的區域網際網路註冊機構（Regional Internet Registry, RIR）APNIC 申請。

然而許多政府對此無法接受，他們認為全球的五個 RIR 只是一個組織，為何必須向他們申請 IP，不像電話號碼是到聯合國的 ITU（International Telecommunication Union，國際電信聯盟）協調。印度政府就曾經派出大法官控告 APNIC 的行為違法，但為時已晚，因為全世界 80%以上的國家認知到 IP 位址是來自於 RIR 時，已經是在西元 2000 年之後，網路已成為重要的商業行為與人類溝通的工具。然而，網路一開始的根源就是標準的公共財，並且在大家還未認知其重要性之前，就已經被設定好運作結構。

談完 IP，講者接續向聽眾介紹 domain name。在 domain name 還沒設計出來之前，使用者要前往任何網站必須記住其 IP 位址，但這對於人腦記憶太過困難，於是美國南加州大學的學者 Jon Postel 提出用 ASCII 碼取代 IP 位址。所有 DNS 都必須到根伺服器（root server）做解析，目前全球只有 13 臺 root server，且大多數都設在美國，後來全球各地也紛紛設立了鏡像伺服器，目前全球已有超過 1 千臺。

（四）美國早預告當前網路治理問題

談到網路治理，Ira C. Magaziner 是不可不知的代表性人物，其曾任美國白宮的首席科技顧問，Magaziner 提到，網路必須人性化，帶領人類走向自由民主的陣營，同時考量到政治上的外交。然而，中國認為網路對於政

權的穩定具有危險，於是啟動金盾計畫，並在 1998 年建立網路長城，對抗美國網路的入侵。

Magaziner 也提到，數位轉型的過程中或許會有許多負面的影響，我們要儘量擴大它的好處，降低它的負面影響。Magaziner 所做的努力包括拜訪許多國家，徵詢國際間的支持，希望能建立一個 IP、domain name 與 root server 的全球共管機制，同時這個組織必須透明且技術中立。

演講最末，講者向聽眾介紹 Magaziner 在當時就曾提出未來在網路上可能發生的一些問題，包括：關稅及稅制、隱私、內容管制、數位簽章及驗證、版權、網路的管理、加密，以及電信自由化。時至今日，Magaziner 定義出的這些問題，有些已經獲得解決，有些雖然還沒，但已成為網路治理領域中應當持續探討的議題。

三、活動剪影

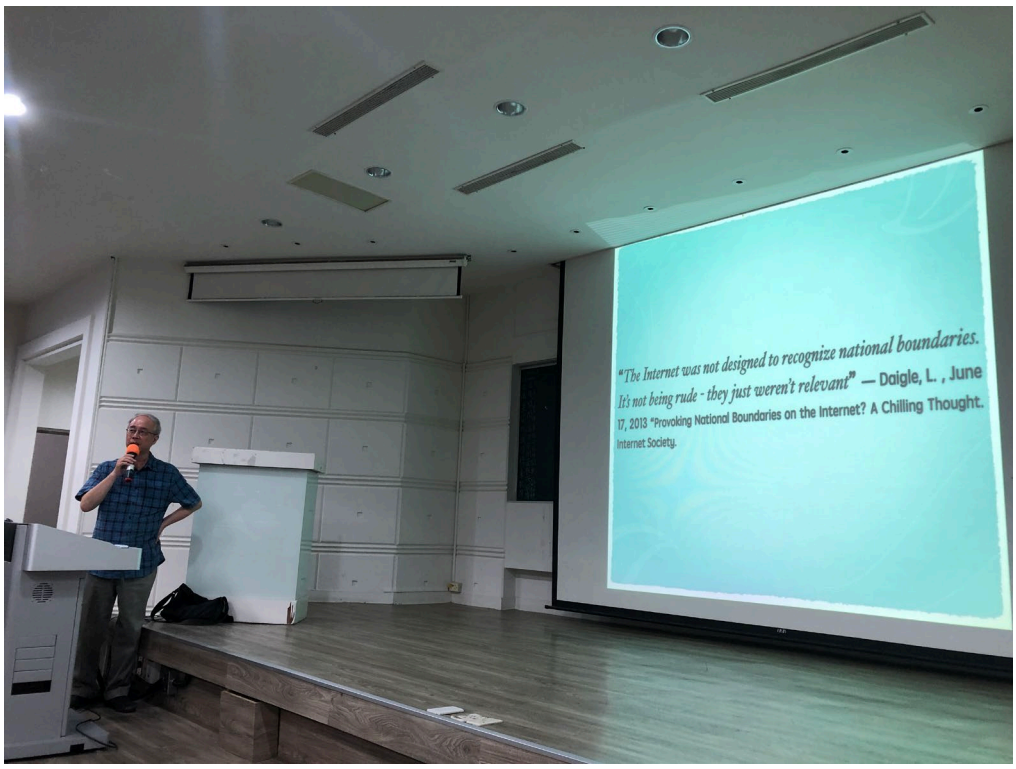


圖 6-1　成功大學講座照片

第三節 陽明交通大學場次

一、活動訊息

- 系所：科技法律學院。
- 場合：專題演講。
- 時間：110 年 10 月 12 日（二）19:00～21:00。
- 地點：新竹光復校區交大浩然圖書館，B1 國際會議廳。
- 人數：54 人，另計線上參與 60 人。
- 講題：網路治理：數位主權是否真實。
- 講師：吳國維／NII 產業發展協進會董事。

二、演講內容摘要

（一）主權的概念

講者首先開宗明義表示：只有專制獨裁政權才會對資訊公開透明、並與人民共享制定網路公共政策的權力感到畏懼。雖然一般人民多數不會積極參與政策制定，但不表示沒有權利參與。

1648 年的西發里亞條約（Peace of Westphalia）是歷史上首次提出主權的概念，其中的 4 項重要原則包括：在國家的領土範圍內，國家具有獨一無二的權利；參加國際組織時，各國不論大小均為一國一票；外交大使在他國國土享有豁免權；主權有神聖不可侵犯的權利，國家內政不受他國干涉。時至今日，主權概念早已今非昔比，然而部分專制獨裁的國家卻依然堅持 1648 年的主權概念。

網路治理的歷史可以追溯至 1986 年，其中多少會碰觸到數位主權的議題，主要在於網路的基礎架構包括 IP、Domain Name 及 Root Server 係為全球互通的單一系統，形同公共財，以 IP 的取得為例，我國必須向 APNIC 申請，但為何政府組織必須向一個非營利組織申請，而不是向 ITU 或聯合國之類的國際組織申請？這就是一項敏感的主權議題。

（二）美國的數位主權觀點

美國在柯林頓總統時期，委請白宮首席科技顧問 Ira Magaziner 規劃一份未來 100 年全球的電子商務結構，因內容涉及全球，自然會碰觸到許多數位主權的議題。Ira Magaziner 首先提到，我們必須儘量注意到人類的自由（human freedom），並且鼓勵市場競爭，讓網路使用者具有自主選擇的權利。

芝加哥學院的 Lawrence Lessig 在其著作《Code and Other Laws of Cyberspace》提到，社會的秩序是由法律、規範、市場及架構（Law、Norms、Market、Architecture）相互制衡。Ira Magaziner 認為，應該讓網路上的社群

自己選擇規範的方法，制定法規的權利屬於社群，而不是政府，當時他也提出了多方利害關係人（Multi-Stakeholder）的治理機制，政府必須與這些利害關係人共享權利。

Ira Magaziner 表示，網路科技的發展日新月異，相對於此，政府的動作太過緩慢及官僚，這對於網路的發展是障礙而非助益，因此，採取多方利害關係人的治理模式較具彈性，且適合網路的發展。

（三）聯合國有關數位主權的討論

2005 年聯合國發布了 WGIG（Working Group on Internet Governance）報告，奠基聯合國對於網路治理的定義，報告中提到，應開創聯合國討論國際共識的形式，這是聯合國首次提出討論國際共識時，政府與非政府組織應該共同參與。

當時聯合國的討論聚焦在 ICANN 組織的歸屬，因為 ICANN 負責管理網路基礎架構，所幸在美國的堅持之下，ICANN 得以保持非營利組織的多方利害關係人治理模式。該報告中也定義了政府、產業、公民社會及技術社群在討論網路治理公共議題時，所各自扮演的角色及功能。

（四）國際學者專家對於數位主權的觀點

國際法學者 Rolf Weber 在《New Sovereignty Concept in the Age of Internet》文章開頭便提到 1648 年的主權概念，強調擁有主權不代表可以為所欲為，例如：人權。公共利益分為許多不同的層次，每個層次的利益也不同，為了達到世界的和平，我們需要尋求全球的公共利益，並且產出的政策必須是對全球都有好處的。主權唯一論顯然違背全球公共利益，因此應具備機制避免政府濫用主權。

Rolf Weber 表示，一個新的世界應該由大家用一個鬆散的主權概念來共同決定全球公共利益，也可採用多方利害關係人治理模式的架構。討論網

路治理時，要把非政府組織納入，Rolf Weber 在通篇文章中告訴讀者，在網路空間有些時候可以談論主權，但有些時候必須放棄主權，從全球利益的角度來討論治理模式。

其他學者專家提出的觀點，例如：瑞士蘇黎世大學的 William J. Drake 教授表示，擁有主權不代表可以為所欲為；喬治亞理工學院的 Milton Mueller 教授亦提過，全球網路空間與領土主權是不相容的，無論是中國、美國或歐洲，都無法創造「數位主權」，除非他們願意完全脫離彼此的聯繫。

（五）中國的數位主權觀點

在 2019 年世界互聯網大會中，由中國現代國際關係研究所、上海社會科學院及武漢大學共同發表的《網路主權：理論與實戰》報告，主張網路主權應依循《聯合國憲章》的框架，但他們忽略了該憲章訂於 1945 年，至今已有多少經過共識決的改變，也選擇性忽略了 WGIG 報告強調非政府組織參與及多方利害關係人治理模式的重要性。

（六）歐洲的數位主權觀點

在引導聽眾閱讀《Digital sovereignty for Europe》報告之前，講者首先請大家檢視 Alexa 網站上全球以及各個國家 500 大網站的排序，可以發現其中名列前茅的幾乎都是美國、中國與少數日本的網站，完全沒有歐洲的網站。

歐盟發現歐洲政府使用的都是美國或中國的雲端服務，此外，不管是從 5G 或 AI 角度來看，歐洲也無法與他國對抗，因此整份報告都環繞在談論雲端服務、5G、AI 以及 IoT 的議題。講者提醒大家在閱讀報告時要特別去思考，這當中的論點是否代表歐盟所有會員國的意見？或是僅為少數國家的聲音？

歐盟強調，歐洲在技術面雖然無法與美國或中國並駕齊驅，但在制定

法規(包括 GDPR 及數位市場法等)方面卻是獨步全球。但講者認為,GDPR 實施後，五大科技巨頭在歐洲的營收並沒有減少，反倒是歐洲的中小企業收入下降，主要原因為導入 GDPR 複雜且昂貴，中小企業乾脆轉為透過五大巨頭行銷。講者表示，任何政策都會有人受益或受害，如果無法理性評估，就無法知道政策是否正確。

該報告中提到資安、資料控管以及網路平臺的行為規範，首先定義出哪些資料不可外流，或是應有必要的管制。報告中主要的三項訴求包括：建立歐洲的資料框架（data framework)、建構可信賴的網路環境、實施競爭與監管法規。

整體而言，歐洲的數位主權觀點著重在如何於未來的數位市場中爭取歐洲的競爭力，避免被淘汰，即使想把資料留在歐洲，也必須透過市場競爭與科技進步的原則，而不是透過強硬的主權概念。

（七）結語

演講最末，講者請聽眾試著思考，站在臺灣的立場，若有機會向國際宣揚我國的數位主權，我們的態度為何？是要像美國、中國，或是歐洲呢？不論我們看到的是哪一個國家對於主權的定義，最後都要回歸到臺灣本身的利益來思考，同時也要注意到，你的利益必須設法與全球其他國家及國際的利益共通並達到平衡，能夠在說服他人的同時，合理爭取到我國的最大利益。

（八）問與答

現場學生提問：Ira Magaziner 在某次的訪問中曾提到，雖然 ICANN 積極避免官僚文化介入網路世界的運作，但隨著 ICANN 組織的壯大，產生內部官僚化的可能性，現在的 ICANN 是否會演變為這樣的狀況？

講者回答：Ira Magaziner 表示 ICANN 最大的問題是沒有透過國際間的

投票或公約賦予的公權力，若有人違反 ICANN 的規則，ICANN 必須回到美國的實體法院處理，因此引發爭議，後來 ICANN 增加開放了新加坡或瑞士法院的選擇。

關於 ICANN 如何讓大家信賴，大家可以參考 ICANN 的章程，其中透過三個機制維持 ICANN 的當責性（accountability），並且可以被究責。第一，ICANN 所有政策都是由下而上（bottom up）形成，不能僅由董事會決定；第二是透明度（transparency），ICANN 所有政策在正式實施之前都必須先在網路上公告，若無強烈抗議，才能進入執行階段；第三為共識決（consensus）。ICANN 的 PDP（Policy Development Procedure）就是依照這些原則進行，在政策發展的過程中如果沒有依照 PDP，任何人都可以否定這項政策。

除了上面三個機制之外，根據 ICANN 董事會的規範，任何一洲都不能超過一定比例的席次，相對就比較不會有官僚化的問題，但這卻會衍生另一個問題，因為任何程序都必須符合上面的三個原則，作業速度就會變慢，因此政策發展的時間會比較長，例如：new gTLD 就花了很長的時間才完成。

三、活動剪影

圖 6-2　陽明交通大學講座照片

第四節東華大學場次

一、活動訊息

- 系所：法律學系。
- 場合：專題演講。
- 時間：110 年 10 月 25 日（一）10:00～12:00。
- 地點：人社一館，第二講堂。
- 人數：74 人。
- 講題：公私協力還是國際政治角力？談全球網路治理在國際主權理論下的美麗與哀愁。
- 講師：蔡志宏／臺北士林地方法院庭長。

二、演講內容摘要

（一）何謂全球網路治理？

「全球網路治理」泛指在全球範圍內對於一切涉及網路事務之資源分配，乃至社會、經濟活動的協調與控制，特別是關鍵網路資源（Critical Internet Resource）——IP 位址（IP address）及域名（Domain Name）之管理、配置與維護。

講者展示了非營利組織 DiploFoundation（簡稱 Diplo）繪製的「網路治理地圖」（A map for a journey through internet governance），透過這張地圖，我們可以對於網路治理涵蓋的 7 個面向與相關的 40 多個議題彼此間的關聯性一目了然。

（二）ICANN 的多方利害關係人治理模式

ICANN（Internet Corporation for Assigned Names and Numbers，網際網路名稱與號碼支配機構）是一個非營利性法人，於 1998 年 9 月在美國加州成立，負責監督管理網際網路技術管理功能（Internet technical management functions）、通訊協定參數及通訊埠（Protocol Parameters and Port）之協調、域名系統（Domain Name System，DNS）之管理、IP 位址之分配暨指派，以及根伺服器系統（Root server system）之管理。

透過 ICANN 的架構圖，我們可以看出董事會係由來自不同社群的代表組成，這也是依據 ICANN 組織章程細則的規定，確保董事會成員來自 ICANN 的各個利害關係團體，同時兼顧全球五大地區及性別平衡等多元標準。講者目前也是 GNSO（Generic Names Supporting Organization，通用域名支援組織）中代表智慧財產權利害關係人組成的團體 IPC（Intellectual Property Constituency）成員之一。

（三）主權與公私協力

談到國際主權，必須從 1648 年的西發里亞條約（Peace of Westphalia）談起，這是歷史上首次提出主權的概念，其中提到：國家可以壟斷權力的行使、各國皆為平等，以及主權象徵反對干涉的權利等原則。根據這樣的傳統國際主權理論，在法理上如何能夠解釋全球網路治理現況：一個沒有公權力之非營利性法人卻主導了 IP 以及域名如此重要性之網路關鍵資源分配及其決策？如此國家如何能有壟斷權力行使？又如何反對外在干涉呢？

對於此一問題，講者提出了行政法上的「公私協力理論」來做說明。意指國家高權主體與私經濟主體本於自由意願，透過正式的公法或私法性質之雙方法律行為，或非正式的行政行為形塑合作關係，並且彼此為風險與責任分擔的行政執行模式。公私協力包括以下幾種類型：授權行使公權力、行政助手、業務委託、公司合資事業（組織型）、民間參與公共建設（計畫型），以及社會自主管理，主要奠基於效率原則、補充性原則，以及合作原則的法理基礎。

意即，ICANN 之所以能夠主導 IP 及域名的分配決策，其實是來自於各國基於自由意願，而與 ICANN 共同協力來治理網路空間。其公私協力之類型是屬於社會自主管理，也就是將有關 IP 及域名的分配決策，交由全球網路社群所形成的自治組織 ICANN 來進行自主管理。既然各國是基於自由意願來與 ICANN 共同協力，就不至於違反國家主權擁有最高壟斷性權力之國際主權理論。

（四）全球網路治理成果的絢爛與美麗

根據社群媒體管理平臺 HootSuite 在 2021 年 1 月所做的統計資料，目前全球人口數為 78.3 億，其中 52.2 億人（66.6%）擁有手機，46.6 億人（59.5%）會使用網路，42 億人（53.6%）屬於活躍的社群媒體使用者。在臺灣，上網的人口數高達 9 成，其中將近 95%是使用行動裝置上網，16-64 歲的上網人

口每天使用網路的時間達到 8 個小時，「網路」對人們而言，幾乎已是無法替代的生活必需品。

從另一個角度來看，根據.com 頂級域名（top-level domain）註冊管理機構 Verisign 的統計資料，截至 2021 年第二季為止，全球的域名註冊總量達到 3.67 億，全年成長量為 280 萬，成長率為 0.7%。若從 1985 年域名有史以來開始計算，平均每年可增加 100 萬個域名，可見域名市場 30 幾年來始終維持穩定的成長。

講者接續介紹了網路號碼分配機構（Internet Assigned Numbers Authority，IANA）從美國商務部移轉至 ICANN 的歷史背景，並以.ir（伊朗）等國家的國碼頂級域名（country code top-level domain，ccTLD）遭到債權人聲請強制執行以抵償債務卻遭駁回的案例，用以說明網路治理在發展過程中，是如何受到主權國家——美國的呵護與扶持。

相對而言，1999 年獲得 ICANN 理事會認可施行的統一爭議解決政策（Uniform Dispute Resolution Policy，UDRP）則可說是一份網路治理世界與主權國家之間的權力界限文件。UDRP 是解決涉嫌域名濫用註冊爭議的一種政策，允許商標持有人透過經認證的爭議解決服務供應商提出投訴，並啟動快速行政流程。UDRP 充分向主權國家展現域名國度的自我管理能力，不僅承認主權國家所保護之商標，也象徵網路世界承認主權國家的司法管轄權。

（五）全球網路治理的那抹哀愁

由於網際網路空間一開始的發展就希望能夠保持最大的自由發展空間，這也使得網際網路與主權國家存在著緊張關係，而抹上幾許哀愁。電子前哨基金會（Electronic Frontier Foundation）創始人 John Perry Bar 在 1996 年提出「網路獨立宣言」時，便提到：網路空間是心靈的新家園，不歡迎工業世界的打擾，網路空間並不位於你的邊界內，不要以為你可以建造它；

強烈表達出網路世界不應受到國家主權干預的立場。

網際網路協會（Internet Society，ISOC）更繼而於 1997 年結合數個國際組織，以「國際網域名稱分配特設委員會」（International Ad Hoc Committee，IAHC）名義提出「國際域名註冊服務之自我規範架構」（Generic Top Level Domain Memorandum of Understanding，gTLD-MoU），以國際電信聯盟（International Telecommunication Union，ITU）秘書處為備忘錄存放機構，同時設立政策諮詢委員會、政策監管委員會、受理註冊機構會議，以及域名行政救濟專門小組，然而這項架構最終因為美國政府不同意而宣告失敗。

中國學者黃志雄在其著作《網路主權論－法理、政策與實踐》更指出：無論是依據國家管轄權之領土原則，或是效果原則，網路空間始終在國家主權所及之範圍內。2011 年，中國、俄羅斯等上海合作國際組織，向聯合國提交「信息安全國際行為準則」，重申與網路相關的公共政策問題屬於各國主權。網路霸權是地理霸權的網路空間投射，以美國為代表的網路中心國家透過技術上的網路管理權、網路規則的制定權及話語權，以及軍事上的制網權（對網路的控制權），獲取左右網路空間的強大力量。

除了以上案例之外，.cat 頂級域名註冊管理機構也曾因加泰隆尼亞獨立公投事件，於 2017 年間面臨來自西班牙政府直接以軍警實體查抄接管的嚴重威脅。凡此種種，皆為全球網路治理在整個發展過程中，面對主權國家所遭遇的糾葛與哀愁。

（六）邁向更複雜的全球網路治理未來

隨著全球網際網路規模的不斷發展擴大，全球網路治理也就面臨更為困難複雜的治理問題。ICANN 最近一輪開放新通用頂級域名（new generic top-level domain，new gTLD）申請，美國亞馬遜公司申請.amazon 頂級域名所引發的事例，即為明證。

本案雖經頂級域名爭議之專家小組認定美國亞馬遜公司勝訴，ICANN負擔爭議程序及專家小組報酬等高額費用，並將該頂級域名授權發交美國亞馬遜公司營運，但在南美洲的亞馬遜河流域國家聯盟（Amazon Cooperation Treaty Organization）隨即控訴此項決定並不具正當性。這樣的過程與結果，到底要認為是全球網路治理社群戰勝主權國家的美麗，還是網路發展後進國家民眾在面對全球網路治理的哀愁，實在難以斷言。其所涉問題的複雜程度，由此可見一斑。

值得一提的是，曾有國際關係學者（Daniel Drezner）指出：當大國之間存在相當程度的共同利益時，小國的偏好會決定大國的策略。小國集體反對大國間的協議時，大國會傾向透過俱樂部式、具有強制力的國際組織（例如：經濟合作發展組織）進行國際管制；當各國間的偏好差異程度微不足道時，大國會傾向採取具有普遍性會員的國際組織（例如：聯合國），以強化所形成國際管制規範的合法性。

或許就是因為全球網路空間的發展，在國際間還存在許多差異，也就在彼此的政治角力下，全球網路治理才以現有模式（私部門領導、多方利害關係人共同參與）存在直至今日。未來，全球網路治理還會如何發展，就讓我們繼續看下去！

三、活動剪影

圖 6-3　東華大學講座照片

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

疫苗護照和 AI 等科技應用如何兼顧數位時代的人權保護？網路及社群平臺對於新聞生態、言論自由和內容秩序該承擔什麼公共責任？又富可敵國但提供免費服務的科技巨頭應被課徵數位稅並強制分拆嗎？以及當國家遭到重大網路攻擊時可以主動進行反擊嗎？如果您關心這些網路政策議題，歡迎報名「2021 網路治理研習營」免費課程活動，除了帶您探討當前重要的網路治理議題外，還有機會贏得多項獎學金！

新冠肺炎疫情讓全球見證網路對當今社會的至關重要。然而，就在網路科技協助我們建立疫情社會「新常態」的同時，卻也衍生侵犯人權、破壞安全、製造社會衝突等新型態的濫用行為，這些問題唯有透過所有多方利害關係人（multi-stakeholder）的溝通對話，才能找到最佳治理方案。

不論您是來自政府部門、民間企業、學研單位、公民團體，或是仍在大專院校就學，如何因應數位變革所帶來的契機與挑戰，需要您的積極參與。「2021 網路治理研習營」為一日免費研習活動，透過專題講習、案例探討、分組演練等方式，帶您認識數位人權、數位經濟、媒體與內容、網路安全等重要議題，以及如何參與這些議題的政策討論。全程參與之學員將有機會贏得新臺幣 1,500 元~6,500 元整獎學金（公務人員除外）。

- 名稱：2021 網路治理研習營。
- 時間：110 年 8 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（8 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：數位主權、網路內容與平臺、網路人權、網路安全、數位經濟，課程最末，也邀請到來自香港的 NetMission（網域使命青年使者計畫）成員，向學員介紹今年的 APrIGF 活動，並分享青年國際參與之經驗。

表 7-1　課前自我預習教材

8/5（四）前	課前預習
1. 影片	● 網路治理發展史 ● 網路安全與基礎建設 ● 網路人權 ● 網路內容與平臺
2. 文章	● What is Internet governance ● Internet Governance Outlook 2021: Digital Cacaphony in a Splintering Cyberspac ● Vint Cerf: Why everyone has a role in internet safety
3. 線上測驗	共 5 道選擇題，網址將以 email 通知錄取學員。

表 7-2　研習營課程表

8/7（六）	項目	課程	講者/主持人
08:30 - 08:45	線上報到		
08:45 - 09:45	專題講習	國際焦點：科技戰與數位主權	吳國維／NII 協進會董事
09:50 - 10:30	案例探討	新聞有價是國際趨勢？	胡元輝／中正大學傳播學系教授 陳奕儒／Facebook 臺灣公共政策經理
10:40 - 11:20	專題講習	內容亂象誰負責？	曾更瑩／理律法律事務所合夥律師 陳奕儒／Facebook 臺灣公共政策經理
11:30 - 12:10	案例探討	數位人權：防疫、AI 和 eID	賈文宇／台灣人權促進會執行委員
12:10 - 13:10	午休		
13:10 - 13:50	專題講習	網路安全：從資安到國安議題	黃勝雄／台灣網路資訊中心執行長
14:00 - 14:40	專題講習	數位經濟：課稅、壟斷和炒股	熊全迪／理律法律事務所初級合夥人
14:40 – 14:50	分組準備		
14:50 - 16:30	分組演練	議題討論 / 角色扮演	講者帶領學員演練
16:30 - 17:10		小組成果報告	學員推派代表、講者總結
17:20 - 17:50	參與分享	經驗分享、參與機會	NetMission
17:50 - 18:00	結業式	結業手續	計畫人員

三、講師簡介

本年度研習營依據課程主題，邀請來自民間企業、技術社群、公民團體等國內相關領域的專家共 6 位擔任講師，另邀請來自香港的 NetMission 成員，分享未來國際參與機會。講師群依姓氏筆畫簡介如下表 7-3：

表 7-3　研習營講師群

講師	經歷與專長
 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 ● 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

講師	經歷與專長
 胡元輝 教授 國立中正大學傳播學系	**經歷** ● 台灣事實查核教育基金會董事長（現任） ● 教育部媒體素養教育推動會委員（現任） ● 優質新聞發展協會常務理事（現任） ● 台灣媒體觀察教育基金會董事（現任） ● 卓越新聞獎基金會董事長 ● 公視基金會、台視總經理 ● 中央通訊社、自立晚報社長 ● TVBS 電視台新聞部總編輯 **專長** ● 傳播經營與管理 ● 傳播政策與法規 ● 公共與公民媒體 ● 新聞製播與採寫
 陳奕儒 公共政策經理 Facebook 臺灣	**經歷** ● 新北市政府秘書處國際事務科 ● 總統副秘書長辦公室 ● 外交部國際組織司、條約法律司、駐奧地利代表處 **專長** ● 國際事務推動及參與 ● 社群建立及開拓 ● 外交及國安政策 ● 國際法及人權

講師	經歷與專長
 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
 賈文宇 執行委員 台灣人權促進會	**經歷** ● 臺北醫學大學醫療暨生物科技法律研究所副教授（現任） ● 國立臺灣科技大學博士後研究員 **專長** ● 憲法 ● 行政法 ● 生醫資訊法 ● 法社會學

講師	經歷與專長
 黃勝雄　執行長 台灣網路資訊中心 （TWNIC）	**經歷** ● 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） ● 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

講師	經歷與專長
 熊全迪　初級合夥人 理律法律事務所	**經歷** ● 台灣金融科技協會會員 ● 台灣／美國紐約州律師 ● 美國華盛頓州會計師（CPA） ● 特許財務分析師（CFA）第一級 **專長** ● 新興科技之法律議題 ● FinTech 議題（ICOs、虛擬貨幣、交易平臺、監理沙盒等） ● 個資保護 ● 一般商務及公司法務

四、報名資格與方式

（一）報名資格

歡迎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）踴躍報名。

- 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（部分課程可能以英文授課，現場不提供口譯）

（二）報名時間

自 110 年 4 月 22 日起，至 110 年 5 月 11 日 09:00 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？
- 若錄取成為學員，是否將進一步參加優秀學員甄選？
- 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 20~25 名學員。

（三）結果公布與通知

評選結果於 110 年 5 月 17 日於本研習營網站公布，並以電子郵件個別通知錄取學員。惟當時正逢我國 COVID-19 疫情升溫，因應社區傳播風險升高，指揮中心宣布自 110 年 5 月 11 日起至 6 月 8 日，提升全國疫情警戒至第二級，經與通傳會討論後，決議暫緩辦理本研習營，並於錄取通知信件中向學員說明：由於近日疫情嚴峻，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，本研習營將延期辦理，待疫情穩定後再擇期舉行，錄取學員的名額將予以保留。

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 110 年 7 月 30 日 17:00 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 小時的課前自我預習：錄取學員須於 110 年 8 月 5 日 23:59 前完成指定的預習課程及線上測驗，逾期未完成線上測驗者將無法獲頒新臺幣 $1,500 元整結業獎學金。

（二）研習營期間

全程出席，並遵守研習營各項規定與紀律秩序等要求。

七、學員獎勵

（一）結業證書及獎學金

全程參與研習營的學員（包含如期完成課前預習與線上測驗），將獲頒結業證書，以及新臺幣$1,500 元整獎學金（公務人員除外）。

（二）優秀學員獎學金（5 名）

主辦單位將組成評選小組，從結業且參與甄選的學員中，選出 5 名本國籍優秀學員，額外頒發新臺幣$1,000 元整獎學金。

（三）國際參與獎學金（5 名）

優秀學員須依主辦單位分工，線上參與 APrIGF 2021 國際會議，並各別摘錄 2 場座談紀錄刊載於活動網站（內容包含：會議資訊、座談紀錄 2 場、參與心得），即可各別獲頒獎學金新臺幣$ 4,000 元整。

（四）yIGF 2021 線上特派員獎學金（2 名）

凡具備在學學生身分之學員，申請參加 2021 APrIGF yIGF 成功錄取者，於 9 月 17 至 20 日參與 yIGF 線上會議，並於社群平臺公開分享各場次活動參與心得，即可獲頒獎學金新臺幣$ 4,000 元整。

（五）TWIGF 座談申辦獎學金（1 名／組）

結業學員可獨自或組隊申辦 TWIGF 座談（Workshop），經 TWIGF 評選最高分者且完成辦理該場座談，並於會後提供紀錄摘要（將載於本網站的【學習資源】），即可獲頒新臺幣$20,000 元整獎學金。徵稿時間依 TWIGF 網站公告為準。

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、線上報名、錄取名單、學習資源等 7 個項目選單，網站首頁如下圖 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

- 台灣網路講堂（twsig）facebook 粉絲團發文

● 購買 Google 廣告


OTT
5G
2021 網路治理研習營
歡迎報名
2021網路
治理研習營


OTT
5G
2021 網路治理研習營
5/29（六）@台北市 IEAT會議中心
歡迎報名2021網路治理研習營
「2021網路治理研習營」為一日免費研習活動，
課程內容包括專題講習、案例探討、分組演練等。
NII產業發展協進會


「2021網路治理
研習營」為一日
免費研習活動，
課程內容包括專題
講習、案例探討、
分組演練等。
NII產業發展協進會


歡迎報名2021網路治理
研習營
NII產業發展協進會
「2021網路治理研習營」為一日免費研習
活動，課程內容包括專題講習、案例探討、
分組演練等。
開啟


OTT
5G
2021 網路治理研習營
5/29（六）@台北市 IEAT會議中心
「2021網路治理研習營」
為免費研習活動，結訓後
還有機會贏得新臺幣...
廣告 NII產業發展協進會
開啟

● 申請刊登台北市電腦公會（TCA）會訊

會員訊息

[精聯電子]
工規行動電腦PA760幫助您提升工作效率 節省作業時間

[力新國際]
營業稅報稅機器人方案 輕鬆應對進項稅額憑證申報

[NII]
歡迎報名2021網路治理研習營

首頁 / 會員服務 / 會員訊息 / 內文

[NII] 歡迎報名2021網路治理研習營

疫苗護照和AI等科技應用如何兼顧數位時代的人權保護？
網路及社群平臺對於新聞生態、言論自由和內容秩序該承擔什麼公共責任？
又富可敵國但提供免費服務的科技巨頭應被課徵數位稅並強制分拆嗎？
以及當國家遭到重大網路攻擊時可以主動進行反擊嗎？

如果您關心這些網路政策議題，歡迎報名參加NII產業發展協進會主辦的「2021網路治理研習營」，除了帶您探討當前重要的網路治理議題外，還有機會贏得多項獎學金！

參考網址：2021網路治理研習營

（發佈時間：2021-05-03）

● 設計電子報

疫苗護照和AI等科技應用如何兼顧數位時代的人權保護？網路及社群平臺對於新聞生態、言論自由和內容秩序該承擔什麼公共責任？又當可敵國但提供免費服務的科技巨頭應被課徵數位稅並強制分拆嗎？以及當國家遭到重大網路攻擊時可以主動進行反擊嗎？
如果您關心這些網路政策議題，歡迎報名「2021網路治理研習營」免費課程活動，除了帶您探討當前重要的網路治理議題外，還有機會贏得多項獎學金！

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：2021年5月29日（六）08:40~18:00
地點：IEAT 會議中心 11F第2會議室

報名時間
即日起至2021年5月10日09:00 截止

錄取公告
2021年5月20日（四）於本活動網站公布，並以email個別通知。

立即免費報名

igcamp@nii.org.tw | https://www.igcamp.tw/
© Copyright 2021 網路治理研習營 All Rights Reserved

三、報名與評選

本次研習營報名期間共收到39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，39 筆報名資料均符合資格，並於5月11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。

評選方式係採兩階段進行－－個別評分及評選會議討論，最後依據 5 位審查委員之共識，選出26位正取學員及7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 24 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下圖 7-2，以大專院校為最多，共有 10 位參加（42%），其他組成分別為：2 位來自公民團體（8%）、3 位來自民間企業(12%)、5 位任職於政府部門(21%)，以及 4 位來自學研單位(17%)。

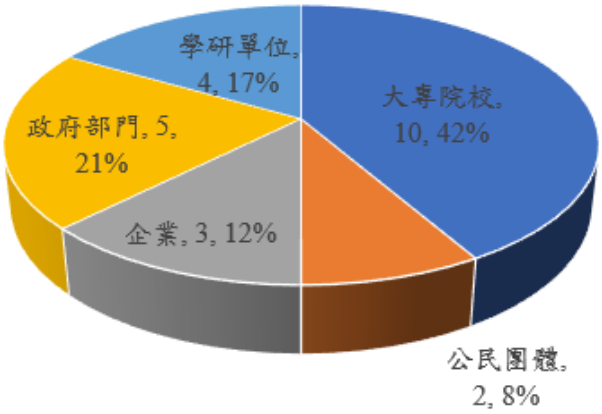


圖 7-2　研習營學員組成概況

若從參加者的年齡分布來看（參閱下圖 7-3），以 20~29 歲為最多，共有 9 位參加（38%），其他年齡層分別為：19 歲及以下 2 位（8%）、30~39 歲 8 位（33%）、40~49 歲 3 位（13%）、50 歲及以上 2 位（8%）。

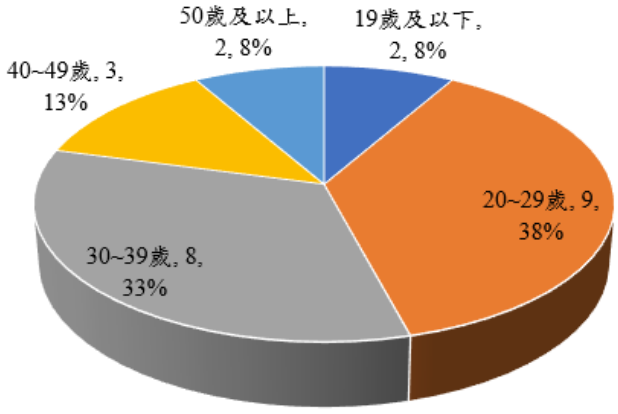


圖 7-3　研習營學員年齡分布

在參與動機方面（參閱下圖 7-4），半數學員均是因為對網路治理議題有興趣（50%），其他的動機分別為：與工作或學業相關 5 位（21%）、想改變目前網路政策 1 位（4%）、想參與網路政策議題討論 6 位（25%）。

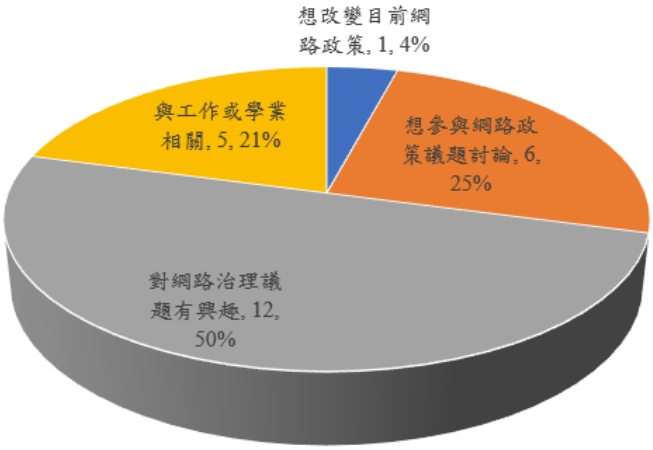


圖 7-4　研習營學員參與動機

執行單位亦參考 IGF 2021 議題徵集結果（本計畫建議書表 3），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（參閱下圖 7-5）。將近 4 成學員最關心內容與平臺治理議題（9 位，38%），其他由高至低依序為：網路安全（6 位，25%）、網路人權（4 位，17%）、新興科技（2 位，8%）、數位經濟（2 位，8%），以及數位包容（1 位，4%）。

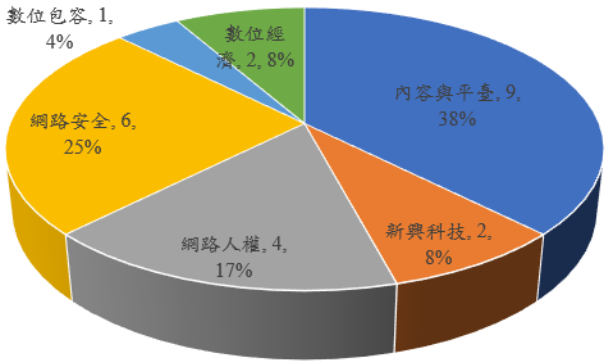


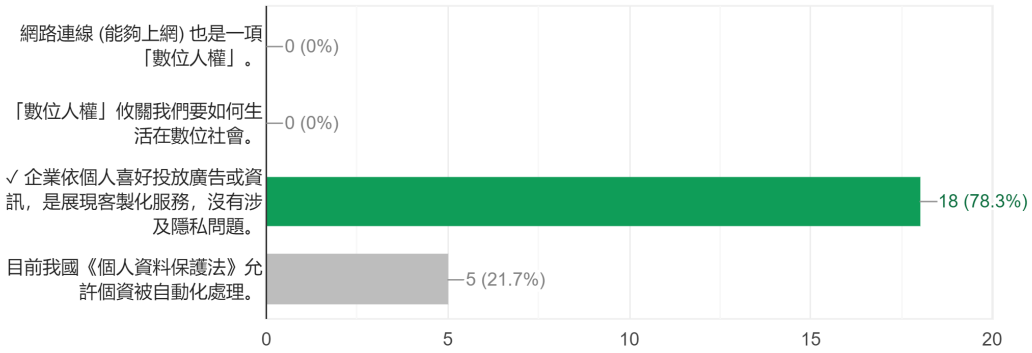
圖 7-5　研習營學員最關心的網路政策議題

五、學員課前預習線上測驗

執行單位針對學員的課前預習教材內容，設計 5 題線上測驗題目，以增進學員落實課前自我預習，進而提升研習課程當日的學習成效。統計結果共有 23 位學員作答，平均分數為 88.7 分，當中有 10 人滿分，僅 1 人低於 60 分。各題答題結果如下圖 7-6 所示。

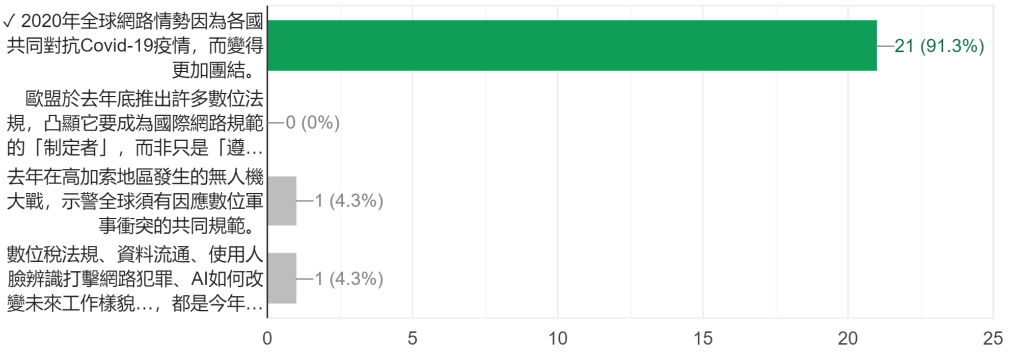
1. 關於「數位人權」的描述，下列何者錯誤?

答對次數：18 (作答總數：23)



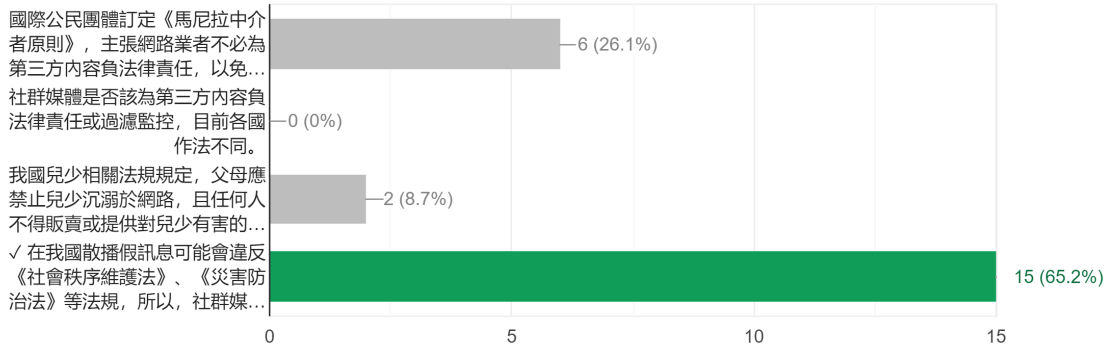
2. 國際專家Wolfgang Kleinwächter 描繪的近期網路治理概況，下列何者為誤?

答對次數：21 (作答總數：23)



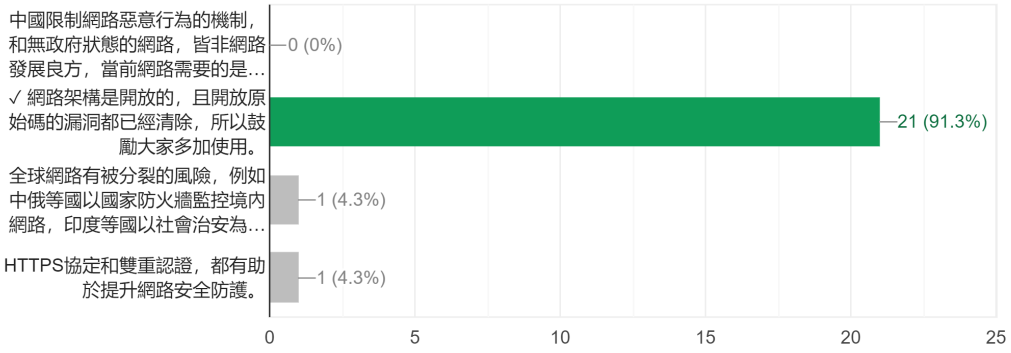
3. 關於使用者提供的網路內容 (如PO文、貼圖、傳影音等，又稱第三方內容，或用戶生成內容)的描述，下列何者錯誤?

答對次數：15 (作答總數：23)



4. 下列哪個不是網路之父 Vint Cerf 對於當前網路挑戰的看法?

答對次數：21 (作答總數：23)



5. 關於網路基礎建設的發展，下列哪個正確?

答對次數：17 (作答總數：23)

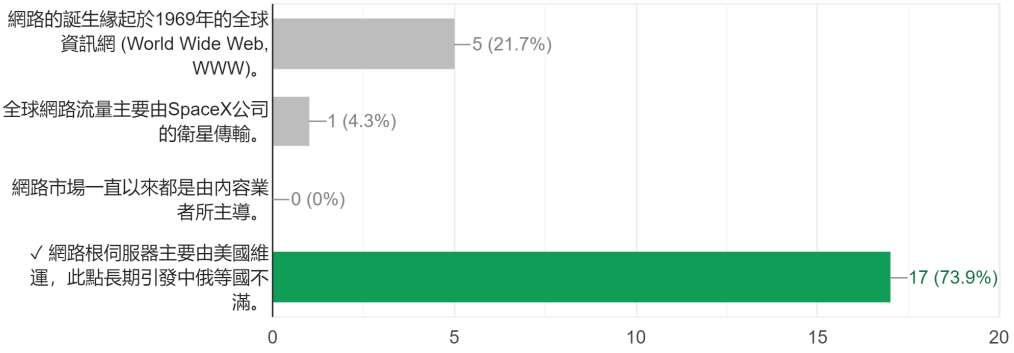


圖 7-6　研習營課前預習線上檢測答題結果

第三節 課程摘要紀錄

一、專題講習與案例探討

（一）國際焦點：科技戰與數位主權

講者：吳國維／NII 產業發展協進會董事

1.數位主權的關注點

談論「數位主權」時，我們首先應當留意及思考的觀點包括：「主權」與「數位主權」的國際法發展趨勢；數位主權的主張是否會對全球網路架構與運作造成破壞，衝擊網路未來發展；不同層次的公共利益，包括全球利益、國家利益、個人利益、環境利益、經濟利益等諸多面向；推理方法論、基礎與論述是否合理，且為國際間能接受的共識；這些利益是否為臺灣的最大利益，並且能與國際接軌。

2.傳統的主權概念

國際間對於「主權」的傳統概念，主要源自於 1648 年的西發里亞條約（Peace of Westphalia），其中包括 4 項重要原則：在國家的領土內，該國政府擁有最高且獨立的權利；國際組織形成決策的過程，不管各國的人口及經濟實力大小，均為一國一票；各國派駐在外的官員擁有外交豁免權；任何國家均不得介入他國主權。

3.網路人口發展史

美國在 1995-1997 年訂定電子商務白皮書時，全球的網路人口還不到 3%，因此多數人尚未思考到網路主權的議題。2003-2005 年聯合國舉辦 WSIS（World Summit on the Information Society）會議時，網路人口成長到 16%，2013-2016 年美國政府將 IANA（Internet Assigned Numbers Authority）的權利交給 ICANN 時，全球的網路人口成長到 46%。到了 2016 年，全球幾乎已認知網路的治理權落在 ICANN 組織。

協助美國訂定電子商務白皮書的白宮首席科技顧問 Ira C. Magaziner，在當時便已提出未來可能引發的網路爭議，包括：關稅及稅制、隱私、內容管制、數位簽章及驗證、版權、網路的管理、加密，以及電信自由化。Magaziner 亦提到，IETF 的治理模式(由下而上、公開透明、每個人擁有同等權利）是解決網路爭議的最佳解方。

4. Rolf H. Weber 的數位主權觀點

國際法專家 Rolf H. Weber 表示，數位時代看待「主權」的議題時，不能再使用 1648 年的傳統概念。1992 年時，聯合國秘書長提到，未來世界的「主權」不再是絕對的，或是具有排他性；2005 年 WGIG（Working Group on Internet Governance）會議的報告資料中也提到，未來談論到網路治理時，我們必須理解，對於網路的發展與應用，政府並非唯一的決策者，包括企業、個人、社群及公民團體等都可以平等的參與討論。

ICANN 採用的多方利害關係人治理模式，是由 IETF 延伸而來的，做決定時採用「共識決」，即使是政府組織也沒有特權，必須與其他組織站在平等的地位，避免任何一個國家濫用權利，導致全球公共利益受損。Rolf H. Weber 認為，各國的稅務、國防、公民政策的安全、公共空間的發言權及法律架構系統，這些範疇依然屬於國家主權管理，但這些領域以外的空間，皆可運用多方利害關係人治理模式。

Rolf H. Weber 提到，國家必須開放容許人民及非政府機構社群參與網路治理的架構，治理必須建立在寬鬆的領土概念上，傳統的國土概念應當重新定義，任何一個國家都不得破壞全球網路公共空間，對於主權的概念必須從國家主權（national sovereignty）轉為打造合作形式、共同共有的主權（cooperative sovereignty）。Rolf H. Weber 認為，在網路世界中不應存在壟斷的權利，網路通訊應超越國家領土的壟斷主張。

5.網路分裂及主權爭議

IETF 的前主管 Leslie Daigle 提到，網路在最初設計時，就忽略了國家的邦界。IP 位址不像電信國碼可以做切割，每一個 IP 位址在全球網路空間都是獨一無二的。然而，2016 年發生史諾登事件後，許多國家開始基於國家安全對網路實施限制，網路之父 Vint Cerf 對此表示擔憂，認為可能造成網路的分裂。

近年來，歐盟也注意到許多大型企業已經壟斷了全球的網路流量，歐盟主席提到，網路的發展將會對歐盟造成威脅，因此歐盟從 2020 年開始也陸續在討論網路主權的議題。

6.結語

瑞士蘇黎世大學的 William Drake 教授，2020 年受邀參加臺灣網路治理論壇座談活動時曾表示，宣告網路主權並不表示可以在網路上為所欲為。

喬治亞理工學院的 Milton Mueller 教授則是提到，網路空間與國家領土主權毫不相干，任何國家都不應宣稱其創造網路主權的概念，因為這會影響到全球網路的連結。網路空間應為全球的公共空間，為鬆散、分散式的治理概念，我們要逐漸進化到超越國界的網路空間。放棄網路主權的概念，並不代表就會傷害到國家利益。

（二）新聞有價是國際趨勢？

1.講者：胡元輝／中正大學傳播學系教授

(1)日漸勢微的新聞產業

紐約時報曾在 1989 年創下金氏世界紀錄，當時週日版發行的報紙多達 1,612 頁，重達 5.5 公斤，但 30 年後，2019 年的發行紀錄只剩下 192 頁，1.8 公斤，從這個例子可以看出報業從輝煌時代到今日的變化，面對了極大的衝擊。

根據「世界報業協會」（World Association of News Publisher, WAN-IFRA）的全球年度調查，2015 年至今每年的總營收皆為下降，儘管數位出版或廣告部分的營收有微幅增加，仍不敵傳統印刷品的消減。

臺灣方面，2016 年無線電視的廣告收入是 33 億多，有線電視是 191 億多，兩者加起來為 220 億多，而網路廣告的收入為 258 億，首度超越電視廣告。在這之後，網路廣告的營收也逐年攀升，電視廣告則是持續衰退，與全球的趨勢相似。

(2)低迷的信任度與閱聽人數

新聞業者面臨的另一個挑戰為「信任度」，依據牛津大學路透社新聞研究所（Reuters Institute for the Study of Journalism）的研究結果，新聞媒體的信任度平均值大約在 40%左右；臺灣的新聞媒體信任度在本次調查的 46 個國家地區當中，排名為第 42 低，信任度只有 31%，當新聞來源為社群媒體時，信任度則是下降至 29%。

從調查當中，也可看出多數閱聽人不再連至官方網站讀取新聞，而是轉變為以平臺為基礎（platform-based）的新聞接收習慣，在不分齡的受訪者當中就占了 73%，若將調查對象限縮至 35 歲以下，比例更是高達 81%。

新聞業者逐漸失去與閱聽人建立直接關係的機會，雖不願意受制於網

路平臺，卻又必須仰賴網路平臺帶來流量並分享廣告收益，因此，有些新聞業者會嘗試繞過平臺業者，直接與閱聽人建立關係，例如：透過電子郵件、行動提醒（mobile alerts）等。相對於此，網路平臺也試圖藉由新聞服務強化平臺的黏著度與資訊流的主導地位，以持續爭取、擴大廣告營收。

(3)新聞是否應為有價？

好新聞需要專業的產業鏈及經濟的支持，才能長存，網路平臺雖然不會自行產製新聞，但仍須承擔相關的公共責任。參考國際間的經驗，講者認為可以從兩個方面著手，第一個是從著作權的角度，賦予新聞媒體新聞鄰接權（neighbouring right）；第二個是從競爭法的角度，要求網路平臺使用媒體機構的新聞或其他內容時必須付費。

今年度澳洲立法的案例，即為前述第二種做法，但這同時也引發爭議，例如：大型媒體或媒體集團易獲較大利益；新聞業者未必會將所獲費用使用於提升新聞品質；再者，新聞業者向網路平臺收費後，如何發揮應有的監督功能？

講者在今年三月提出「思考平臺付費新模式」，建議由新聞媒體、平臺業者、公民團體、學者專家等多方利害關係人代表，組成具獨立性質的基金，再由大型網路及社群平臺提撥一定比例的營收，該基金可依合理比例將款項分別運用於公共、獨立與商業媒體通過審核之提案，以真正挹注於優質新聞的推動。在講者提出這項模式之後，加拿大及美國亦有類似的概念被提出來討論。

講者表示，如果我們認同好新聞是好民主的支柱，就必須考量新聞是否應為有價，並且一起承擔這個價錢，包括平臺業者也應以公共責任的角度來共同承擔。

2.講者：陳奕儒／Facebook 臺灣公共政策經理

(1)澳洲的「新聞媒體議價法」

科技的發展改變了使用者的習慣，使得媒體營運的要素——廣告受到相當大的影響，也造成廣告方式的改變。澳洲政府在今年 2 月時準備通過的「新聞媒體議價法」，要求網路平臺業者與新聞發布商進行議價，雙方在議價過程中若未能達成協議，將由政府出面仲裁。講者認為這項法律對於網路平臺業者與新聞發布商之間的關係有很大的誤解。

Facebook 在美國提供「News tab」這項產品，這是 Facebook 與新聞發布商之間經過商業協議後，再將新聞上架，除了「News tab」以外，其他出現在 Facebook 平臺上的新聞，多是因為新聞發布商自己張貼在其粉絲專頁，或是平臺上的使用者自發性分享的資訊，並非由 Facebook 主動去取用這些新聞內容。然而，澳洲的法規是以 Facebook 主動去取用這些新聞內容為前提所設計的，經過與澳洲政府及媒體協商之後，「News tab」這項產品未來也會在澳洲上架。

(2)Facebook 係「平臺」業者

講者表示，Facebook 做為一個平臺，新聞發布商可以自行選擇是否要在平臺上分享新聞，而且傳播這些新聞都是免費的，甚至，當使用者點擊這些新聞而連結到發布商的網站時，還能為發布商的網站帶來流量。Facebook 也發現，有些新聞業者可能缺乏健全的環境，以致於無法讓他們產出的新聞被更多人看到，透過 Facebook 平臺的傳播，也可以為新聞業創造價值。

(3)Facebook 持續支持新聞產業的成長

Facebook 亦在全球投入資源於培養新聞人才，以國內為例，Facebook 自 2019 年起已連續三年與「財團法人卓越新聞獎基金會」合作，並在 2020

年新設立及獨家贊助「新聞敘事創新獎」，鼓勵臺灣的新聞產業以創意與創新的敘事方式進行報導。目前也在規劃一個新的計畫，針對資源相對不足的地方記者提供支持。其他像是與事實查核組織合作，降低不實訊息的傳播，以及舉辦推廣活動提升民眾的新聞素養，也都是 Facebook 致力的方向。

未來 Facebook 也會與新聞記者及新聞發布商持續合作，尋求能夠陪伴新聞業蓬勃成長的永續解方。

3.問與答

問：Facebook 過去皆強調自己為純粹的科技平臺公司，所以不需負擔新聞媒體的責任，但因為 Facebook 是透過演算法來傳播訊息的媒體，想請問 Facebook 對於自身的定義為何？

答：陳奕儒經理回答，雖然 Facebook 對於部分內容會承擔發布的責任，但 Facebook 是平臺業者這點毋庸置疑，因此對於平臺上其他非由 Facebook 發布的內容，並無法負擔責任。

問：有些人認為新聞產業的衰退或是造成民主問題，是因為平臺透過演算法讓消費者更能看到想看的內容，如果將「新聞是民主的必要條件」加諸於媒體經濟，是否代表我們預設 Facebook 應該為公共利益負責，並強迫其推送高品質的新聞給閱聽人？

答：胡元輝教授回答，演算法背後有其商業邏輯，但新聞並非純粹的商品，在民主政府當中被賦予特定的價值與任務，因此，在演算法的治理上，可以思考如何達到比較好的目標，例如：平臺業者提供使用者多一點選擇、在演算法的機制中加入一些透明化的需求，或是透過一些配套機制，提高演算法的正面作用，降低負面作用，讓演算法可以同時符合商業需求、使用者需求，以及公共利益。

問：請問講者對於中國實施網路限制有何看法？

答：陳奕儒經理回答，目前國際間有幾種網路治理的模式，中國的模式是政府的介入程度比較高，而這樣的模式也受到一些國家認同，對於網路的開放及發展潛力不免令人擔憂。民主的國家應該有能力設計出一套有效，且能兼顧人權及民主的網路治理方法。胡元輝教授則表示，網路治理是政治治理的一環，所以兩者之間的管制模式應當會是一致的，就其個人立場而言，這是一種較為落伍的體制，中國應當逐漸開放社會更多的聲音，讓人性得以正面發展。

（三）內容亂象誰負責？

1.講者：曾更瑩／理律法律事務所合夥律師

(1)網路平臺的責任

過去普遍的認知是，內容提供者應當對資訊的內容負責，但在網路誕生之後，情況就不同了。講者請學員思考，當內容提供者把資訊放到網路上，如此一來，網路服務提供者的地位是否等同於內容提供者，應當對其傳遞的內容負責？

以往人們可能會認為，網路與電話及電信管線一樣，屬於科技技術，所以不必對傳遞的內容負責，但後來出現了搜尋引擎、部落格及社群媒體等平臺，大部分的資訊都是透過這些平臺傳遞，使得網路平臺逐漸轉變成為「中間人」的角色。在現實世界中，「中間人」是需要負擔責任的。

(2)美國的管制模式

美國在 1996 年通過的《通信端正法》（CDA）第 230 條規定，互動式電腦服務的提供者或使用者，就非出於己的資訊內容，不應被視為出版人及發表人；這是被稱為「善良撒馬利亞人條款」的免責規範。

依據該法，任何人皆無須為他人提供的內容負責，對於他人的不當言論（例如：色情、暴力等不當內容）加以限制時，也不需要負責。惟與使用者簽訂合約時，應當告知未成年使用者，基於保護之義務，系統會使用哪些過濾機制進行監控，避免兒少受到傷害。換言之，在美國，平臺業者除了保護兒少的義務之外，對於網路內容採取作為或不作為都沒有責任。

但這也引起相關的爭議，2020 年 5 月 28 日美國總統川普簽署了行政命令，導致平臺業者被認定不當壓制言論自由（例如：暫時關閉帳號或刪除文章），聯邦主管機關對其究責更為容易，在美國國內引發許多要求修正 CDA 230 的建議與聲浪。

(3)歐盟的管制模式

歐盟在 2020 年 12 月 5 日公布數位服務法（DSA）草案，宣示建立歐盟單一市場之宏大的藍圖。

法案中將所有的網路中介服務分成四個層次，訂定不同的責任義務。網路平臺歸類在 Hosting，其義務與責任為，當資訊服務的提供者，對於平臺上傳遞的非法行為或內容實際上並不知情時，無需負擔責任，但知情後就必須移除該項內容。為了鼓勵網路平臺主動監控內容，法規中也提到，中介服務者如果主動調查平臺內容的合法性，不會因此喪失免責的保護；此外，平臺也沒有主動監控內容的義務。

簡而言之，歐盟的管理模式為：平臺如果知情，就必須採取行動（作為），但並沒有積極知情或監控的義務。

(4)臺灣的管制模式

臺灣目前並沒有一般性免責或歸責的原則性法律，大部分的網路內容法律責任都是在發布人（實際的行為人），但有少數的平臺義務，例如：著作權法、兒童及少年福利與權益保障法、兒童及少年性剝削防制條例等，屬於知情始須採取行動之管制方式。最強烈要求平臺負責的法律是「網際網路內容涉及境外應施檢疫物販賣至國內或輸入時應採取措施」，要求平臺應主動審查廣告內容並採取移除措施。另外，我國目前對於不實訊息的防範，則是採業者自律之方式處理。

最新版的「數位通訊傳播法」草案當中，有關網路平臺的責任較趨近於歐盟的做法。法規中提到，數位通訊傳播服務提供者對其提供使用之資訊，應負法律責任，但對其傳輸或儲存之他人資訊，不負審查或監督義務。以及，數位通訊傳播服務提供者對於第三人為供他人使用而儲存之資訊，在不知其為違法行為或資訊，或是在知悉後，移除資訊或使他人無法接取之，就不負賠償責任。

據講者了解，主管機關所委託的相關研究計畫當中，對此提出的建議包括：網路平臺宜提供透明度報告，告訴使用者其如何管理網路內容；加註警語，例如：提醒使用者哪些資訊為不實訊息；在法院或主管機關發布正式命令的情況下，網路平臺才能移除內容。

課程最末，講者建議，臺灣可以思考未來希望網路平臺怎麼做，是要積極的審查，或是像美國模式，給予網路平臺較大的免責原則。

2.講者：陳奕儒／Facebook 臺灣公共政策經理

(1)多樣化的網路問題

Facebook 將平臺上的問題大致區分為 A（Actor，行為人）、B（Behavior，行為），以及 C（Content，內容）三種不同的架構，對於不同架構的問題，處理的手法也會不同。再者，網路上的內容可能因為所在國家的不同，對於「有害」或「違法」具有不同的認定標準，若再加上「不正確」的內容，這三項元素所組成的問題樣態就會更為複雜。

(2)網路內容規範的原則

在談網路內容規範時，首先要確認規範之目的及手段，Facebook 認為網路需要由法律來釐清責任，讓平臺業者在保護網路安全的同時，也能維護網路上的自由。平臺業者負責任的對象主要應該是社會及使用者等多方利害關係人，而非僅限於政府。

Facebook 在 2020 年 2 月發布「擘劃網路內容規範的未來方向」（Charting a Way Forward: Online Content Regulation）白皮書，彙整 Facebook 認為網路規範應當解決的問題，包括：內容規範如何以最佳方式達成，減少有害言論，同時保有言論自由；規範應如何加強平臺的問責性；規範是否應該界定網路平臺上哪些「有害內容」應被禁止。

Facebook 認為，問責機制應該強調系統面，而不是對特定內容負責，例如：在系統的設定上建立風險評估的 sop，避免發生可能預見的問題，或是解決已發生的挑戰。此外，問責機制也應該藉由提供透明度報告的方式接受公評，透明度應著重在說服整體社會平臺已盡到應盡的責任。

(3)通知及採取行動（內容移除要求）

參考歐盟的法規，平臺業者收到內容移除要求時應當採取行動，才有免責的權利。Facebook 對於內容移除要求的作業程序為，接到主管機關通

知後，首先會依據 Facebook 的政策針對違規內容進行檢視，接下來再依據當地的法令法規進行檢視，若內容確實違法，也必須思考一旦配合政府政策移除內容時，是否會違反國際人權相關的標準，經過以上程序後，再向主管機關回報處理結果，同時採取適當措施並通知用戶。

講者表示，各國對於通知及移除（notice & takedown）的做法，會依據當地的法令法規與風俗民情而有不同，因此，對於網路內容的管理除了網路平臺應負起責任之外，公民社會與政府也應該適當發揮其功能。

3.問與答

問：紐約大學一些參與政治廣告研究案的研究者帳號被 Facebook 停權，原因為其濫用 Facebook 的使用者條款，但對於遭停權的使用者來說，這個理由並不完全成立。請問 Facebook 對於資料揭露及存取的政策為何？對於第三方研究者所提出較為敏感的意見，Facebook 的態度又是如何？

答：陳奕儒經理回答，對於特定個案，因為講者手邊並無相關資料，無法提出評論，但 Facebook 必定是有充分的理由可支持這項決定的來由。

關於資料透明度的議題，應該以目標為原則，讓平臺業者依據各別公司或產品的性質與服務的限制，提供足夠的資訊，藉以說服社會公眾。

Facebook 是在美國註冊的公司，所有的使用者資料也都儲存在美國加州，在與研究者合作時，提供的一定是無法識別特定當事人的資料，或是原本就屬於公開的資料。只要研究者是基於合規的方式進行研究，都可以申請重新開放遭停權的帳號。

Facebook 也有一些資料是完全開放給所有的研究者，例如：政治廣告的 API（Application Programming Interface）。在臺灣從 2019 年 11 月開始已經累積了大量的資料庫，Facebook 也希望臺灣有更多研究者來申請 API，進行政治社會議題廣告的分析。

（四）數位人權：防疫、AI 和 eID

講者：賈文宇／台灣人權促進會執行委員

1.什麼是人權？

一個國家是否重視及保護人權，並非只是關注多數人的需求、利益，或是國際名聲，而是去關注群居生活當中的「每一個個人」。當群體中的個人與群居的社會產生不一致時，人權最大的價值是去協商誰應該退讓，或是彼此之間的關係應當如何調合，而非只是採用價格最低廉或最方便解決問題的手段，甚至是為了公共利益而犧牲個人的人權。

2.數位人權

以網路上常見的「打卡送小菜」為例，使用者看似自發性的透過打卡而自願放棄人權（交出個資），講者請學員思考其中代表的意義為何。現代人在網路上打卡，不完全是為了得到利益，有時只是出於社交的需求，當你的社交對象大多都已經在網路平臺上時，相對的，你也必須申請帳號加入網路平臺。

網路已逐漸類似水電等基礎建設，是人類生活當中不可或缺的一部分，對於數位人權的剝削，可能會隨著這種「不得已而使用」的情況攀附而上。多數人都了解並認同隱私很重要，但隱私與現實生活中的實體物品最大的差異就是我們很容易對它無感，而且一旦外洩之後就很難收回來，隨著超級電腦與演算法的興起，加速資訊的運算與推理，也就更容易導致權力的失衡。

講者認為，強調保護隱私未必是產業的絆腳石，以歐盟的 GDPR 為例，有些人甚至認為這是正當的貿易壁壘，因此人權的議題已確實發生在現代自由市場的經濟活動當中。

3.隱私與資訊自主

個資蒐集與利用之「目的」是最為重要的，換言之，人們對於目的外的蒐集與利用都應該抱持警覺。我們常會聽到「個資是數位時代的石油」，但個資與石油的本質完全不同，其中包含了大量的個人特徵，即便資料經過去識別化，隨著運算能力的發展，仍有可能拼湊出真實的資料。

4.防疫中的數位人權

基於防疫之要求而犧牲數位人權，是否真為必要之惡亦值得我們思考。根據研究，東亞國家特別偏好數位監控的防疫措施，然而，若真要監控數位足跡，還是有比較能兼顧資訊自主及隱私的做法，例如：使用社交距離 app，理由為這是基於使用者自願的情況下才會開始使用的工具，並且衛生部門必須在病患的同意下，才能對外分享資料。當民眾自願配合某項政策，這項政策才容易成功。

5.eID

eID 在我國並非新的議題，早在 1998 年國內就已提出相關的規畫，後來因為引發諸多質疑，在今年初內政部宣告暫緩政策。

政府欲轉型為「數位國家」的立意良好，但實在還有太多配套措施需要一併考量。對此，中央研究院法律學研究所的邱文聰研究員即表示，我國至少應立法規範身分證的使用範疇，此外，民主國家應是政府對人民透明，因此，必須建立一套使人民得以查看及監督自己的資料如何被蒐集與利用的機制。

（五）網路安全：從資安到國安議題

講者：黃勝雄／台灣網路資訊中心執行長

1.網路安全風險日漸重大

過去資訊相關的議題只有資訊部門需要關注，隨著資訊的普及化，越來越多部門皆需仰賴資訊系統提供服務，尤其在 COVID-19 疫情期間，上網對於人們而言，不再只是單純的休閒活動，而是重要的生命線。

網路安全會隨著時間演變出不同的議題與攻擊手段，根據世界經濟論壇 2020 全球風險報告，網路安全相關風險發生的頻率相當高，對整個社會造成的衝擊也相當大，不再像過去只是發生在資訊系統裡的微小漏洞，機敏資料的洩漏或是關鍵基礎設施的破壞，已經對國家安全造成影響。

2.網路政策如何定義

網路政策就如同開車時須有各項可供遵循的交通規則，這些政策不像一般的法案，須要經過立法院三讀通過才能執行。

全球與網路相關的機構包括：ICANN、ITU、IGF、APNIC、IETF 及 NATO 等，國內則有負責.tw 域名註冊及 IP 位址發放的 TWNIC，這些組織或多或少都有參與網路政策的制定，但各個組織所制定的政策特性並不完全相同，大致可以區分為 6 種屬性：多方利害關係人、由下而上治理、是否訂定相關標準、是否透過合約規範、政府是否參與，以及是否訂定全球強制規範的義務。

3.網際空間如何被規範

現行實體空間中所有與資訊安全相關的法律，在網路空間也一體適用。根據芝加哥學院 Lawrance Lessig 在 1999 年提出的理論，網路空間的行為準則是由 4 個驅動力所規範，包含：法律、他律規範或利害關係人訂定的共識、技術標準，以及市場。

過去數十年，多是由科技引領法律，但歐盟的 GDPR 出現後，訂定了科技必須符合法律的相關要求；網路安全也有可能因為利害關係人所訂定出，多數人願意遵守的共識規範，而影響技術架構與市場行為。

4.跨境網路犯罪調查不易

講者以跨境網路犯罪為例，說明發生資安事件時，在全球的環境中會發生哪些連鎖行為。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進入下一步的司法作為。

網路犯罪難以查到特定的攻擊者，並且持續在發生，加上多層斷鏈（伺服器 IP、域名註冊人，以及攻擊操作者，三方可能位在不同的法律管轄區）的特性，加深了犯罪偵查的困難度。

法律與管轄權具有地理的限制，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衝突。

5.限制網路內容接取

目前國內可以限制網路內容接取的相關法律只有兒少法第 46 條，以及動物傳染病防治條例第 38-3 條，其他情境下，除非取得法院的判決，否則無法任意限制網路內容接取。

講者接著介紹 TWNIC 整合國內 ISP 建構的 DNS RPZ（Response Policy Zone）政策機制，各家 ISP 的 DNS 可與 TWNIC 串接，一旦 RPZ 寫入黑名單，全臺灣的解析系統皆會進行屏蔽。RPZ 的啟動必須確定是否符合正常程序，包括來自於法院判決、禁制命令，或是行政處分。

6.未來方向

網路犯罪因嫌疑人無法特定，講者建議未來偵辦的方向可以朝虛擬資源扣押實施，依據刑事訴訟法第 133-2 條，採用非附隨於搜索之扣押命令，將網域名稱及 IP 位址列為應扣押之物。未來 TWNIC 也會規劃資安通報的信任夥伴清單，當發生情節重大的資安事件時，如何採取 RPZ 的措施進行相關下架。

此外，網路上不當內容的處理程序涉及網站管理者、域名註冊者、域名銷售者等多個單位，應當建立適當的轉介程序，方可符合正常程序的法治化要求。另一方面，在法律之外，也應同時發展技術面及規範面的防堵措施，以多軌並進的方式，才能提升治理框架的效能。

最末，講者表示，未來的戰爭很可能都是始於網路攻擊，資安與國安必然會整合為一，我們必須了解網路攻擊在目前的國際法當中有無適用的規範。

7.問與答

問：中國建立大規模的網軍部隊，面對這樣的情勢，我們應該如何防範？

答：過去在「資安即國安 1.0」的階段時，包括政府公部門及關鍵基礎設施都要做到最完善的保護，「資安即國安 2.0」將防護的範圍擴大至犯罪調查及軍方的參與，相對的，軍方在網路的能量以及專業能力都有大幅度的提升，並提升警檢調在網路犯罪調查上的情資交換。因為涉及國安，政府可能無法大肆宣傳目前有哪些作為，但據講者的了解，政府確實投入相當多的心力及資源。

問：假若未來資安與國安架接在一起，在談論軍力的概念時，是否可能依照實際專業的層級以及一般民眾理解的層級，分別去評估軍力的數值與標準？

答：某些涉及國安的資料政府並無法公開，若是可以公開的原則性推動策略及方向，政府都會定期釋出相關的政策白皮書，讓所有利害關係人知悉。「資安即國安 1.0」是以防衛為主，「資安即國安 2.0」除了加強防衛，同時擴大到軍方的攻擊防禦能力，以及犯罪調查的情蒐能力。面對網路戰爭需要強化的能力，除了攻擊與防禦之外還包括韌性，一旦網路無法運作時，才能立刻採取備援措施或替代方案。

（六）數位經濟：課稅、壟斷和炒股

講者：熊全迪／理律法律事務所初級合夥人

1.數位巨頭的壟斷與治理策略

科技巨擘的優點是帶來破壞式的創新及產業革命，但同時也存在導致市場壟斷的缺點。反壟斷的精神即在於保護市場的競爭機制，促進經濟效益的最大化，但也有一些國家是出於壓制抗議活動，或是加強政治控制。

各國政府對於反壟斷的行動漸趨熱烈，美國眾議院司法委員會反壟斷小組在去年 10 月發布的調查報告中，即認定四大科技巨頭：Google、Apple、Facebook 及 Amazon 壟斷市場，該小組認為四大巨頭應進行拆分，並呼籲美國應修改反托拉斯法，以更符合數位時代的市場現況。

歐盟則是在去年 12 月公布「數位市場法」（DMA）草案，今年也正式對 Google 及 Facebook 展開反壟斷調查。DMA 著重在保障數位市場的競爭，如同網路世界的反托拉斯法，該法規範的對象主要是大型的網路平臺，將其稱為「守門人」（gatekeeper），依法應盡的義務包括：使中小企業有機會參與市場及取得資料權限、不能僅圖利旗下平臺與違反公平競爭原則等；若未能遵守規範，最高可能面臨達全球營業額 10%的罰金，甚至被要求結構重組或拆分部分業務。

DMA 的相關疑慮包括未充分界定何為數位市場，也有意見認為法案目的不應是「破壞特定企業的主導地位」，而是著眼於確保競爭過程公平公正，此外，依企業規模而異的法案內容，可能導致中小企業寧願限縮企業規模，以迴避規範等。

臺灣在今年 6 月 30 日，也由公平會委員會議決議針對數位平臺展開產業營業概況分析調查，然而最難判斷的依然是市場如何界定的問題。

2.數位經濟的課稅議題

全球數位稅制的起因，在於過去以實體經濟為主的課稅原則，難以適用於數位經濟，有些大型電商會刻意將利潤配置在低稅率地區的控股公司，以躲避高稅負。

全球數位稅的概念為，全球年營收超過 200 億歐元（約新臺幣 7,200 億元），且淨利率超過 10%的大型跨國集團，其淨利率超過 10%的部分會被認定為剩餘利潤，其中 2~3 成的課稅權須重新分配給消費市場國。

對臺資企業而言，因為營收達標者較少，預期大部分的臺資企業無須將其超額利潤分配至其他國家課稅；反之，許多國際大型數位經濟企業可能必須分配部分利潤至臺灣課稅。

但臺灣也會面臨到一些挑戰，例如：我國與美國及中國並無租稅協定，恐怕難以取得新數位經濟課稅方案的分配稅源，此外，一旦這項方案確定後，我國也必須重新審視營業稅及營所稅的數位經濟課稅方式，並導入新的課稅規則。

3.財經網紅或投資群組是否踩到法規紅線

依據「投信投顧法」第 4 條，經營證券投資顧問業務且從中取得報酬者，須取得金管會核准同意；因此，如果是在社群平臺推薦他人買股票並從中獲取利益時（例如：收取會員費用），便會涉及相關刑責。另外，也可能涉及「證券交易法」第 155 條第 6 款，意圖影響股票價格而散布流言或不實資料。預期未來可能會採用監理科技（Reg Tech）的模式來監控網路上炒股的情形。

二、分組演練

（一）線上分組方式

分組演練為本次線上辦理研習營最大的挑戰，在講師、學員以及執行單位工作人員三方無法實際面對面的情況下，如何進行分組，並讓各組內部的討論得以順暢展開，結束分組討論後，又要如何讓所有參加者順利返回原本的線上會議室，需要在活動辦理前進行充分的動線規劃及模擬演練。

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：網路內容、網路安全，以及數位經濟，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 6～8 位學員，經過 100 分鐘的討論後，再由各組指派代表報告討論結果，主要重點彙整如下表 7-4。

表 7-4　研習營學員成果報告彙整表

組別	**1. 網路內容**
題目	如何管理網路內容
1 項共識 **多項意見分歧**	本組討論後初步達成 1 項共識：平臺至少可以對危害普世價值的內容自行進行管理，然而，關於如何定義「危害普世價值的內容」，小組的意見呈現分歧。有些成員認為可隨機抽出一定人數（例如：10 人）的用戶，投票表決是否應下架爭議的內容；亦有成員認為社群可推選一位管理者，若管理者認定應刪除之內容就直接刪除。 對於爭議性內容的處理方式，小組亦未達成共識。部分主張應保留於平臺，因為平臺不應自定刪除標準，這同時也是基於民主的精神；另有部分主張平臺應依照各國法律制度及價值進行法遵；亦有部分主張法律應強制平臺的自律機制及跨平臺運作。
組別	**2. 網路安全**
題目	釣魚網站的相關治理方案
共識	本組建議透過建立白名單的機制來管理釣魚網站資安威脅。首先ICANN可評估修改與受理註冊機構之間的合約，並將白名單的列表規範標準化，請受理註冊機構在不違法的前提下提供註冊資料，建立統一的資料庫。另一方面則是透過公私部門間的協作，整合釣魚網站名單，定期比對及更新白名單資料庫，同時 ICANN 也應設置服務窗口，提供後續受理申訴機制。 除此之外，政府平時也應辦理講習或成立官方帳號，供民眾了解資訊安全及如何應對，公民團體則可協助收集民眾對於資安議題之意見，回饋於政府及研究機構修訂相關政策。

組別	3. 數位經濟
題目	支持壟斷或反壟斷？
共識	本組討論後的立場是傾向於反壟斷。雖然數位平臺規模越大越能提供精準的服務，且經濟效益可能高於拆分後市場，而反壟斷可能阻礙平臺的創新以及社會的經濟發展，但在探討壟斷的議題時，尚需考慮平臺掌握的其他權力，例如：演算法、經濟權力、文化權力等，也可能對民主運作及個人權利造成負面影響。其他支持反壟斷的見解包括：公平競爭是市場運作的前提；政府適度介入可以保護使用者的權益；避免單一平臺導致少數意見遭到排擠。 臺灣畢竟是小的經濟體，需要國際的聲量並往外發展，若能取得市場優勢是件好事，政府應思考如何讓大企業持續成長，並產生外溢效果，同時扶植小型企業，例如：由大企業投資上下游的小型或新創產業。

第四節　圖文影音紀錄

一、各式設計物

配合本研習營採線上辦理，執行單位製作之設計物包含：議程表圖片、視訊背景圖片，以及研習證明書，成品如下圖 7-8 所示。


2021 網路治理研習營
2021 Internet Governance Training Camp
研習證明書
TRAINING CERTIFICATE
王 小 明
Hsiao-Ming Wang
於 2021 年 8 月 7 日
參加本研習活動共計 8 小時，特此證明
has completed the 8 hours training program
on 7 Aug 2021
指導單位：國家通訊傳播委員會
主辦單位：財團法人中華民國國家資訊基本建設產業發展協進會
協辦單位：

圖 7-8　研習營設計物

二、活動紀錄

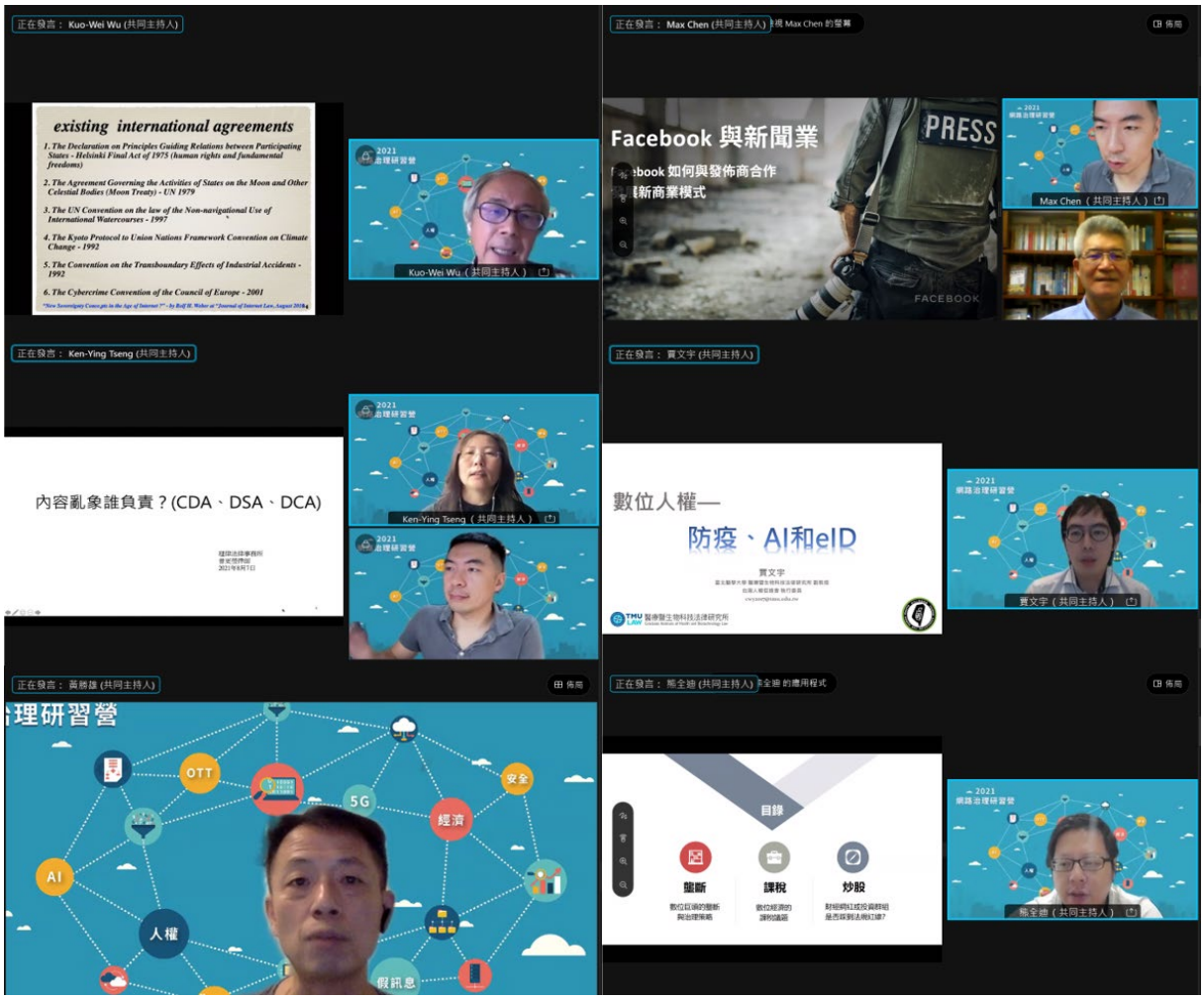


圖 7-9　研習營活動紀錄

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://www.igcamp.tw/resources/，參閱圖 7-10），供各界自行參考使用。

圖 7-10　研習營課程簡報資料與錄影檔

第五節活動成效評估

本次研習活動依據柯氏（Kirkpatrick）學習評估模式，和一般常用的評估工具，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）。

本次問卷調查係採用線上問卷，並於結業式後進行，問卷內容分為：課程內容滿意度、行政會務滿意度、學員自我評估，以及其他，共計 4 個單元。

因線上問卷不如實體問卷容易回收，加上為使學員放心填寫，問卷係採用不記名方式，不易掌握未填寫者名單，故本次僅自全程參與課程的 21 位學員當中回收 14 份問卷，回收率為 67%，統計結果說明如下。

一、課程內容滿意度

本年度學員對於預習教材及授課內容之滿意度（包含非常滿意及滿意，參閱下圖 7-11）都達 70%以上，對於分組演練的滿意度則僅有 43%，推測是因為線上分組演練相較於學員熟悉的實體課程分組方式討論不易，較難達到有效的演練成果，以致學員滿意度偏低。

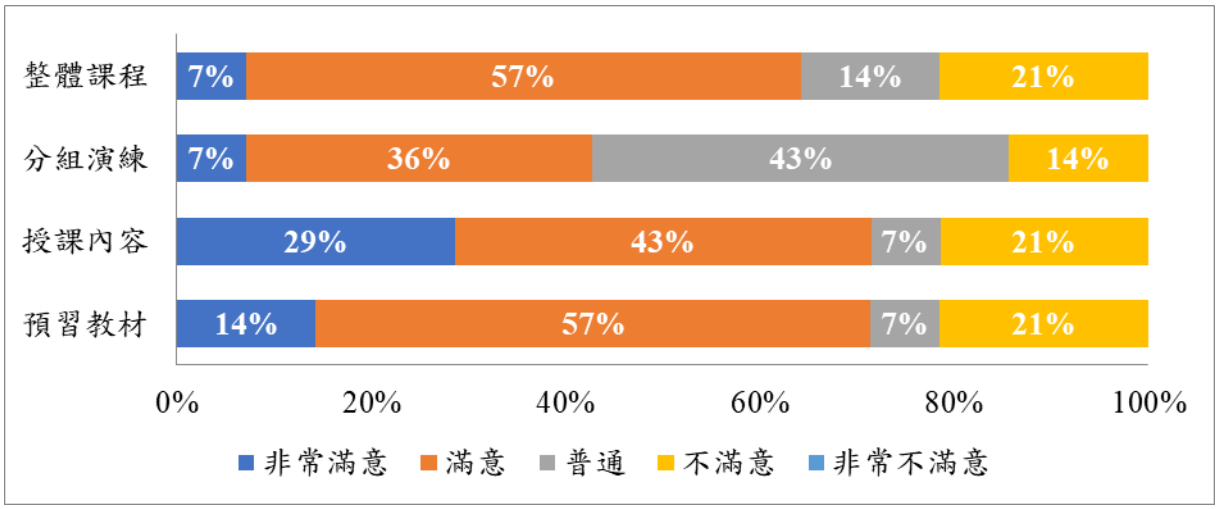


圖 7-11　研習營「課程內容」滿意度

二、行政會務滿意度

因本研習營係採用線上辦理，執行單位無需提供場地、交通、住宿及餐飲等細項服務，故問卷調查中僅就整體的行政會務安排進行調查，統計結果滿意度（包含非常滿意及滿意）近 80%（參閱下圖 7-12）。

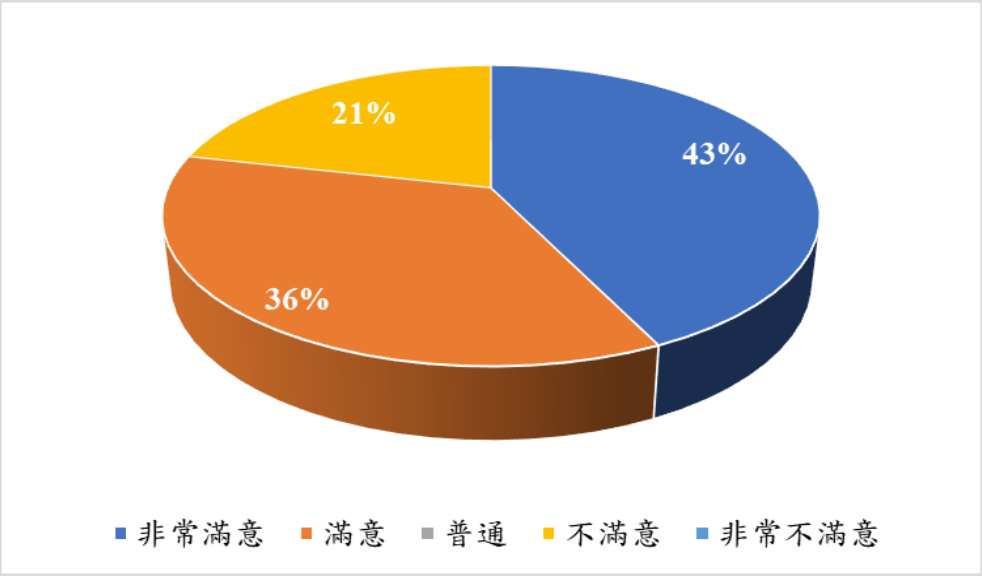
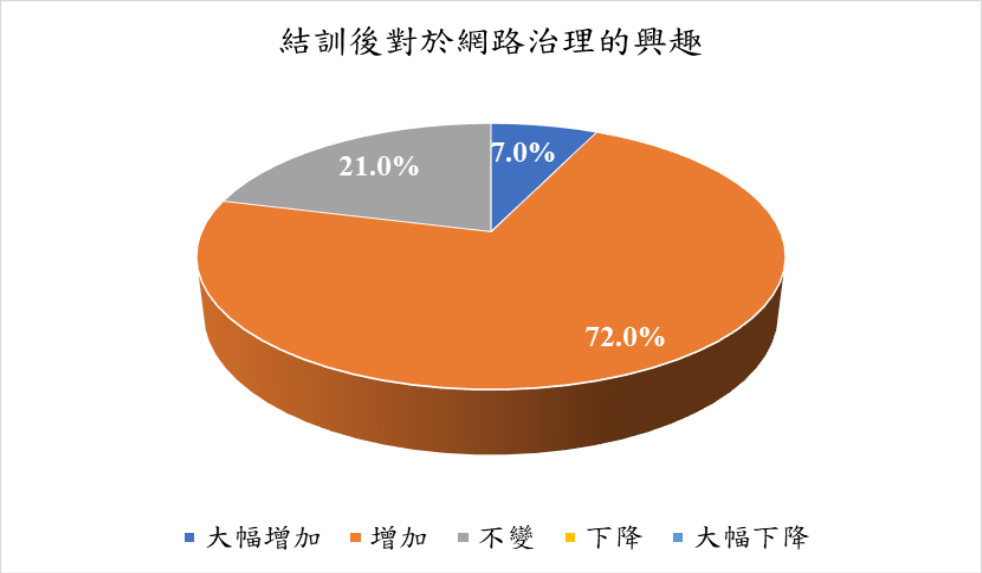


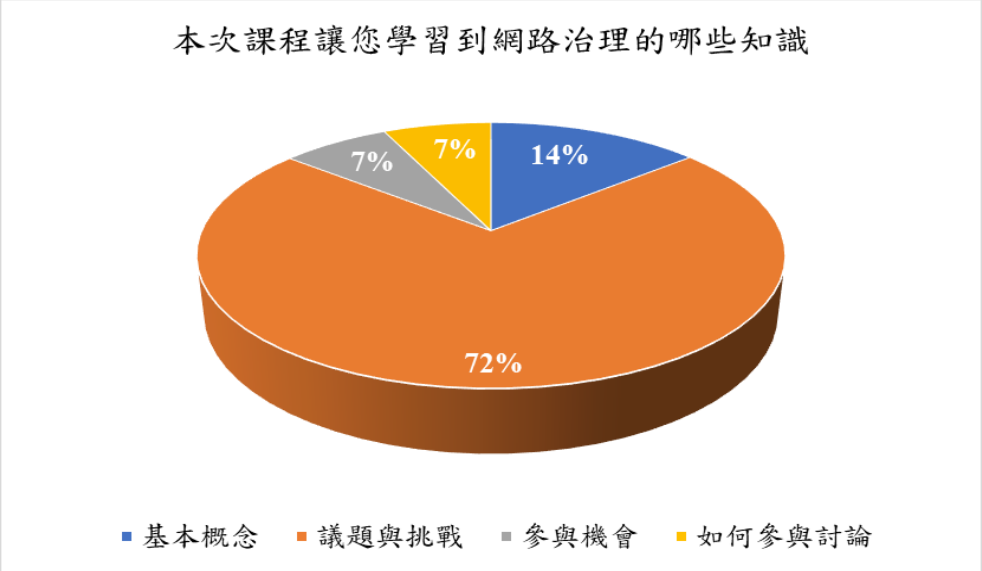
圖 7-12　研習營「行政會務」滿意度

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（參閱下圖 7-13）。

將近 80%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「議題與挑戰」最多，約占 70%；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 57%為最高。





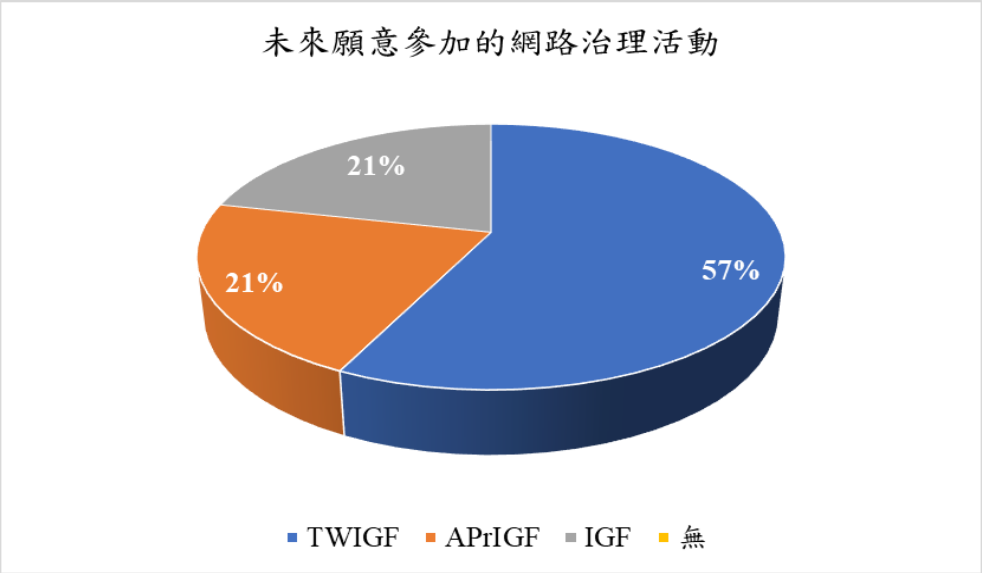


圖 7-13　研習營學員課後自我評估

四、其他建議

問卷的最後一個單元，則是針對本次研習營之辦理是否符合學員的期待，以及收穫最多的分別是哪幾堂課程進行調查（參閱下圖 7-14）。

將近 60%的學員表示本研習營符合期待（包含符合期待與超越期待）；收穫最多的課程以「網路安全：從資安到國安議題」明顯居高，達到 79%。

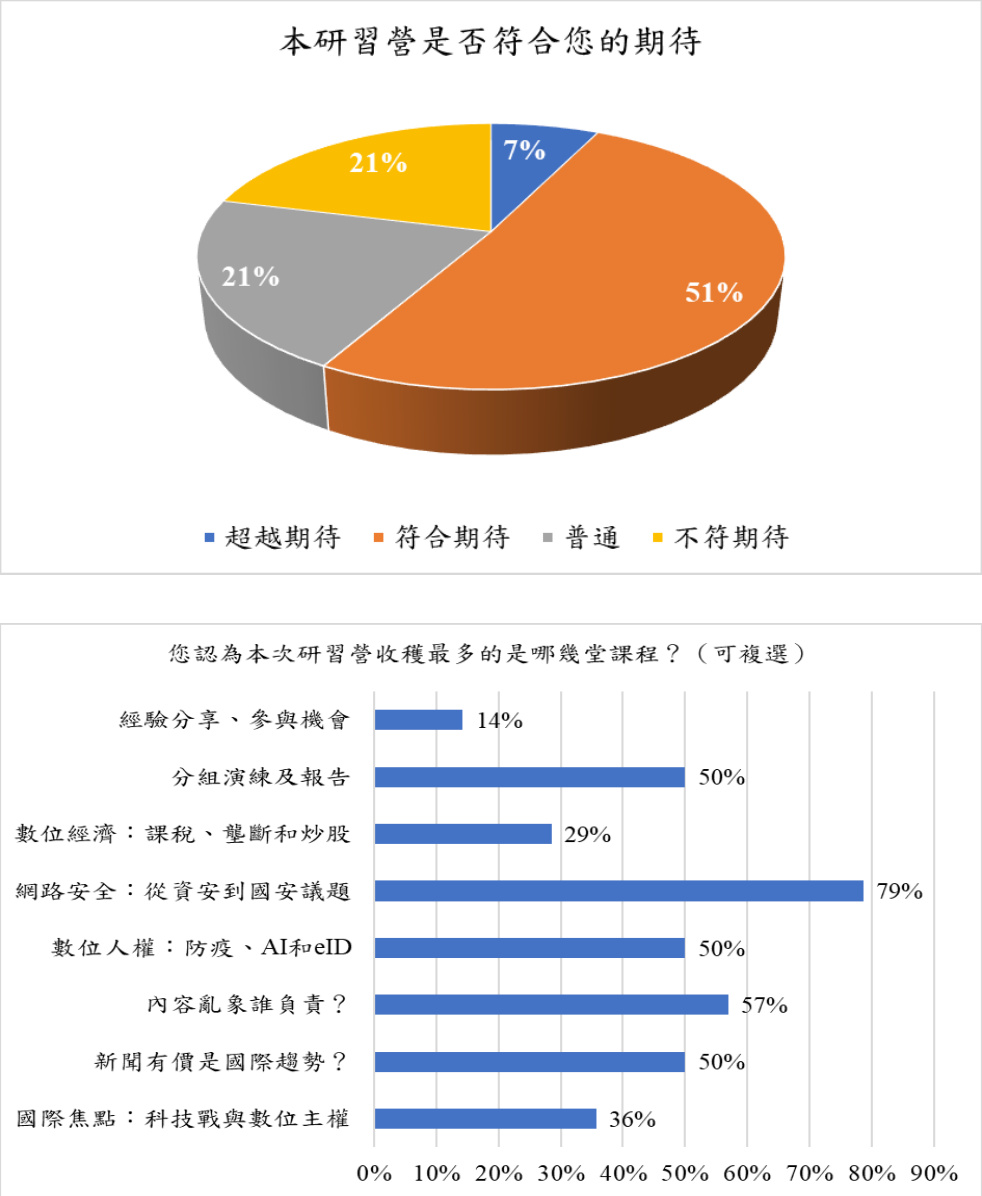


圖 7-14　其他建議調查結果

問卷最末亦設計了 3 題開放性的問答題，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，各項題目及答題之結果彙整如下。

- 您會建議我們未來透過何種方式或管道，協助您持續學習或理解網路治理相關課題？

  學員的回答相當多樣化，包括：演講活動、影片、podcast、發布研究資料、clubhouse、研討會等。

- 關於本次研習營，您覺得辦得不錯的地方有哪些？

  ✧內容豐富，資訊充足，議題實際且貼近時事，討論相當精彩。

  ✧提供課前預習教材，避免學員對於課程主題掌握不足。

  ✧分組的活動設計，讓學員體驗多方利害關係人運作模式，各組講師帶領討論也很專業。

  ✧邀請外國專家與會。

  ✧雖然是線上辦理，但流程十分順暢。

  ✧完全免費。

- 關於本次研習營，您認為哪些方面還有改進的空間？

  ✧可惜沒辦法辦理實體會議，讓學員之間有更多互動機會。

  ✧課程太緊密，若干課程時間延後超過，希望未來可以增加 QA 時間。

  ✧可能需要資訊相關背景的人參加活動比較好理解。

  ✧若無著作權相關問題，建議提前公開課堂簡報，以利學員熟悉課堂內容，可以提前查詢更多相關資料。

第六節 學員獎勵活動

一、選拔優秀學員參與國際會議

本屆 21 位結業學員當中，有 14 位表達同意參加優秀學員甄選的意願。本次評選小組由 3 位帶領分組討論的講師及本計畫協同主持人共同組成，從角逐學員中遴選 5 位優秀學員線上參加 APrIGF 2021 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。每位講師至多可推薦 2 位優秀學員，再共同討論這些學員的特色與潛力，最後透過投票或評分等方式，決議正、備取優秀學員名單。

經過講師的共識決，本屆優秀學員分別為：林○德（無界塾專案助教）、陳○耀（台灣智慧家庭股份有限公司 CEO）、湯○樺（私人企業軟體工程師）、楊○楷（臺大法律研究所公法組畢業，現任替代役）、蔡○安（前羅秉誠政委助理，於今年秋季入學哈佛大學法學院碩士班），額外獲頒「優秀學員獎學金」新臺幣$1,000 元整。

今年 APrIGF 的大會主題是「邁向包容、永續及可信賴的網路」，在 8 月下旬完整的 APrIGF 議程（參閱表 7-5）公布後，執行單位即篩選出與本計畫關連性較高的 10 個議程（參閱表 7-6），並與 5 位優秀學員討論，完成分工，指派每一位學員參加 2 個場次，並撰寫座談紀錄。

執行單位已將 5 位優秀學員撰寫的座談紀錄（內容包含：會議資訊、座談紀錄及參與心得）彙整為報告（參閱本報告附錄 4），且刊載於本研習營網站的「學習資源」專區，並依據本活動獎勵辦法，各頒發「國際參與獎學金」NT$ 4,000 元整予 5 位優秀學員。

表 7-5　APrIGF 2021 議程表

Time (UTC)	27 Sep (Mon)	Time (UTC)	28 Sep (Tue)	Time (UTC)	29 Sep (Wed)	Time (UTC)	30 Sep (Thu)
				03:00 – 04:00 (60 mins)	S5. Why open and interoperable Internet infrastructure is key to the Internet's continued success Details	03:00 – 04:00 (60 mins)	S7. Internet Rules: Judicial and Regulatory developments impacts digital rights in Asia Details
					S8. Building digital information literacy skills for trust and well-being Details		S14. Human rights impact of Covid-19 technologies and the role of businesses Details
04:00 – 07:00 (3 hours)	Capacity Building Program for Fellows and Newcomers	04:00 – 05:30 (90 mins)	Opening Plenary	04:00 – 04:20 (20 mins)	Break / Social	04:00 – 04:20 (20 mins)	Break / Social
				04:20 – 05:20 (60 mins)	S4. Decrypting the encryption debate in Asia-Pacific Details	04:20 – 05:20 (60 mins)	S12. MANRS for Policy Makers to improve global routing security Details
					S13. Weaponization of surveillance amod a pandemic in South Ease Asia Details		S11. Digitally-led, Inclusive Growth in the Age of COVID-19 Details
		05:30 – 05:50	Break / Social	05:20 – 06:10	Showcase 2: Internet's	05:20 – 06:10	Showcase 3: Is the internet

Time (UTC)	27 Sep (Mon)	Time (UTC)	28 Sep (Tue)	Time (UTC)	29 Sep (Wed)	Time (UTC)	30 Sep (Thu)
		(20 mins)		(50 mins)	Technical Success Factors Details	(50 mins)	trusted forever? — The issue about the pirate site on “Manga” and freedom of expression in Japan Details
		05:50 – 06:50 (60 mins)	S1. Critical Times: Impact of Digitalization on Climate Change Details	06:10 – 06:30 (20 mins)	Break	06:10 – 06:30 (20 mins)	Break
			S3. Helping kids learn in times of pandemic Details	06:30 – 07:30 (60 mins)	S6. Citizen-Centered Approach on Tackling Hate Speech, Hindering State Authoritarianism and Algorithmic Censorship of Tech Platforms Details	06:30 – 07:30 (60 mins)	Special Session by UN IGF DC-ISSS: A workplan for greater online security and safety
		06:50 – 07:40 (50 mins)	Showcase 1: Transnational conversations on reclaiming freedom of expression online Details		S15. The Impact of the Global Pandemic on Schools on Internet Governance Details		Rapporteur Session by the Fellows

Time (UTC)	27 Sep (Mon)	Time (UTC)	28 Sep (Tue)	Time (UTC)	29 Sep (Wed)	Time (UTC)	30 Sep (Thu)
		07:40 – 07:50 (10 mins)	Break	07:30 – 07:50 (20 mins)	Break / Social	07:30 – 07:50 (20 mins)	Break / Social
		07:50 – 08:50 (60 mins)	S2. Don't shoot the messenger, intermediary liability principles under threat Details	07:50 – 08:50 (60 mins)	S9. More than wor(l)ds : Can AI effectively monitor online harms?Details	07:50 – 09:20 (90 mins)	Closing Plenary
			Session by the Fellows		S10. Advancing Internet Freedom in Asia-Pacific via applying UNESCO's Internet Universality ROAM Principles and Indicators Details		
		08:50 – 09:10 (20 mins)	Break / Social	08:50 – 09:10 (20 mins)	Break / Social		
		09:10 – 10:00 (50 mins+)	Townhall session	09:10 – 10:00 (50 mins+)	Townhall session		

表 7-6　優秀學員參與 APrIGF 2021 場次表

日期	UTC 時間	臺灣時間	撰寫摘要	議程主題
27 Sep (Mon)	04:00 – 07:00 (3 hours)	12:00 – 15:00 (3 hours)	自由參加	Capacity Building Program for Fellows and Newcomers
28 Sep (Tue)	04:00 – 05:30 (90 mins)	12:00 – 13:30 (90 mins)	湯○樺	Opening Plenary
	07:50 – 08:50 (60 mins)	15:50 – 16:50 (60 mins)	楊○楷	【S2】Don't shoot the messenger, intermediary liability principles under threat
29 Sep (Wed)	03:00 – 04:00 (60 mins)	11:00 – 12:00 (60 mins)	陳○耀	【S5】Why open and interoperable Internet infrastructure is key to the Internet's continued success
	03:00 – 04:00 (60 mins)	11:00 – 12:00 (60 mins)	蔡○安	【S8】Building digital information literacy skills for trust and well-being
	06:30 – 07:30 (60 mins)	14:30 – 15:30 (60 mins)	林○德	【S6】Citizen-Centered Approach on Tackling Hate Speech, Hindering State Authoritarianism and Algorithmic Censorship of Tech Platforms
	07:50 – 08:50 (60 mins)	15:50 – 16:50 (60 mins)	湯○樺	【S9】More than wor(l)ds : Can AI effectively monitor online harms?

日期	UTC 時間	臺灣時間	撰寫摘要	議程主題
30 Sep (Thu)	03:00 – 04:00 (60 mins)	11:00 – 12:00 (60 mins)	林○德	【S7】Internet Rules: Judicial and Regulatory developments impacts digital rights in Asia
	03:00 – 04:00 (60 mins)	11:00 – 12:00 (60 mins)	陳○耀	【S14】Human rights impact of Covid-19 technologies and the role of businesses
	06:30 – 07:30 (60 mins)	14:30 – 15:30 (60 mins)	蔡○安	Special Session by UN IGF DC-ISSS: A workplan for greater online security and safety
	07:50 – 09:20 (90 mins)	15:50 – 17:20 (90 mins)	楊○楷	Closing Plenary

二、TWIGF 座談申辦活動

為鼓勵學員結業後仍可持續參加網路治理相關活動，尤其是國內網路治理的年度盛會 TWIGF，本計畫額外提供新臺幣 2 萬元整 TWIGF 座談申辦獎學金，結業學員若成功申辦 TWIGF 2021 座談（workshop），經 TWIGF 評選最高分者且完成辦理該場座談，並於會後提供紀錄摘要（將載於研習營網站的【學習資源】），即可獲頒獎學金。

本年度的 TWIGF 年會活動訂於 12 月 10 日至 11 日舉辦，主題為「新冠疫情後的網路治理」，並自 9 月上旬開始徵求工作坊（座談）提案，執行單位亦發出通知予研習營結業學員，鼓勵其踴躍參與提案。

TWIGF 已於 10 月 15 日截止提案，並於 11 月 1 日公告錄取的工作坊清單，經確認本年度未有研習營結業學員參與提案，推測可能的原因為，申辦 TWIGF 座談對於研習營學員而言門檻過高，以致申請意願較低。

三、yIGF 2021 線上特派員活動

配合本年度研習營選拔優秀學員線上參與 APrIGF 2021 之目標，本研習營亦同時鼓勵符合資格之學員踴躍申請參加 yIGF（Youth IGF）。

由 NetMission 推動的 yIGF，每年皆會與 APrIGF 聯合舉辦，藉以提高青年參與網路治理討論的認知及能力。基於 IGF 將多方利害關係群體平等聚集在一起的任務，yIGF 為年輕世代提供了一個開放的平臺，使他們可以自由的表達與交流對於網路治理的觀點。

本年度的 yIGF 於 9 月 17 至 20 日（UTC 時間 03:00-06:00）連續辦理 4 天的線上活動，主題為「Envisioning a sustainable Internet for today and tomorrow」，入選的參加者將可與亞太地區的青年人才，以及網路治理社群當中具備豐富經驗的專家們，共同討論當前的熱門議題。

凡具備以下任一項資格，即可提出申請：

- 在亞太地區大學或研究所接受高等教育的學生；或
- 18-30 歲之間目前根基或來自於亞太地區的青年專業人士；或
- 曾參與亞太地區網路治理活動的學員或研究員（alumni or fellows）。

執行單位於 8 月 20 日提供 yIGF 申請資訊予本次參與研習營的所有學員，並鼓勵學員踴躍提出申請。經 yIGF 主辦單位遴選後，本研習營學員許◯能（國立臺北教育大學臺灣文化研究所碩士在職專班）順利錄取，並於活動結束後在社群平臺公開分享活動參與心得，執行單位依據本活動獎勵辦法，頒發「yIGF 2021 線上特派員獎學金」NT$ 4,000 元整（由外部資源挹注）。

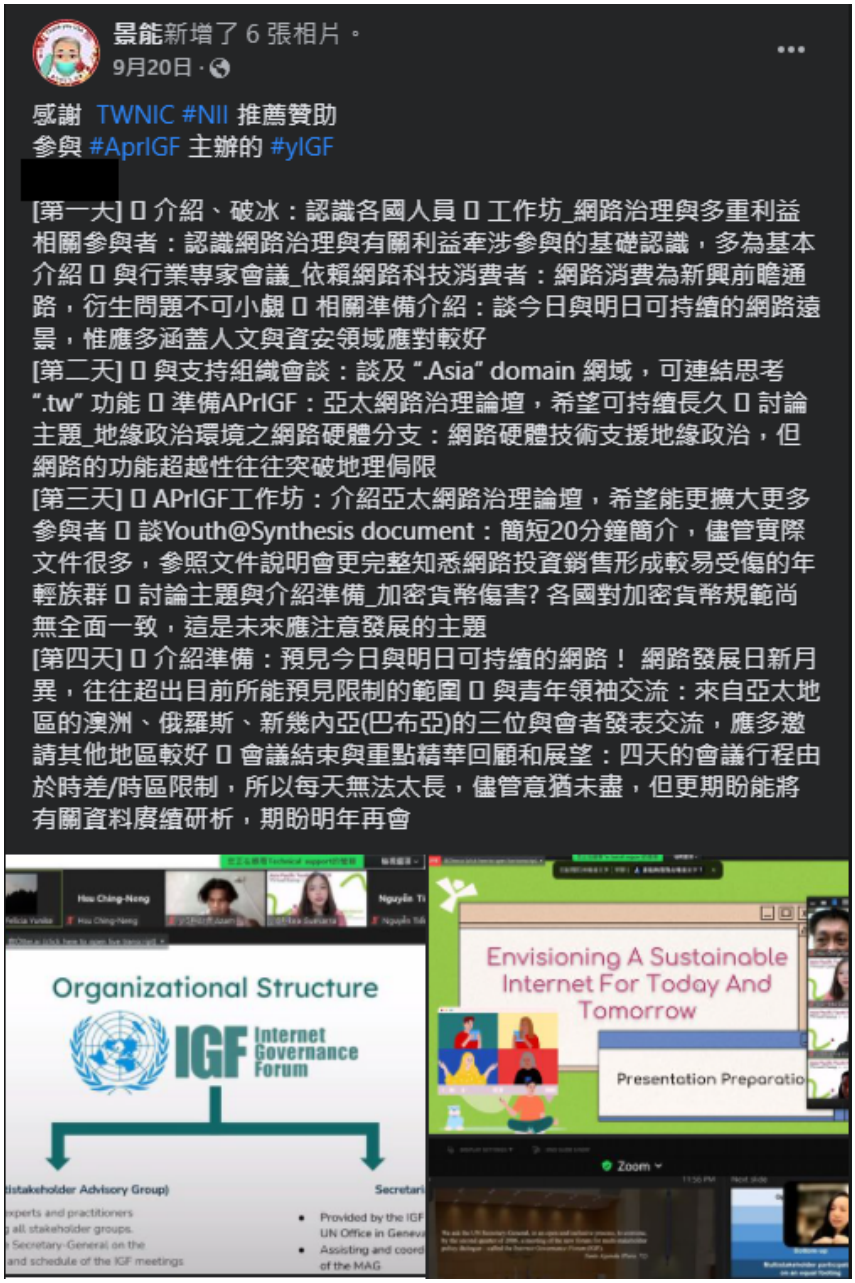


圖 7-15　學員許○能於 facebook 分享 yIGF 活動參與心得

第八章 課程影片製播

第一節 執行概況

本工作項主要係將「2021 網路治理研習營」全日課程剪輯成為 2 小時視訊課程且上傳至網路，並從中製成 3 支 5 分鐘以上的精華短片且上傳至 YouTube，以作為網路治理議題的數位教材（參閱表 8-1）。精華短片需有字幕、影片標題有網路治理相關關鍵字，以及需提供「影片點閱流量分析」。

表 8-1 課程影片製播總表

序號	類型	片名	製播方式	片長
1	2 小時視訊課程	2021 網路治理研習營—課程影片	執行單位企劃剪輯	2 小時 15 分
2	精華短片	5G 熱潮來了，我們生活要改變了！「智慧生活」是什麼？ 5G is here, our life is going to change forever!	與網紅合作，雙方共同企劃腳本，執行單位協助安排訪談，並提供後製建議	12 分 31 秒
3	精華短片	2021 網路治理研習營—課程精華（一）	執行單位企劃剪輯	8 分 25 秒
4	精華短片	2021 網路治理研習營—課程精華（二）	執行單位企劃剪輯	8 分 14 秒

執行單位於本計畫執行期間，除持續推廣影片外，亦定期查看 YouTube 頁面是否有新增留言，以即時回應。

第二節 2 小時視訊課程

一、製播方式

本計畫於線上辦理「2021 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，由四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）。

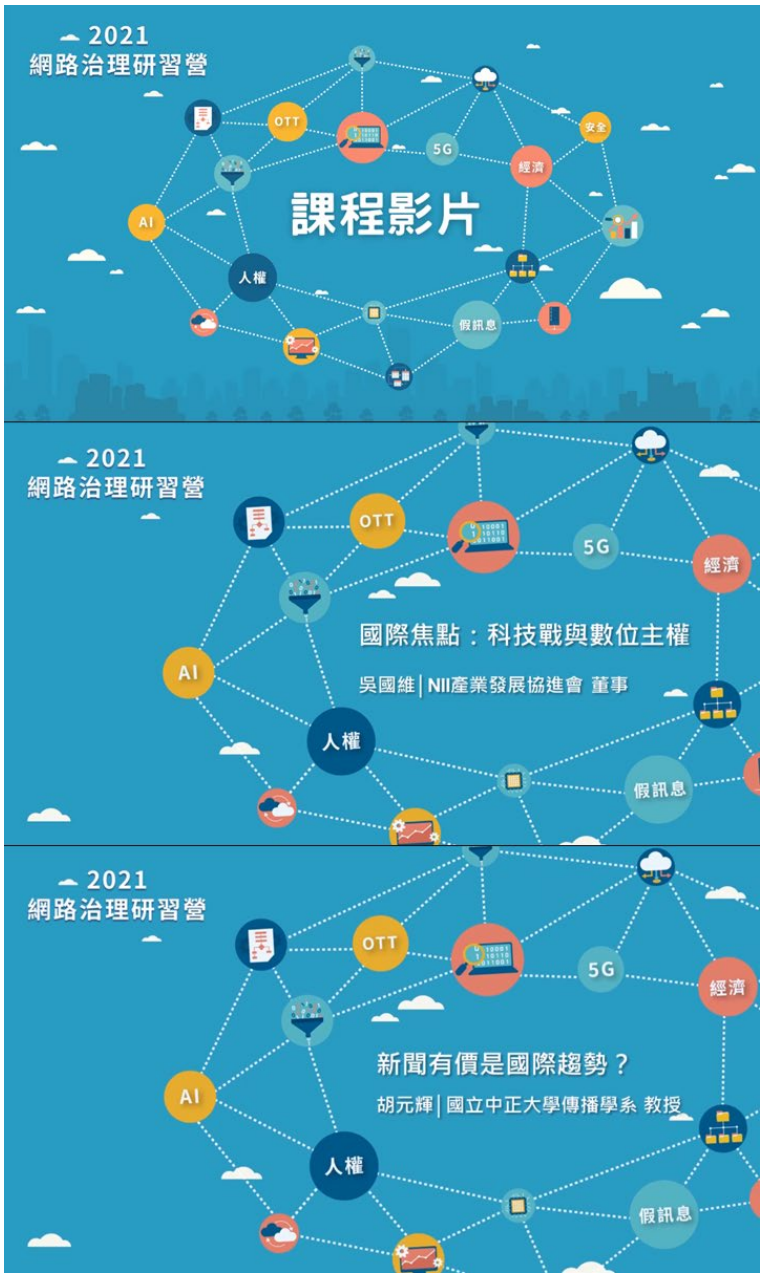


圖 8-2　課程影片視覺設計

本課程影片相關資訊彙整如下：

- 片名：2021 網路治理研習營—課程影片
- 片長：2 小時 15 分
- 網址：https://youtu.be/WRyIS7p2OyM
- 課程內容：

  ✧國際焦點：科技戰與數位主權

  講者：吳國維 / NII 產業發展協進會 董事

  ✧新聞有價是國際趨勢？

  講者：胡元輝 / 國立中正大學傳播學系 教授

  ✧內容亂象誰負責？

  講者：曾更瑩 / 理律法律事務所 合夥律師

  ✧網路安全：從資安到國安議題

  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 #數位主權 #科技戰 #新聞議價法 #網路內容 #CDA230 #數位服務法 #網路安全 #資安即國安
- 公開日期：2021 年 9 月 2 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。

考量研習營課程內容稍有難度，即便剪輯過後也不易吸引大眾觀看，參考去年度的執行經驗，藉由與 YouTuber 合作，可快速將影片推播至上萬名觀眾眼前，因此執行單位於本計畫啟動會議中即徵詢通傳會同意，篩選國內奈米網紅（粉絲數 1 千~1 萬）或網路媒體共同合作，期可達到一定規模的推廣成效。

在短片主題的設計上，係挑選與大眾關聯性較高，且近期較為熱門的網路治理議題，合作方式為雙方共同企劃影片內容，再依據各自的專業領域，由網紅負責主持、訪問、拍攝、製播影片，執行單位則是負責研擬引言及訪談題目、協助挑選剪輯重點、提供專有名詞等文字資料。

惟考量本年度計畫預算規模不若去年，本年度僅足以合作製播 1 支短片，其餘 2 支短片則由執行單位在剩餘的預算內自行製播，合先敘明。

二、短片內容

（一）短片 1

本短片係與去年曾經合作，且成果頗受到好評的網紅馮韋元再次合作。馮韋元為中文聽說讀寫流利的法國人，於 Yahoo 任軟體工程師，工作也受到 GDPR 等規範影響，屬於多方利害關係人之技術社群，與本計畫屬性具相關性；其 YouTube 頻道的訂閱人數超過 12 萬，發布的影片數將近 200 支，內容多為學習語言、戶外活動、探討文化差異等，形象相當正面，具備一定程度的群眾影響力。

本次合作的影片係以 5G 為主軸，提醒觀眾在迎接 5G 到來的同時也要認識相關的風險，並建立網路安全意識，才能促進 5G 蓬勃發展。影片採用訪談的方式進行，由馮韋元擔任主持人，受訪者為台灣網路資訊中心（TWNIC）的黃勝雄執行長，採討的內容涵蓋：什麼是 5G 及在臺灣有哪些 5G 智慧已經上路、目前網路攻擊問題與對使用者的影響、5G 智慧生活的安全風險與 4G 有何不同、民眾應具備的 5G 防護新思維。

圖 8-3　精華短片 1 示意圖

本短片相關資訊彙整如下：

- 片名：5G 熱潮來了，我們生活要改變了！「智慧生活」是什麼？

  5G is here, our life is going to change forever!

- 片長：12 分 31 秒
- 網址：https://www.youtube.com/watch?v=sCE6qMwOOIk
- 主持人：馮韋元
- 受訪專家：黃勝雄／台灣網路資訊中心 執行長
- 內容：

  ✧5G 功能簡介

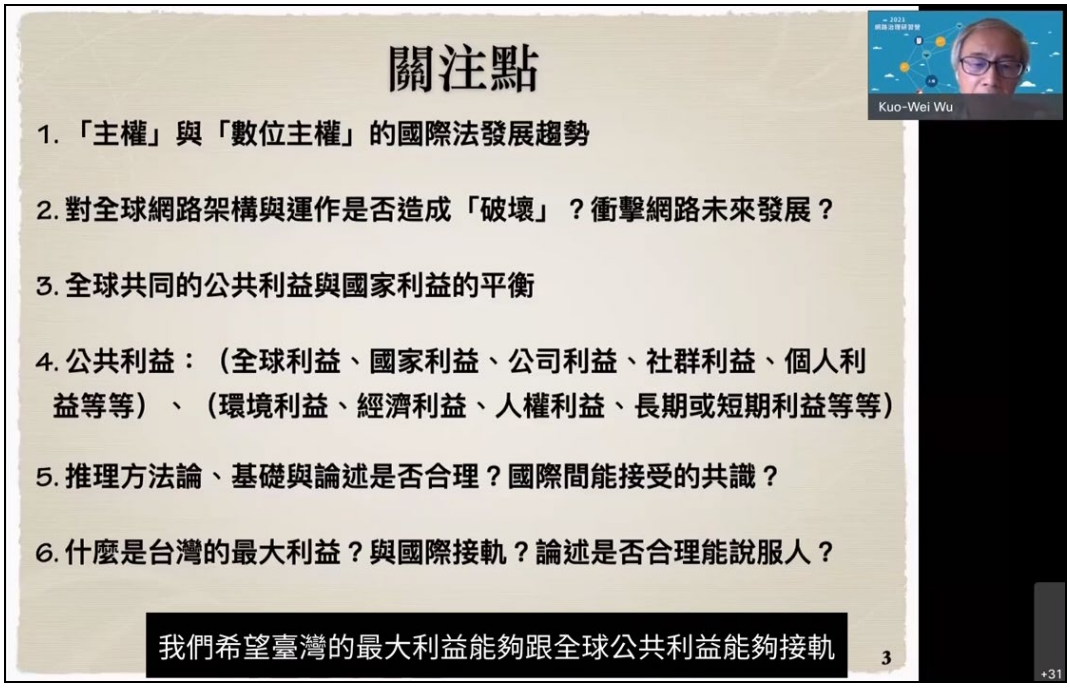
  ✧伴隨 5G 而來的新型態網路攻擊

  ✧使用者的因應之道

- 關鍵字：#5G 功能 #5G 安全 #5G 使用 #智慧生活
- 公開日期：2021 年 10 月 19 日

（二）短片 2

本短片係剪輯自 2 小時視訊課程影片，摘錄 NII 產業發展協進會吳國維董事演講「國際焦點：科技戰與數位主權」當中提及「數位主權的關注點」，以及台灣網路資訊中心黃勝雄執行長演講「網路安全：從資安到國安議題」當中提及「網路安全風險日漸重大」兩個段落。



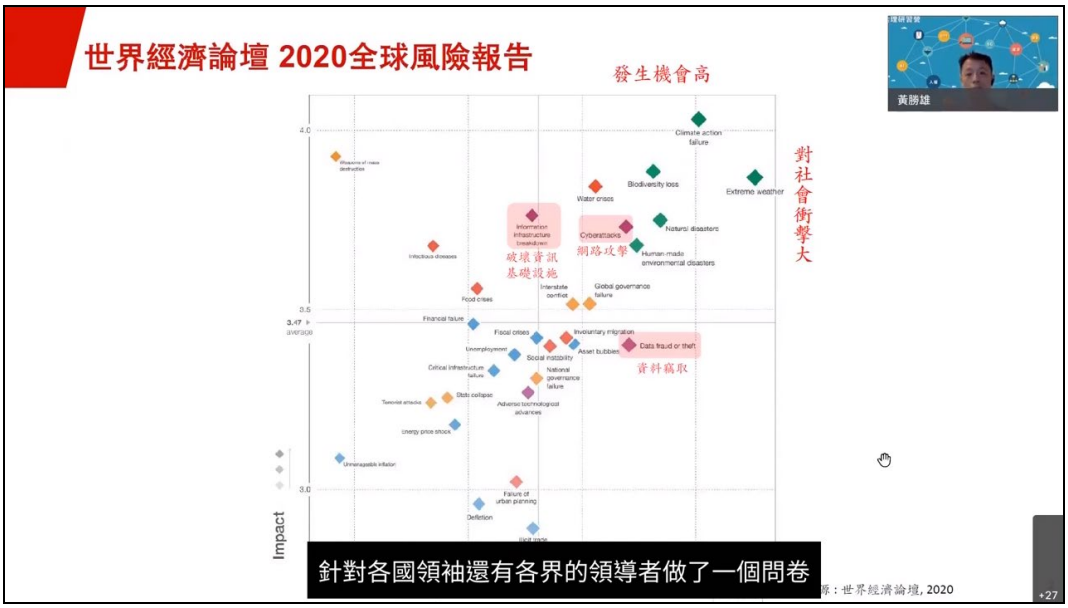


圖 8-4　精華短片 2 示意圖

本短片相關資訊彙整如下：

- 片名：2021 網路治理研習營—課程精華（一）數位主權的關注點有哪些？如何因應日漸重大的網路安全風險？
- 片長：8 分 25 秒
- 網址：https://www.youtube.com/watch?v=0nTcD1hM7oA
- 內容：

  ✧數位主權的關注點

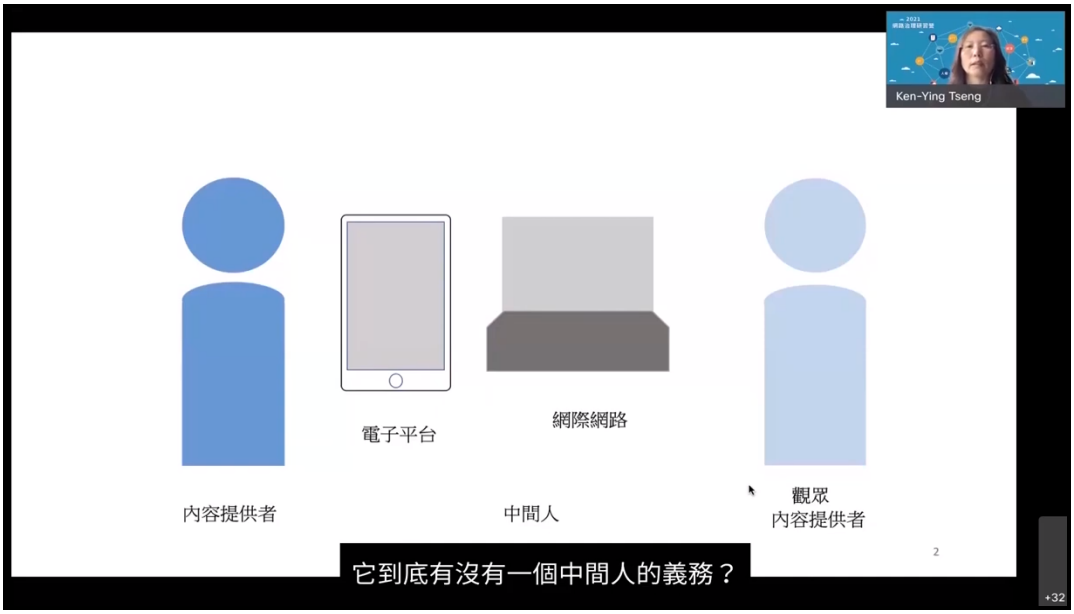
  講者：吳國維／NII 產業發展協進會 董事

  ✧網路安全風險日漸重大

  講者：黃勝雄／台灣網路資訊中心 執行長
- 關鍵字：#數位主權 #網路治理 #網路安全 #資安即國安 #2021 網路治理研習營
- 公開日期：2021 年 9 月 30 日

（三）短片 3

本短片同樣剪輯自 2 小時視訊課程影片，摘錄理律法律事務所曾更瑩律師演講「內容亂象誰負責？」當中提及「誰應該對網路平臺的內容負責」，以及台灣網路資訊中心黃勝雄執行長演講「網路安全：從資安到國安議題」當中提及「網路空間如何被規範」兩個段落。



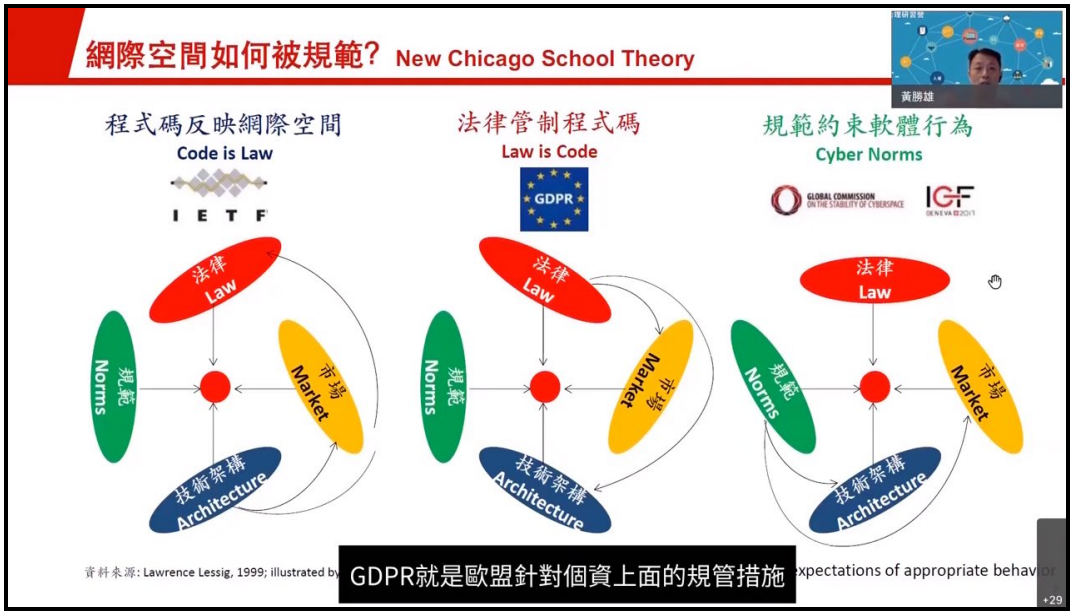


圖 8-5　精華短片 3 示意圖

本短片相關資訊彙整如下：

- 片名：2021 網路治理研習營—課程精華（二）誰應該對網路平臺的內容負責？網路空間如何被規範？
- 片長：8 分 14 秒
- 網址：https://www.youtube.com/watch?v=Me5KWy_mclw
- 內容：

  ✧誰應該對網路平臺的內容負責

  講者：曾更瑩／理律法律事務所 律師

  ✧網路空間如何被規範

  講者：黃勝雄／台灣網路資訊中心 執行長
- 關鍵字:#網路內容 #網路規範 #網路治理 #2021 網路治理研習營
- 公開日期：2021 年 11 月 3 日

第四節 影片廣宣

由於短片 1 係公開於合作網紅之 YouTube 頻道，且觀看次數已破萬次，無須本計畫另行投入廣宣資源，另一方面，考量 2 小時課程教學影片對於一般視聽者的吸引力較低，為使廣宣預算達到最大化運用，執行單位係以短片 2 及短片 3 為標的，透過購買 YouTube 廣告進行推廣。

短片 2 及短片 3 的影片介紹欄位內，亦列出 2 小時課程教學影片的連結，便於有興趣進一步了解研習營課程內容的觀眾快速前往觀看，達到間接宣傳的效果，除此之外，2 小時課程教學影片亦可做為未來辦理網路治理研習營的課前預習教材，持續發揮效益。

圖 8-6　YouTube 廣告示意圖

在執行單位所設定之廣宣預算內，短片 2 的曝光次數為 1.92 萬次，觀看次數增加 381 次；依據 YouTube 所設定的分眾，影片觀看次數最高的分眾為「愛書人」(81%)，其次為「電視節目迷」(9%)；女性觀眾略高於男性(197 人：167 人)；年齡層以 55-64 歲最多，65 歲以上居次(參閱圖 8-7)。

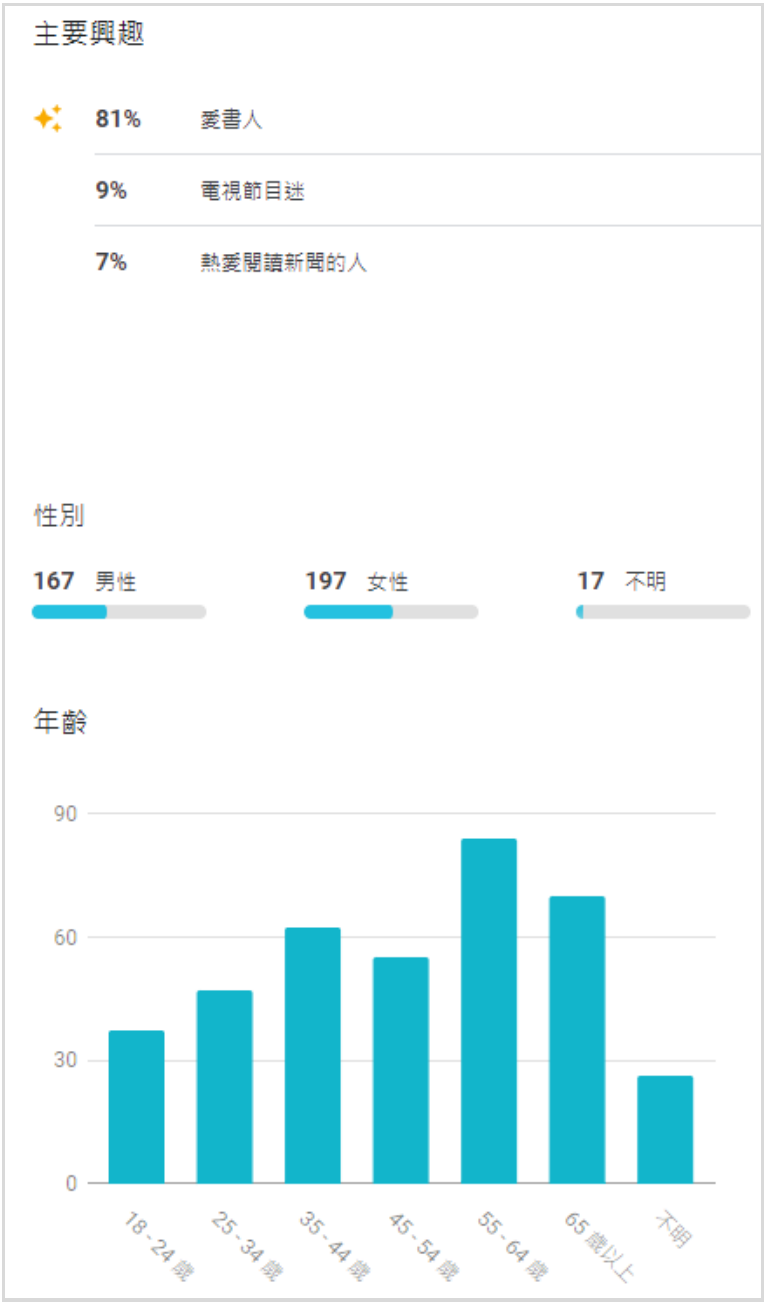


圖 8-7　短片 2 廣宣成效

短片 3 的曝光次數為 2.66 萬次，觀看次數增加 570 次；依據 YouTube 所設定的分眾，觀看次數最高的分眾亦為「愛書人」(63%)，其次為「輕度電視觀眾」(18%)；女性占比明顯高於男性（313 人：249 人）；年齡層以 65 歲以上最多，35-44 歲居次（參閱圖 8-8）。

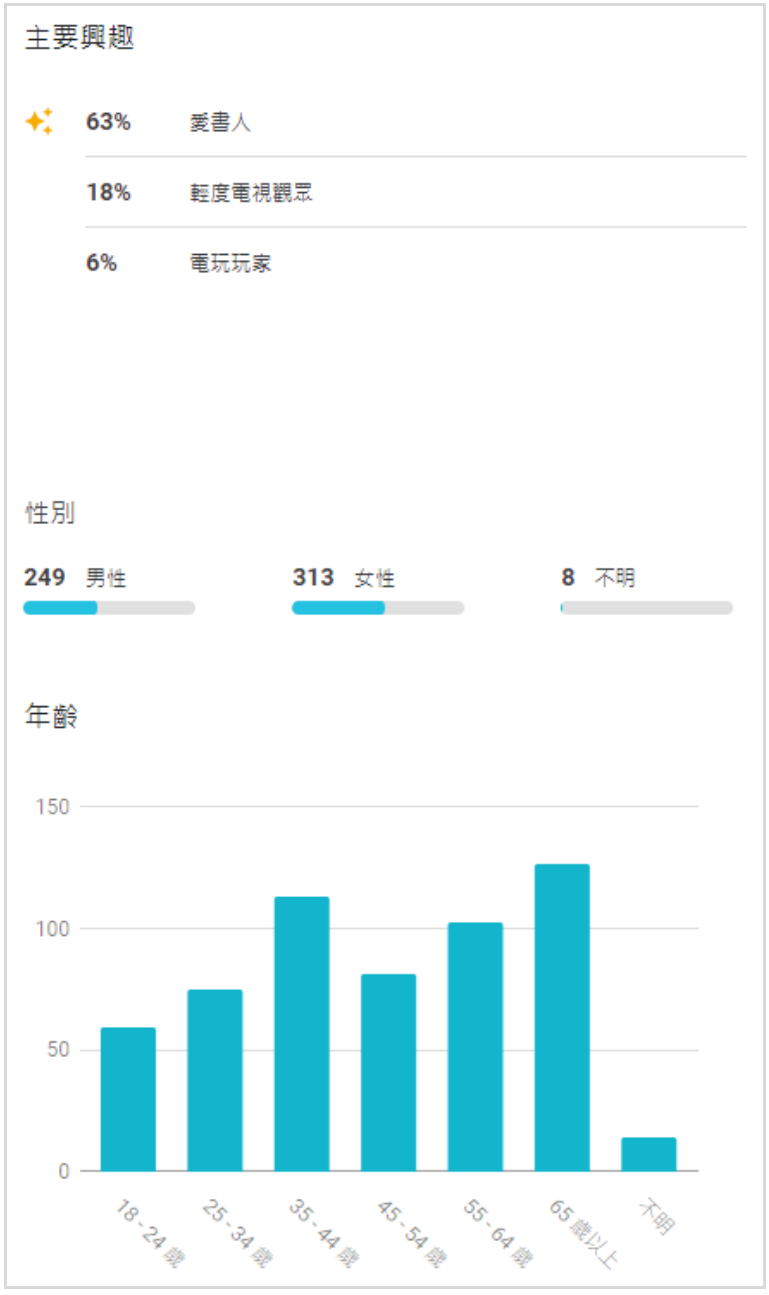


圖 8-8　短片 3 廣宣成效

第五節 流量統計分析

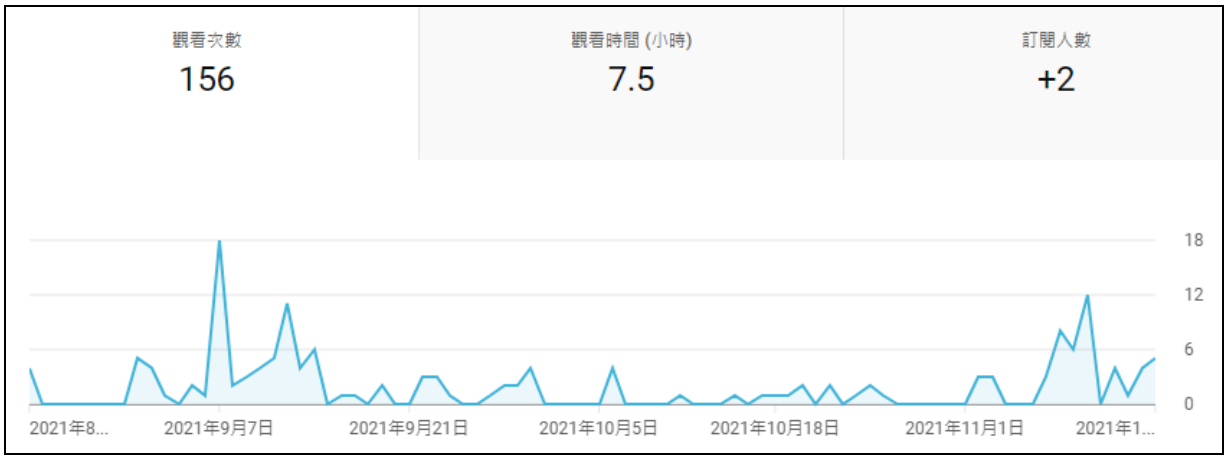
以下針對本計畫產出之 2 小時視訊課程影片及 3 支精華短片流量進行分析，惟短片 1 係公開於合作網紅之 YouTube 頻道，相關數據資料皆由網紅提供（統計至 10 月 31 日），其來源資料介面與執行單位所使用的略有差異，但雙方的數據均來自 YouTube 平臺，統計規則一致。

配合本報告期末送審時程，除短片 1 之外，其餘影片之流量均統計至 11 月 15 日，合先敘明。

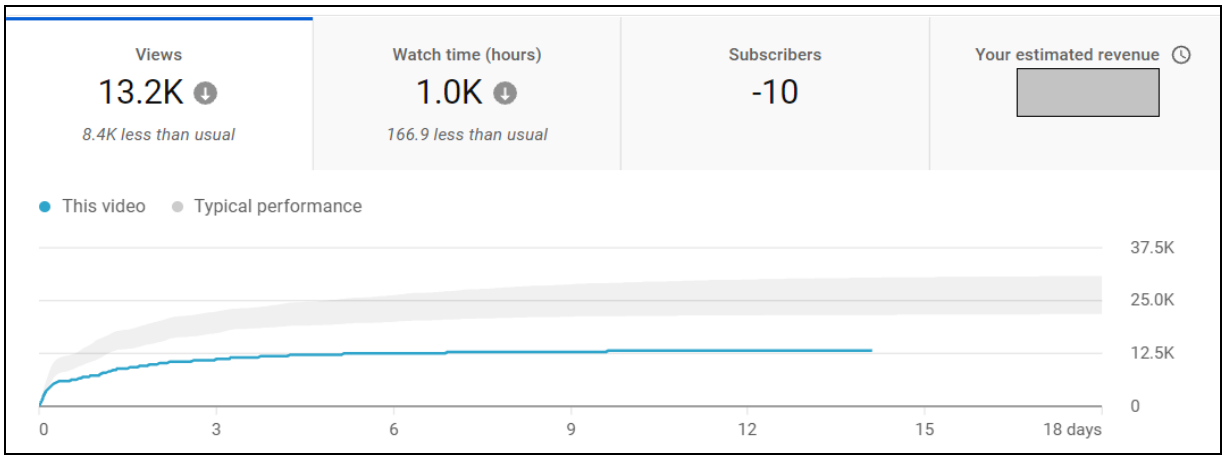
一、觀看次數與時間

2 小時視訊課程影片的觀看次數為 156 次，累積觀看時數達到 7.5 小時；短片 1 的觀看次數為 1.32 萬次，累積觀看時數達到 1,000 小時；短片 2 及短片 3 的觀看次數分別為 438 次與 580 次，累積觀看時數分別為 4.6 小時與 4.1 小時（參閱圖 8-9）。

2 小時視訊課程影片



短片 1：5G 熱潮來了，我們生活要改變了！「智慧生活」是什麼？



短片 2：2021 網路治理研習營—課程精華（一）

短片 3：2021 網路治理研習營—課程精華（二）

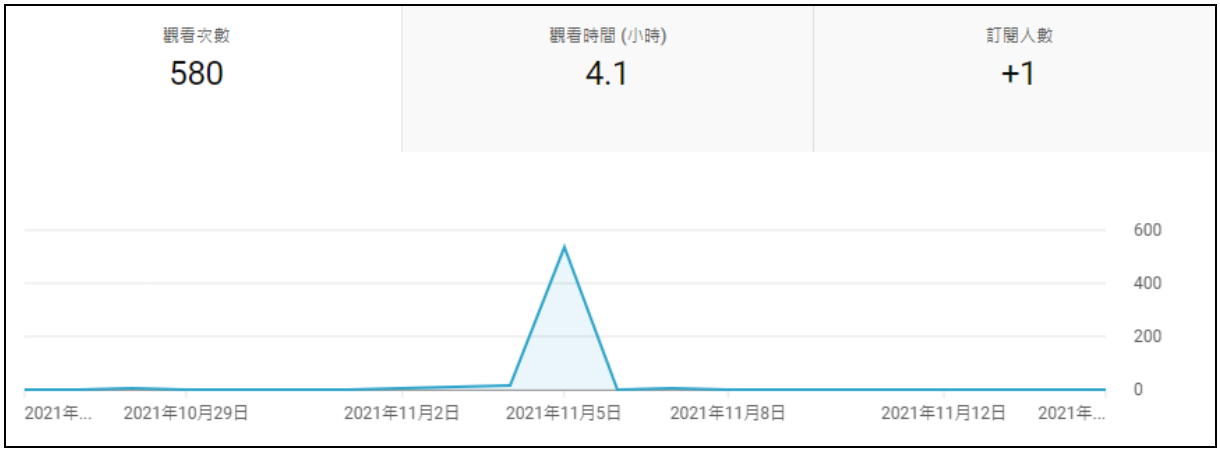


圖 8-9　影片觀看次數及時間

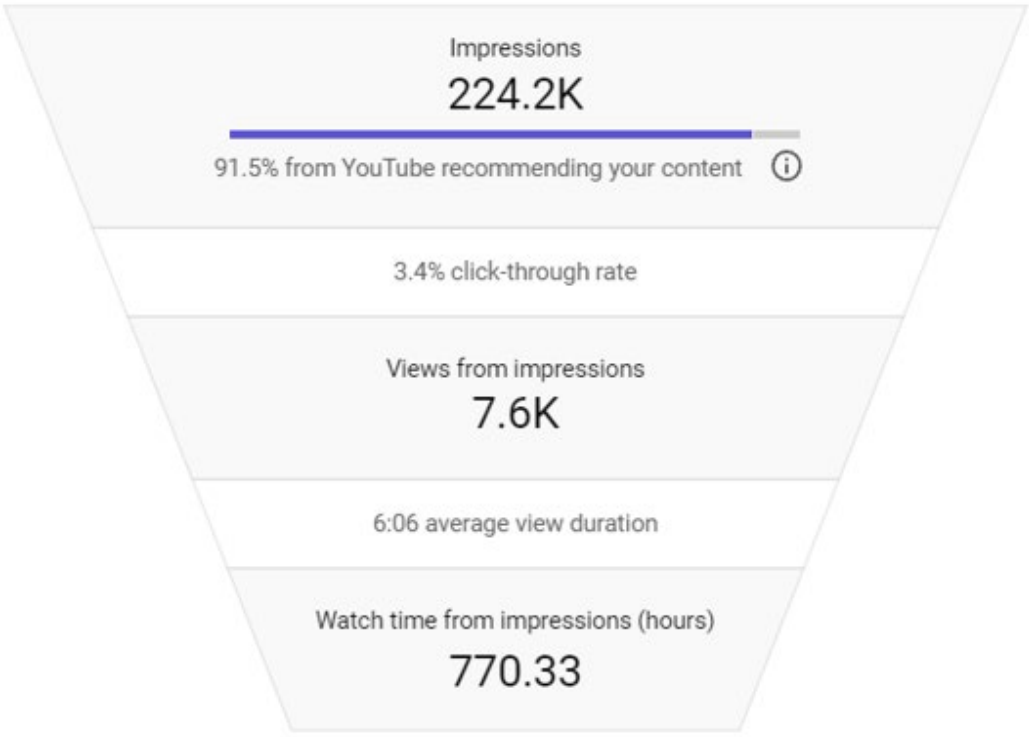
二、曝光次數與流量

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。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 235 次，3 支精華短片則依序為 22.4 萬次、214 次及 150 次，其中短片 3 因為 11 月初才剛公開，故自動曝光的次數明顯低於其他影片。

來自曝光次數的點閱率，2 小時視訊課程影片為 6.4%，3 支精華短片則依序為 3.4%、8.4%及 6.0%（參閱圖 8-10）。

2 小時視訊課程影片

短片 1：5G 熱潮來了，我們生活要改變了！「智慧生活」是什麼？



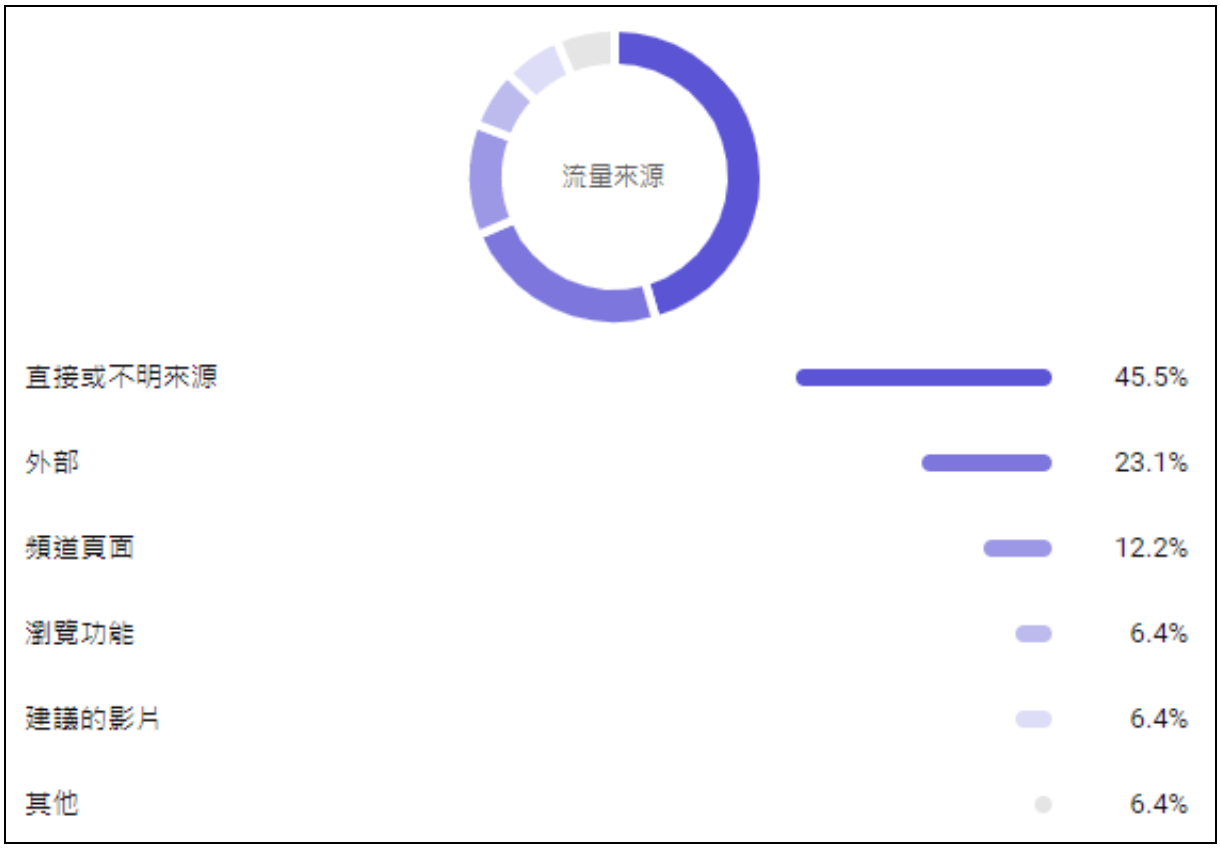
短片 2：2021 網路治理研習營—課程精華（一）

短片 3：2021 網路治理研習營—課程精華（二）

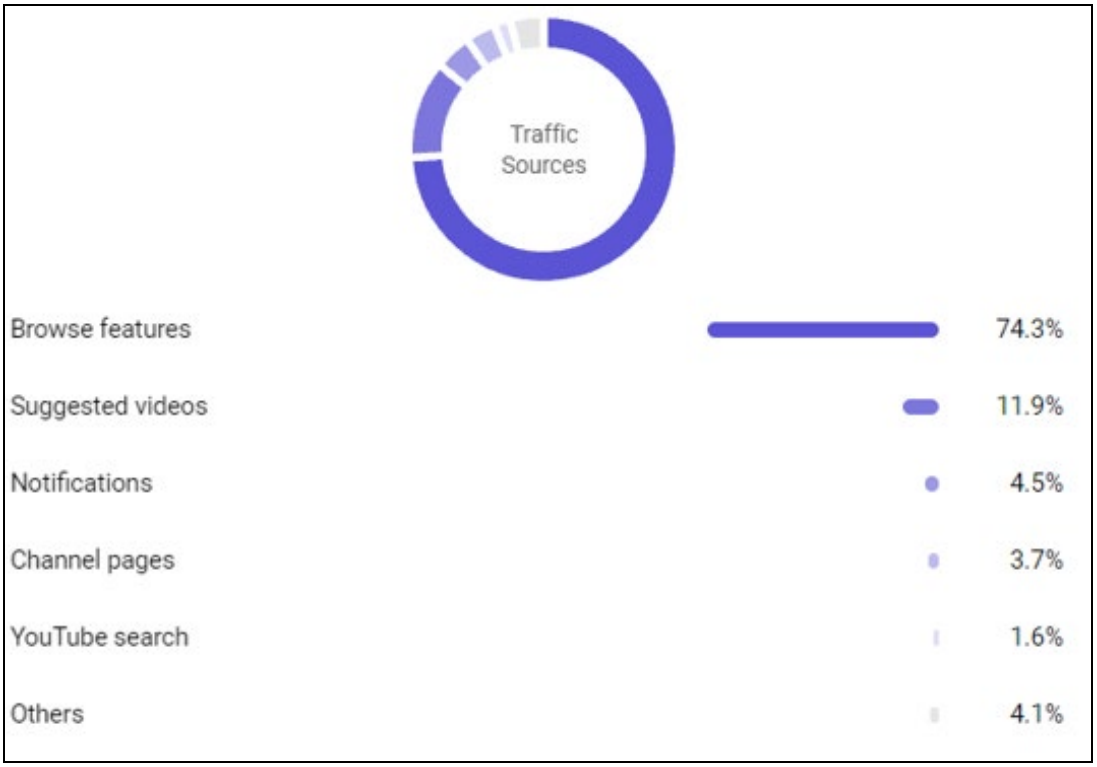
圖 8-10　影片曝光次數及點閱率

YouTube 統計的影片「流量來源類型」，可以顯示觀眾是透過哪些管道找到該影片。根據統計結果，2 小時視訊課程影片將近半數（45.5%）的流量來自「直接或不明來源」（YouTube 定義：直接輸入網址、書籤和不明應用程式）；與網紅合作的短片 1 主要流量（74.3%）則是來自「瀏覽功能」（YouTube 定義：流量來自首頁/主畫面、訂閱內容動態消息和其他瀏覽功能）；透過 YouTube 廣告加強推廣的短片 2 及短片 3，流量則明顯來自「YouTube 廣告」，比例分別為 83.1%及 95%（參閱圖 8-11）。

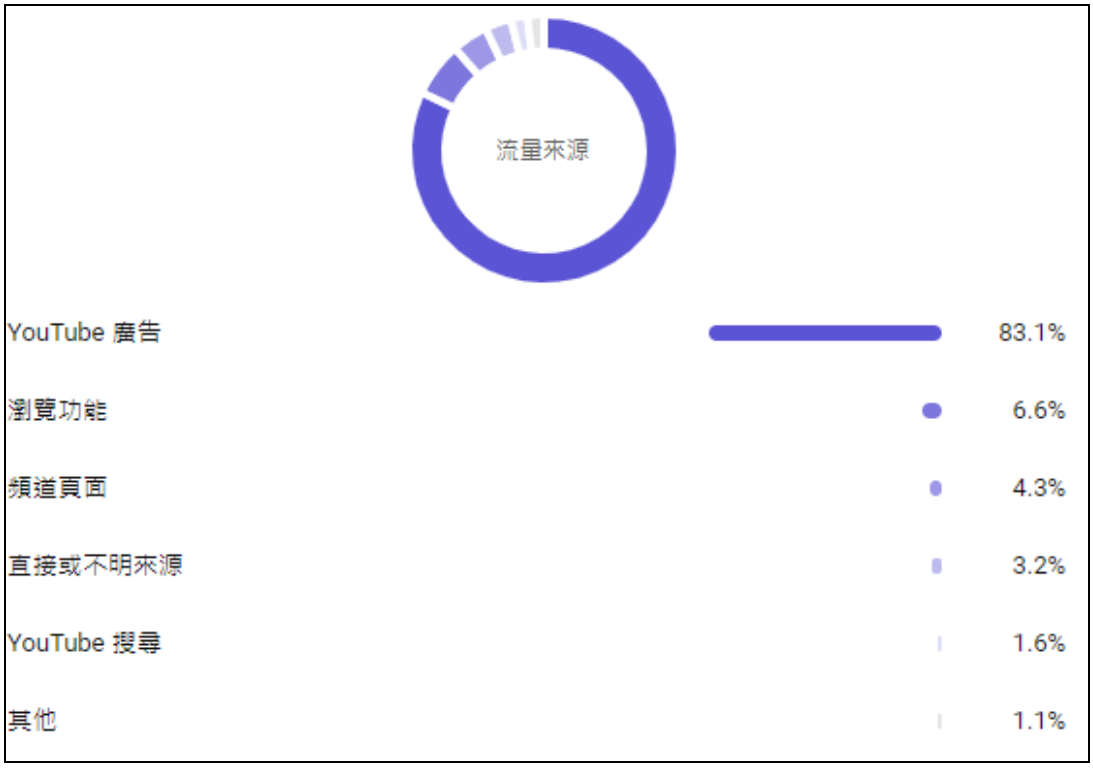
2 小時視訊課程影片



短片 1：5G 熱潮來了，我們生活要改變了！「智慧生活」是什麼？



短片 2：2021 網路治理研習營—課程精華（一）



短片 3：2021 網路治理研習營—課程精華（二）

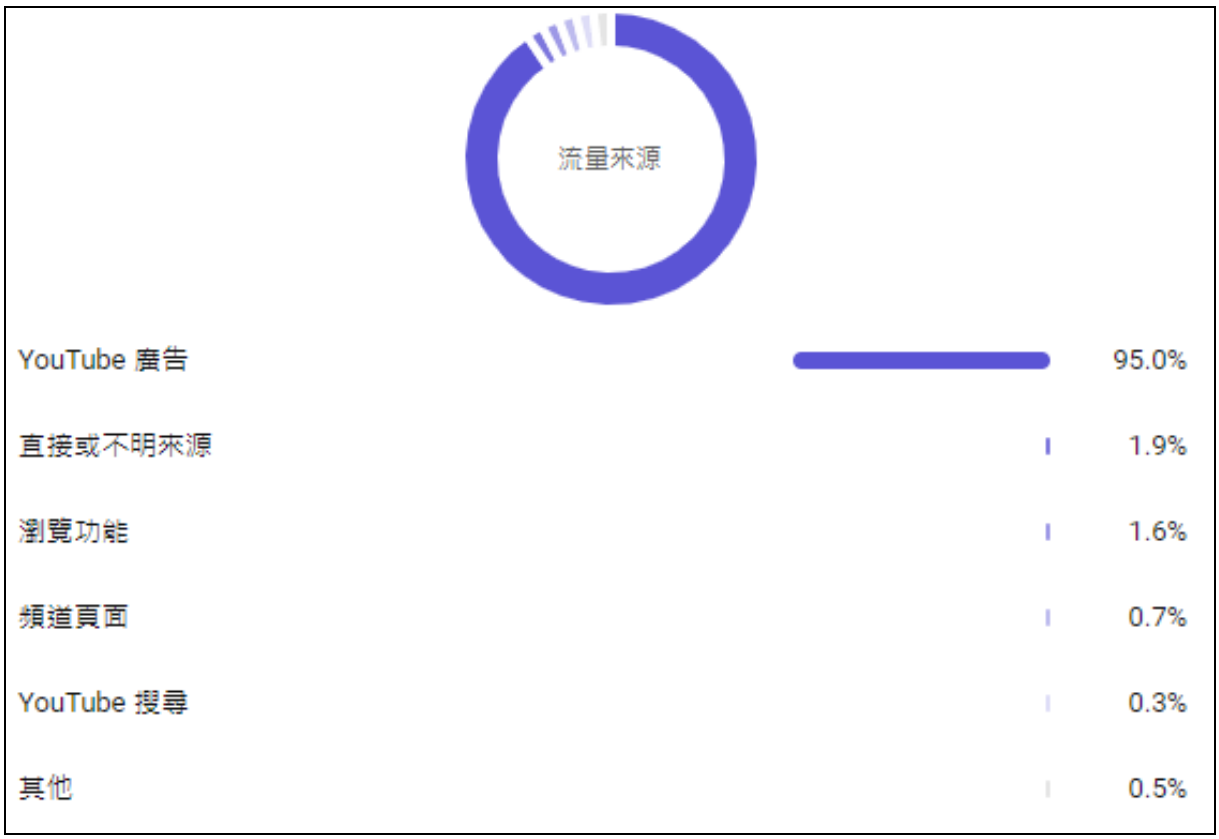


圖 8-11　影片流量來源

三、觀眾性別與年齡

YouTube 管理後臺針對單一影片所提供的觀眾性別與年齡分析，需於影片達到一定程度的瀏覽量後才能進行，本次的 4 支影片當中，因 2 小時視訊課程影片尚未達到可分析的人數門檻，故以下僅呈現 3 支精華短片的分析數字。

短片 1 的觀眾以男性居多（57.2%），年齡層以 45 歲~54 歲為最多，35 歲~44 歲居次；短片 2 的觀眾恰為男女性各半（50.0%），年齡層以 55 歲~64 歲為最多，65 歲以上居次；短片 3 的觀眾以女性居多（56.1%），年齡層以 65 歲以上最多，35 歲~44 歲居次（參閱圖 8-12）。

短片 1：5G 熱潮來了，我們生活要改變了！「智慧生活」是什麼？

短片 2：2021 網路治理研習營—課程精華（一）

短片 3：2021 網路治理研習營—課程精華（二）

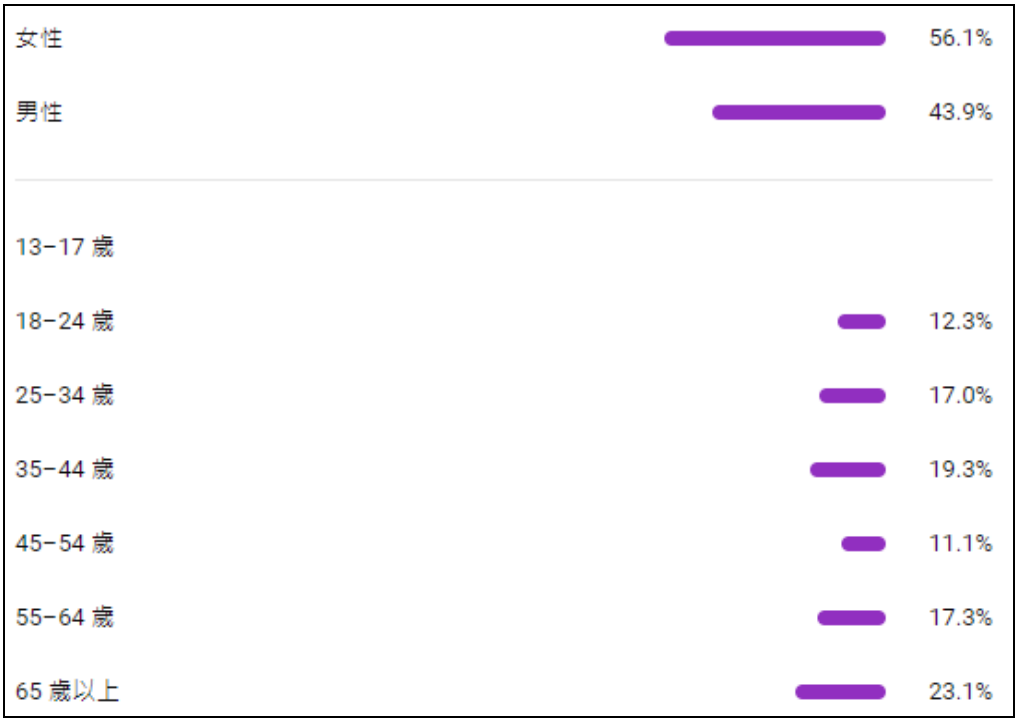


圖 8-12　觀眾性別與年齡分布

第九章 國際會議 EuroDIG 參與報告

第一節 會議簡介

一、會議背景

歐洲網路治理論壇（European Dialogue on Internet Governance, EuroDIG）於 2008 年由數個組織、政府代表與專家創立，為歐洲地區討論網路治理公共政策議題的一個開放性平臺，提供多方利害關係人意見交流、溝通對話、經驗分享、學習最佳實務運作，以及促進合作的機會，進而期能整合不同國家的歧見，塑造歐洲共同的網路價值與觀點。其主要支持單位包括歐盟執委會（European Commission, EC）、歐洲廣播聯盟（European Broadcasting Union, EBU)、歐洲電信業者協會（European Telecommunications Network Operators' Association, ETNO）、歐洲網路資訊中心（RIPE NCC）等。

EuroDIG 旨在成為歐洲地區促進網路治理政策討論和決策的平臺，而非形成決策的正式場合，每年於不同的歐盟城市舉辦年度論壇。**其議程的形成，於近年改為「完全開放所有人參與」，也就是公開徵求提案後，不再進行評選作業，而是將所有提案依主題分成不同場次，讓同一場次的提案者和有興趣的民眾共同組成籌辦小組，討論和規劃其講者及議題等細節。**而在 EuroDIG 結束後，主辦單位也會將討論成果彙整成報告，並提交至聯合國 IGF 供全球參考。

二、2021 年會議資訊

受到 COVID-19 疫情持續的影響，於 2021 年 6 月 28 日至 30 日登場的第 14 屆 EuroDIG，第二度以線上方式進行。本次大會主題為「邁向歐洲的數位十年」（Into Europe's Digital Decade），討論主題分成「連 網 與 素養」、「網路治理生態系統發展」、「人權與資料保護」、「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」8 大類別，焦點會議和座談共有 22 場（議程請詳 https://eurodigwiki.org/wiki/Consolidated_programme_2021），吸引超過 700 人線上參與，當中包括 160 多位非歐洲國家的民眾。本計畫線上參與的場次如下表 9-1 所列，並於後續章節摘要相關討論重點。

表 9-1　EuroDIG 2021 線上參與場次

主題類別	編號*	場次名稱
網路治理生態系統發展	WS 1	Digital services regulation – opportunities and challenges 數位服務規範—機會與挑戰
人權與資料保護	WS 7	Human vs. algorithmic bias – is unbiased decision-making even a thing? 人為 vs. 演算法偏見—無偏見的決策值得關注嗎？
創新與經濟	WS 15	5G User perspective and implementation 5G 的用戶觀點和實施
媒體與內容	FS 4	European mediascape – How to (re)create a trusted public sphere? 歐洲媒體景觀—如何重塑可信賴的公共領域？
	WS 10	Fake News – Dissolving Superstitions with Media Literacy 假新聞—以媒體素養消除迷信
	WS 12	Best practices of self- and co-regulation of platforms towards a legal framework 邁向法規框架的平臺自律和共管最佳實踐
技術與維運	WS 9	Content moderation on the Internet infrastructure level – Where does censorship begin?

主題類別	編號*	場次名稱
		網路基礎建設的內容管理—審查是從何處開始的？
跨領域 / 其他	WS 5	Crypto Wars 3.0 – can privacy, security and encryption co-exist? 加密戰 3.0—隱私、安全和加密能否共存？

*WS 代表座談會議（Workshop Session）；FS（Focus Session）代表焦點會議。

第二節 會議重點摘要

一、數位服務規範——機會與挑戰

(一) 歐盟「數位服務包裹法案」簡介

本場會議首先由歐盟執委會資通訊網絡暨科技總署（DG CONNECT）法律官員 Denis Sparas 簡介歐盟「數位服務包裹法案」包含《數位服務法》（Digital Service Act, DSA）草案與《數位市場法》（Digital Market Act, DMA）草案，期能藉由鼓勵供應商和用戶採取問責制和負責任的行為等方式，促進歐盟市場的良好運作；並規範大型服務供應商的市場主導地位，為歐洲業者提供公平的競爭機會。

(二) 對《數位市場法》看法

倫敦帝國理工學院（Imperial College London）經濟學教授 Tommaso Valletti 表示，DMA 不會取代消費者保護和競爭的法規，而是補充現有的監管框架，並作為事前的工具。然而，法規未涵蓋合併和收購議題是個缺點，目前許多企業家的主要目標是將事業出售給大型業者，因此，應該建立一個開放和多樣化的生態系統，讓歐洲企業家得以在數位經濟中生存和發展。

Google 歐洲、中東和非洲地區競爭部門總監 Oliver Bethell 則認為，雖然 DMA 之確保服務市場競爭力、增加創新和消費者選擇等立法目標很重要，但需要更明確化，才能讓業者理解和遵循，減少訴訟和衝突。另外，法規還需保持修訂的彈性，而業者的產品設計也應該要考量法規的遵循。

(三) 對《數位服務法》看法

國際人權組織 Article 19 資深法務 Gabrielle Guillemin 指出，雖然民間團體肯定 DSA 對內容審核政策透明度的詳盡義務規範，以及對於基於善意而努力主動刪除非法內容的業者提供保護傘。但是，他們也擔心通知和行動系統（notice-and-action system）可能會對言論自由產生寒蟬效應，因為

缺乏資源的小公司很可能無法詳細審核內容，但又為了遵循法規而採取擴大刪除內容的做法。

推動塑造網路常規的非營利組織——網路與管轄權網絡（Internet & Jurisdiction Policy Network）內容計畫主任 Frane Maroevic 表示，跨國司法管轄權將是 DSA 的一項重大挑戰，因為法規要處理非法內容，但卻沒有提供定義，而每個國家的非法內容皆有所差異，未來可能導致法律衝突。

(四) 會議共識（結論與建議）

- 「數位服務包裹法案」應支持一個開放、多元和競爭的生態系統，讓小型參與者，尤其是歐洲的創業家，也能夠生存。
- 「數位服務包裹法案」應該要足夠細緻和明確，如此業者才能理解並遵循法規，但同時也要保有彈性，並且可以根據實證和市場反應進行修訂和更新。
- 產品設計是達成常規遵循的要素，因此，產品設計應該注意現有法規，並盡可能幫助實現立法目標。
- 「數位服務包裹法案」應處理特有議題，例如：內容治理條款可能造成寒蟬效應；並提升法規的明確性，例如：盡職調查（Due Diligence）等責任、適用地區和域外效力。

二、人為 vs. 演算法偏見—無偏見的決策值得關注嗎？

(一) 機器學習簡介

本場會議首先由 IBM 公司 AI 研究員 Karthikeyan Natesan Ramamurthy 簡介機器學習的概念。他表示，機器需要透過資料學習，但是偏頗的資料會導致偏頗的預測，而且在建立系統的每個步驟都可能出現偏見，進而可能導致侵犯人權和其他社會高度重視的原則，因此，我們需要制定政策來降低風險。

(二) AI 決策偏見及改善建議

國際人權組織歐洲理事會（Council of Europe）政策發展小組共同主席 Zoltán Turbék 也指出，機器學習可以改善人類決策，但使用有偏見的資料會導致不合理的決策。因此，正如人類決策需有糾正措施，使用 AI 系統也需有透明度、可解釋性等機制，尤其當 AI 決策會影響人權時，例如：用於司法系統，必須非常小心謹慎。同樣的，日本 RIKEN 中心革新智能研究院（RIKEN Center for Advanced Intelligence Project)AI 安全部門負責人 Hiromi Arai 亦表示，機器學習和決策是所謂的黑盒子模式（人類無法得知機器的決策過程和原因），如果用於工作聘僱或教育，將對人類生活產生重大影響，所以，我們必須關注 AI 決策的偏見問題。

俄羅斯科學與技術學院（Skolkovo Institute of Science and Technology）資深科學家 Ekaterina Muravleva 則呼籲在開發系統時，就應該採取特殊措施，以避免導致偏頗的預測，同時也不能依賴基於機器學習技術的系統，應該將這些系統視為輔助或建議工具，而不是主要的解決方案。

另外，Turbék 還就政策規範提出建議。他表示，民間企業的自律很重要，但因為不具有約束力，所以，國家也需要訂定法規進行監管，國際間也需要相互合作，例如：聯合國教科文組織（UNESCO）、歐盟、經濟合作暨發展組織（OECD）等單位在此領域都相當積極。總之，AI 監管沒有單

一的最佳解決方案，需要的是企業、政府和國際間的合作和互補。

(三) 會議共識（結論與建議）

- 演算法的偏見對於會影響人權的敏感決策，尤其令人擔憂。機器學習的結果應該只被視為最終由人類做決策時的一項投入（input）而已。
- 解決歧視和傷害問題需要廣泛的了解偏見。偏見可以在開發和使用特定 AI 系統的所有步驟中產生，包括決定系統所要使用的演算法、資料和情境。還有一些機制可以讓人類和機器合作，以做出更好的決策。
- 需要有降低演算法決策風險的政策，包括：限制措施、安全機制、審核機制和演算資源都需備妥。此外，努力提高參與決策的 AI 系統的透明度和可解釋性，亦為首要之務。應考慮列出使用中的 AI 系統和資料，並禁止使用某些高風險和高危害性的 AI 系統。
- 一些科技公司在各個層面已經建立自律機制，民間企業的自律很重要，但終究還是不足。各種監管工作需要相互補強，且不同的利害關係人之間需要加強合作，以產生綜效。
- 平等和公平是一種具有強烈文化意涵的價值觀。它們是解決偏見的重要原則，但要就這些原則達成跨文化的共識並不容易。此外，也需要討論未來我們想要生活在什麼樣的社會中。

三、5G 的用戶觀點和實施

(一) 歐盟部署 5G 的挑戰

歐盟執委會（EC）未來連網系統政策官員 Achilleas Kemos 表示，如果沒有無所不在的連網，歐洲將無法實現數位十年的目標，包括城市和鄉村的 5G 高覆蓋率。他強調，5G 必須成為歐洲在數位領導力競賽中的關鍵資產之一，當前必須進行大膽投資，將歐洲是行動網路基礎設施技術領導者的既有優勢，轉化為行動，在整個歐洲部署具競爭力的高品質網路。

歐洲國家頂級域名註冊管理機構委員會(CENTR)戰略計畫總監 Amelia Andersdotter 則指出，歐洲 5G 部署的一個關鍵挑戰是電信基礎設施仍以國家為界，歐洲仍是 27 個獨立的市場，有各自的頻譜政策、內容管理策略和網路服務責任規範。然而，要建立區域性的凝聚力相當不易。

(二) 人權和健康議題

國際電信設備大廠 Ericsson 法律顧問暨人權專家 Théo Jaekel 提及該公司進行的 5G 人權評估研究，確認 5G 的潛在風險包括工作、安全、健康、個資隱私等，且 Ericsson 也從其供應商的角度，提出因應措施。Jaekel 並以個資隱私為例表示，無所不在的 IoT 設備將產生無數的個資，對隱私帶來新的挑戰，但許多新型連接設備的新創公司可能不習慣處理隱私和相關的政府規範等問題。因此，Ericsson 期望能透過以身作則，鼓勵其他業者考量 5G 的風險和影響性。

義大利 Ramazzini 癌症研究中心研究總監 Fiorella Belpoggi 則分享其團隊近期文獻分析的研究發現。她表示，即使是 2G ~ 4G 的低頻段都可能有致癌及影響生育和發育的風險，更何況是使用高頻段的 5G，而且目前高頻段對健康影響的研究不足，因此，除了需要進行 5G 對健康長期影響的評估外，也建議修訂公眾和環境的射頻曝露限制。

(三) 會議共識（結論與建議）

- 對歐洲而言，發展高速通訊基礎設施尤其是 5G，是一項戰略重點。COVID-19 疫情蔓延是加速推出 5G 的催化劑。
- 5G 網路可能帶來安全和隱私的風險，因此，需要對所有風險進行徹底評估，包括對未來工作、健康和環境的影響，並讓產業界和其他利害關係人在部署 5G 網路時，就開始因應這些問題。
- 歐盟成員國面臨的經濟和法律挑戰，阻礙 5G 的快速部署，包括國家頻譜政策、安全規範等，都缺乏凝聚力。

四、歐洲媒體景觀—如何重塑可信賴的公共領域？

(一) 歐洲公共領域平臺的需求

主持人歐洲廣播聯盟（European Broadcasting Union, EBU）媒體副總監 Liz Corbin 表示，媒體產業經歷動蕩的十年，原本用來蒐集和報導新聞的平臺如 Google 和 Facebook，卻造成大規模的破壞，助長政治混亂、民眾分裂、社會兩極化。因此，如何遏制科技巨頭的權力擴張，以及讓民眾找到值得信賴的資訊，成為歐洲的迫切議題。

歐洲議會議員 Petra Kammerevert 指出，歐洲人不斷抱怨科技巨頭的濫用行為，並把無法接受之處嘗試進行監管，然後就繼續在 Google 搜尋、在 Amazon 購物、在 TikTok 觀看影片，這是因為缺乏其他替代性的選擇。因此，需要建立一個為歐洲人服務的公共領域系統，它是透過共同開發和投資實現的，但不能以利潤為導向，且是獨立不屬於任何一個人，每個內容創造者也要為其內容負責。

同樣的，電視新聞記者暨製作人 Matthias Pfeffer 也認為歐洲需要建立自己的公共領域平臺。Pfeffer 表示，現今科技巨頭結合技術和經濟的力量已經達到前所未見的權力集中，唯利是圖的發展模式已經破壞公共領域，導致社會分裂，威脅民主體制，這除了需要法規導正外，還需要建立歐洲公共領域平臺，一個致力於啟蒙和批判性調查、言論自由和民主參與、多元化和多歐洲視角的獨立性非營利平臺，而不是靠出售用戶資料和操弄用戶訊息來獲利的既有平臺。

(二) 相關案例和法規

瑞典廣播電臺數位新聞戰略主管 Olle Zachrison 介紹歐洲廣播聯盟（EBU）的「歐洲觀點」（A European Perspective）新聞計畫，包括西班牙、芬蘭等國的 10 家公共服務公司，透過發布來自歐洲其他地區的數位新聞推薦，為歐洲民眾開拓新視野和新觀點，同時亦是提供可信賴和多樣化的新

聞服務。

牛津大學社會法律中心研究員 Giovanni De Gregorio 則表示，過去歐洲對於數位媒體採取自由的態度，並使用業者自律的監管方式。而今改為採取言論自由和其他權利等不同途徑，聚焦於透明度和問責制，因此，推出《數位服務法》。雖然此法案仍然只是因應問題的一個步驟，而非解決方案，但是有助於邁向問責制的新框架，以及重建媒體格局。惟如何確保提高社群媒體的透明度，仍是一大挑戰。

(三) 會議共識（結論與建議）

- 包括歐洲議會和歐洲廣播聯盟（EBU）等參與者，對於透過創新努力，以建立一個值得信賴的歐洲媒體空間，皆表示支持。
- 歐盟《數位服務法》與《數位市場法》是處理現有平臺主導地位的第一步。然而，所有法規（包括著作權相關法規）都應避免造成意外後果，並要尊重人權和基本價值觀。
- 僅靠單一機構是無法解決問題，而是需要以多方利害關係人的方法，來建立一個和諧的系統。在此系統中，硬性和軟性監管的要素在各自的界限、任務和問責機制內，保持平衡。尤其對於享有重大利益的平臺，應該要求其制定透明的自我／共同監管措施。
- 個別用戶是最後一道防線，每個人都在各自的背景環境中解讀內容，所以，應該透過媒體教育強化其防禦能力。

五、假新聞—以媒體素養消除迷信

(一) 媒體素養的重要性

喬治亞媒體發展基金會（Media Development Foundation Georgia）執行長 Tamar Kintsurashvili 表示，該國所面臨的不實訊息主要和俄羅斯有關，他們將宗教武器化，以在社會中製造衝突和分裂。所以，其基金會除了和 Facebook 合作，將此類內容標記為錯誤訊息以減少被進一步散播外，也培養學生的媒體素養，讓他們了解前後文（context），進而能夠自行揭穿錯誤訊息。

美國媒體素養聯盟（Consortium for Media Literacy）創辦人 Tessa Jolls 也指出，幫助民眾備妥獲取、分析、評估和創造訊息的能力非常重要，媒體素養已被美國駐世界各國的大使館列為戰略重點，且北大西洋公約組織（North Atlantic Treaty Organization, NATO）國家也視媒體素養為戰略防禦優先事項，因為他們意識到民眾能否抵禦操弄的訊息，並決定是否傾向民主的唯一方法，正是媒體素養。

(二) 媒體素養推動案例

葡萄牙網路安全中心（Portuguese Cybersecurity Centre）發展與創新部成員 Sofia Rasgado 介紹該國的媒體素養推動情況。她表示，媒體素養已經納入學生的公民課程中，培養他們對網路內容的批判性，及安全的使用網路和社群媒體。其他推動措施還包括舉辦全國媒體素養暨公民大會，以及以媒體素養為主題，製播 12 集的 YouTube 影片和一系列的廣播節目、舉辦內容創作競賽、廣開線上課程等，且其中一門 2020 年開辦的線上課程已有 1 千多人參加。

德國之聲（Deutsche Welle, DW）記者 Amalia Oganjanyan 則是分享烏克蘭的媒體素養推動經驗，例如：2020 年有一個針對 12 到 15 歲學生開設的線上課程，課程內容包含遊戲和測驗，獲得廣大迴響。另外，她也建議

透過結合電視節目和大型國際線上會議的方式，推動媒體素養。

(三) 會議共識（結論與建議）

- 以不實或虛假訊息操弄媒體資源，可能會助長暴力衝突。
- 媒體素養的一項要點就是教育民眾，在大多數情況下，訊息的上下文是取決於知識、經驗和態度等各種既有資訊。
- 青年需要更深入了解媒體素養，才能辨別來源的準確性。

六、邁向法規框架的平臺自律和共管最佳實踐

本場座談介紹 4 個透過網路平臺自律和共管框架處理網路有害內容的案例。主持人——世界報業協會（World Association of News Publishers）媒體政策和公共事務執行長 Elena Perotti 表示，雖然歐洲有軟性法律的安排，例如：旨在規範有害內容的自願性行為準則，但它們不足以在確保言論自由的同時，解決極端主義內容和不實訊息。

(一) 基督城呼籲

負責協調「基督城呼籲」(The Christchurch Call)的紐西蘭政府官員 Paul Ash 表示，「基督城呼籲」是多方利害關係人方法共同監管的一個例子，政府和民間企業在努力消除網路極端主義內容的過程中，還諮詢學術界和民間社會。不過，共同監管最複雜的是協調不同機構中的不同問責制和權力結構，這顯然比直接立法解決方案更加困難。

(二) Facebook 監督委員會

Facebook 監督委員會(Facebook Oversight Board)委員 Cherine Chalaby 表示，該委員會於 2020 年成立的主因包括：網路主權問題的興起、社群媒體平臺對用戶的影響、與 Facebook 服務相關的案件增加，以及需要加強對用戶的合法性。他認為，企業不該成為平臺上言論的最終仲裁者，用戶應該有發言權，他們的案件應該由獨立的上訴機構審理。Chalaby 並說明委員會是由 20 名有信譽的思想家和領導者組成，針對用戶對 Facebook 和 Instagram 內容政策的上訴，做出獨立決定，且這些決定對 Facebook 具有約束力。

(三) 歐盟不實訊息行為守則

英國通訊管理局（OFCOM）國際政策經理 Lewis McQuarrie 表示，歐盟《不實訊息行為守則》(Code of Practice on Disinformation）被形容為全球第一個產業界自願同意的文件，包括 Facebook、Google、Twitter、Mozilla 及

廣告商都已簽署，以讓用戶和研究界對廣告投放進行更嚴格的審查，並使政治性廣告更加透明。此守則是自律和共同監管的混合體，它由歐盟執委會制定，且業者於第一年將受到監管機關、民間社會、學術界等利害關係人監督其實施成效。McQuarrie 認為，當涵蓋公共團體且其運作透明時，自律和共同監管工具就能運作良好。

(四) 歐洲數位媒體觀察站

歐洲數位媒體觀測站（European Digital Media Observatory, EDMO）秘書長 Paula Gori 表示，EDMO 是一個獨立平臺，旨在成為一個採取多方利害關係人和跨領域方法的事實核查團體，一方面保護知情決定（informed decisions）和基本權利，另一方面也希望能夠避免民眾對媒體和平臺失去信任。除了事實核查外，EDMO 還提供免費的媒體素養培訓課程。

(五) 會議共識（結論與建議）

- 政府在平臺經濟發展初期對業者採取自由態度，導致平臺的權力大到足以影響公共領域。儘管有自願行為準則之類的軟性法律來規範有害內容，但它們不足以在確保言論自由的同時，解決極端主義內容和不實訊息等嚴重問題。
- 業者自律、共同監管、多方利害關係人／跨領域的治理模式，面臨需要協調不同問責制和權力結構的挑戰。更重要的是，它們應該具有內部和外部的合法性。
- 在外部，治理模式的決策品質和時效性必須得到認可；在內部，它必須有強大的查核和制衡機制。
- 政府、科技公司和民間社會應該透過對話展開全球合作，訂定一種以人權為基礎的對抗不實訊息和有害內容的解決方案。

七、網路基礎建設的內容管理——審查是從何處開始的？

(一)《數位服務法》的相關規範

主持人哥本哈根大學（University of Copenhagen）資訊與創新法律中心副教授 Sebastian Felix Schwemer 指出，在基礎設施層進行內容審核，可能會帶來很多問題。歐洲《數位服務法》（DSA）草案和建立基礎邏輯架構及維護網路正常運作的服務提供商有關，因此，本場座談探討他們在「非內容層」進行「內容審核」的角色。

歐盟執委會法律官員 Denis Sparas 首先簡介 DSA 目標，包括它是現有《電子商務指令》（e-Commerce Directive）規則的現代化，尤其是在處理網路空間的非法內容和系統性風險方面；釐清網路任何一層的責任規則，並為服務供應商的行為提供法律確定性；提高內容審核決策的透明度、確保問責制，並促進更好的監督。Sparas 也指出《電子商務指令》包含有條件的責任豁免，但它在多大程度上可適用於基礎設施層的服務，仍待釐清。

歐洲國家頂級域名註冊管理機構委員會（CENTR）政策顧問 Polina Malaja 表示，雖然 DSA 草案確認域名和註冊管理機構是中介機構（intermediaries），且對於終端用戶的非法內容享有責任豁免，但僅限於符合中介機構類別條件的服務項目（例如：只提供暫存或託管服務）。然而在實務上，註冊管理機構的服務無法歸類於這些類別，且技術層和註冊層無法鎖定特定內容，他們只能暫停底層的基礎設施，而且會對所有相關服務造成影響，因此，草案將對營運商帶來法律上的不確定性。

(二) 從基礎設施層處理內容的問題

牛津網路研究所（Oxford Internet Institute）Corinne Cath-Speth 博士表示，通常網路基礎設施公司不願將自己定位為明確的政治參與者。然而，當他們進行干預時，卻又往往試圖在沒有相關的政策框架下執行，而且也沒有後續的究責措施。可預見的是基礎設施層的政治把關和內容審核將會

繼續發生。所以，我們需確保有更成熟的框架來因應這種情況，且這些框架需要公開，讓主要參與者有一定程度的問責制，也讓網路用戶有一定程度的可預測性。

英國通訊管理局（OFCOM）網路技術負責人 Fred Langford 說明阻斷可以從網址（URL）、網域名稱系統（DNS）著手，也可以透過內容傳遞網路（Content Delivery Network, CDN）清除暫存檔，或是在 Wi-Fi 和搜尋結果中進行過濾。但他也強調，有些是非常粗魯的工具，以 DNS 阻斷為例，它會關閉整個網站，而不是當中的特定內容，因而衍生是否符合比例原則的問題。

(三) 會議共識（結論與建議）

- 《數位服務法》（DSA）旨在使相關規則現代化，並限制處理數位空間風險的法律不確定性，包括關鍵服務供應商的責任問題，及必要的技術輔助功能。
- 基礎設施中介機構自 2000 年歐盟《電子商務指令》頒布以來，一直處於定位不明狀態。而今必須釐清其責任豁免，並闡明它於數位服務中的分類。
- 最近的案例顯示，某些基礎設施供應商不情願的採取可能被認為是內容審核的行動，在政策不透明的情況下，以臨時方式暫停平臺服務。但基礎設施服務的潛在選項有限，這些選項往往是臨時性的解決方案（清除暫存檔），或是反應過度（限制訪問）。
- 我們應該牢記針對非法內容的措施要符合比例原則，並預知基礎設施層的意外後果。目前內容審核的實施情況並不理想，透明度報告對於避免錯誤也無幫助。既然如此，從更廣泛的基礎設施層可以期待什麼呢？

八、加密戰 3.0—隱私、安全和加密能否共存？

(一) 允許破解加密的法規議題

歐洲刑警組織（Europol）資料保護資深專員 Jan Ellermann 表示，加密可以保護隱私，並幫助在專制政權中的人們生存，但隱私不應該優先於打擊犯罪。而儘管維持安全和自由的平衡，是艱難任務，因為要獲得更高的安全就需要妥協某些自由，但是我們仍然需要一個能夠兼顧處理所有組織犯罪和尊重基本權利的法律框架。另外，執法部門也應該要獲得非常明確的授權，來破解個別和正當案件的加密資料。

都柏林三一學院（Trinity College Dublin）Stephen Farrell 博士認為，我們應該將討論焦點從允許執法機構破解加密的通用法則，轉移到執法機構何時以及如何破解加密的具體規範。網路觀察基金會（The Internet Watch Foundation）首席技術長 Dan Sexton 也認同應該聚焦討論具體的允許解密條件，例如：被加密的兒童虐待資料需要及早破獲，以防止被散播出去。

不過，德國資料保護與資訊自由聯邦委員會（Federal Commissioner for Data Protection and Freedom of Information）官員 Ulrich Kelber 表示，允許執法機構破解加密，並不會阻止犯罪分子以牢不可破的方式加密他們的通訊，但卻可能削弱社會的線上通訊基礎設施，為犯罪分子和網路戰爭創造新的技術場景，也為廣泛監控人民創造條件。在民主社會中，對加密通訊的信任是必要的，但它會因當局能夠輕易取得加密訊息而受到破壞。

(二) 加密、隱私和安全應該共存

民主與科技中心（Centre for Democracy and Technology）歐洲辦公室主任 Iverna McGowan 認為，加密、隱私和安全之間的關係不應該用錯誤的框架和錯誤的二分法來描述。隱私很重要，在民主的運作中，隱私是通往許多其他權利的門戶。因此，後門程式是非常糟糕的主意，一旦破壞加密將會危害國家的民主發展。

網際網路協會（ISOC）網路信任主任 Robin Wilton 也強調，隱私、安全和加密這三個概念必須共存，但需要有更謹慎及一致的定義和理解，才能進行建設性的對話。例如：英國《網路安全法》草案，原本的名稱《網路危害法》其實是更準確的描述。Wilton 並指出，此法案雖然沒有提到加密，但網路業者可能會為了避免遭到罰款或入獄的風險，而取消加密服務，因為法規要求業者承擔非法和有害內容的責任。最後，他引用英國知名網路安全專家 Robert Hannigan 的主張作為結尾——為了解決少數人的問題而削弱每個人的安全，並不是一個好的主意。

(三) 會議共識（結論與建議）

- 信任加密通訊在民主社會中是必要的，但這種信任會因當局能夠輕易取得加密訊息而遭到破壞。這將是自由通訊的終結，因為它無法阻止犯罪分子以牢不可破的方式加密他們的通訊，但是卻會弱化每個人的加密。因此，解決方案不應該比問題更加糟糕。
- 重點應從允許執法部門破解加密的通用法規，轉移到執法部門何時可以這樣做，以及如何進行的要求，並進行公開討論。
- 應該避免聚焦在加密、隱私和安全的錯誤框架和二分法上，但要更好的闡明其條件和概念，以避免使用時的誤解和不一致。
- 必須加強多方利害關係人參與共同探討科技進步的後果。在歐盟層面，需要採取具體行動來確保這種參與的正式結構，並克服現有框架的分歧，以及分散式的討論和辯論。

第三節 心得與建議

本次會議本計畫所參與的場次，有諸多內容亦是國內目前關心的議題，討論過程和結果可供通傳會相關政策參考之處，摘要如下：

- 歐盟《數位服務法》：會議結論建議此法應該處理刪除非法內容的條款可能造成寒蟬效應的問題。另外，也建議提升法規的明確性，例如：有關盡職調查等責任、法規的適用地區和域外效力，都需要說明清楚。

- 5G 風險：會議結論建議要評估和因應 5G 對未來工作、健康和環境的影響。相關議題可參考本報告第四章「案例研析：5G 網路的治理議題初探」。

- 媒體素養：有講者提到北大西洋公約組織（NATO）國家（包含北美和歐洲共 30 國）已將媒體素養列為戰略防禦優先事項，凸顯媒體素養成為許多國家的重要施政項目。另有講者分享葡萄牙和烏克蘭的多元活潑推動方式，亦具參考價值。

- 內容和平臺治理：相關會議的結論為單一機制無法解決假訊息等內容問題，而是需要業者自律、法律、多方利害關係人共同監管等所有機制。此共識和我國《數位通訊傳播法》草案強調的兼容自律、他律、法律等公私協力概念具一致性。但講者們也提醒要賦予這些機制的內部和外部合法性，內部合法性指有強大的查核和制衡機制，外部合法性指治理模式的決策品質和時效性必須獲得認可，此點可供我國參考。

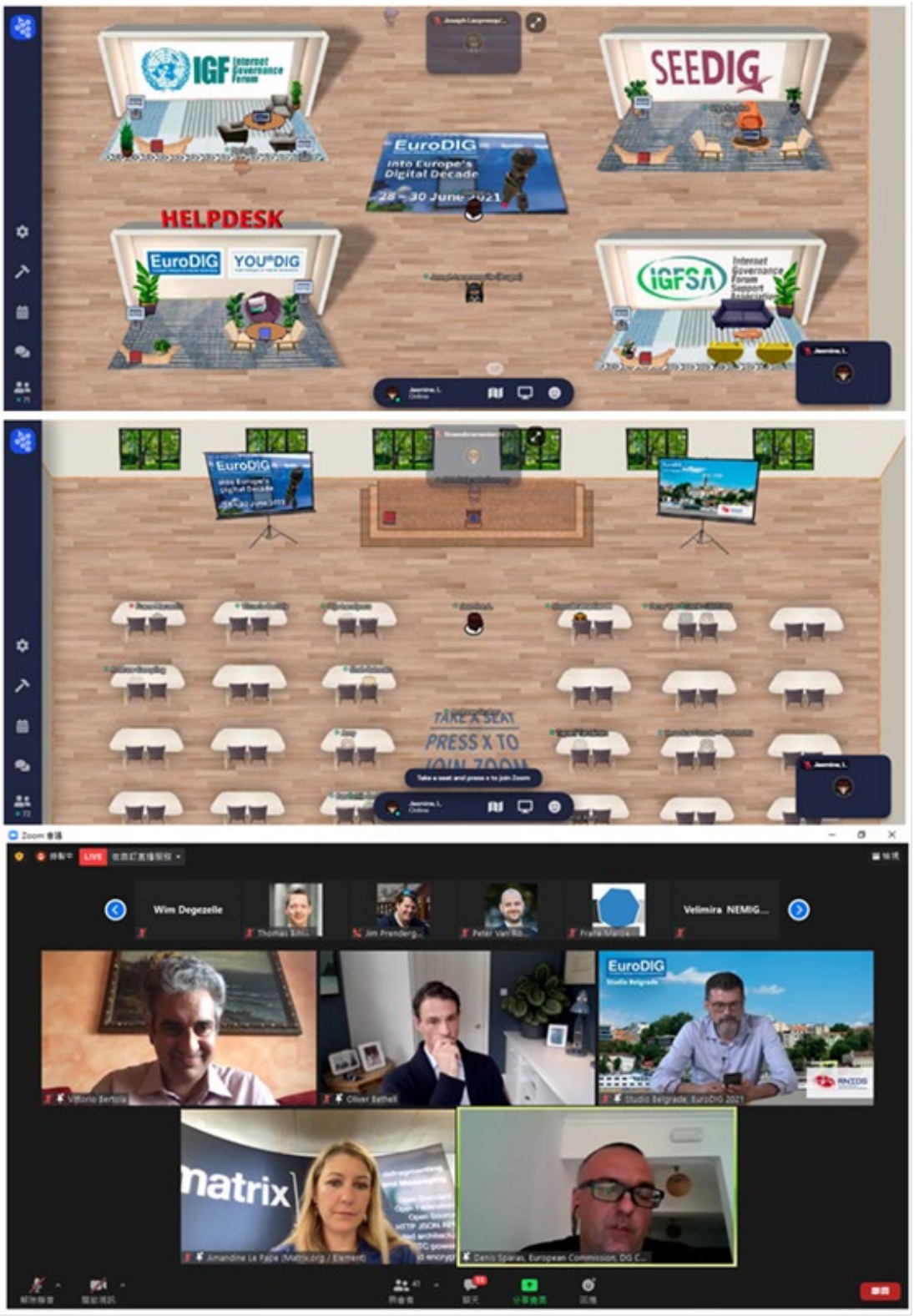
- 從技術層處理非法內容：會議結論強調處理非法內容要符合比例原則，不該期待從技術層來解決內容問題。此議題可參考本報告第五章第六節「二、建議事項之（一）立即可行之建議第 3 點」。

- 加密：會議結論為可信任的加密通訊，是民主社會的必需品，一旦遭

到破壞，將是通訊自由的終結點。雖然我國《電信管理法》僅要求電信業者配合通訊監察工作，「沒有」解密的法定義務，但隨著各國執法機關高度期盼能破解加密資料以打擊犯罪，加密議題將持續成為國際討論焦點，亦是通傳會可以關注的議題之一。

以上摘要亦顯示，未來我國應該持續參與 EuroDIG，以掌握重要治理議題的國際觀點。此外，適逢歐洲議會「外國勢力干預歐盟民主程序（含假訊息)特別委員會」專程於 11 月初訪臺，並表示要將臺灣經驗帶回歐洲，甚至考慮在臺灣設立對抗假訊息中心，或許未來我國有機會受邀於 EuroDIG 擔任講者，分享我國的對抗假訊息政策（可參照本報告第五章第六節「二、建議事項之（一）立即可行之建議第 2 點」）。

第四節 線上參與系統畫面



本頁：登入系統頁面，及座談 WS 1 數位服務規範—機會與挑戰

下頁：座談 WS 12 邁向法規框架的平臺自律和共管最佳實踐

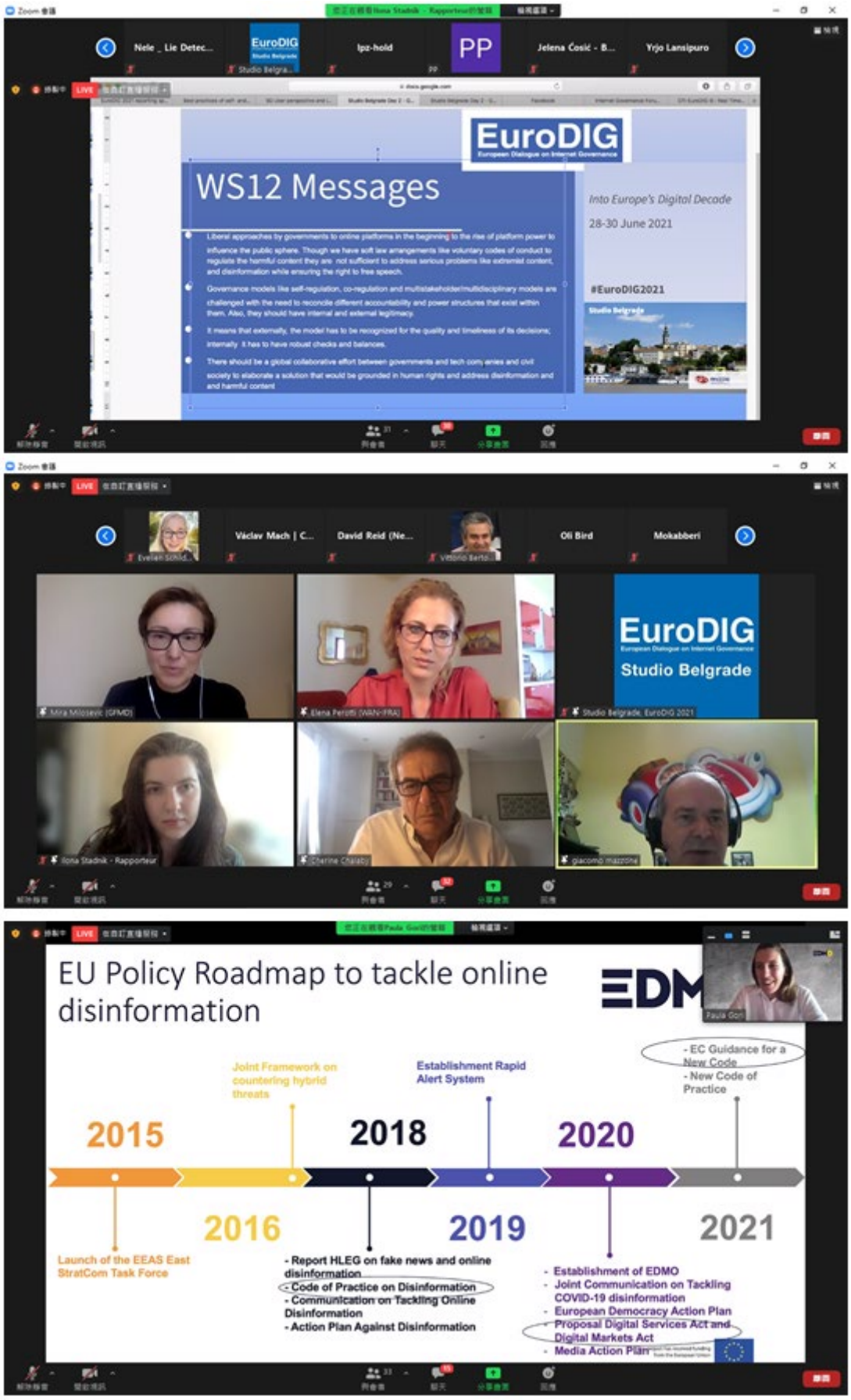


圖 9-1　EuroDIG 2021 線上參與系統畫面

第十章 建議事項

本章彙整本計畫所有工作項目之結論與建議，建議事項分成「立即可行之建議」及「中長期建議」，前者指一年內的執行建議，後者則為超過一年以上的執行建議。

一、英國《網路安全法》草案

（一）結論

1. 草案評價兩極，但英國社會對立法規範網路平臺有高度共識

英國各界對於草案的看法可分成「立法過度」和「立法不足」兩大類。一方面，維權團體等人士擔心草案迫使大型平臺業者充當網路警察，審查使用者的內容，加上違者將被處以嚴刑峻罰，可能導致業者過度審查，對言論自由帶來寒蟬效應。但另一方面，公益團體等單位指出草案對於有害、具民主重要性、新聞等內容的保護不足，對種族主義和虛假訊息等內容也無著墨。儘管如此，在歷經挾帶網路因素的多起恐怖攻擊、少女瀏覽大量自殺網路訊息而輕生身亡，以及引發英國首相親上火線和百萬民眾請願反制網路種族歧視等重大事件的英國社會，對於立法規範網路平臺已經形成高度共識，歧見的部分其實只是執行方向和細節。

2. 英國政策發展原本嚴謹且採多方模式，但最終在壓力下倉促提案

英國政府費時約 3 年半，終於在 2021 年 5 月推出《網路安全法》草案並送英國議會審議。數位部表示，英國信守多方利害關係人模式的網路治理，是確保網路自由開放和安全的最佳方式。因此，不論是綠皮書或白皮書階段，皆可見政府進行多元廣泛且頻繁的公眾意見徵詢，例如：白皮書階段舉辦 100 場利害關係人會議、17 場部長級會議，還有超過 2,400 份徵詢意見。然而，受到 COVID-19 疫情影響以及輿論的壓力，數位部的提案時程似乎被迫提前進行，且嚴謹做法也未能堅持到最後。這或許也是草案出現諸多定義不明條文，以及規範內容遭致眾多批評的一大主因。

（二）建議事項

1. 立即可行之建議：觀察國際發展趨勢，並進行國內政策溝通

(1)平臺責任觀點逐漸轉為「問責」，但我國國情不同需更審慎因應

除了英國《網路安全法》草案外，同樣處於立法程序的歐盟《數位服務法》草案和澳洲《網路安全法》，皆涉及網路業者對於網路內容的責任規範。此外，美國總統拜登就職前也曾表示贊成廢除保障網路業者對平臺內容免責的《通信端正法》第 230 條。由此顯示，國際間對平臺責任的觀點，正由過去的「免責」逐漸轉變為「問責」。我國通傳會亦研擬「新版」《數位通訊傳播法》，規範平臺業者責任。此次科技巨頭或許不會如同 2018 年透過亞洲網路聯盟（AIC）要求我國撤案重審。惟我國國情有別，相較於英國社會因為歷經重大事件而對立法規範網路平臺形成高度共識，雖然國內也曾發生因網路霸凌或假訊息而自殺身亡的憾事，但目前社會各界對於涉及言論自由的網路規範仍是看法分歧，且缺乏理性討論的空間，動輒冠以「數位威權」、「網路戒嚴」之名。因此，我國對於相關政策法規的推動恐需更加審慎，正如行政院政務委員羅秉成表示：「臺灣社會對此議題高度敏感……我們沒有超前的條件」。

(2)現階段可先進行國際案例深入研究和國內政策溝通

目前我國對平臺業者採取自律方式，但網路上的公然侮辱、毀謗、霸凌、假訊息、危害國家安全和兒少安全、商業廣告等內容，已有既有法律或透過修法加以規範。此做法不但是英國最近處理足球員遭網路霸凌的方式，也是英國上議院所建議的「嚴重的危害應由法律來定義犯罪，而非由業者自行審查有害內容並加以處置」。因此，現階段我國可針對如前述的先進國家相關法案進行深入研究、綜合比較及追蹤立法進展。研究範圍除了草案條文外，也必須了解其政策發展過程、社會情境、各界看法，以掌握國際總體趨勢、釐清特殊國情規範，進而從中找出可供我國參酌之處。

此外，我國也需要透過公正客觀的研究調查，以及充分的多方利害關係人溝通，了解國內對於網路內容治理的民意動向和社會共識，以強化相關政策或立法的正當性和支持度。例如：英國的白皮書即指出 75% 英國成人對於上網感到擔憂、61%英國人希望政府為打擊假訊息做得更多……，且白皮書公布之後還進行多元且頻繁的公眾意見徵詢，這些政策發展措施值得我國學習。

2. 中長期建議：建立市場競爭制度，且將媒體素養列為重要施政項目

(1) 建立市場競爭制度

英國維權團體和上議院認為，從市場競爭制度來建立業者的問責，將是更好的方式，因為目前市場缺乏競爭，迫使民眾只能使用少數平臺；但如果是競爭激烈的市場，平臺業者就必須積極回應用戶對言論自由和隱私等訴求，凸顯促進競爭對維護數位人權的至關重要。因此，應該立法建立新的市場競爭事前（ex ante）規範。此項能夠促進數位市場公平競爭、維護言論自由等人權，又相對不會引發社會爭議的事前規範方式，亦值得我國主管機關著手進行研議（依據立法院初審通過之相關組織法，涉及的行政部門包括通傳會、公平會、數位發展部），且可參考歐盟《數位市場法》草案。

(2) 將媒體素養列為重要施政項目

英國《網路安全法》草案將 OFCOM 強化推動媒體素養的職責入法，雖然條文簡短，且對於如何執行或須達成什麼目標也幾乎沒有著墨，但如果草案獲得通過，形同法律認可媒體素養對於促進網路安全的價值。我國教育部自 108 年推動「媒體素養教育行動方案」，以提升各級學生和國人於獲取資訊、解讀資訊和分享資訊的能力。另一方面，各部會也依其職掌領域推動提升媒體素養的相關工作，例如：通傳會舉辦 110 年度「廣電媒體素養公民培力合作」活動、衛福部等單位於 107 年舉辦「兒少權益與媒

體識讀暨媒體素養桌遊培力工作坊」。隨著媒體素養的重要性日益在國際上獲得正式認可，建議教育部將媒體素養列為重要且長期施政項目，且於其「透過多元管道，培養全民素養」面向，納入上述各部會的宣導活動，除了可避免資源重複之外，也可盤點出尚未納入宣導的族群，並予以補強。此外，還可善用民間的力量，邀請民間單位響應宣導活動或提供宣導資源，尤其網路平臺業者可能樂於共襄盛舉，因為這也是他們展現善盡教育用戶和促進安全網路環境之責的良機。

二、5G 網路的治理議題初探

（一）結論

1. 我國 5G 安全策略和民主國家同一陣線

在「資安即國安」的戰略下，我國 4G 網路釋照即依據「行動寬頻業務管理規則」相關規定，禁止中製設備用於核心網路、傳輸骨幹及基地臺等重要設施，且 5G 網路亦比照辦理。因此，2019 年美國在台協會前處長酈英傑即表示，臺灣「率先」意識到中製電信設備的風險並禁用，值得其他國家效仿。而 2020 年美國也將我國和全球 60 多個國家同列為淨網計畫的「乾淨國家和地區」，且國內五大電信業者亦全是「乾淨的電信商」；同年，臺美雙方還發布「5G 安全共同宣言」，強化 5G 資安合作，且宣言所推動的防護措施亦呼應 32 個國家共同發布的「布拉格提案」。由此顯示，我國的 5G 安全防護在因應地緣政治的美中對抗的選擇上，以及相關的策略方向，皆和民主國家站在同一陣營，符合民主國家的潮流。

2.5G 覆蓋距離屢創新高，可望縮減偏鄉的連線落差

正如國際間擔憂 5G 建設成本高昂等因素恐怕加深城鄉數位建設落差，通傳會「強化偏鄉地區 5G 寬頻服務與涵蓋——普及偏鄉寬頻接取環境計畫」也指出相同問題，且因為既有的「電信事業普及服務基金」額度有限，故透過政府補助部分經費的方式（不超過核定總工程經費的 50%），推動偏鄉 5G 網路建設，惟仍面臨補助經費對電信業者吸引力有限的挑戰。而此挑戰隨著 5G 毫米波的通訊覆蓋距離不斷刷新紀錄（目前為 10 公里），可望獲得紓解，包括技術社群和產業界都看好此發展趨勢有助於縮減 5G 網路的連線落差。5G 有機會以具成本效益的方式，將寬頻服務擴展至鄉村和郊區。

3.5G 促進節能環保或增加耗能污染，尚無統一定論

目前國際間對於 5G 網路究竟是促進節能環保，或是增加耗能汙染，並無統一定論。主張 5G 促進節能環保者認為，5G 結合智慧連網有助於其他產業提升能源使用效益；代表案例為英國電信商 O2 預估至 2035 年之前，5G 可為英國減碳 2.69 億噸，幾乎等同英格蘭 2018 年的碳排放總量。而主張 5G 不利節能環保者則強調，5G 網路的基礎建設各種設備和施工、資料傳輸儲存量將大增、換機潮增加電子廢棄物等因素，將大幅增加耗能及汙染；代表案例為法國氣候最高委員會（HCC）預估，5G 網路至 2030 年將使法國的能源消耗增加 2.5 倍，碳排放量增加 18～44%。

4.5G 健康風險亦無國際共識，歐盟將檢視電磁波曝露限制值

有鑑於歐洲民眾對於 5G 健康風險有所疑慮，尤其是 5G 所使用的頻段範圍遠高於 4G，甚至未來還可能使用「至高頻」（30～300 GHz），歐盟執委會和歐洲議會等單位近年來持續委託執行相關研究，結果發現 5G 是否影響人類健康沒有一致結論，且很少有 26 GHz 和更高頻率的健康影響研究。另一方面，雖然歐盟非游離電磁波曝露指南的依據來源——國際非游離輻射防護委員會（ICNIRP）的 RF EMF 指南，於 2020 年發布的更新版本已將 5G 運作頻率納入，ICNIRP 並強調沒有證據證明電磁波會造成任何健康影響，惟這份指南也遭抨擊為沒有回應長期曝露的問題，且沒有納入人類和動物組織的非熱能效應或生物效應。也因此，歐洲議會 STOA 小組認為，未來需要投入更多研究，並透露歐盟執委會衛生局不排除審查非游離輻射電磁波曝露限制值的可能性。

（二）建議事項

1. 立即可行之建議：將節能列為 5G 基地臺架設許可等審核，追蹤國際 5G 健康影響研究，了解歐美全國性資安認知宣導

(1)將節能列為 5G 基地臺架設許可等審核，響應 2050 年淨零碳排

在 2050 年達成淨零排放及各國著手研議碳關稅的國際趨勢下（全球已有 130 個國家宣布推動淨零排放，且歐盟預計 2026 年起徵收碳關稅），行政院已指示環保署積極修改《溫室氣體減量及管理法》，並納入「2050 年淨零排放」目標，同時還要研議碳定價。由此凸顯節能減碳可能成為所有產業的共同責任。其實部分國內電信業者已經有所行動，例如：遠傳電信和台達電子合作於 5G 基地臺使用節能系統、中華電信加入民間推動的「台灣淨零排放倡議」等。因此，建議通傳會可將節能列為 5G 基地臺架設許可的審核項目，或建設偏鄉 5G 網路補助案的加碼補助項目，抑或是參考法國氣候最高委員會（HCC）建議的訂定 5G 網路頻段使用碳足跡規範，以鼓勵或要求所有電信業者以節能方式布建和營運 5G 網路。

(2)追蹤國際 5G 健康影響研究、WHO 報告及歐盟電磁波檢視結果

通傳會於 2020 年進行首波 5G 釋照，釋出 1800MHz、3.5GHz 及 28GHz 三個頻段，且預計 2023 年的第二波釋照可能增加 37 ~ 40GHz 的「至高頻」。雖然國內亦有電磁波安全的相關研究，但似乎沒有著墨高頻段的部分。此外，我國的一般民眾環境電磁波曝露指引及基地臺電磁波管制標準亦是參考國際非游離輻射防護委員會（ICNIRP）的標準值而訂定。通傳會長期向民眾宣導行動通訊電磁波的正確觀念，一方面讓民眾了解目前基地臺電磁波致癌風險的證據不足，另一方面也教導民眾使用行動電話時如何減少電磁波的曝露。因此，在當前國際間對於 5G 健康風險尚無共識的情況下，建議通傳會追蹤先進國家 5G 高頻段的健康影響研究，以及 WHO 預計於 2022 年發布的電磁波健康風險評估報告，同時也建議行政院環保署了

解歐盟對非游離輻射電磁波規範的檢視結果，以為國人的電磁波安全嚴格把關，同時也作為未來持續和民眾宣導正確知識的參考。

(3)了解歐美全國性資安認知宣導，做為我國提升民眾資安意識參考

我國提升資安向來不遺餘力，不但自 2019 年實施《資通安全管理法》，且第六期「國家資通安全發展方案（110 年 ~ 113 年）」對於 5G 網路的安全維護更有進一步規劃。例如：通傳會將修訂「5G 資通安全維護計畫」的稽核計畫及標準作業程序；行政院資安處和經濟部及通傳會（協辦）將制定我國 IoT 資安檢測驗證框架、優先策略及清單項目。由此顯示我國整體資安防護已具備法律基礎和配套制度。正如「布拉格提案」和 GSMA 協會等單位皆呼籲「5G 網路安全是所有利害關係人的共同責任」，我國第六期資安發展方案指出當前國人資安意識不足的問題，並責成通傳會提升民眾的資安意識。因此，建議了解美國的全國資安認知月（National Cybersecurity Awareness Month）和歐盟的網路安全日（Safer Internet Day）等計畫，其長期（兩者皆從 2004 年舉辦迄今）透過全國性／國際性的認知宣導活動之實施策略、措施和具體成效，以做為我國推動民眾資安意識的參考。

2. 中長期建議：成立個資保護專責機關，防止 5G 的個資濫用和監控

5G 的數位人權議題包含因應企業和政府可能濫用資料，進行更精準的廣告投放、監控或是政治操弄。我國自 2012 年開始實施《個人資料保護法》，並由各目的事業主關機關分散管理，而後由國家發展委員會成立「個人資料保護專案辦公室」，且作為個資法的法律主政機關，惟迄今尚未取得歐盟《一般資料保護規則》（GDPR）的適足性認定。面對 5G 時代的個資保護新挑戰，有賴政府加速設立獨立的個資保護專責機關，釐清不同型態的個資蒐集和使用風險，並透過修改《個人資料保護法》為這些資料量身訂做適用的規範（包含跨境傳輸規範），以真正落實個資保護，同時也增進民眾對於數位發展的信賴。

三、全球網路自由度及政策趨勢

（一）結論

1.報告以具體數字驗證治理觀念轉變及國家強化網路監管成為全球常態

《2021 網路自由度報告》以具體數字，也就是過去一年來有 48 國（占調查國家的近 7 成）祭出新規監管科技公司，驗證近來平臺責任觀念轉變的說法。正如報告所述，過去全球對於網路規範的態度是由美國主導，傾向讓科技產業自由發展，但卻導致各種網路危害和濫用行為層出不窮，且業者的自律機制顯然無法解決問題，於是各國政府開始轉為強化監管網路，並成為全球常態。惟在缺乏以網路自由開放作為共同願景下，各國政府監管數位領域是各行其是。

2.歐盟第三種監管方式及我國政策獲肯定，可為全球網路自由帶來希望

承上述的治理觀念轉變，身為人權團體的自由之家也有條件的認同政府監管措施。例如：報告認為「在民主堅強的國家中，精心設計的平臺規範或可減輕線上危害，同時加強透明度和問責制」。此外，報告也肯定歐盟著重透明度和正當程序的「第三種」網路監管方式，並認為我國《網際網路視聽服務法》草案（雖然通傳會已表示暫緩推動）也具同樣精神，而且還讚揚包含我國在內的排名前 5 名國家，為下滑的全球網路自由帶來希望。惟報告也提出警語，類似的法規會遭到獨裁者濫用於監控或打壓人民，甚至連民主國家都可能採用過於廣泛的審查和資料蒐集要求，以致全球言論自由和數位人權陷於空前的危機。

3.報告呈現全球趨勢並評比各國政策，可為檢視施政和研究索引的工具

自由之家的全球網路自由度研究計畫已持續進行 10 餘年，且研究結果經常獲得國際各大媒體的報導。《2021 網路自由度報告》更是由美國政府和荷蘭政府等單位贊助，且動員全球超過 80 位研究人員才得以完成。因此，報告可謂具有相當的可信度和品質。再就報告的內容而言，除了包括全球

和各國的網路自由度評比結果外，還針對評比的 21 項指標介紹過去一年來該國的相關政策或法規。因此，未來可將每年一度的報告作為了解全球網路規範趨勢、檢視我國施政成效，以及檢索各國政策或法規案例的工具。

（二）建議事項

1. 立即可行之建議：檢討改善防疫資料的使用、於國際分享我國普及上網和打擊假訊息政策、研析國際監管影音平臺和 DNS 處理違法內容等議題

(1) 與指揮中心分享國際正反案例，推動我國檢討改善防疫資料的使用

《2021 網路自由度報告》指出，各國普遍沒有防止疫情資料遭到濫用的措施，新加坡的執法單位、澳洲的情報機關等，都坦承可從國家 COVID-19 疫情追蹤 apps，取得民眾個資。但加拿大政府已經終止行政和執法部門及醫療單位等機構，共享個資；亞美尼亞政府更是停止從電信公司蒐集追蹤接觸者的資料。我國在報告中得分較低的項目，包括被認為疫情資料的蒐集使用缺乏合法性和比例原則，當中也提及通傳會為了「簡訊實聯制」疑似遭用於警方辦案而出面澄清等事件。正如加拿大隱私專員辦公室（OPC）強調疫情期間需要提高隱私保護，我國也應檢討改善相關法規和措施，通傳會可從作為電信事業主管機關和負責推動我國網路治理符合國際潮流之業務角度，藉由分享上述國家案例和我國得分，讓防疫決策最高機關——中央流行疫情指揮中心了解國際上的不同見解與做法。

(2) 於國際會議分享我國普及上網成果和打擊假訊息經驗

我國於《2021 網路自由度報告》的網路連線類別幾乎得到滿分。報告形容我國提供有意義且負擔得起的網路連線、沒有顯著的數位落差、政府致力將行動服務升級為 4G 和 5G、民眾亦可自由選擇網路服務供應商。由此顯示，通傳會所推動的數位基礎建設及縮短偏鄉數位落差、電信法規鬆綁及電信批發價格管理等措施，值得提供給其他國家參考。此外，報告也讚揚我國的公私部門以創新工具打擊假訊息，通傳會作為抑制假訊息散播的「抑假」統籌機關，並與社群平臺合作即時處理假訊息，亦可將相關措施分享給國際社會。至於分享的場合，主要可透過主動申辦 APrIGF 的座談會議。此外，適逢歐洲議會「外國勢力干預歐盟民主程序（含假訊息）特別委員會」專程於 11 月初訪臺，並表示要將臺灣經驗帶回歐洲，或許未

來我國也有機會受邀於 EuroDIG 擔任講者，分享我國的對抗假訊息政策。

(3) 研析德國監管擴及影音平臺、美國 CDA 修正提案、DNS 處理違法內容

根據《2021 網路自由度報告》，德國《網路執法法案》近期實施的修正案已將適用範圍擴及影音平臺；以打擊假訊息為立法宗旨之一的《國家媒體協定》也將監管範圍從無線電廣播擴及新型媒體，並規定平均收視超過 2 萬次的媒體創作者（如 YouTuber）須申請執照等。上述法規及其可能造成的內容審查等問題，或可供通傳會參考。當然，涉及平臺對第三方內容是否免責的美國 CDA 第 230 條修正案，也需掌握其立法進展。報告指出，今年（2021）以來至少有 9 項改革案提交國會，而當中較佳的是著重透明度和正當程序的《平臺問責制和消費者透明度法》草案。

此外，從 DNS 處理非法內容的問題亦值得研析。加拿大發生法院對 ISP 的侵權網站封鎖令，被業者基於維護言論自由而上訴至最高法院的案例；但德國卻是 ISP 聯合娛樂產業推動從 DNS 封鎖侵權網站，並帶來法外限制通訊自由的隱憂；而歐洲國家頂級域名註冊管理機構委員會（CENTR）於 RIPE 82 會議主張應從內容層而非 DNS 處理內容問題；英國通訊管理局（OFCOM）網路技術官員於 EuroDIG 2021 表示，以 DNS 阻斷產生不符合比例原則問題。我國曾於 2019 年封鎖宣傳中國大陸惠臺措施的 www.31t.tw 網站，且據報載通傳會也考慮從「網路層措施防制假訊息擴張」（楊綿傑，2020），因此，相關的國際案例、倡議和討論，可供通傳會參考。

2. 中長期建議：

(1) 持續推動透明開放的治理政策，以利人民數位福祉及獲國際聲譽

我國首度被納入全球網路自由度評比即獲得全球第 5 名的殊榮，是多年來包含政府在內的多方利害關係人共同努力的成果，除了讓國人得以享有全球最自由行列的數位環境和其帶來的數位福祉外，此番成果還獲得國際媒體的主動宣傳。例如：美國之音、自由亞洲電臺、印度時報等媒體皆以「臺灣網路自由度高居全球第五」為題，報導全球的評比結果；美國 CNN

電視「全球公共廣場」（Global Public Square）節目也指出「臺灣網路自由度超越德、美等民主國家」；美國時事雜誌外交家（The Diplomat）更是報導「中國大陸和臺灣的網路自由度是天壤之別」（Cook & Funk, 2021）。

為此，推動透明且開放的網路治理政策，是我國須持續努力的工作，並可參考《2021 網路自由度報告》提出的 5 個優良網路法規要素，包括依企業的類型和規模量身制定義務；要求業者對於內容審核、資料使用、廣告業務須有透明度；對於第三方內容應有強力的中介機構安全港保護條款；確保正當程序和申訴管道的暢通；強韌的加密和隱私標準。

此外，外交家雜誌在前述所指報導提到一個問題——我國某些法律對於誹謗和散播假訊息的處罰過重（亦為自由度報告中得分較低項目），且易被執法機關濫用，即使最終被獨立的司法機關駁回，但可能已經造成傷害；值得我國省思。或許通傳會可從《數位通訊傳播法》的內容規範介接其他部會，以及罰則等項目，推動相關法規的檢討與修正。

四、大專校園講座辦理

本工作項要求於大專校園內辦理 50 人以上的網路治理實體講座，然而今年度自 5 月開始，國內因受到 COVID-19 疫情之影響，配合中央流行疫情指揮中心因應各級警戒對於集會活動人數有不同的管制上限，甚至在三級警戒期間幾乎全國大專院校皆改採線上遠距教學方式，學生無須到校上課，以致於本工作項必須暫時停擺，所幸最後於計畫期限內順利完成辦理 3 場次實體講座。

考量國際間有專家認為未來疫情可能成為常態，再加上大專院校學生已逐漸適應線上教學模式，執行單位建議未來在校園講座的辦理上可放寬形式，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，授課對象也可不限於單一學校或科系，將可提升講座辦理效益。

五、人才培訓課程辦理

本計畫原規劃補助 1 名優秀學員出國參加 APrIGF 2021 會議，惟受到全球 COVID-19 疫情影響，中央流行疫情指揮中心呼籲國人應避免所有非必要之出國行程，執行單位只得刪減此項獎勵，改以其他方案替代。或許是因為缺乏可實際出國參與國際會議之誘因，以致於今年度報名參加研習營的人數明顯低於前幾年。未來倘若全球疫情好轉，使得國際間的網路治理會議得以重返實體，建議仍可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。

本年度的研習營為 1 日的線上活動，雖然學員回饋之意見認為活動流程十分順暢，但亦有學員表示課程太過緊湊，也因為受限於課程時間，無法提供講師及學員充分的時間進行問答。建議通傳會未來可考量提高課程辦理經費，將研習營天數拉長為 1.5～2 天，使講師及學員可以有更充裕的時間進行教學及交流，實作上可考量先辦理 0.5～1 天的線上課程，再辦理 1 天實體（或依實際情況調整為線上）課程，惟需留意應預留充足的招生及評選時間。

未來規劃課程內容時，執行單位可將本計畫所研析之國際趨勢及政策建議編寫成課程教材，並邀請合適的專家前來主講，或做為課前自我預習的教材，亦可於課程中保留一堂課，專門介紹當前關鍵通傳議題，並邀請通傳會長官擔任講師。

為鼓勵研習營結訓學員持續參加網路治理相關活動，本計畫尋求外部資源挹注，額外提供學員新臺幣 2 萬元整「TWIGF 座談申辦獎學金」，以及 4,000 元整「yIGF 2021 線上特派員獎學金」。在執行單位的推廣下，1 名學員順利錄取 yIGF 取得獎學金，但另一方面，學員對於申辦 TWIGF 座談則明顯意願較低，推測可能的原因為，申辦 TWIGF 座談對於研習營學員而言門檻過高，未來或可調整推廣方向，鼓勵學員先從參加感興趣的 TWIGF

座談及撰寫座談摘要入門，逐漸培養蓄積相關領域的知識。

由於本研習營採線上辦理，問卷調查亦是透過線上方式實施，然而，線上問卷不若實體問卷容易回收，加上為使參加者放心填寫，問卷係採「不記名」方式，故不易掌握填寫者及未填寫者名單。未來可考量提供適度誘因提高問卷的填寫率，例如：完成問卷者須出示填畢畫面，方可核發培訓證書。此外，問卷亦可標示完成進度比例，使填表人知道目前的填表進度，並可預期需要花費的時間。

六、課程影片製播

相較於 YouTube 平臺上五花八門、平易近人的娛樂性質影音，網路治理影片對於大眾的吸引力相對較低，即便是國際性的聯合國 IGF、被譽為多方治理模式典範的 ICANN，或是我國最大的網路治理社群 TWIGF，其 YouTube 頻道的影片觀看次數極少超過 3 位數。

本年度執行單位在極為有限的預算內自行剪輯的 2 支短片，透過購買 YouTube 廣告加強推廣之下，雖將觀看次數從 2 位數提升到 400～500 次以上，但相較於執行單位以數倍預算與網紅合作的短片，公開不到兩週的時間即可累積觀看次數達到 1.3 萬次，依然是望塵莫及，這也凸顯出推廣的「通路策略」之重要性。透過慎選調性符合本計畫且形象正面的合作夥伴，可善用其既有的通路（頻道訂閱者），快速鎖定目標受眾。

然而，如同「專案管理三角形」的三個元素所定義的，專案品質往往取決於預算、時程及範疇，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。本年度計畫受限於預算規模，僅勉強足夠對外尋求合作製播 1 支短片，未來若通傳會提高影片製播預算，可考量增加與網紅合作的影片數量，或是嘗試與 1～2 位網紅合作，應更能擴大推廣版圖。

根據本次購買 YouTube 廣告的流量數據分析，點擊廣告觀看影片的使用者分眾以「愛書人」明顯居多，未來在預算允許的前提下，或可尋求與「知識型」網紅合作的機會（依據今年詢價的結果，單支影片製播費用約 20～35 萬），推廣的管道也可不限於 YouTube，而是選用合作對象點閱率較高的平臺。

七、國際會議 EuroDIG 參與

本計畫參與場次中，可供通傳會相關政策參考之處包括：

- 歐盟《數位服務法》：會議結論建議該法應該處理刪除非法內容的條款可能造成寒蟬效應的問題。另外，也建議提升法規的明確性，例如：有關盡職調查等責任、法規的適用地區和域外效力，都需要說明清楚。
- 5G 風險：會議結論建議要評估和因應 5G 對未來工作、健康和環境的影響。相關議題可參考本報告第四章「案例研析：5G 網路的治理議題初探」。
- 媒體素養：有講者提到北大西洋公約組織（NATO）國家（包含北美和歐洲共 30 國）已將媒體素養列為戰略防禦優先事項，凸顯媒體素養成為許多國家的重要施政項目。另有講者分享葡萄牙和烏克蘭的多元活潑推動方式，亦具參考價值。
- 內容和平臺治理：相關會議的結論為單一機制無法解決假訊息等內容問題，而是需要業者自律、法律、多方利害關係人共同監管等所有機制。此共識和我國《數位通訊傳播法》草案強調的兼容自律、他律、法律等公私協力概念具一致性。但講者們也提醒要賦予這些機制的內部和外部合法性，內部合法性指有強大的查核和制衡機制，外部合法性指治理模式的決策品質和時效性必須獲得認可，此點可供我國參考。
- 從技術層處理非法內容：會議結論強調處理非法內容要符合比例原則，不該期待從技術層來解決內容問題。此議題可參考本報告第五章第六節「二、建議事項之（一）立即可行之建議第 3 點」。
- 加密：會議結論為可信任的加密通訊，是民主社會的必需品，一旦遭到破壞，將是通訊自由的終結點。雖然我國《電信管理法》僅要求電信業者配合通訊監察工作，「沒有」解密的法定義務，但隨著各國執法機關高度期盼能破解加密資料以打擊犯罪，加密議題將持續成為國際討論焦點，亦是通傳會可以關注的議題之一。

附錄

附錄 1：「2021 網路治理研習營」學員手冊

附錄 2：「2021 網路治理研習營」講師手冊

附錄 3：「2021 網路治理研習營」課程簡報（僅提供講師授權公開部分）

附錄 4：APrIGF 2021 線上參與摘要報告

附錄 1.「2021 網路治理研習營」學員手冊

2021 網路治理研習營（IG Camp 2021）

學員手冊

課程時間： 2021 年 8 月 7 日（六）08:30~18:00

課程地點： Webex 線上會議室

指導單位： 國家通訊傳播委員會 NATIONAL COMMUNICATIONS COMMISSION

主辦單位： 財團法人中華民國國家資訊基本建設產業發展協進會 National Information Infrastructure Enterprise Promotion Association

協辦單位： 財團法人 TAIWAN NETWORK INFORMATION CENTER 台灣網路資訊中心　NETMISSION.asia www.nma.asia

目　錄

一、 課程表

時間	課程		講者 / 主持人
08:30-08:45	線上報到		
08:45-09:45	專題講習	國際焦點：科技戰與數位主權	吳國維 / NII 協進會董事
09:50-10:30	案例探討	新聞有價是國際趨勢？	胡元輝 / 中正大學傳播學系教授 陳奕儒 / Facebook 臺灣公共政策經理
10:40-11:20	案例探討	內容亂象誰負責？(CDA、DSA)	曾更瑩 / 理律法律事務所合夥律師 陳奕儒 / Facebook 臺灣公共政策經理
11:30-12:10	專題講習	數位人權：防疫、AI 和 eID	賈文宇 / 台灣人權促進會執行委員
12:10-13:10	午休		
13:10-13:50	專題講習	網路安全：從資安到國安議題	黃勝雄 / 台灣網路資訊中心執行長
14:00-14:40	專題講習	數位經濟：課稅、壟斷和炒股	熊全迪 / 理律法律事務所初級合夥人
14:40-14:50	分組準備		
14:50-16:30	分組演練	議題討論 / 角色扮演	講者帶領學員演練
16:30-17:10		小組成果報告	學員推派代表、講者總結
17:20-17:50	參與分享	經驗分享、參與機會	NetMission
17:50-18:00	結業式	結業手續	計畫人員

二、 Webex 線上會議室

1. 會議室連結：https://reurl.cc/kZWZpG，大小寫需一致。
2. 操作手冊請參閱附件 1。
3. 本研習營為免費活動，凡參加即表示同意遵守活動各項規定與紀律秩序等要求。

三、 分組討論資料

1. 分組名單

組別	成員
網路內容	高〇鼎、陳〇耀、高〇軒、林〇築 管〇良、林〇貞、龔〇幃、蔡〇安
網路安全	周〇渟、周〇慧、朱〇華、湯〇樺 林〇德、潘〇萍、張〇芝、林〇萱
數位經濟	王〇勛、許〇能、莊〇霖、蔡〇軒 楊〇楷、張〇瑜、楊〇傑、方〇宇

2. 各組討論題目

(1) 網路內容：

- 網際網路平臺是否應為刊載或張貼在平臺上的內容負責？
- 私人經營的網際網路平臺是否合適為國家或社會監控或查證平臺上所刊載或張貼的內容？

(2) 網路安全：

- DNS 濫用框架 （DNS Abuse Framework ）探討。

(3) 數位經濟：

- 數位平臺的壟斷：我們如何從治理角度看待數位平臺的市場優勢地位？
- 網路世界萬萬稅：我們應對數位經濟課稅嗎？

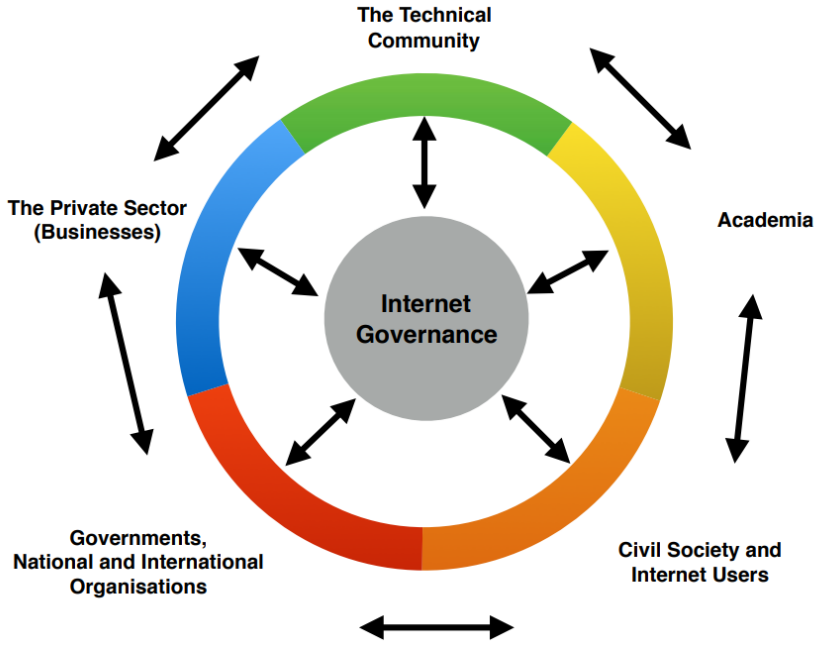
3. 參考時程

(1) 14:50 – 15:10 確認討論題目、分配「多方利害關係人」角色(參考圖 1) 。

(2) 15:10 – 16:00 以角色扮演方式，進行討論。

(3) 16:00 – 16:30 歸納討論結果 (參考表 1) 、推派報告者、準備報告內容 (彙整為電子檔)

(4) 16:30 – 17:10 小組報告 (10 分鐘*3 組，整體預留 10 分鐘緩衝時間)



資料來源：RIPE NCC

圖 1 網路治理與多方利害關係人

表 1 共識與歧見

大類	ICANN 對於討論結果 / 決策立場的分類	
共識	1. 完全共識	在最後一次宣讀中，小組當中沒有人反對該建議。
	2. 共識	大多數人同意，少數人不同意。
歧見	3. 強烈支持，但存在顯著反對意見	儘管大部分成員都支持該建議，但仍有顯著數量的成員不支持。
	4. 意見分歧 / 無共識	存有多種不同觀點，但任一觀點皆缺乏強力支持。此情況可能肇因於無法消弭的歧見，或缺乏強而有力、能說服他人的觀點。
建議	5. 少數人觀點	只有少數人支持的建議，或少數人提出的建議未獲得眾人支持或反對。

四、 結訓獎勵

1. **結業證書 & 獎學金：**全程參與研習營的學員 (包含如期完成課前預習與線上測驗) ，將獲頒結業證書，以及新臺幣$1,500 元整獎學金（公務人員除外）。
2. **優秀學員獎學金 (5 名) ：**主辦單位將組成評選小組，從結業且參與甄選的學員中，選出 5 名本國籍優秀學員，額外頒發新臺幣$1,000 元整獎學金。
3. **國際參與獎學金 (5 名) ：**優秀學員須依主辦單位分工，線上參與 APrIGF 2021 國際會議，並各別摘錄 2 場座談紀錄刊載於活動網站（內容包含：會議資訊、座談紀錄 2 場、參與心得），即可各別獲頒獎學金 NT$ 4,000 元整。
4. **yIGF 2021 線上特派員獎學金(2 名) :** 凡具備在學學生身分之學員，申請參加 2021 APrIGF yIGF 成功錄取者，於 9 月 17 至 20 日參與 yIGF 線上會議，並於社群平臺公開分享各場次活動參與心得，即可獲頒獎學金 NT$ 4,000 元整。
5. **TWIGF 座談申辦獎學金 (1 名 / 組) ：**結業學員可獨自或組隊申辦 TWIGF 座談 (Workshop) ，經 TWIGF 評選最高分者且完成辦理該場座談，並於會後提供紀錄摘要 (將載於本網站的【學習資源】) ，即可獲頒新臺幣$20,000 元整獎學金。徵稿時間依 TWIGF 網站公告為準。

五、 結業手續

項目	說明及注意事項
1. 問卷調查表	• 請填寫**線上問卷調查表**（請點選超連結前往），將您本次參與研習營的心得感想回饋予我們。
2. 獎學金領據	• 符合結訓資格之學員，主辦單位將於 8 月 10 日前以電子郵件方式寄發獎學金領據電子檔。 • 領據請列印紙本填寫，並於 8 月 17 日前寄回主辦單位，未成年者（未滿 20 歲）須由法定代理人簽章。 • 獎學金統一安排於 9 月 15 日匯款，未於規定期限內寄回領據者，將遞延至下一週期（10 月 15 日）匯款。
3. 獎學金領取姓名公開同意書	• 依《財團法人法》第 25 條第二項規定辦理。 • 須勾選是否同意主辦單位於官方網站公開您的姓名「全名」或「遮蔽部分姓名」，若皆不同意，則須勾選「自願放棄獎學金」。 • 未成年者（未滿 20 歲）須由法定代理人簽章。
4. 結業證書	• 符合結訓資格之學員，主辦單位將於 8 月 10 日前以電子郵件方式與學員確認結業證書寄送地址。 • 結業證書將於 8 月 20 日前以掛號信寄送到學員指定的地址。

附件 1：Webex 操作手冊

1. 登入線上會議室

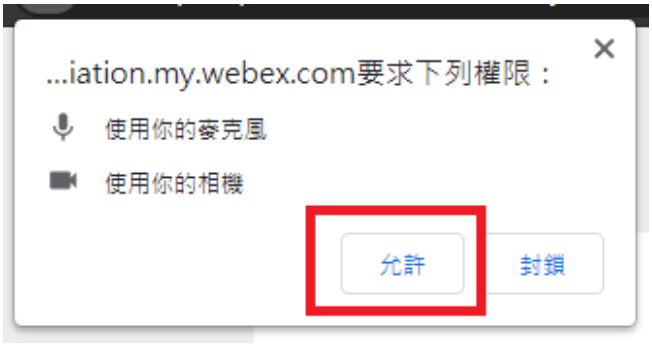
(1) 請於 8 月 7 日（六）上午 08:40-09:00 之間登入線上會議室，以完成線上報到，若超過 09:10 登入者視同遲到。

線上會議室連結：https://reurl.cc/kZWZpG

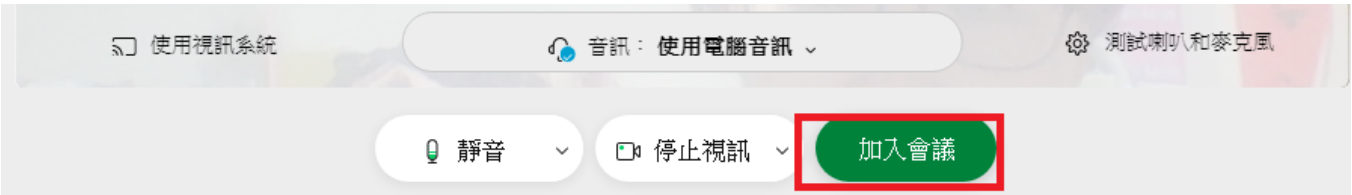
(2) 點選從您的瀏覽器加入。

(3) 在姓名欄內輸入「組別_中文全名」後，按下「以訪客身份加入」，亦可使用自己的 webex 帳號登入，但請一律使用「組別_中文全名」。

(4) 允許系統存取您的麥克風及相機。



(5) 按下「加入會議」，即可進入會議室。



2. 配合事項

(1) 系統會預設開啟視訊，學員可自行按下「停止視訊」，但課程期間請儘量保持視訊為開啟狀態，以利講師觀察學員反應，提高課程互動性。學員麥克風皆預設為靜音，您無法自行取消靜音，課程中如有需開啟麥克風時，統一由主辦單位開啟。

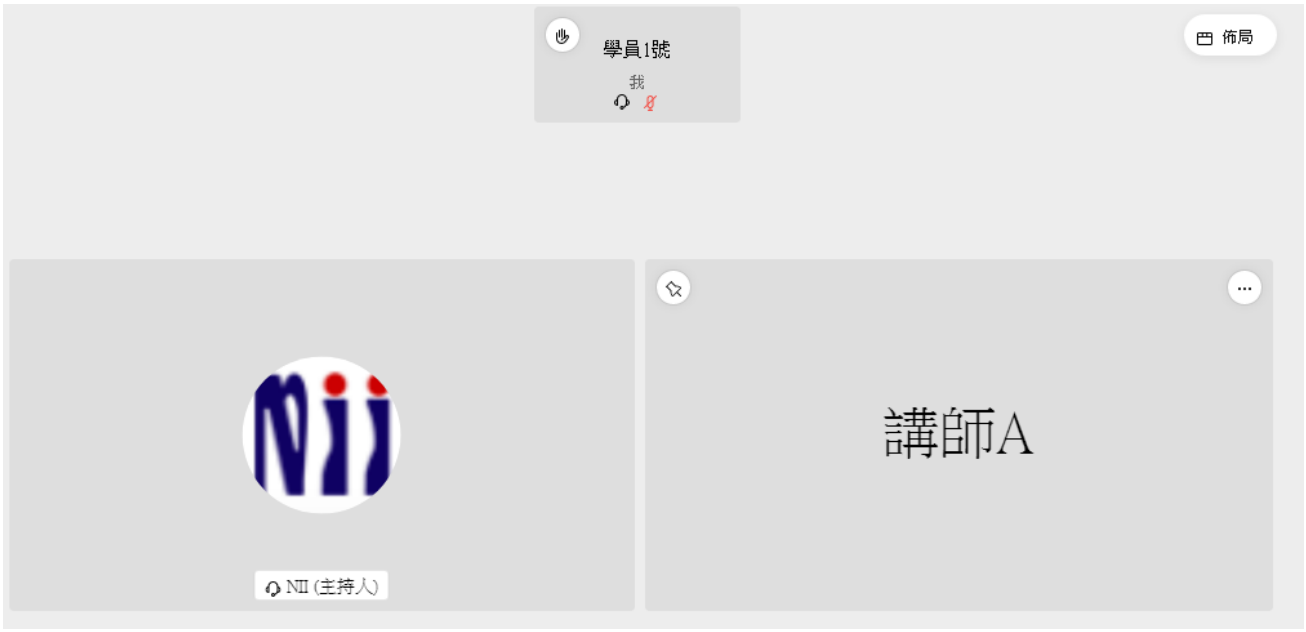
(2) 課程進行中如欲提問，請利用「舉手」功能。

(3) 學員可利用畫面最上方的「佈局」功能，自行設定畫面呈現方式。

(4) 不論您選用哪一種「佈局」，課程進行中可多加利用「移至舞台」功能，將講師固定在主畫面。

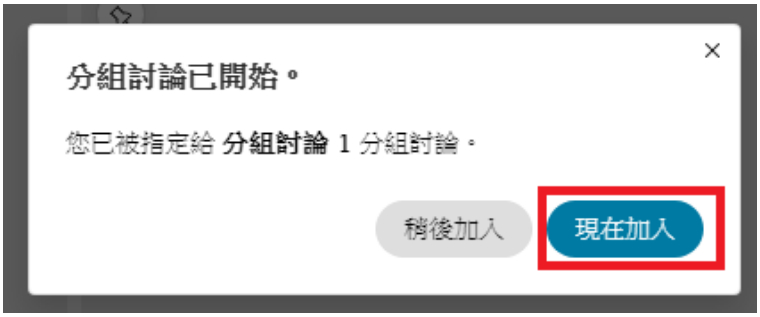

學員1號
我
NII (主持人)
移至舞台
聊天

「移至舞台」後的畫面如下。



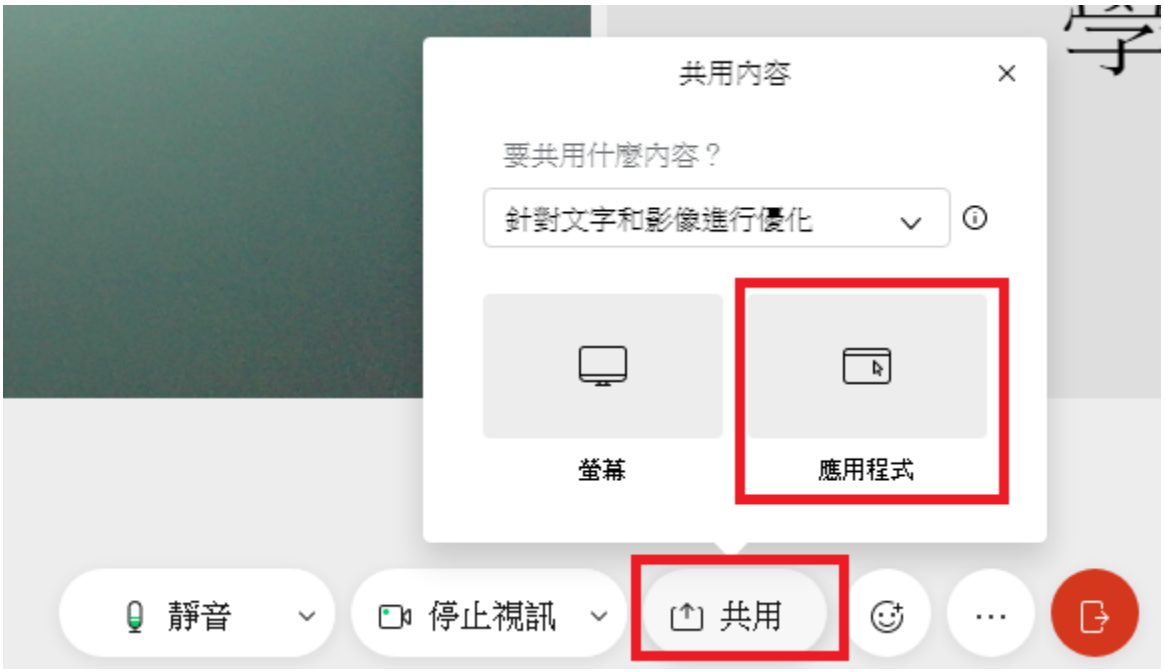
3. 分組討論

(1) 主辦單位已依據您填回出席調查表時所選擇的志願組別預先完成分組，進到「議題討論 / 角色扮演」課程時，Webex 會自動將您移動至所屬組別，請按下「現在加入」按鈕，即可與領隊講師及其同組學員展開討論。



(2) 畫面右側會顯示分組討論已持續的時間，以及您所屬組別中的成員姓名。

(3) 討論過程中如有需要分享畫面予其他學員，請先取得領隊講師的同意，再按下「共用」按鍵，選取要分享的應用程式

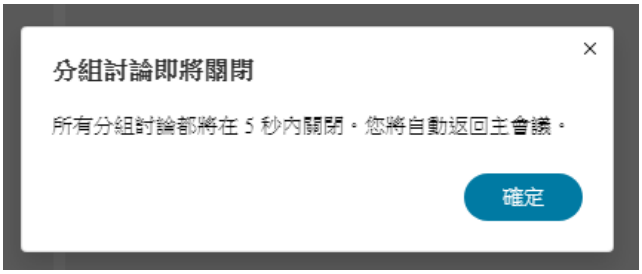


(4) 按下「視窗」按鍵後，選取要分享的視窗，再按下「分享」。

(5) 分享的視窗最下方會出現下列圖示，代表畫面已成功分享出去。

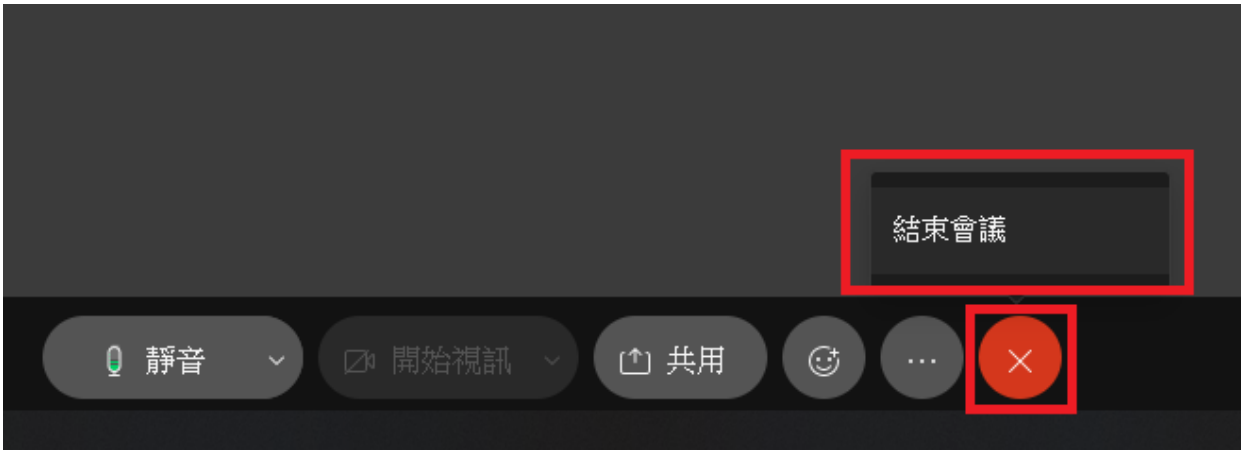
(6) 按下「停止共用」，即可結束分享畫面。

(7) 分組討論時間即將結束前，Webex 會顯示下列畫面，時間截止時，即自動將您移動回原先的主會議室。



4. 結束會議

(1) 按下「X」按鈕，再按下「結束會議」即可離開會議室。



(2) 若主辦單位按下「結束會議」，則所有參加者皆會自動離開會議室。

附件 2：中英詞彙對照表

英文	簡稱	中文	說明
Applicant Guidebook	AGB	申請指南	ICANN 組織於 2012 年發布，說明 New gTLD 申請規則及審核方式的指南。
American Standard Code for Information Interchange	ASCII	美國訊息交換標準代碼	電腦用於儲存、傳輸和列印英語（或「拉丁語系」）文本的一種通用字元編碼標準。
At-Large Advisory Committee	ALAC	一般使用者諮詢委員會	ALAC 代表網際網路個人使用者向 ICANN 提出建言，其組成成員係來自網際網路之使用社群中，關切 ICANN 運作之人士。
Country Code Names Supporting Organization	ccNSO	國碼域名支援組織	由 ccTLD 管理者組成，負責向 ICANN 提出有關 ccTLD（如：.us、.tw、.jp 等）與國際化域名 ccTLD（如：「.台灣」、「.рф 」（Russia）等）的政策性建言。
Country code top-level domain	ccTLD	國碼頂級域名	專門為國家、領土和地理區域留存的頂級域名，這些名稱源於國際標準化組織（International Organization for Standardization，ISO）發布的 ISO 3166-1 國家代碼清單。 ccTLD 可以按照 ISO 3166-1 標準訂定雙字母國家代碼（例如：.jp 代表日本、.ke 代表肯亞），或者使用非 US-ASCII 的當地文字代表國家和地區名稱。 鑒於 ccTLD 由各國自行管理，不同 ccTLD 的註冊規則和政策亦各有不同。

英文	簡稱	中文	說明
Domain Abuse Analysis Report	DAAR	域名濫用活動通報	蒐集域名註冊管理機構及受理註冊機構有關域名註冊濫用報告的系統。
Domain Name System	DNS	網域名稱系統	網域名稱系統是網際網路的一項服務。作為將域名和 IP 位址相互對應的一個分散式資料庫。
Data Protection Authority	DPA	資料保護機關	泛指歐洲經濟區境內所有 GDPR 執法機關。
European Data Protection Board	EDPB	歐洲資料保護委員會	EDPB 是一個獨立的歐盟機構，工作是確認歐盟境內的資料保護執法狀況一致，並推廣歐盟各國 DPA 的協作。
Expedited Policy Development Procedure	EPDP	加速版政策制定流程	顧名思義是 PDP 加速版，省略一般 GNSO 發起 PDP 時的「議題報告」（Issue Report）流程。
Government Advisory Committee	GAC	政府諮詢委員會	由國家級政府（National Governments）、國際論壇承認之經濟體（Distinct Economies as recognized by International Fora）、多國政府組織（Multinational Governmental Organizations）及條約組織（Treaty Organizations）以會員代表或觀察員身分所組成之諮詢委員會，任務為向董事會表達政府與公眾事務單位的關切事項。
General top-level domain	gTLD	通用頂級域名	網路號碼分配機構（IANA）管理的頂級域（TLD）之一。
General Data Protection Regulations	GDPR	通用資料保護規則	在歐盟法律中對所有歐盟個人關於數據保護和隱私的規範。

英文	簡稱	中文	說明
Generic Names Supporting Organization	GNSO	通用域名支援組織	GNSO 負責向 ICANN 提出有關通用頂級域名之政策性建言，由 gTLD 登記註冊管理機構、受理註冊機構、智慧財產權團體、企業團體、網路服務供應商團體、非營利組織團體及個人使用者團體所組成，下設理事會（Council）管理相關政策制定程序。
Internet Assigned Numbers Authority	IANA	網路號碼分配機構	是一系列網路協調職能，旨在確保全球唯一協定參數的有序分配，其中包括網域名稱系統根區和網路協定位址空間的管理。
Internet Corporation for Assigned Names and Numbers	ICANN	網際網路名稱與號碼支配機構	ICANN 是一全球、非營利、共識導向的國際組織（International corporation），1998 年 9 月成立於美國加州，負責監督管理網際網路技術管理功能（Internet technical management functions）、通訊協定參數及通訊埠（Protocol Parameters and Port）之協調、域名系統（DNS）之管理、IP 位址之分配暨指派，以及根伺服器系統（Root server system）之管理。
Internationalized Domain Names	IDN	國際化域名	包含代表當地語言、書寫方式與 26 個基本拉丁字母"a-z"不同字元的域名。
Internet Engineering Task Force	IETF	網際網路工程任務組	一個由關心網路基礎架構與運行穩定的網路設計師、開發工程師、維運人員和研究者組成，開放、全球化的大型國際社群。IETF 負責開發和推廣自

英文	簡稱	中文	說明
			願網際網路標準，特別是構成網路通信協定的標準。
ICANN Managed Root Server	IMRS	N/A	ICANN 負責維運的根伺服器，又稱 L-Root。
Internet Protocol	IP	網際網路通信協定	供網路上的電腦透過各式實體鏈路（physical links）快速互相通信。
Name Collision Analysis Project	NCAP	域名衝突分析計畫	ICANN 董事會指示 SSAC 負責執行，針對域名衝突的研究分析計畫。
Non-commercial Stakeholder Group	NCSG	非企業團體	GNSO 中代表非企業團體，包括私人及非營利組織之利害關係人所組成的團體。
Office of Chief Technology Officer	OCTO	技術長辦公室	ICANN 技術長辦公室，負責研究、提供資訊與內外部的人才培訓、組織能力建構，以及與多方利害關係人合作推動 DNS 安全。
Policy Development Procedure	PDP	政策制定流程	ICANN 社群中的支援組織（SO）欲制定新政策時，須經歷「由下而上、多方利害關係模式」的政策制定流程。
Registration Directory Service	RDS	註冊目錄服務	由頂級域名的註冊管理機構和受理註冊機構提供的線上服務。一般大眾可以透過此服務查詢域名註冊資料。
Root Server System Advisory Committee	RSSAC	根伺服器系統諮詢委員會	負責向 ICANN 董事會提出有關網域名稱根伺服器運作之建言。
Security and Stability Advisory Committee	SSAC	安全與穩定諮詢委員會	負責就網路域名系統的安全與穩定，提出政策建議。
System for Standardized Access/Disclosure	SSAD	標準化存取/揭露系統	EPDP 小組設想中，未來可供具合理目的之第三方存取/容許受理註冊機構

英文	簡稱	中文	說明
			合法揭露非公開註冊資料的標準化系統。
	WHOIS		用來提供註冊目錄服務（RDS）的技術協定（protocol），在 ICANN 社群中常用來代稱 RDS。

附錄 2.「2021 網路治理研習營」講師手冊

2021 網路治理研習營（IG Camp 2021）

講師手冊

課程時間： 2021 年 8 月 7 日（六）08:30~18:00

課程地點： Webex 線上會議室

指導單位： 國家通訊傳播委員會 NATIONAL COMMUNICATIONS COMMISSION

主辦單位： 財團法人中華民國國家資訊基本建設產業發展協進會 National Information Infrastructure Enterprise Promotion Association

協辦單位： 財團法人 TAIWAN NETWORK INFORMATION CENTER 台灣網路資訊中心

NETMISSION.asia www.nma.asia

目　錄

一、 課程表

時間	課程		講者 / 主持人
08:30-08:45	線上報到		
08:45-09:45	專題講習	國際焦點：科技戰與數位主權	吳國維 / NII 協進會董事
09:50-10:30	案例探討	新聞有價是國際趨勢？	胡元輝 / 中正大學傳播學系教授 陳奕儒 / Facebook 臺灣公共政策經理
10:40-11:20	案例探討	內容亂象誰負責？(CDA、DSA)	曾更瑩 / 理律法律事務所合夥律師 陳奕儒 / Facebook 臺灣公共政策經理
11:30-12:10	專題講習	數位人權：防疫、AI 和 eID	賈文宇 / 台灣人權促進會執行委員
12:10-13:10	午休		
13:10-13:50	專題講習	網路安全：從資安到國安議題	黃勝雄 / 台灣網路資訊中心執行長
14:00-14:40	專題講習	數位經濟：課稅、壟斷和炒股	熊全迪 / 理律法律事務所初級合夥人
14:40-14:50	分組準備		
14:50-16:30	分組演練	議題討論 / 角色扮演	講者帶領學員演練
16:30-17:10		小組成果報告	學員推派代表、講者總結
17:20-17:50	評選優秀學員		

二、 Webex 線上會議室

1. 會議室連結：https://reurl.cc/kZWZpG，大小寫需一致。
2. 操作手冊請參閱附件 1。

三、 分組討論資料

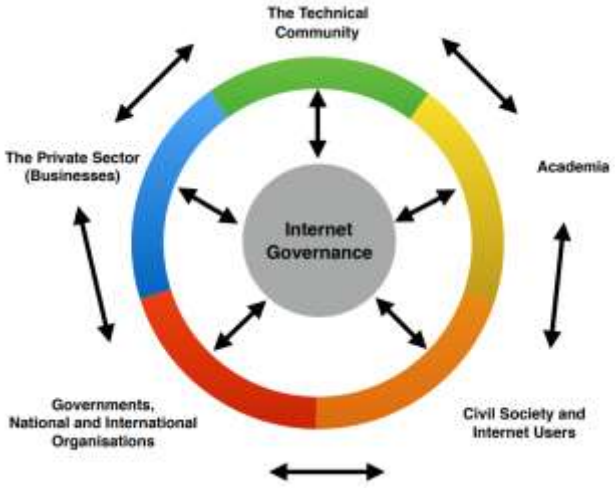
1. 參考時程

(1) 14:50 – 15:10 確認討論題目、分配「多方利害關係人」角色（參考圖 1）。

(2) 15:10 – 16:00 以角色扮演方式，進行討論。

(3) 16:00 – 16:30 歸納討論結果（參考表 1）、推派報告者、準備報告內容（彙整為電子檔）

(4) 16:30 – 17:10 小組報告（10 分鐘*3 組，整體預留 10 分鐘緩衝時間）



資料來源：RIPE NCC

圖 1 網路治理與多方利害關係人

表 1 共識與歧見

大類	ICANN 對於討論結果 / 決策立場的分類	
共識	1. 完全共識	在最後一次宣讀中，小組當中沒有人反對該建議。
	2. 共識	大多數人同意，少數人不同意。
歧見	3. 強烈支持，但存在顯著反對意見	儘管大部分成員都支持該建議，但仍有顯著數量的成員不支持。
	4. 意見分歧 / 無共識	存有多種不同觀點，但任一觀點皆缺乏強力支持。此情況可能肇因於無法消弭的歧見，或缺乏強而有力、能說服他人的觀點。
建議	5. 少數人觀點	只有少數人支持的建議，或少數人提出的建議未獲得眾人支持或反對。

2. 各組討論題目

(1) 網路內容—曾更瑩律師：

- 網際網路平臺是否應為刊載或張貼在平臺上的內容負責？
- 私人經營的網際網路平臺是否合適為國家或社會監控或查證平臺上所刊載或張貼的內容？

(2) 網路安全—黃勝雄執行長：

- DNS 濫用框架 （DNS Abuse Framework ）探討。

(3) 數位經濟—熊全迪律師：

- 數位平臺的壟斷 : 我們如何從治理角度看待數位平臺的市場優勢地位？
- 網路世界萬萬稅：我們應對數位經濟課稅嗎？

四、 評選優秀學員

1. **評選委員：**本研習營 3 位分組領隊講師（曾更瑩律師、黃勝雄執行長、熊全迪律師），以及主辦單位梁理旋副執行長、林郁敏資深經理。
2. **線上會議室：**meet.google.com/kwk-zqof-pcj
3. **目標：**評選 5 名優秀學員（及備取 1 名）線上參與 9 月 27 日至 30 日於尼泊爾加德滿都辦理之 APrIGF 2021 國際會議。
4. **獎勵：**

   (1) 優秀學員獎學金$1,000 元整。

   (2) 依主辦單位分工，線上參與 APrIGF 2021 國際會議，並各別摘錄 2 場座談紀錄刊載於活動網站（內容包含：會議資訊、座談紀錄 2 場、參與心得），另可獲頒獎學金$4,000 元整。

5. **評選規則：**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。每位講師可推薦 2 名優秀學員，再共同討論這些學員的特色與潛力，最後透過投票或評分等方式，決議正、備取優秀學員名單。

附件 1：Webex 操作手冊

1. 登入線上會議室

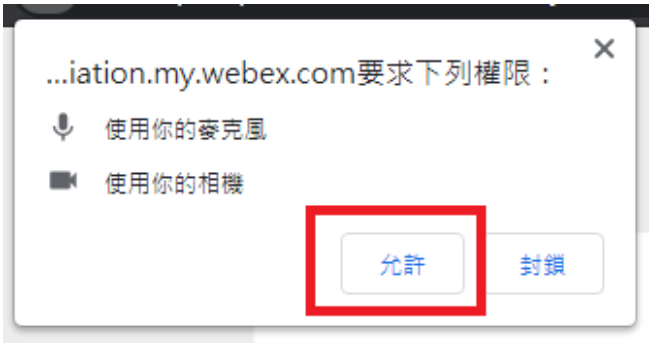
(1) 8 月 7 日 (六) 請於您講課的時間前 10 分鐘登入線上會議室，我們會利用兩堂課中間的休息時間與您測試系統連線。

線上會議室連結：https://reurl.cc/kZWZpG

(2) 點選從您的瀏覽器加入。

(3) 在姓名欄內輸入「中文全名」後，按下「以訪客身份加入」，亦可使用自己的 webex 帳號登入，建議使用「中文全名」以利辨識。

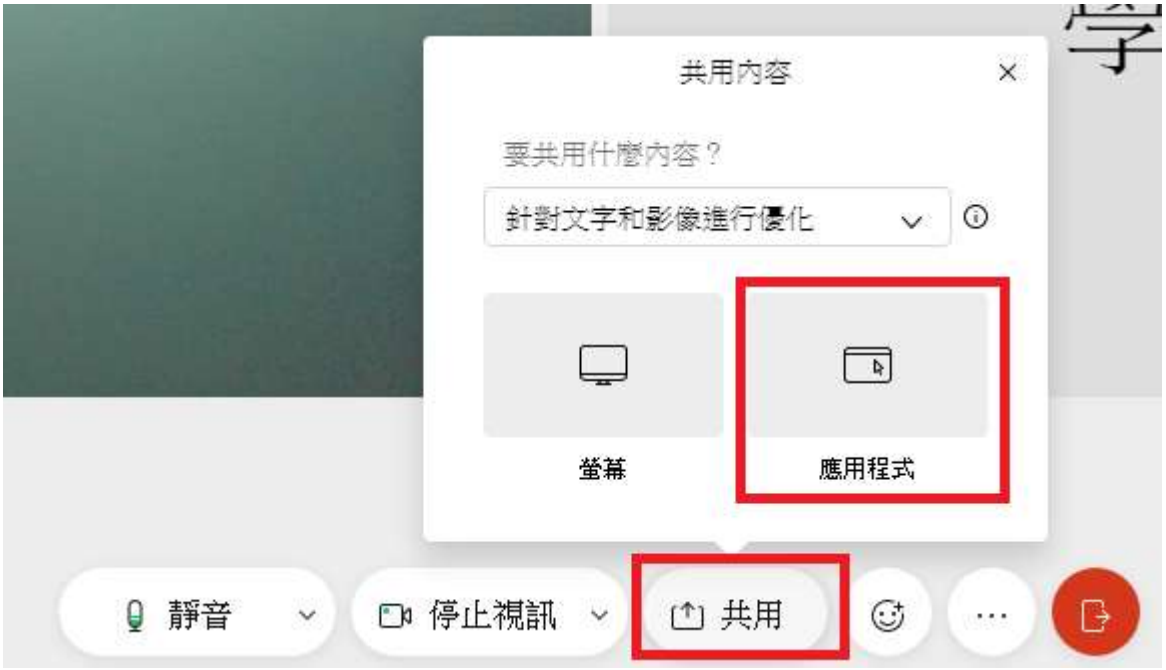
(4) 允許系統存取您的麥克風及相機。



(5) 按下「加入會議」，即可進入會議室。

2. 分享簡報

(1) 按下「共用」按鍵，選取要分享的應用程式。



(2) 按下「視窗」按鍵後，選取要分享的視窗，再按下「分享」。

(3) 分享的視窗最下方會出現下列圖示，代表畫面已成功分享出去。播放簡報時，建議第一次先按 enter，之後再使用上下按鍵切換頁，會比較順。

(4) 按下「停止共用」，即可結束分享畫面。

3. 學員配合的事項

(1) 登入後，系統會預設開啟視訊，學員可自行按下「停止視訊」，但課程期間請儘量保持視訊為開啟狀態，以利講師觀察學員反應，提高課程互動性。學員麥克風皆預設為靜音，您無法自行取消靜音，課程中如有需開啟麥克風時，統一由主辦單位開啟。

(2) 課程進行中如欲提問，請利用「舉手」功能。

(3) 學員可利用畫面最上方的「佈局」功能，自行設定畫面呈現方式。

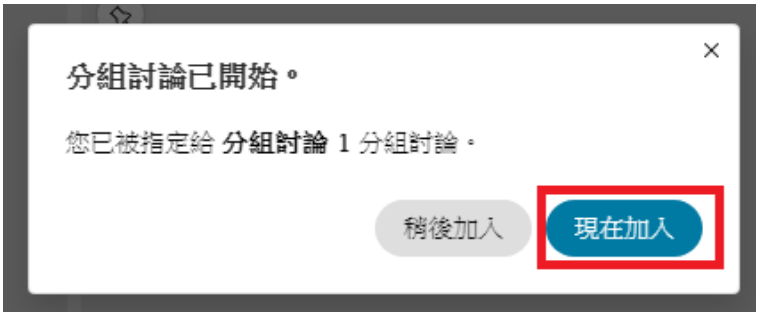
(4) 不論您選用哪一種「佈局」，課程進行中可多加利用「移至舞台」功能，將講師固定在主畫面。

附錄 2-12

「移至舞台」後的畫面如下。

4. 分組討論

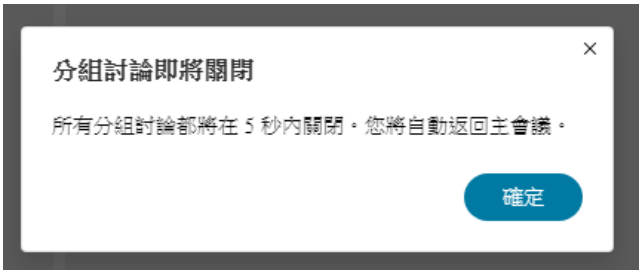
(1) 主辦單位已依據學員填回出席調查表時所選擇的志願組別預先完成分組，進到「議題討論 / 角色扮演」課程時，Webex 會自動將領隊講師及學員移動至所屬組別，請按下「現在加入」按鈕，即可與學員展開討論。



(2) 畫面右側會顯示分組討論已持續的時間，以及您所屬組別中的成員姓名。

(3) 討論過程中，學員如有需要分享畫面，須先取得領隊講師的同意。

(4) 主辦單位將派員加入各組，協助講師留意討論時間。分組討論即將結束前，Webex 會顯示下列畫面，時間截止時，即自動將您移動回原先的主會議室。



5. 結束會議

(1) 按下「X」按鈕，再按下「結束會議」即可離開會議室。

附錄 3.「2021 網路治理研習營」課程簡報（僅提供講師授權公開部分）

《2021網路治理研習營》

新聞有價是國際趨勢？
基金模式的意義與價值

胡元輝
中正大學傳播學系
2021/08/07


"All the News That's Fit to Print"

The New York Times

Late Edition

VOL. CLIV ... No. 53,075 NEW YORK, SUNDAY, DECEMBER 26, 2004 $3.50

ECONOMIC RALLY FOR ARGENTINES DEFIES FORECASTS

AFTER RECORD '01 DEFAULT

Ignoring Orthodox Advice Results in 8% Growth for 2 Years Running

By LARRY ROHTER

U.S. IS SUGGESTING GUARANTEED ROLE FOR IRAQ'S SUNNIS

POST-BALLOT ADJUSTMENT

The Hope Is to Draw More Voters From a Minority That Once Ruled

By STEVEN R. WEISMAN

Have No Baggage, Can't Travel

Flight cancellations and delays left thousands of travelers separated from their luggage during the Christmas holidays. The problem was especially serious for US Airways at Philadelphia International Airport, above. The Transportation Department is investigating. Page 36.

GOVERNORS UNITE IN MEDICAID FIGHT

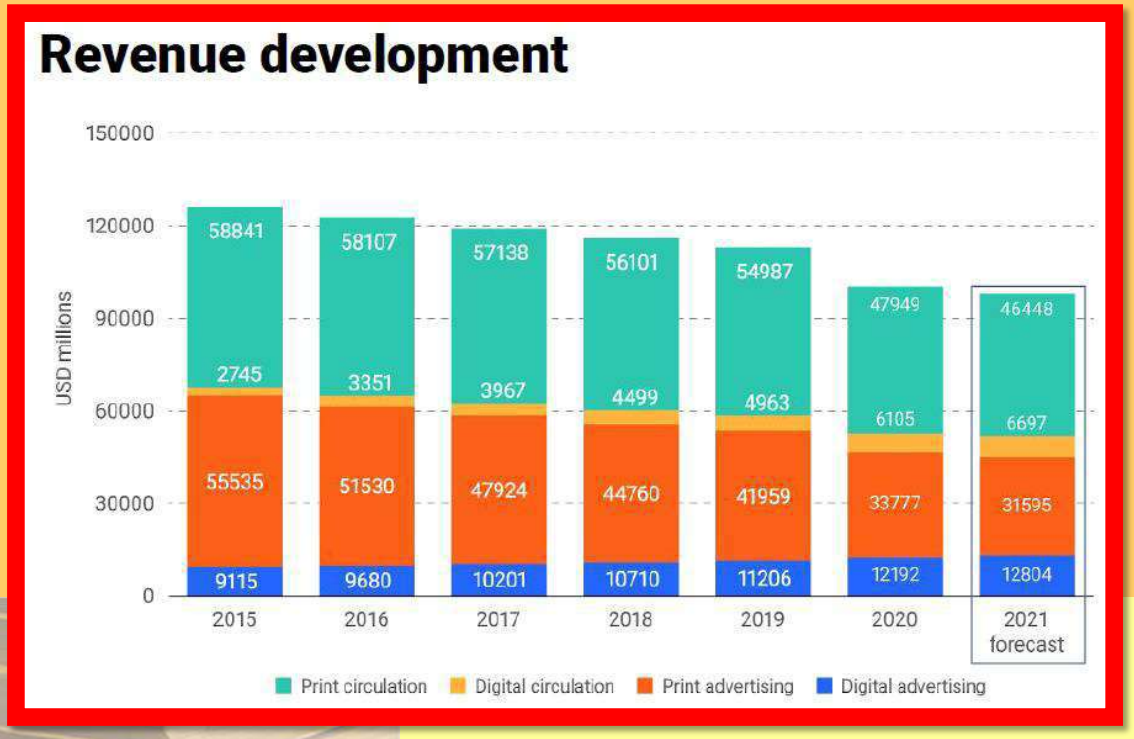
As Nuclear Secrets Emerge, More Are Suspected

1989年 : 1612頁 / 5.5公斤
2019年 : 192頁 / 1.8公斤

新聞生態的根本性變遷

Fundamental Transformation

新聞媒體的營運挑戰（全球）



資料來源：World Association of News Publishers

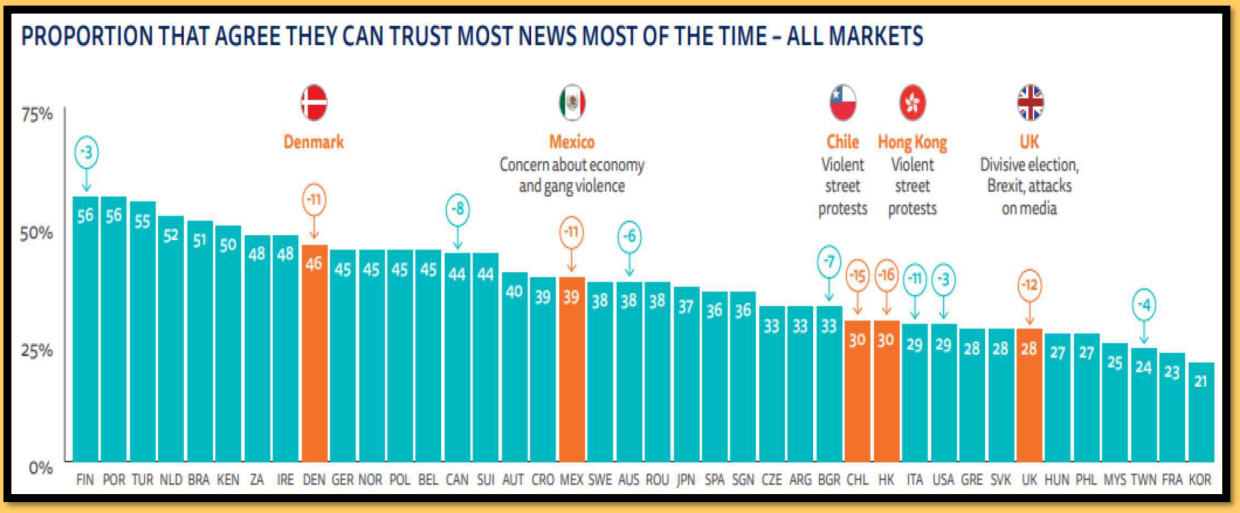
新聞媒體的營運挑戰（台灣）

整體廣告量

單位:千元	無線電視	有線電視	報紙	雜誌	廣播	戶外	網路
2010	5,060,629	19,861,782	11,955,662	5,549,827	4,482,972	3,288,964	8,551,000
成長率%	16.5%	25.6%	19.5%	9.7%	19.2%	14.9%	22.3%
2011	4,899,729	21,175,082	10,674,408	5,677,641	4,139,539	3,680,282	10,215,000
成長率%	-3.2%	6.6%	-10.7%	2.3%	-7.7%	11.9%	19.5%
2012	3,999,707	20,059,287	9,522,068	5,340,950	3,555,348	3,591,644	11,601,000
成長率%	-18.4%	-5.3%	-10.8%	-5.9%	-14.1%	-2.4%	13.6%
2013	3,817,132	20,992,491	8,679,067	5,293,617	3,120,841	4,168,427	13,680,000
成長率%	-4.6%	4.7%	-8.9%	-0.9%	-12.2%	16.1%	17.8%
2014	3,681,093	20,906,497	7,906,026	4,844,362	3,122,120	4,287,798	16,177,000
成長率%	-3.6%	-0.4%	-8.9%	-8.5%	0.0%	2.9%	18.3%
2016	3,370,710	19,163,422	5,079,743	3,114,994	2,080,615	3,870,662	25,871,000
2017	3,059,603	18,300,268	4,187,630	2,318,190	1,739,528	3,640,478	33,097,000
成長率%	-9.2%	-4.5%	-17.6%	-25.6%	-16.4%	-5.9%	27.9%
2018	2,975,699	17,691,661	3,664,243	1,984,498	1,873,731	4,251,412	38,966,000
成長率%	-2.7%	-3.3%	-12.5%	-14.4%	7.7%	16.8%	17.7%
2019	2,821,694	16,543,225	3,065,170	1,681,337	1,853,784	4,377,855	45,841,000
成長率%	-5.2%	-6.5%	-16.3%	-15.3%	-1.1%	3.0%	17.6%

資料來源: MAA媒體白皮書

新聞媒體的信任挑戰（全球）



資料來源：Reuters Institute for the Study of Journalism

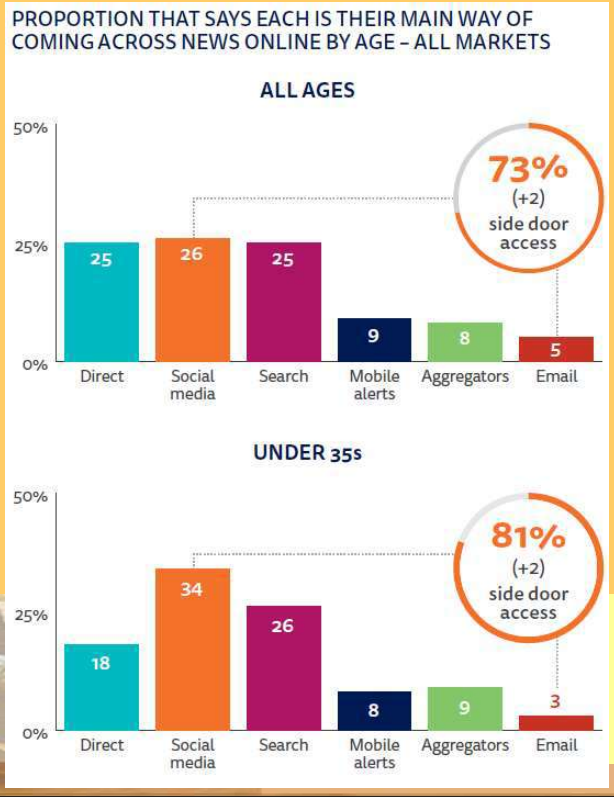
新聞媒體的信任挑戰（台灣）

News overall	News I use
31% (+7) 42/46	38%

News in search	News in social
29%	21%

資料來源：Reuters Institute for the Study of Journalism

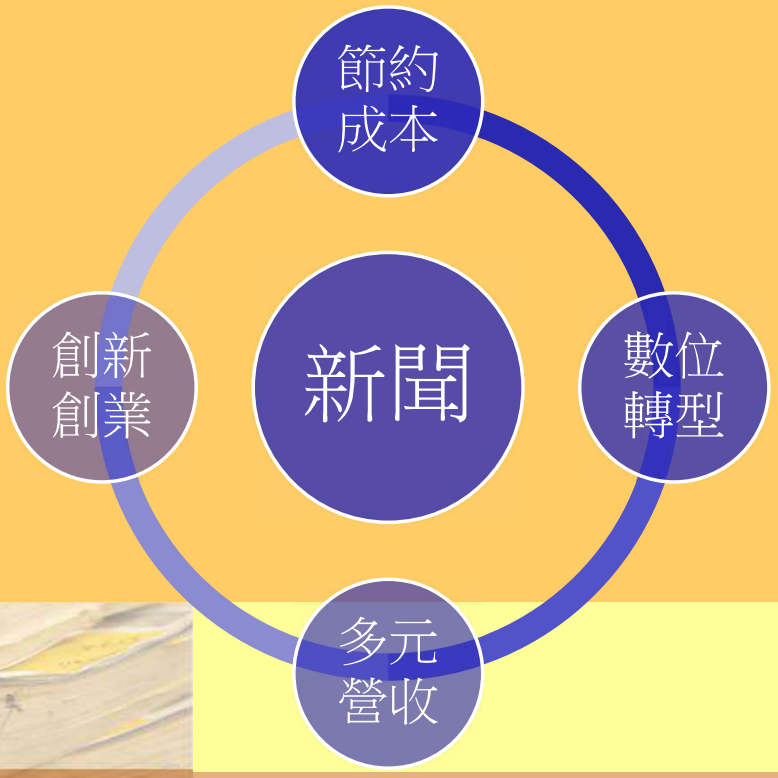
網路平台對新聞媒體的衝擊



以平台為基礎(platform-based)的新聞接收習慣

資料來源：Reuters Institute for the Study of Journalism

新聞業的因應之道



新聞業者與網路平台的愛恨情仇

- 新聞業者大幅失去與其消費者建立**直接關係**的機會，新聞媒體雖不願受制於網路平台，卻又必須仰賴網路平台帶來流量並分享廣告收益。
- 新聞媒體嘗試繞過平台業者的中介，直接與新聞消費者建立關係，其方法包括運用**電子郵件**、**行動提醒**(mobile alerts)等。
- 網路平台藉由新聞服務強化平台的黏著度，亦希望強化資訊流的主導地位，以持續爭取、擴大廣告營收。

新聞有價？

有價
- 好新聞不會從天而降
- 好新聞需要經濟支持

有價
- 科技不是元凶
- 新聞必須長存

有價
- 平台雖不產製
- 責任猶須承擔

各國政策作為(平台)

- **德國**與**西班牙**分別於2013年及2014年頒布新著作權法案，賦予新聞媒體新聞鄰接權(neighbouring right)。
- **歐盟**於2019年6月生效實施的新著作權指令中納入鄰接權概念，要求各會員國在兩年內透過國內修法予以實施。
- **澳洲**政府從競爭法出發，於2021年2月通過一項強制性法規草案，要求Google和Facebook使用澳洲媒體機構的新聞或其他內容必須付費。

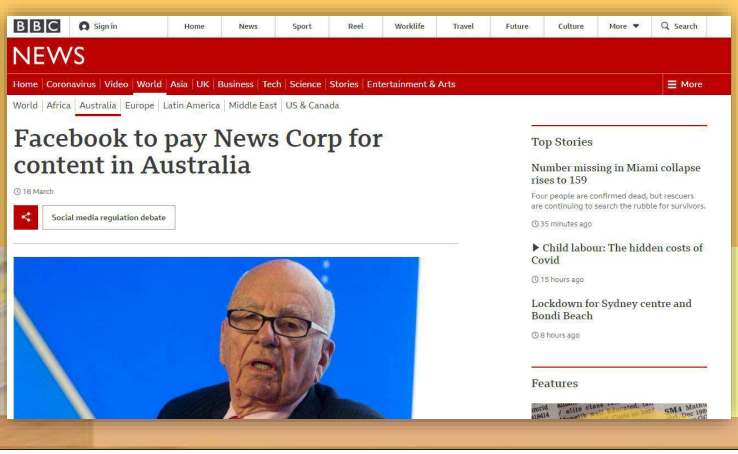
澳洲立法的問題

- **大型媒體或媒體集團**易獲較大利益，中小型、公共或獨立、另類媒體因協商力量薄弱，受惠有限。
- 新聞業者未必會將所獲費用直接或完全投入**新聞採編作業**，以提升整體新聞的品質。
- 新聞媒體與平台業者的不對等關係益趨深化，可能斲傷媒體應有的**監督功能**。

圖片:The Guardian

澳洲立法的問題 (BBC News)

- **News Corp** spearheaded a lobbying campaign in Australia - with support from its traditional rivals - to get politicians to make the tech firms pay for news content from its sites.。
- Analysts looking at Australia's media law have long suggested that it is primarily **designed to help big firms** like News Corp as opposed to smaller media titles.

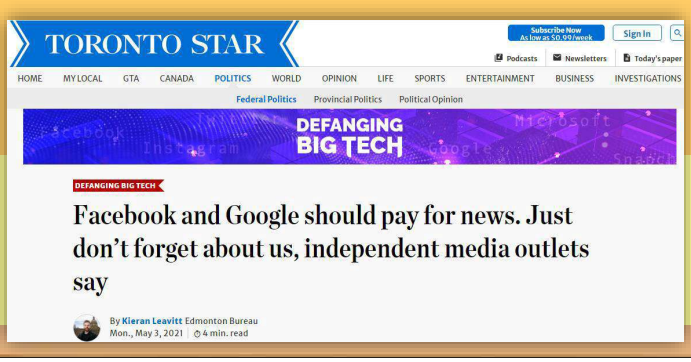


思考平台付費新模式

- **設立基金**：大型網路與社群平台將其一定比例的營收提撥給依法設立的基金。
- **基金組成**：由相關利益關係人組成，包括新聞媒體、平台業者、公民團體、學者專家等各方面代表。
- **運作方式**：基金具獨立性質，依合理比例分別運用於公共、獨立與商業媒體，後者經費補助可依據提案進行審核，以真正挹注於優質新聞的推動。

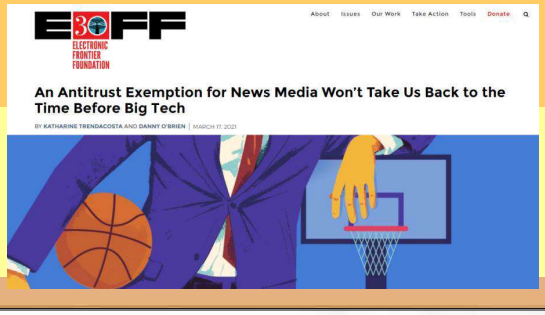
加拿大的回應 (Toronto Star)

- Emma Gilchrist, editor-in-chief of The Narwhal and chair of Press Forward, an organization of independent news outlets, says she hopes the government's plan helps **foster innovation** in the industry, rather than **just prop up established news outlets**.。
- "If Facebook and Google do have a responsibility for helping to create a **healthy news organization**," ···Gilchrist said the government could also **set up an independent fund** that digital platforms pay into and then gets distributed to media companies.



美國的回應 (Electronic Frontier Foundation)

- Journalism Competition and Protection Act：few truly small, independent media operations exist right now. And in the case of certain companies—like the ones owned by the Murdochs or the Sulzbergers—it would be a mistake to assume the ills of the industry are actually being visited upon them: or that **catering to their needs will trickle down to the rest of the journalistic ecosystem**.
- The Australian proposal：the companies can still, it seems, **separate the big players from the small**.



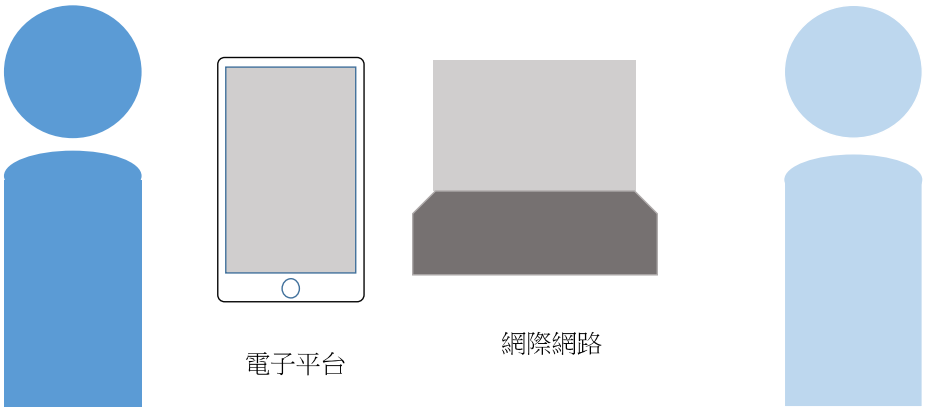
好新聞是好民主的支柱


敬請指教

內容亂象誰負責？(CDA、DSA、DCA)

理律法律事務所
曾更瑩律師
2021年8月7日

1



2

現象與影響

- 假新聞/不實資訊
- 煽動暴力或仇恨之言論
- 網路霸凌
- 色情猥褻言論或圖像/影響兒童身心
- 性交易
- 販賣槍枝
- 毒品交易
- 盜版影片、遊戲
- 操縱選舉
- 對抗政府
- COVID-19疫情

3

美國管制模式

4

美國

- 1996 年通過的「Communications Decency Act」第 230 條規定，互動式電腦服務的提供者或使用者，就非出於己的資訊內容，不應被視為出版人及發表人，是被稱為「善良撒馬利亞人條款」的免責規範。

5

CDA Section 230 (c)

(c)PROTECTION FOR "GOOD SAMARITAN" BLOCKING AND SCREENING OF OFFENSIVE MATERIAL

(1)TREATMENT OF PUBLISHER OR SPEAKER No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2)CIVIL LIABILITY No provider or user of an interactive computer service shall be held liable on account of—

(A)any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B)any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

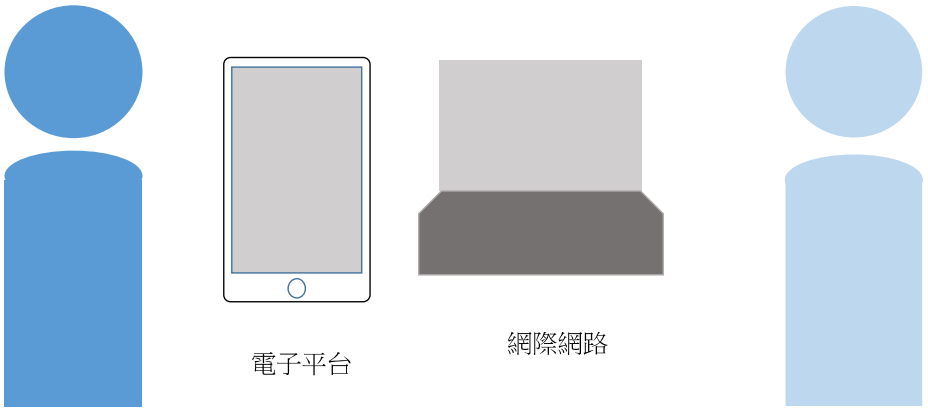
6

CDA Section 230 (d)

- **(d)OBLIGATIONS OF INTERACTIVE COMPUTER SERVICE** A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

7

美國模式: 平台"動"(作為)與"不動"(不作為)都沒有責任
(只有保護兒少的義務)



8

CDA 230 爭議

- 2020年5月28日川普簽署行政命令，當推特或臉書這類企業被認定不當壓制言論自由 (例如暫時關閉帳號或刪除文章)，聯邦主管機關對其究責更為容易。

  川普簽署的行政命令重點包含：

  （一）若社群平台「編輯或修改」使用者的貼文內容，那麼其依據CDA 230所獲得的「法律免責」保護，將不再適用。

  （二）若平台方「封鎖或刪除」使用者貼文，聯邦通信委員會（FCC）須釐清是否存在「欺詐」、「藉口」...等與平台的服務條款相違背的動機動作。

  （三）檢視政府在社群平台上投放的廣告，是否因為平台方本身觀點，而遭到不當限制。

  （四）白宮應建立市民投訴管道，以便檢舉平台有關的偏見與不當對待。

- 美國國內也有許多修正CDA 230的建議與聲浪

9

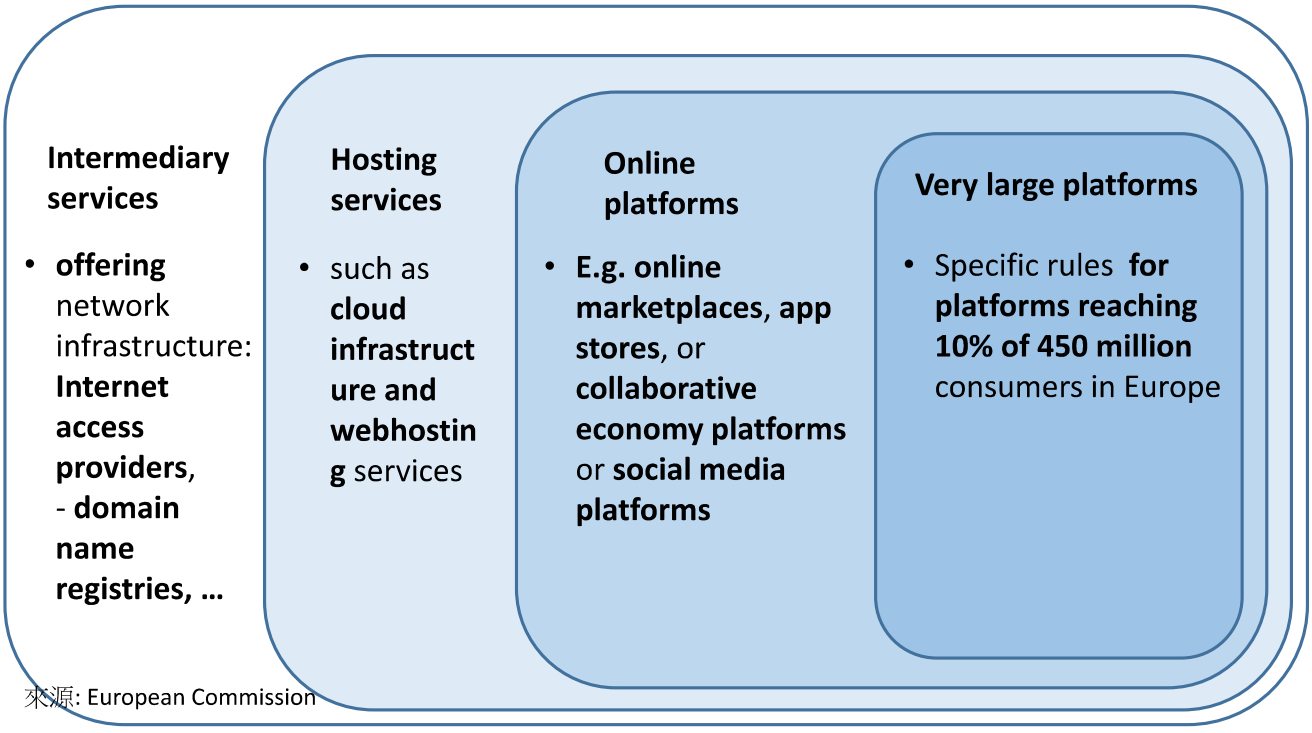
歐盟管制模式

10

歐盟

- 歐盟成員國德國、法國近年來對於反仇恨言論多所著墨
- 歐盟在2020年12月5日公布 Digital Service Act (DSA)草案，宣示建立歐盟單一市場之宏圖

11



來源: European Commission

	VERY LARGE PLATFORMS	ONLINE PLATFORMS	HOSTING SERVICES	ALL INTERMEDIARIES
Points of contact	•	•	•	•
Legal representatives	•	•	•	•
Terms and conditions	•	•	•	•
Reporting obligations	•	•	•	•
N&A	•	•	•	
Statement of reasons	•	•	•	
Complaint handling	•	•		
OOC	•	•		
Trusted flaggers	•	•		
Abusive behaviour	•	•		
KYBC	•	•		
Reporting criminal offences	•	•		
Advertising transparency	•	•		
Reporting obligations	•			
Risk assessment and mitigation	•			
Independent audits	•			
Recommender systems	•			
Enhanced advertising transparency	•			
Crisis protocols	•			
Data access and scrutiny	•			
Compliance officer	•			
Reporting obligations	•			

Cumulative obligations

來源: European Commission

Online Platform的義務與責任(Hosting)

- 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)

14

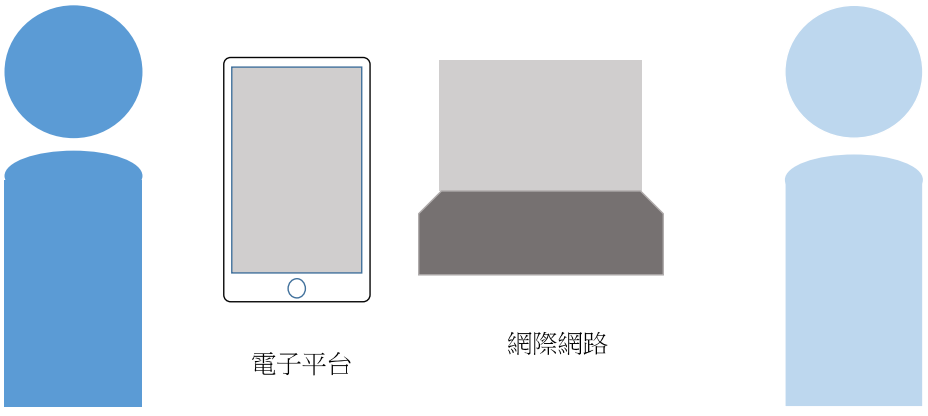
其他原則

- Providers of intermediary services shall not be deemed ineligible for the exemptions from liability referred to in Articles 3, 4 and 5 solely because they carry out voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content, or take the necessary measures to comply with the requirements of Union law, including those set out in this Regulation. (主動採取行動不會喪失免責資格)
- No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers. (沒有主動監控內容的義務)

15

歐盟未來模式:

平台如果知情，就必須採取行動(作為)
但是沒有積極監控的義務



16

台灣管制模式

17

現行法律規定中的平台責任

- 無一般性免責或歸責之原則性法律
- 大部分的網路內容法律或是對於假消息的規範的法律均處罰實際的行為人
- 著作權法、兒童及少年福利與權益保障法、兒童及少年性剝削防制條例等採取notice and take down 或知情始須採取行動之管制方式
- 網際網路內容涉及境外應施檢疫物販賣至國內或輸入時應採取措施 ---要求平台主動審查廣告內容並採取移除措施
- 假消息防範目前以業者自律之方式處理

18

數位通訊傳播法草案 (平台責任)

第13條	數位通訊傳播服務提供者對其提供使用之資訊，應負法律責任。 數位通訊傳播服務提供者對其傳輸或儲存之他人資訊，不負審查或監督義務。 通訊傳播主管機關得召集各目的事業主管機關依數位通訊傳播服務對於兒童及少年之影響程度，指定數位通訊傳播服務提供者設置經訓練之專責人員，配合辦理兒童及少年福利與權益保障法第四十六條第一項所定事項。 前項訓練，由衛生福利部自行或委託辦理。
第14條	提供接取服務之數位通訊傳播服務提供者對其使用者之侵權行為，有下列情形者，不負賠償責任： 一、所傳輸之資訊係由使用者所發動或請求。 二、資訊之處理係經由自動化技術予以執行，且未就傳輸之資訊為任何篩選或修改。
第15條 免責原則	數位通訊傳播服務提供者對於第三人為供他人使用而儲存之資訊，於符合下列情形之一時，不負賠償責任： **一、不知有違法行為或資訊，且於他人請求損害賠償時，就所顯示之事實或情況，亦不能辨別該行為或資訊為違法。** **二、於知悉行為或資訊為違法後，移除資訊或使他人無法接取之。** 前項第三人不包括受數位通訊傳播服務提供者指揮監督之人。
第16條 免責原則	提供前二條以外服務之數位通訊傳播服務提供者，有下列情形之一者，對其使用者之侵權行為，不負賠償責任： **一、所傳輸之資訊係由使用者發動或請求，且未改變使用者存取之資訊。** **二、經權利人通知或知悉其使用者涉有侵權行為後，移除或使他人無法接取涉有侵權之內容或相關資訊，或為其他適當之處置。**

19

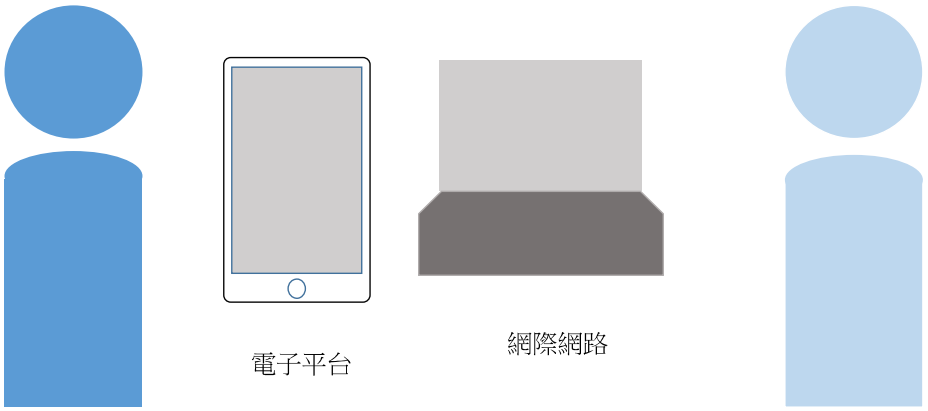
主管機關委託研究建議

- 透明度報告
- 加註警語
- 資訊阻斷令(司法或行政命令)

20

台灣未來模式:?

平台應該....? 或無須....?



21

Thank you for listening!

請多指教!

22

網路安全：從資安到國安議題

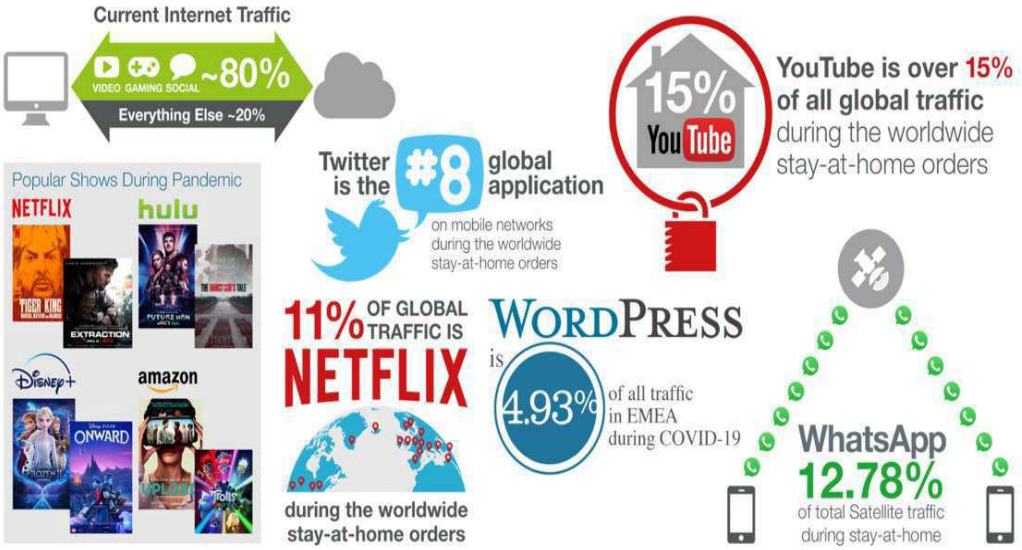
Dr. Kenny Huang　黃勝雄博士
CEO, TWNIC
huangk@twnic.tw

世界經濟論壇 2020全球風險報告

發生機會高

資料來源：世界經濟論壇, 2020

COVID-19 疫情對網際網路影響



資料來源: Sandvine, 2020

3

Cybersecurity: Internet policy development reference frameworks

	non-enforceable policy	Enforceable norms recognized within international law
Global public goods	x	
International spaces and shared resources		x
Critical infrastructure protection		x

characteristics	ICANN	ITU	IGF	APNIC	TWNIC	IETF	NATO
multistakeholder	x		x	x	x		
bottom-up model of governance	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

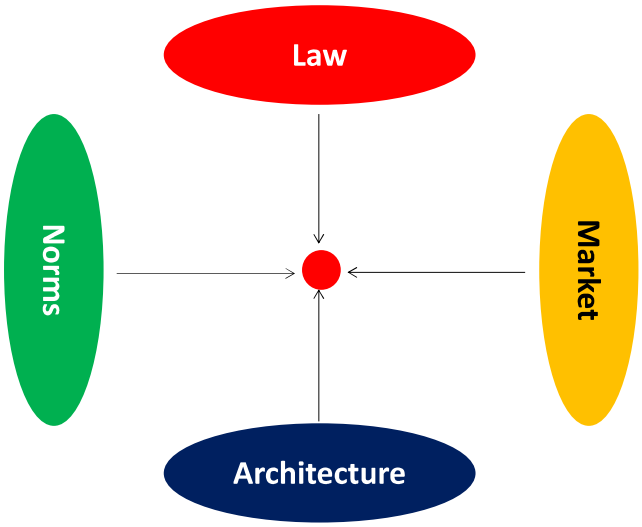
4

Cybersecurity : Other referenced areas of international law

Areas of international law that can be used for reference with regard to protecting the core of the Internet include:	law of the sea
	air law
	space law
	international human rights law
	international telecommunication law
	law of treaties
	international trade law
	antiterrorist laws and policies

5

Pathetic dot theory (New Chicago School theory)

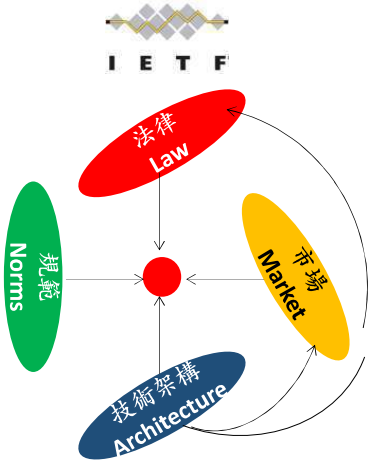


Source: Lawrence Lessig, 1999; illustrated by Dr. Kenny Huang

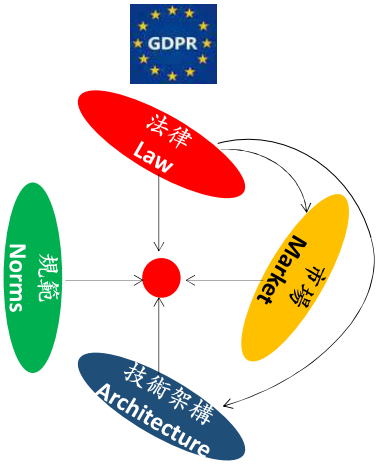
6

網際空間如何被規範? New Chicago School Theory

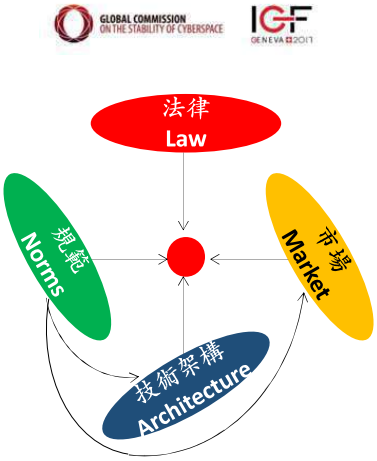
程式碼反映網際空間
Code is Law



法律管制程式碼
Law is Code



規範約束軟體行為
Cyber Norms



資料來源: Lawrence Lessig, 1999; illustrated by Dr. Kenny Huang

Norm: Shared expectations of appropriate behavior
Oxford dictionary

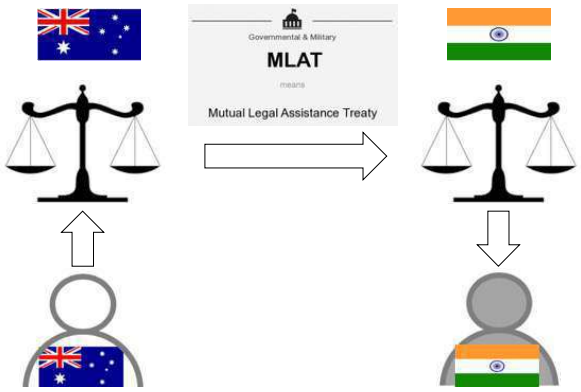
跨境網路犯罪調查案例

澳洲網路犯罪執法人員

發現勒索病毒的解密金鑰可能存放在網路的一台伺服器。
必須在它被刪除前儘速扣押。

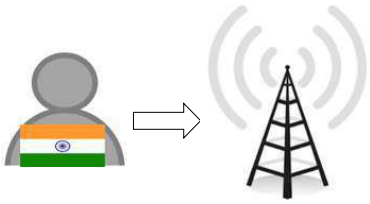
① 檢查網路 WHOIS資料庫，發現此伺服器地點在印度。

```
inetnum:        42.106.0.0 - 42.107.255.255
netname:        VODAFONE-IN
descr:          Vodafone India Ltd.
descr:          Formerly Hutchison Max Telecom Limited
country:        IN
org:            ORG-HMTL1-AP
admin-c:        CH999-AP
tech-c:         IA79-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-IN-HUTCHVAS
mnt-routes:     MAINT-IN-HUTCHVAS
mnt-irt:        IRT-HUTCHVAS-IN
status:         ALLOCATED PORTABLE
```



② 首次啟動司法互助程序(澳洲-印度)

MLAT: Mutual Legal Assistance Treaty

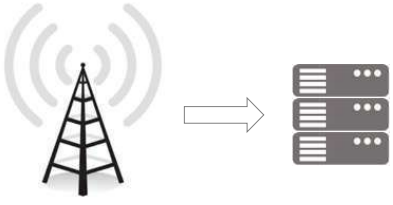


③ 一個月後，印度執法人員至伺服器所在的機房

9

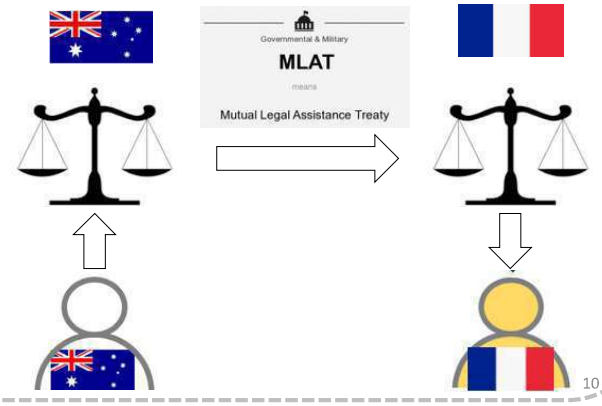
④ 情境 1：印度電信公司拒絕配合，本案無法執行

④ 情境 2：印度電信公司同意配合

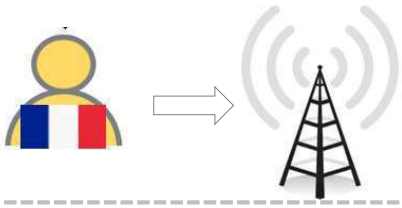


發現本伺服器為跳板，前一站伺服器位置在法國

⑤ 啟動第二次司法互助程序(澳洲-法國)



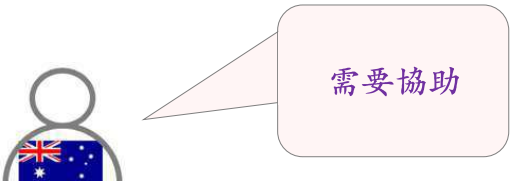
10



⑥ 一個月後，法國執法人員至伺服器所在機房

⑦ 為時已晚 !!
解密金鑰已經刪除

11



Question ?

✓ 如何確認IP位址是合法的IP持有者所發送
✓ 網路資訊中心註冊資訊可更有效反映IP位址所在區域或國家

制定網際網路政策 Internet Policy

✓ 網路服務提供者ISP發放的IP位址與IP持有機構可以完整記錄到 WHOIS資料庫
✓ 無揭露使用者個資，僅提供 IP 區塊持有機構聯繫資訊

12

不實廣告

Domain

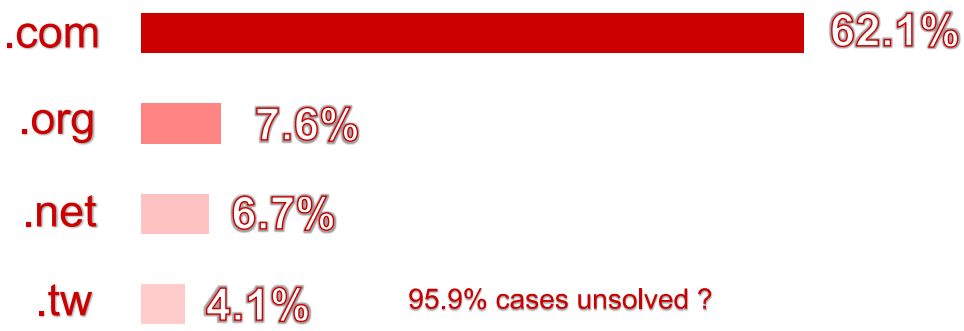
scam associated with a domain name

URL

scam associated with an URL hosted by platform providers

13

網路犯罪頂級域名統計



資料來源: CIB, 2020 Jan-Aug

14

SCIENTIFIC AMERICAN 175

Subscribe

SHARE

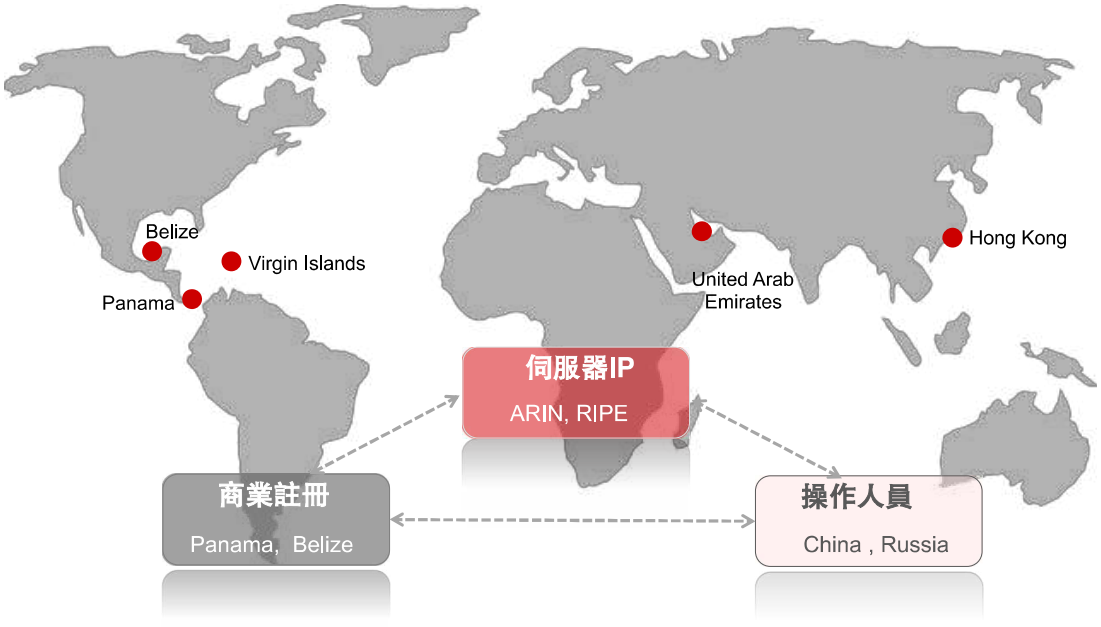
Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers

Sony, Google, RSA and now Citigroup are just some of the prominent victims of cyber attacks as defenses at large organizations prove porous and attackers elude detection

.. invasive attacks on a much regular basis, but IP address unknown

15

網路犯罪： 多層斷鏈



16

IP address and jurisdiction

IP address

(Physical location)

→

Cyber attribution

(Determining the actor responsible for a cyberattack)

Jurisdiction

(By Court)

→

No Jurisdiction,
No authority,
No Law enforcement

17

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

18

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

19

法律原則與執行工具

不告不理原則

§刑事訴訟法 268：
法院不得就未經起訴的案件進行審判

無罪推定原則

§刑事訴訟法 154：
未經審判證明有罪前，推定其為無罪

法院命令

扣押命令

行政處分

§兒少法46
§動防條例 38-3

20

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

21

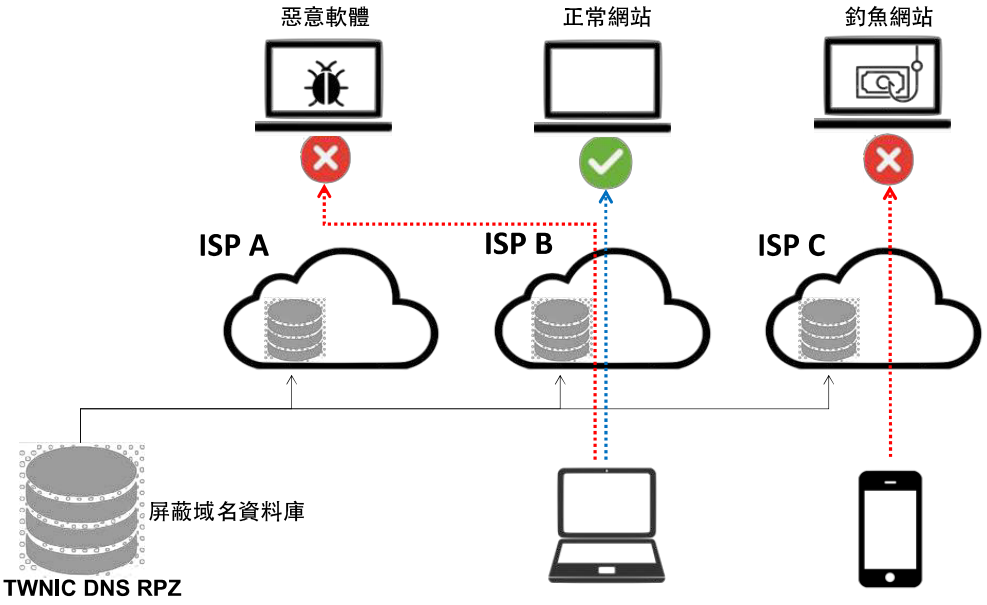
域外效力：限制網路內容接取

- 法律依據：現有具限制網路內容接取法律
  - 兒少法46條 (衛福部)
  - 動物傳染病管制條例38-3條 (農委會)
- 限制接取、瀏覽及移除不當網路內容 範例
  - 網路違法內容經目的事業主管機關公告者，網路平台提供者、應用服務提供者、電信業者應限制內容接取、瀏覽或移除相關網路內容
- 依行政程序法執行域名沒入處份
  - 沒入處份應以域名註冊人為相對人，以書面送達或其他適當方法使其知悉才能發生效力。
  - 提供沒入處份網頁讓社會大眾與註冊人知悉法律依據及原因。

22

TWNIC RPZ 屏蔽技術

回應政策域 RPZ (Response Policy Zone)

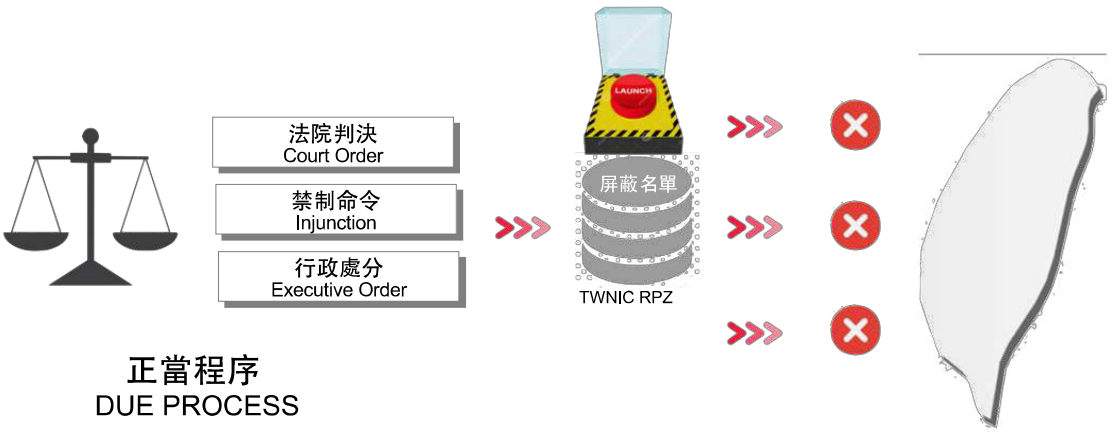


資料來源：黃勝雄博士

23

TWNIC RPZ 政策機制

回應政策域 RPZ (Response Policy Zone)



正當程序
DUE PROCESS

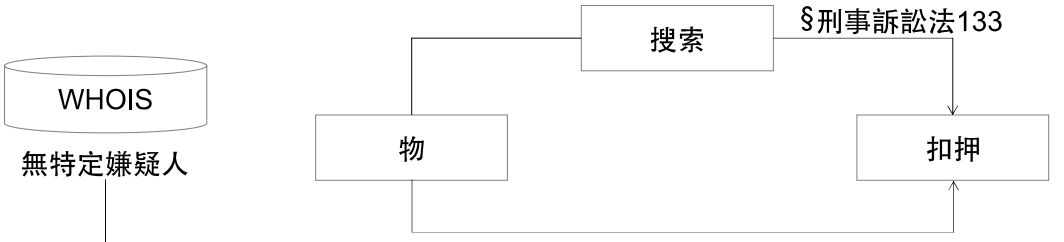
24

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

25

未來方向1： 虛擬資源扣押



Domain/IP 非附隨於搜索之扣押命令
§刑事訴訟法133-2　　應扣押之物: 網域名稱 / IP 位址

Domain / IP 單獨宣告沒收程序
§刑事訴訟法455-34

原則：經法院裁定
例外：
1. 證據扣押
2. 同意扣押
3. 緊急扣押

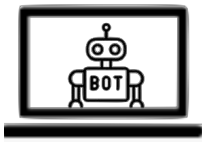
*沒入與扣押為實質控制其使用、阻礙其原本使用

26

情況(二)案件之聲請要件: 四種資安事由且影響資安情節重大

Malware

惡意軟體



Botnets

殭屍網路

Phishing

網路釣魚

Pharming

網址嫁接

	四種資安事由
1	**惡意軟體**：指未經使用者同意安裝於裝置上，妨害裝置運作，收集敏感資訊或取得進入個人電腦系統管道的惡意軟體。惡意軟體包括病毒、間諜軟體，勒索軟體及其他垃圾軟體。
2	**殭屍網路**：指受到惡意軟體感染，並受遠端管理員控制而執行活動的複數殭屍電腦，經由連接網際網路組合而成之網絡。
3	**網路釣魚**：指攻擊者透過發送詐欺性或外觀相似的電子郵件，或引誘終端使用者至冒充的網站，進而誘使受害者揭露個人、企業或財務上的敏感資訊（例如：帳戶號碼、登入帳號及密碼）。部分網路釣魚活動是以誘使使用者安裝惡意軟體為目的。
4	**網址嫁接**：指透過域名系統劫持或域名系統中毒的方法，將不知情使用者的連線轉接至詐欺網站或服務。域名系統劫持指攻擊者利用惡意軟體將受害者的連線轉接至攻擊者的網頁而非受害者原先要求的網頁。域名系統中毒將導致域名系統伺服器對帶有惡意代碼之錯誤IP位址作出回應。網絡釣魚與網址嫁接不同之處在於：前者是引誘使用者輸入個人資訊，後者則涉及域名系統的修改。

27

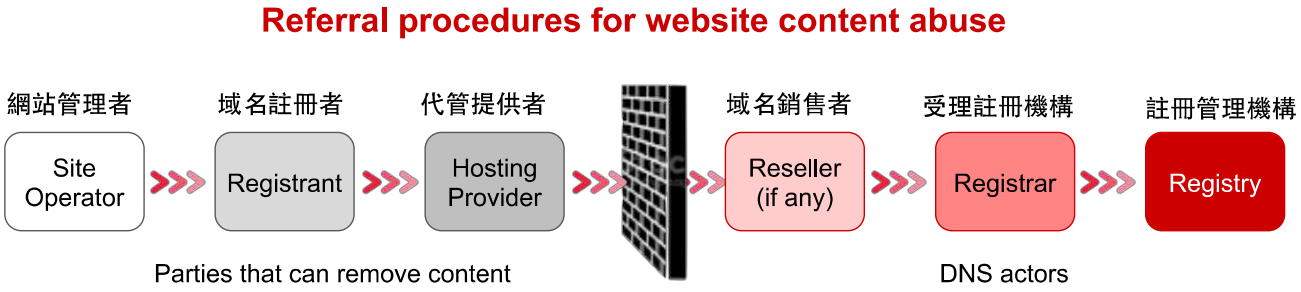
情況(二)案件之聲請人要件：成為信任夥伴

信任夥伴要件

1	是否為合法成立之機構、或政府機關?
2	資安是否為其業務範圍?
3	是否為在資安問題處理上具有公信力之機構或機關?
4	判定網域名稱有資安問題前，是否經過確實調查程序?
5	判定網域名稱有資安問題前，是否有一定內部流程審核確認以遵守調查程序?
6	是否曾因判定網域名稱有資安問題引起爭議?

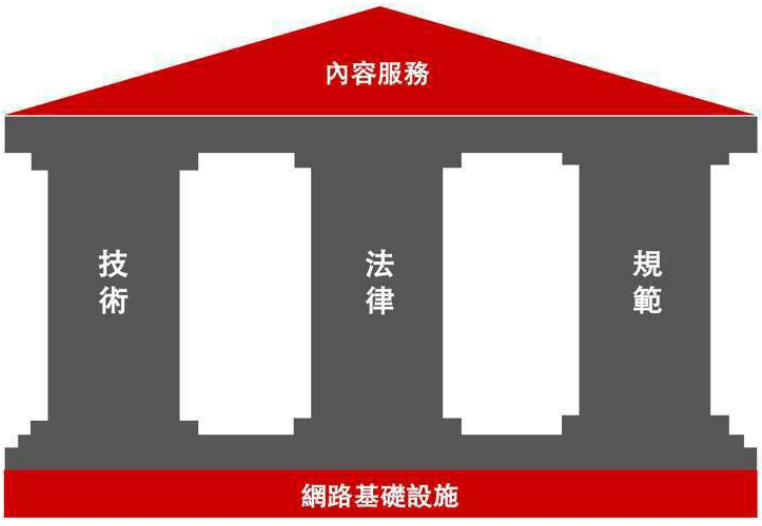
28

未來方向2：不當內容處置轉介程序制度化



29

未來方向3：多軌並進提升治理框架效能



30

域名濫用治理框架 DNS Abuse Framework

Technical Regime
.TW DNS query : 1.7T queries =>1.2T abuse queries
TWCERT : 200K cases / month

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			網路管轄權
技術 1 malware 2 botnet 3 phishing 4 pharming	**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 法院命令 2 扣押命令 3 行政命令	**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

31

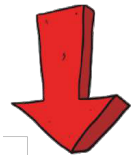
防制網路犯罪努力方向 Way Forward

Criminals

Access to ***21th century technology*** at a very low to no cost

Law enforcement

Saddled with ***19th century law*** with ***20th century technology***



Both technological tools and legal tools have to be updated for polices and national security agencies to keep us safe in this context

32

地緣政治與網路分裂

乾淨網路

THE Clean NETWORK

Clean CARRIER | Clean APPS | Clean STORE
Clean CLOUD | Clean CABLE | Clean PATH

多方利害關係人模式
Multistakeholder Model

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

新IP

INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2017-2020

TSAG-C83
TSAG
Original: English

Question(s): N/A
Geneva, 23-27 September 2019

CONTRIBUTION

Source: Huawei Technologies Co. Ltd. (China), China Mobile Communications Corporation, China Unicom, Ministry of Industry and Information Technology (MIIT)

Title: "New IP, Shaping Future Network": Propose to initiate the discussion of strategy transformation for ITU-T

網路主權模式
Cyber Sovereignty Model

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

33

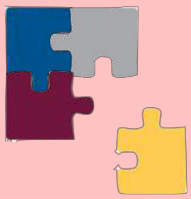
網路治理模式

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
- 聯合國網路專家組 UN GGE

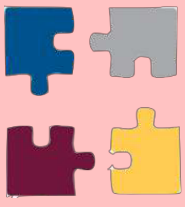
有限介入模式
Limited intervention

- 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



34

集體行動問題 collective action problem

- 所有人希望網路更安全
- 建構安全網路成本高，受益者眾多(非競爭/非排他)
- 每個人認為他人會解決安全問題，自己無需參與
- 所有人如此思考，難以實現網路安全

	排他性 Excludable	非排他性 Non-Excludable
競爭 Rival	私有財 Private Goods 冰淇淋、汽車	公共資源 Common Resources 乾淨水資源、魚類
非競爭 Non-Rival	團體財 Club Goods 有線電視、行動網路	公共財 Public Goods 國家安全、網路安全

35

網際規範主要場域

國際政府機構
International Governmental Organizations

雙邊/多邊協定
Bilateral/Multilateral Agreements

非政府機構/團體
Non-governmental Organizations & Advocacy Groups

技術標準政策機構
ICANN/RIRs/IETF

36

Zeljka Zorz, Managing Editor
May 10, 2016

Share this article

DARPA calls for help to improve cyber attack attribution

9th annual (ISC)2 Security Congress in Orlando, FL – Trainings, Keynotes and More!

Reliable cyber attack attribution is currently almost impossible, and the Defense Advanced Research Projects Agency (DARPA) wants to find a solution for that problem.

37

Why Cyber Attribution matters

- 自衛權
  - 聯合國憲章51條：國家遭受武力攻擊，享有自衛權
  - 塔林手冊13條：國家遭受等同武力程度之網路攻擊，可行使自衛權，包含武力或網路反制措施
- 先發制人
  - 塔林手冊15條：一國存在對他國具實施武裝攻擊的意圖或機會，受威脅國家可採「先發制人」主動發動預防性攻擊措施，包含武力或網路攻擊。
  - 塔林手冊9條:一國遭受他國網路攻擊，可對責任國採等比例反制措施。
- Cyber Operations
  - 塔林手冊13條：觀察敵國攻擊成員組成是個人單獨事件、或為具規模網路行動，若為後者視為集合式武力攻擊
  - 塔林手冊29條: 發動攻擊行動者不易界定軍人或平民，平民若參與敵對網路攻擊行動則視同交戰團體，喪失受攻擊之保護。
  - 塔林手冊9、15條：國家並非受攻擊後才可採取行動，國家有權利採取「緊急反制措施」，在受到傷害前實施「先發制人」權利。

Forbes

243,833 views | May 6, 2019, 03:08am

Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First

Kate O'Flaherty Contributor
Cybersecurity
I'm a freelance cyber security journalist.

38

39

附錄 4. APrIGF 2021 線上參與摘要報告

國家通訊傳播委員會
「網路治理國際議題觀測與人才培育」
委託研究採購案

APrIGF 2021 線上參與摘要報告

報告人：2021 網路治理研習營優秀學員
（林○德、陳○耀、湯○樺、楊○楷、蔡○安）

中華民國 110 年 10 月 22 日

目　錄

圖目錄

一、 會議資訊

2021 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 27 至 30 日在尼泊爾加德滿並同步以線上方式舉辦。APrIGF 2021 的大會主題為「邁向包容、永續及可信賴的網路」(Towards an Inclusive, Sustainable, and Trusted Internet)，討論主題即如同年度大會主題所列，包括：包容、永續，以及信賴共 3 類，簡述如下：

- 包容（Inclusion）

「包容」是為了促進網路的近用與公平所規劃採取的行動，不僅包括網路的接取，同時也涵蓋使用網路的技能。「包容」也涉及多方利害關係人的參與，以確保在多方利害關係治理模式的決策過程中，所有聲音都能得到平等的對待。亞太地區固有的多樣性及險峻的地理環境，對於確保所有人的數位連接帶來艱鉅的挑戰。利害關係人應當如何共同努力，確保任何人皆能使用可靠且負擔得起的網路？APrIGF 鼓勵各界針對這項關鍵問題展開多學門的討論。

- 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。

- 信賴（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的觀點，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、 參加場次

日期	UTC 時間	臺灣時間	撰寫摘要	議程主題
27 Sep (Mon)	04:00 – 07:00 (3 hours)	12:00 – 15:00 (3 hours)	自由參加	Capacity Building Program for Fellows and Newcomers
28 Sep (Tue)	04:00 – 05:30 (90 mins)	12:00 – 13:30 (90 mins)	湯○樺	Opening Plenary
	07:50 – 08:50 (60 mins)	15:50 – 16:50 (60 mins)	楊○楷	【S2】Don’t shoot the messenger, intermediary liability principles under threat
29 Sep (Wed)	03:00 – 04:00 (60 mins)	11:00 – 12:00 (60 mins)	陳○耀	【S5】Why open and interoperable Internet infrastructure is key to the Internet’s continued success
	03:00 – 04:00 (60 mins)	11:00 – 12:00 (60 mins)	蔡○安	【S8】Building digital information literacy skills for trust and well-being
	06:30 – 07:30 (60 mins)	14:30 – 15:30 (60 mins)	林○德	【S6】Citizen-Centered Approach on Tackling Hate Speech, Hindering State Authoritarianism and Algorithmic Censorship of Tech Platforms
	07:50 – 08:50 (60 mins)	15:50 – 16:50 (60 mins)	湯○樺	【S9】More than wor(l)ds : Can AI effectively monitor online harms?
30 Sep (Thu)	03:00 – 04:00 (60 mins)	11:00 – 12:00 (60 mins)	林○德	【S7】Internet Rules: Judicial and Regulatory developments impacts digital rights in Asia
	03:00 – 04:00 (60 mins)	11:00 – 12:00 (60 mins)	陳○耀	【S14】Human rights impact of Covid-19 technologies and the role of businesses
	06:30 – 07:30 (60 mins)	14:30 – 15:30 (60 mins)	蔡○安	Special Session by UN IGF DC-ISSS: A workplan for greater online security and safety
	07:50 – 09:20	15:50 – 17:20	楊○楷	Closing Plenary

日期	UTC 時間	臺灣時間	撰寫摘要	議程主題
	(90 mins)	(90 mins)		

三、 場次摘要

（一）開幕會議：COVID-19—以網際網路為命脈

會議名稱	開幕會議：COVID-19—以網際網路為命脈 Opening Plenary : COVID-19: Internet as a Lifeline
會議時間（UTC）	2021 年 9 月 28 日 04:00－05:30

摘要：

開幕儀式由網路治理研究所（Internet Governance Institute，IGI）的創辦人暨執行長 Babu Ram Aryal 擔任主持人，首先主持人針對 APrIGF 這個活動進行簡單扼要的介紹，過程中我們可以看見有手語老師在現場協助翻譯，以提供聾啞人士能夠一起參與這場會議，畫面不僅溫馨感人，也體現了 APrIGF 對每個人的尊重及包容性。在場參與的人士無不戴著口罩，在這嚴峻的疫情環境下，每個人也都做好防疫的措施，眼前所見的情形正是目前全球所面臨的危機，也正是開幕會議所要探討的議題。

今年的 APrIGF 活動是在尼泊爾的首都加德滿都舉行，在開幕儀式開始時，我們可以聽到會議中播放著尼泊爾的國歌，名為〈唯一百花盛開的國度〉的歌曲，相當的悅耳動聽，想必尼泊爾人對自己的國家應該是有滿滿的愛，緊接著也帶來尼泊爾當地的民俗舞蹈，女孩身上穿的服飾讓我聯想到我們臺灣的原住民，而舞蹈背後播放的音樂感覺跟泰國的音樂很類似，我想或許是因為地緣關係，導致他們的文化都有互相影響，才會具有相似的元素。

接續則是由一名年紀相當小的女孩帶來歌唱表演，雖然過程中聽不懂她在唱什麼，但伴隨著吉他的配樂以及小女孩融入感情的歌聲，讓人不自覺的陷入其中。最後則是雙人舞蹈表演，搭配宗教意味濃厚的音樂，有點像是臺灣官廟文化上會看到的表演，所以顯得別具親切感。在這歷時將近半小時的表演中，讓我們不禁體會到 APrIGF 本身不僅是一場與網路相關的會議，它也代表著不同國家之間文化上的交流，這一切也在主持人的宣告下正式展開序幕。

開幕會議由來自尼泊爾通訊及資訊技術部的秘書 Baikuntha Aryal 博士擔任首席嘉賓，另邀請到 DotAsia 的執行長 Edmon Chung、代表 yIGF 出席的 Bea Soriano Guevarra、網際網路協會（Internet Society，ISOC）的亞太區副總 Rajnesh Singh、聯合國 IGF 秘書處主任 Chengetai Masango，以及 IGI 的主席 Manohar Kumar Bhattarai 共同參與。

開幕會議的議題主要圍繞著 COVID-19 進行討論，全球受到 COVID-19 影響將近兩年的時間裡，它是如何改變人類的生活型態？在這個過程中，網路扮演什麼樣的角色？以及面臨什麼樣的挑戰？抑或是其中隱藏著其他機會的崛起？

COVID-19 的危機造成許多國家經歷了封城，人們無法像以往自由的出門活動，所以大多數人都待在家中透過網路來進行各種活動，這也促使許多社群推動加快網路的速度，以及多數在家工作者，必須透過一些 App 來進行線上會議，因為這些需求的增加，迫使該技術大幅成長，各大公司無所不用其極的想透過這些技術來取得先機獲利。

在使用這些軟技術的過程中，我們也會關注到有些地區，他們的基礎建設相對較為落後，因此這對他們來說將會是一項挑戰。或許正是因為 COVID-19 造就的環境，讓他們不得不開始正視這個問題，但在解決此類技術相關的問題時，也會需要具備相對應的人才，因此會出現人才短缺的問題，在這過程中，我們必須集結各領域的專家，一起針對問題提出好的解決方案，並且讓大眾了解到加強亞太地區網路安全及彈性所帶來的好處，以及培養良好的網路素養，讓網路世界的未來能夠更加健康完善。

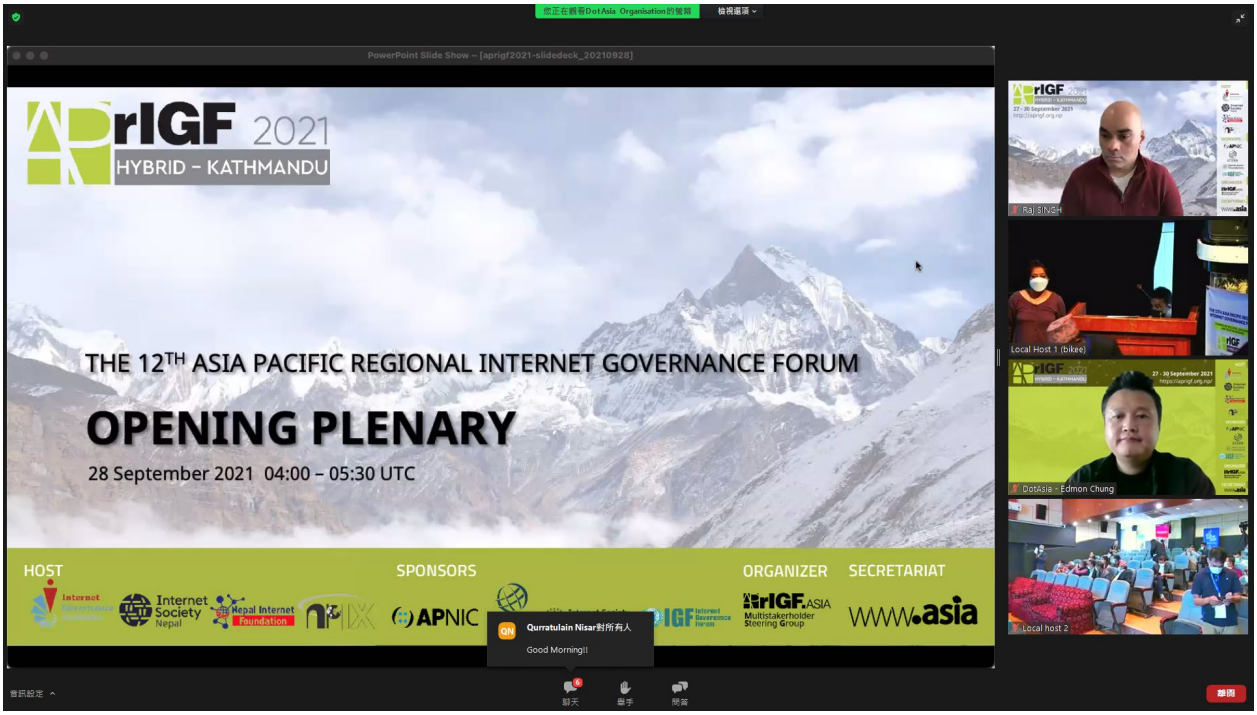

PowerPoint Slide Show – [aprigf2021-slidedeck_20210928]
APrIGF 2021
HYBRID – KATHMANDU
THE 12TH ASIA PACIFIC REGIONAL INTERNET GOVERNANCE FORUM
OPENING PLENARY
28 September 2021 04:00 – 05:30 UTC
HOST
SPONSORS
ORGANIZER
SECRETARIAT
APNIC
Qurratulain Nisar對所有人
Good Morning!!
Raj SINGH
Local Host 1 (bikke)
DotAsia - Edmon Chung
Local host 2

圖1. 開幕會議畫面截圖

（二）【S2】受威脅的網路中介責任原則

會議名稱	【S2】受威脅的網路中介責任原則 【S2】Don’t shoot the messenger, intermediary liability principles under threat
會議時間（UTC）	2021 年 9 月 28 日 07:50 – 08:50

摘要：

本會議主持人為國際人權組織 Article 19 亞洲數位專案經理 Michael Caster，Caster 首先說明網路中介者（intermediary，以下簡稱中介者）主要可分為四類：第一是最基礎的網路服務供應商（internet service providers，ISP），第二是提供網站的公司，第三是社群媒體平臺，第四是搜尋引擎。接著 Caster 提到規範中介者法律責任的政策——馬尼拉原則（Manila Principles），以及責任的形式（例如：notice and take down）。

第一位與談人是印度「網路自由基金會」的特邀律師 Vrinda Bhandari，其分享印度的相關經驗。印度主要是依據安全港（Safe Harbor）模式，但在 2011 年制定了《資訊技術法》（Information Technology Act），此項規定要求中介者主動移除不當言論，已超出原先 notice and take down 要求的範圍，若是受法律、政府要求，甚至應在 3 天（72 小時）內移除言論。使用者可以依據這些規定，要求中介者移除不當言論，且中介者應有效回應其要求。此外，該法亦要求中介者應有相關的專責機構，處理此類爭議。

第二位與談人是印尼「東南亞言論自由網路」（SAFEnet）的執行長 Damar Juniarto。Juniarto 提到，印尼政府在 2021 年因為 COVID-19 疫情而制定了新的管制法律，重點包括：搜尋引擎、社群媒體、網站等中介者，若未在政府規定下向政府註冊，即可能被封鎖；可能要求中介者限制、刪除特定違法的言論；要求中介者在 24 小時內移除違反印尼法律的內容，若未依此行動，政府可以要求 ISP 擋掉中介者。印尼政府的這些要求，可能對網路上的言論造成寒蟬效應。

第三位與談人是馬來西亞網路新聞媒體「當今大馬」（Malaysiakini）的執行

長暨聯合創辦人 Premesh Chandran。Chandran 表示，該平臺依守則禁止發表特定言論（例如：種族歧視），在 COVID-19 疫情期間，用戶於平臺上發表評論批評司法運作，政府認為平臺應為這些言論負責。然而，平臺並不具審核言論之責任，講者認為，這將會過度加重平臺的負擔，也使平臺變成實質的發布者（publisher），於是對此提起訴訟，目前雖然敗訴，但希望後續可以上訴到最高法院，並主張這些加諸平臺的義務侵害使用者的言論自由。

最後一位與談人是韓國高麗大學法學教授，同時身為非政府組織 OpenNet 執行長的 Kyungsin Park，其主要分享亞洲以外的管制中介者經驗。Park 首先介紹歐盟在 2000 年實施的《電子商務指令》（Directive on electronic commerce），其中提到中介者不應被要求為其未意識到的內容（not aware of）負責；也不應要求中介者進行一般性的監控（monitoring）；notice and take down 是選項而不是強制，否則可能造成過於嚴格的中介責任。

Park 將德國的《網路執行法》（Network Enforcement Act，NetzDG）視為歐盟管制框架中，對中介者要求更嚴格的移除責任的例子。依據 NetzDG，平臺應在一定時間內移除違反德國法律的言論。Park 批評 NetzDG 的定義過於模糊，容易使平臺有不透明、非正當程序的審查制度，以致於過度實施管制，影響言論自由；然而，NetzDG 亦獲得菲律賓、馬來西亞、越南、新加坡等亞洲國家的迴響。

最末，Park 建議回歸美國《通信端正法》（Communications Decency Act，CDA）第 230 條，對平臺採取較為寬鬆的要求，而不是強迫平臺控制言論。


台灣大哥大 4G
15:50
100%
Zoom
離開
REC
LIVE
已啟用即時轉錄文字（字幕）
誰能夠看到此轉錄文字？
and I guess it's time for
解除靜音
停止視訊
分享內容
18
與會者
更多

圖2. S2 場次畫面截圖

（三）【S5】開放且可交互運作的網路基礎建設為何是網路持續成功的關鍵？

會議名稱	【S5】開放且可交互運作的網路基礎建設為何是網路持續成功的關鍵？ 【S5】Why open and interoperable Internet infrastructure is key to the Internet's continued success
會議時間（UTC）	2021 年 9 月 29 日 03:00 – 04:00

摘要：

這場座談共由 5 名講者參與，開場由主持人，網際網路協會（Internet Society，ISOC）的政策與宣傳資深經理 Adrian Wan 介紹目前的網路狀態，平鋪直敘的介紹內容，相當適合網路治理與網路協議的初學者聆聽。

第二位講者是香港 Tech for Good Asia 的創辦人兼董事 Charles Mok，與第一位講者不同的是，他特別提到了政府以及科技巨頭在這方面的角色。

第三位講者是來自臺灣的陳映竹（YingChu Chen），她特別提到了區塊鏈，並認為區塊鏈目前發展的方向可能不太對，期待後面會有更好的發展。

第四位講者是來自「亞太網路資訊中心」（APNIC）的高級研發官 George Michaelson，他以技術的角度告訴我們網路成功的因素在於沙漏頸的 IP（網際網路分層模型又稱之爲「沙漏模型」，IP 位在模型中央的沙漏頸部），並且提醒我們關於網路治理的政策應該要從對應的層次下手，不能所有問題都從 IP 層開始解決。

第五位講者是來自孟加拉，現為泰國亞洲理工學院（Asian Institute of Technology，AIT）博士後研究生的 Pavel Farhan，他在投影片中提出了 7 點「開放且可交互運作的網路基礎建設原則」，分別是：人權必須被保護及推廣、倡導解決網際網路碎片化根本原因的措施、促進合作以提升網路安全及信任、主動保護以及支援全球資訊的自由、鼓勵採取措施以提高網路可用性、承諾維護及加強多方利害關係人治理模式，以及鼓勵網路開放去中心化以及互聯特質，另外是提

到在開發中國家的網路可存取性的問題。

接著 Wan 開放兩個問題，第一個提到關於中心化網路的缺點，Wan 回應這樣可能速度會比較慢，而且會有隱私及安全的問題。

第二個問題是關於孟加拉民眾對於網路近用能力的擔憂。首先由同樣來自孟加拉的 Pavel 回答，他提到沒有辦法一夜之間就教會大家怎麼使用網路，但是目前還沒有明確的答案來回答這個問題。我國講者陳映竹的答案則十分具體，她建議從教育民眾網路可以如何改善他們的生活來著手，例如：取得更好的工作、增加收入或是取得娛樂等，首要是找到當地民眾的主要需求。

圖3. S5 場次畫面截圖

（四）【S8】為社會信任建立數位資訊識讀能力

會議名稱	【S8】為社會信任建立數位資訊識讀能力 【S8】Building digital information literacy skills for trust and well-being
會議時間（UTC）	2021 年 9 月 29 日 03:00 – 04:00

摘要：

本場次由「國際圖書館協會聯合會」（International Federation of Library Associations and Institutions，IFLA）亞太地區委員會的 Winston Roberts 擔任主持人，邀請澳洲「昆士蘭州立圖書館」（State Library of Queensland）執行長 Louise Denoon、「尼泊爾圖書館協會」（Nepal Library Association）主席 Gita Thapa、「新加坡國家圖書館」（National Library Board of Singapore）社群參與主管 Sara Pek 擔任與談人，討論如何藉由各國圖書館之力推動國民數位識讀能力。

Denoon 以「圖書館的超能力」作為起頭，表示圖書館是社群裡受信任的友善空間，是資訊交流的場域，在數位時代圖書館員也成為數位資訊工作者（information professionals）。由於數位時代產生了數位資訊落差，澳洲政府每年都會調查與公布「數位包容指數」（Australian Digital Inclusion Index），「包容」程度又可分為三個指標，分別是近用性（Access）、可負擔性（Affordability）及使用能力（Ability），圖書館則是在此三方面都提供公眾幫助（例如：提供免費網路、電腦），尤其是在 Ability 面向，圖書館會協助弱勢族群（例如：老年人）獲取網路資訊，以及使用視訊軟體與家人聯繫，或者錄製保存少數族群的語言。

接著 Thapa 介紹尼泊爾所推動的數位識讀工作。2013 年至 2017 年間，尼泊爾政府教育部推動「資通訊科技（ICT）教育計畫」，其目標包括平等近用教育資源、提升教育品質、降低數位落差等。由於尼泊爾的地形限制，45%國民居住於山區，網路、電信服務的普及與品質都受到限制，各地圖書館也未必有數位資源，因此該計畫便對各地圖書館展開調查並提供資源（包括對圖書館員的訓練），例如：READ（Rural Education and Development）組織協助展開關於使用手機、app、電腦、社群媒體、搜尋引擎、不實訊息、網路安全的教育訓練；TAG（Tech

Age Girls）組織也提供類似教育訓練；Hamro Palo 組織則是提供了「網路安全工具箱」（Online Safety Toolkit）。

Thapa 也分享了網路上對於青少年主要的安全威脅包括：性騷擾、早婚（early marriage）、人口販運及網路霸凌，對此 Internet Watch Foundation Nepal 與其他組織合作，建立了兒少網路危害內容匿名通報機制。除此之外，相關組織也進入校園針對網路安全進行宣講、提高防範意識。最後，Thapa 強調圖書館員與 ICT 專業人員合作的重要性。

Pek 則是介紹新加坡的資訊識讀工作，她表示在資訊爆炸、不斷更新的時代，讓人更容易接收不實訊息、網路威脅，因此人們必須學會新的技能——數位識讀，而圖書館便是作為重要的學習場所。新加坡國家圖書館於 2013 年啟動一項數位識讀計畫「S.U.R.E.」，主要目標是提高公眾關於資訊接受與辨別的意識，S.U.R.E.包括「Source」、「Understand」、「Research」、「Evaluate」四個面向，以區分群眾（在學學生、上班族、老年人／終身學習）的方式提供訓練，希望提升批判思考能力。以在學學生族群為例，國家圖書館與教育部合作，將數位識讀納入課綱中，圖書館員會就數位識讀內容進行宣講，並介紹圖書館的數位資源；國家圖書館也會與其他組織合作，針對上班族舉辦活動，內容包括區辨不實訊息、介紹事實查核工具等。

2020 年，新加坡國家圖書館進行了「新聞報導特展」，展示了歷史報導文章，也設計了讓公眾參與的抓出不實訊息遊戲。在 COVID-19 疫情期間圖書館也針對疫情相關不實訊息對公眾進行宣講、介紹相關資源及事實查核的最佳做法（best practices）。


LIVE
on Otter.ai (click here to open live transcript)
Recording
Live Transcription (Closed Captioning) has been enabled
Who can see this transcript?
PowerPoint Slide Show – [aprigf2021-slidedeck_20210928]
APrIGF 2021
HYBRID – KATHMANDU
29 September 2021 03:00 – 04:00 UTC
S8. BUILDING DIGITAL INFORMATION LITERACY SKILLS FOR TRUST AND WELL-BEING
Moderator
Winston Roberts, IFLA
Speakers
Louise Denoon, State Library of Queensland
Gita Thapa, Nepal Library Association
Sara Pek, National Library Board of Singapore, and IFLA
HOST
SPONSORS
ORGANIZER
SECRETARIAT
Winston Roberts

圖4. S8 場次畫面截圖

（五）【S6】以公民為中心作為方法解決仇恨言論、阻礙國家權威主義及技術平臺演算法的審查制度

會議名稱	【S6】以公民為中心作為方法解決仇恨言論、阻礙國家權威主義及技術平臺演算法的審查制度 【S6】Citizen-Centered Approach on Tackling Hate Speech, Hindering State Authoritarianism and Algorithmic Censorship of Tech Platforms
會議時間（UTC）	2021 年 9 月 29 日 06:30 – 07:30

摘要：

該場次由人權律師 Gayatri Khandhadai 代表 APC（Association for Progressive Communications）開場，談論仇恨言論目前在印度遇到的問題。Khandhadai 從青少年遇到的網路仇恨言論可能會造成身分認同的困難開始說起，雖已有相關法規制定，但 COVID-19 之下，這兩年當地的宗教歧視言論以及社區暴力成長趨勢劇烈，而相關平臺 Facebook 卻未對此進行任何措施，因此 APC 寄信到 Facebook，公開並且強調該議題的嚴重性。Gayatri Khandhadai 並在該節結尾強調，未來使用相關科技包含 AI、數位平臺等，皆應更重視相關議題。

印尼事實查核中心 Mafindo 的聯合創辦人 Harry Sufehmi 以《如何建立一個事實審核的社群》作為分享主題。身為一名工程師，Sufehmi 在 2012 年觀察到社群媒體上的仇恨言論，因此建立了 Mafido 事實查核演算法，Mafido 有著容易加入以及包容多元的特性，傳遞出對該議題積極關注的態度，也建立清楚的制度。目前 Mafido 已有來自 17 個城市的 9 萬多名成員，並與政府、國際組織、學術及各社群合作，期許未來可以依靠該演算法的運作，矯正不實訊息及仇恨言論。

最後一名分享者是 Nest Centre for Journalism 的 Dulamkhorloo Baata，他以《論蒙古誤傳／不實訊息現狀—蒙古事實查核中心的學習與觀察》作為分享主題。身為一名記者，他合作創立了 Nest 中心及 NGO 蒙古事實查核中心（Mongolian Fact Checking Center，MFCC），並指出幾個關鍵趨勢包含：

1. 網路的不實訊息會隨著選舉期間增加。

2. 網路的不實訊息其目的在於將重要議題從大眾中消失／忽略。

3. 仇恨言論大多針對女性。

Baata 也分享，從 2020 年 COVID-19 爆發之後，警察總署及通訊管理委員會聯合制定相關條文，禁止網路媒體傳播未經證實消息，並警告了約 290 個網站以及關閉了 134 個網站。

MFCC 目前致力於培養相關的人才，並邀請大眾舉報、辨認錯誤訊息，該組織期望可以成為蒙古第一個臉書的 TPFC（Third-Party Fact-Checking），致力於加註標記，使民眾辨識不實訊息。

提問者詢問：誰決定這叫做錯誤訊息？誰有權力編輯那些程式碼？關於這兩個問題，Baata 表示他們 MFCC 是有被全球認可負責蒙古區域審查的單位，而他們自己更會跟進確認訊息是否真實。

至於為什麼覺得女性更適合加入這個領域？Sufehmi 表示，因為男性多半是家庭的收入來源，因此女性有更多的自由可以進行事實查核。Baata 則表示，目前 MFCC 是一個全女性的組織，她認為事實查核需要具備耐心的特質，而女性有這樣的特性可以去肩負這個任務。Khandhadai 則回應，女性適合是因為我們就身處在這樣的環境中，不論是從家庭亦或是學校，這些仇恨言論就在身邊，而作為被攻擊的對象，因為我們可以看得到，所以更應該也更有資格去出聲對抗它。

最後講者們呼籲面對不實訊息、仇恨言論，應該隨時關注並且勇於起身對抗，我們都希望可以活在一個信任的網路社群，並不需畏懼它對我們的歧視、隱瞞、欺騙，而這需要大家一起看著它，並討論它。

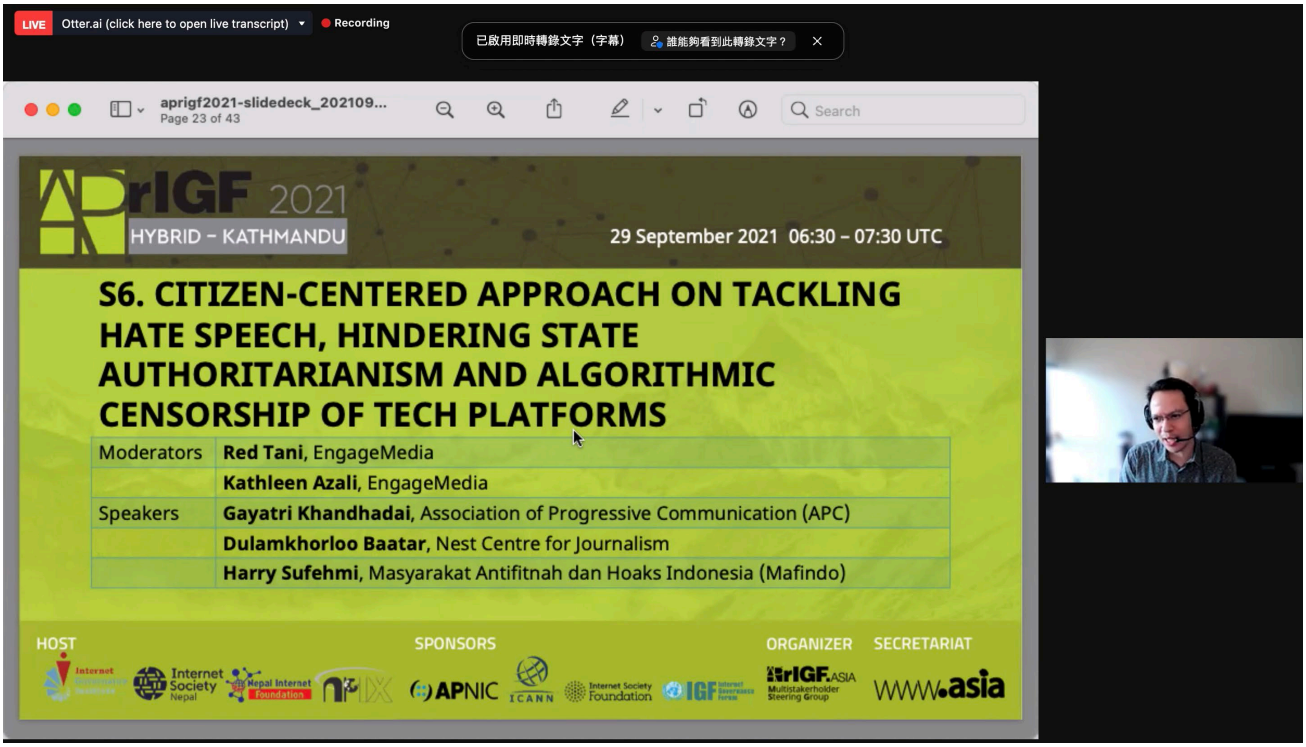

LIVE
Otter.ai (click here to open live transcript)
Recording
已啟用即時轉錄文字（字幕）
誰能夠看到此轉錄文字？
aprigf2021-slidedeck_202109...
Page 23 of 43
Search
APrIGF 2021
HYBRID – KATHMANDU
29 September 2021 06:30 – 07:30 UTC
S6. CITIZEN-CENTERED APPROACH ON TACKLING HATE SPEECH, HINDERING STATE AUTHORITARIANISM AND ALGORITHMIC CENSORSHIP OF TECH PLATFORMS
Moderators
Red Tani, EngageMedia
Kathleen Azali, EngageMedia
Speakers
Gayatri Khandhadai, Association of Progressive Communication (APC)
Dulamkhorloo Baatar, Nest Centre for Journalism
Harry Sufehmi, Masyarakat Antifitnah dan Hoaks Indonesia (Mafindo)
HOST
SPONSORS
ORGANIZER
SECRETARIAT
Internet Society Nepal
Nepal Internet Foundation
APNIC
ICANN
Internet Society Foundation
IGF
APrIGF ASIA
Multistakeholder Steering Group
www.asia

圖5. S6 場次畫面截圖

（六）【S9】AI 能否有效監控網路危害？

會議名稱	【S9】AI 能否有效監控網路危害？ 【S9】More than wor(l)ds : Can AI effectively monitor online harms?
會議時間（UTC）	2021 年 9 月 29 日 07:50 – 08:50

摘要：

此會議由斯里蘭卡致力於事實查核的「Watch Dog」共同創辦人 Safra Anver 擔任主持人，邀請了「哨兵計畫」（The Sentinel Project，防止種族滅絕的國際非政府組織）的專案經理 Saahithiyanan Ganeshanathan 及全球經理 Raashi Saxena，以及來自孟加拉的網站代管公司「EyHost」商業策略及發展主管 Shah Zaidur Rahman 擔任與談人，共同探討 AI 是否能夠有效監控現今的網路危害問題。

近年來 AI 的熱潮已席捲全球，它的技術為世界帶來很大的改變，當前的議題要討論的是，我們能否透過 AI 技術有效監控網路對人類帶來的危害。這個議題涵蓋的層面相當廣泛，現今網際網路早已成為人類生活不可或缺的一部分，人們可以自由的在網路上進行各種行為活動，在網路世界中，難以避免產生一些仇恨言論或是傷害他人的行為，針對這些問題，我們是否能夠有效透過 AI 技術來監控，抑或該怎麼使用 AI 來防止這些行為產生？是本會議主要討論的議題。

首先我們要了解在使用 AI 這項技術前，必須先分析我們要解決的問題，進而訓練 AI 來幫助我們解決遇到的問題。針對網路暴力言論行為的問題，它是相當深層多元的存在，我們必須探討問題所存在的時空背景，以及在不同的文化或地區，都會產生不同的觀感，它所帶來的衝擊讓我們必須與更多方面的專家一起討論與交流，共同建立一套有效監控網路上所帶來的危害。

過程中我們會藉由 AI 技術對資料進行大規模的搜尋、分類以及刪除網路上各種有害的內容，我們希望它能夠相當即時的在訊息傳達至無論是社群、大眾以及個人之前將危害的訊息刪除。這一切聽起來似乎相當完美無瑕，但在實行的過程中，我們仍然需要考量到它的技術中是否有侵犯到人權及倫理的問題，這都是在設計過程中所會面臨到的問題，但相信藉由此會議中集結所有 AI 技術相關人

員、以及人權方面的權威，大家集思廣益共同朝這個目標努力制定出一套完善的系統，一定可以有效監控網路上的各種危害訊息。

我們希望未來大家能夠有一個更良好的網路使用環境，不僅可以透過 AI 的技術監控，達到讓使用者無法濫用來危害他人，也可以保護我們原有的言論自由，共創一個更美好且完整的網路時代。

網路的發展雖然為社會帶來無數好處，徹底改變人與人之間聯繫與交流的方式，但也成為某些人作惡的工具，一旦網路遭到濫用做出危害他人的行為，將對社會造成巨大的傷害，並加劇社會上的緊張情勢，其所導致的後果，小則傷及個人至群體，大則損害國家甚至全球。

網路上的仇恨亦會蔓延至現實世界的暴力行為，在這過程中我們必須讓參與者了解到網路上的危害具有相當大的複雜性，很難去定義它的存在，因此光靠 AI 的技術解決會有一定的侷限，卻也充滿無限的可能，這也是為何講者們如此積極與各相關領域的專家共同討論這個議題，希望在制定這套系統前，大家能夠深刻的體會到它對於監測網路上的危害具有極大的影響力，並且也能夠集結各位與會者的想法及意見，反映出對該議題的各種有效解決方案。


LIVE
APrIGF 2021
HYBRID – KATHMANDU
27 - 30 September 2021
http://aprigf.org.np
HOST
Antonio
Safna Anver
Saahithiyanan
Raashi Saxena
.asia
DotAsia - Kelvin
48:06

圖6. S9 場次畫面截圖

（七）【S7】網路規範：司法及監察發展影響亞洲數位權利

會議名稱	【S7】網路規範：司法及監察發展影響亞洲數位權利 【S7】Internet Rules: Judicial and Regulatory developments impacts digital rights in Asia
會議時間（UTC）	2021 年 9 月 30 日 03:00 – 04:00

摘要：

該會議由國際人權組織 Article 19 亞洲數位專案經理 Michael Caster 開場，Caster 觀察到近年 COVID-19 促使政府制定許多規範，雖宣稱是為了要打擊不實訊息，但實際上卻可能成為國家監控或限制人民的手段之一。

言論自由是人民的基本權利，Caster 呼籲國家在限制言論自由時，仍須遵守以下三個原則：

1. 必須有法律規範，並且有精準的執行內容。
2. 以國家安全為由制定規範時，仍須尊重並保護其他權利。
3. 必須有具體實質的內容，且以最小侵害為原則。

來自馬來西亞的 Gayathry Venkiteswaran 是該地區言論自由與媒體權利領域的專家，他首先爬梳了馬來西亞假新聞緊急法令制定的背景，並舉出三個例子來說明該法令引發民眾恐懼，導致只敢在私底下發表言論，無法在大眾面前傳達自己的立場。

來自印度的講者 Apar Gupta 則是一名律師，他參與近年來的網路關閉問題以及資通訊法律訴訟，網路關閉成為政府進行言論監控的手段之一，使得公務人員及新聞媒體等在發表言論時受到嚴密的審查，Gupta 呼籲應重視政策制定過程的透明度。

東南亞言論自由網路（SAFEnet）的執行長 Damar Juniarto 以《將印尼關閉網路告上法庭》為主題，分享 2019 年 9 月印尼政府在非法情況下關閉了西巴布

亞省四個城市的網路通訊服務一事，因此 SAFEnet 與 AJI（Alliance of Independent Journalists）在同年 11 月向雅加達行政法院提起訴訟，但該行動卻沒有趨緩 2021 年更多省份及城市被限制網路使用的狀況。政府宣稱根據 Article 40 的相關法源制定該措施，而請願者則要求宣布該法條違憲，且未來進行任何關閉網路行動前需有詳細的行政命令，目前還有新的威脅包含 Article 13 及 15，Juniarto 邀請參加者持續關注這個議題的發展。

提問者詢問：如何辨別假新聞與不實新聞？Venkiteswaran 回答，這兩個詞彙需要非常小心使用，並注意不同國家有著不同的解釋，依據他的觀點，假新聞嘗試要捕捉所有訊息，包含那些不可信的內容，卻不去定義或理解他怎麼公布出來的；而錯誤訊息則代表，個人經歷了自己的搜尋以及定義，但內容仍舊是錯誤的。Venkiteswaran 覺得後者的發生是一個非常好的學習，因為確立任何立場時，必須事先搜尋相關法律，跟進相關議題，並在討論當中知道這是錯誤的，這是一個可以促進對話的機會。

最後講者皆認為，人民必須持續關注及跟進言論自由與監控的議題，對於如何區分不實以及錯誤言論需要抓緊整個脈絡才有辦法掌握，不可片面相信或使用政府的資訊，也期望人民互相對話，並參考國際人權組織 Article 19 的三個檢驗標準去一一審視這些法條制定的正當性，以促進人權發展。

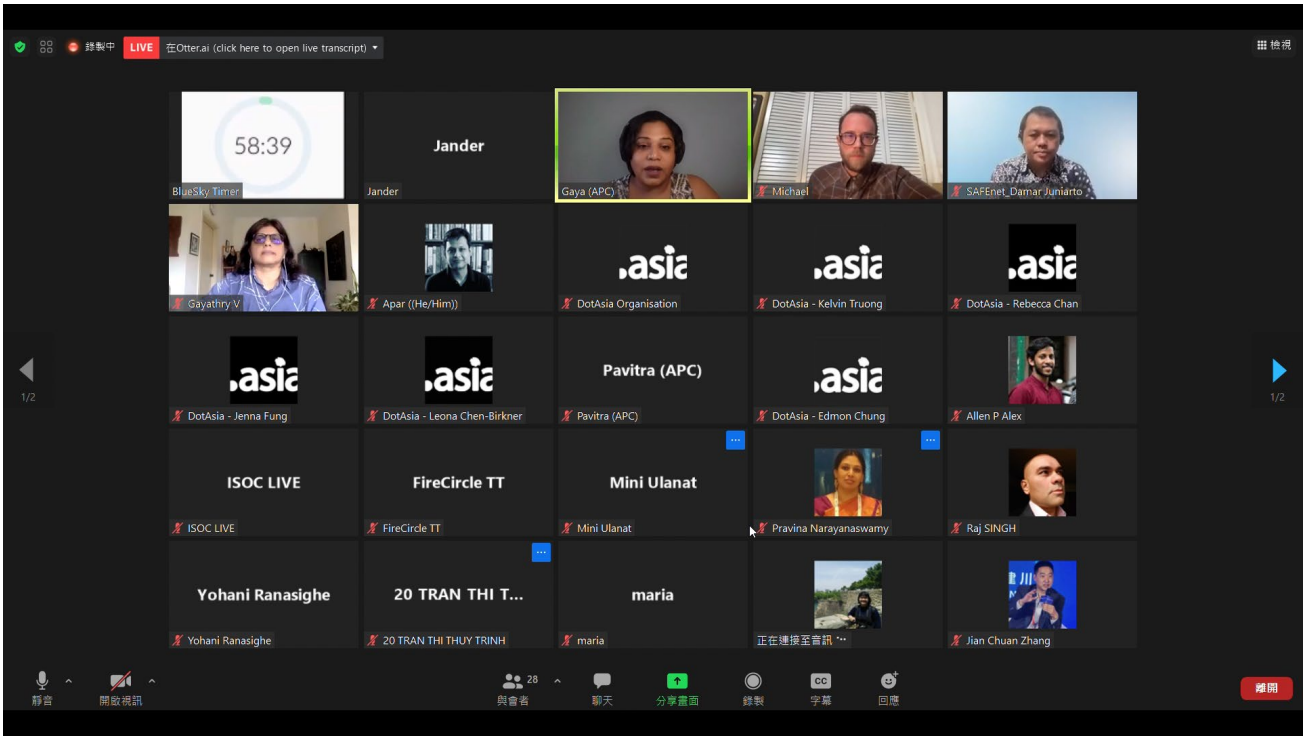

錄製中
LIVE
在Otter.ai (click here to open live transcript)
檢視
58:39
BlueSky Timer
Jander
Jander
Gaya (APC)
Michael
SAFEnet_Damar Juniarto
Gayathry V
Apar ((He/Him))
DotAsia Organisation
DotAsia - Kelvin Truong
DotAsia - Rebecca Chan
DotAsia - Jenna Fung
DotAsia - Leona Chen-Birkner
Pavitra (APC)
Pavitra (APC)
DotAsia - Edmon Chung
Allen P Alex
ISOC LIVE
ISOC LIVE
FireCircle TT
FireCircle TT
Mini Ulanat
Mini Ulanat
Pravina Narayanaswamy
Raj SINGH
Yohani Ranasighe
Yohani Ranasighe
20 TRAN THI T...
20 TRAN THI THUY TRINH
maria
maria
正在連接至音訊
Jian Chuan Zhang
1/2
1/2
靜音
開啟視訊
28
與會者
聊天
分享畫面
錄製
字幕
回應
離開

圖7. S7 場次畫面截圖

（八）【S14】COVID-19 技術對人權的影響與對企業的作用

會議名稱	【S14】COVID-19 技術對人權的影響與對企業的作用 【S14】Human rights impact of Covid-19 technologies and the role of businesses
會議時間（UTC）	2021 年 9 月 30 日 03:00 – 04:00

摘要：

本場次主持人為「人權與商業研究所」（Institute of Human Rights and Business，IHRB）的全球問題高級顧問 Salil Tripathi，前半場次為 Tripathi 與聯合國見解及言論自由權問題特別報告員 Irene Khan 的問答互動，主要是介紹 COVID-19 疫情期間關於不實訊息及言論自由的問題，其中提到了記者因為報導疫情而被政府攻擊的情況。

第二位與談人是澳洲新南威爾斯大學（UNSW Sydney）的法律及資訊系統教授 Graham Greeleaf，他主要從目前澳洲的做法來做說明示範，大致上是從法規面來做解釋。澳洲的做法有類似臺灣的社交距離 APP（應該也是採用 Apple 及 Google 的暴露通知 API），另外是有類似臺灣的資料刪除法規，像是在一定時間後就要刪除、疫情結束後要刪除，以及限制使用目的等。澳洲的做法主要是有一個 COVIDSafe APP，可以用來掃描場所條碼（類似臺北通），但是 COVIDSafe 的 Android 及 iOS 版本有開放原始碼。

第三位與談人是「挪威電信」（Telenor Group）亞洲區的永續發展副總裁 Manisha Dogra，他介紹了馬來西亞政府利用電信業者的手機位置資訊，來整理及分析疫情是如何擴散的。

最後一位與談人是 Rohini Lakshane 顧問，他與主持人同樣來自「人權與商業研究所」，其研究了包括臺灣、中國、新加坡等 11 個國家，是如何利用手機來做居家隔離監控的狀況，以及有部分國家利用攝影機來判斷民眾是否有戴口罩。

圖8. S14 場次畫面截圖

（九）UN IGF DC-ISSS 特別場次：提升網路安全之工作計畫

會議名稱	UN IGF DC-ISSS 特別場次：提升網路安全之工作計畫 Special Session by UN IGF DC-ISSS: A workplan for greater online security and safety
會議時間（UTC）	2021 年 9 月 30 日 06:30 – 07:30

摘要：

本場次由聯合國網路治理論壇（UN IGF）DC-ISSS（Dynamic Coalition on Internet Standards, Security and Safety）計畫資深政策顧問 Mark Carvell 擔任主持人，邀請 DC-ISSS 第一組（Security by Design, Sub-group on IoT）主席 Yuri Kargapolov、DC-ISSS 第二組（Education and Skills）副主席 Janice Richardson，以及 DC-ISSS 第三組（Procurement, Supply Chain Management and the creation of a business case）主席 Mallory Knodel 擔任與談人，討論如何推動網路安全。

本場次先由 DC-ISSS Coordinator Wout de Natris 介紹 DC-ISSS 計畫，其目標是要針對現有關於網路安全的 ICT 標準，規劃執行及落實方案，並建立多方夥伴合作架構，以及減少理論與實踐間的落差。由於對私部門來說，並未有法律強制其採用網路安全標準，因此通常欠缺相關知識及誘因，DC-ISSS 自 2019 年起，希望藉由社群的力量，相互影響創造理解及誘因。DC-ISSS 共分為三個工作小組，分別是「Security by Design, Sub-group on IoT」、「Education and Skills」，以及「Procurement and Supply Chain Management」，其目標為對公部門及私部門政策制定者提出建議、提供相關指引及標準。

第二組副主席 Richardson 接著分享，對現代產業來說，雲端運算、大數據、電子商務、AI、加密技術的需求急劇上升，因此現階段對於員工的重新訓練非常重要，尤其是培養批判思考、抗壓性及應變力、分析及解決問題、樂於學習等能力。因此第二組的目標就是要在學校及工作場所推廣應對數位化變局相關能力，並且希望遊說將網路安全、網路治理等議題納入 ICT 課程。2021 年 7-9 月的工作目標是要擴大諮詢利害關係團體、對相關產業需求進行調查，並對公眾進行問卷

以釐清最佳做法。2021 年 10-12 月則是會進行初步結論建議之撰寫，並於 IGF 2021 會議中發表。

第三組主席 Knodel 分享，第三組的目標是要針對數位科技的採購產出政策建議，之所以著重採購面向，是希望對於業界引發興趣及創造需求，因此企圖在採購訓練課程中納入網路安全及數位產品安全議題。該組希望彙整提出對於全球公私部門，採購過程及供應鏈中有關安全議題的最佳做法及指引，並發展落實執行方案。該組成果會在 2022 或 2023 IGF 會議中呈現。

第一組主席因故未到，因此由主持人 Carvell 代為說明第一組的工作內容。第一組的 Security by Design 主題在諮詢利害關係人後，有鑑於 IoT 對個人生活及產業影響劇烈，該小組決定先著重於此一子議題，目標是要找出現有 IoT 網路安全制度中的落差，並彙整不同安全性通訊協定（protocol）進行比較分析。另外一個與 IoT 有關的主題是身分管理系統（Identification Management）的安全性，希望彙整提出安全及信任機制。Carvell 表示，該組現正進行利害關係人（包括政府、NGO、產業界等）問卷調查，若時程允許，會在 12 月的 2021 IGF 會議中報告初步發現。

圖9. UN IGF DC-ISSS 特別場次畫面截圖

（十）閉幕會議：APrIGF 的多方利害關係人治理模式與多元性

會議名稱	閉幕會議：APrIGF 的多方利害關係人治理模式與多元性 Closing Plenary – Sail, not Drift: Multistakeholderism and Diversity at APrIGF
會議時間（UTC）	2021 年 9 月 30 日 07:50 – 09:20

摘要：

閉幕會議的主持人為人權律師 Gayatri Khandhadai，她同時也是 APrIGF 利害關係人參與委員會的聯合召集人。Khandhadai 表示，APrIGF 的精神為引入不同的專家觀點，希望可以讓更多人參與及提問，共同討論網路治理的議題，增加亞洲地區參與的多樣性（包含性別、種族等）。

在開始討論前，Khandhadai 邀請大家在文字雲程式中輸入自己認為「真正的多方利害關係人治理模式所需要的東西」，並透過大家輸入的字共同組成文字雲圖像，其中最多人輸入的文字會最為明顯。結果顯示，最大的文字是 diversity（多元性）。

來自「亞太網路資訊中心基金會」（APNIC Foundation）的 Sylvia Cadena，分享其參與多方利害關係人治理之經驗。最初會有一份草案文件，經過他人檢視後進行修改，接著各方在圓桌上交換意見，再次討論，最後再產出結案報告。這是一個長期的對話，也建立了一個長期的連結，將企業、公民、非政府組織等不同的參與者連結在一起，最後成為一個網路治理的生態系統。Cadena 鼓勵本次會議的參與者繼續完成自己的報告，並在自己的國家、脈絡下行動、對話，儘量融入更多的多方利害關係人。

來自尼泊爾電信管理局（Telecommunication Authority）的 Ananda Rag Khanal 分享多方利害關係人治理模式在尼泊爾的實踐，當政府要制定政策時，會先經過一番討論，容納多樣的意見，例如提倡管制（或不管制）的相關 NGO 立場，以及經營上可能會受到影響的產業界（industry）立場。公民社會與學術界對於網路治理的參與較不熱絡，產業界則是有時候會加入，值得提醒的是，多方利害關係

人也可能受到國內政府的法律或政策影響。

Khanal 表示，如何將多方利害關係人納入公共領域，也是一大挑戰，關鍵點在以最重要的議題來組織串連、引起不同參與者的興趣，有時多方利害關係人的身分並不代表他的意見，因此我們也要關注真正不同的「意見」，如果總是由同一批人提出相同的見解，這樣就稱不上是多方利害關係人治理模式了。此外，多方利害關係人治理模式指的是多樣參與，輸入意見後進入決策程序，若無真正的「決策」，光是討論的話其實並不完整。

接著，主持人 Khandhadai 與現場的專家展開問答。

問：對於 APrIGF 有什麼期待？想要看到什麼樣的 APrIGF？

答：繼續強化多樣參與，例如公民社會可以有很多種。

問：我們如何傾聽、整合他人的意見？

答：科技的進展讓溝通更為容易，多方利害關係人治理模式也是其他領域、文化的多樣化，對話、組織都需要時間，也需要學習。

問：如何強化政府或管理者的參與？如何讓他們有參與動機？

答：不同的政府有不同的動機，但最重要的動機是「人民想要什麼？」需考量的是他們有多少預算？我們討論的議題，涉及誰的權利？對誰有助益？例如，網路霸凌對政府而言是重要的問題，他們自然會對我們所討論的議題感興趣。但因為民選政府部門會有輪替、任期問題，政策立場容易產生變動，所以有時候可能較難有長期一致的立場與政策設計。此外，參與時的外交禮儀也十分重要，以免在討論過程中，不小心冒犯他人或團體，影響下一次的連結。然而，對此亦有人主張，容納合理的憤怒及聲音，也是多樣化的一環。

閉幕會議到此結束，接著舉行閉幕式，APrIGF 秘書處代表 Edmon Chung（亦為 DotAsia 執行長、新任 ICANN 董事）、yIGF 代表 Amogh Palleri Chettuparambil、尼泊爾主辦地的代表 Bikram Shrestha（亦為 Nepal Internet Foundation 負責人）、聯合國 IGF 多方利害關係人諮詢小組主席（Chair of the Multistakeholder Advisory

Group of UN IGF)Anriette Esterhuysen、特別來賓 Dhanraj Gyawali(Secretary of the Prime Minister's Office and the Council of Minister）、2023 IGF 主辦國日本代表依序致詞，最後則進行主辦國的交接儀式，APrIGF 2021 會議至此圓滿落幕。

圖10. 閉幕會議畫面截圖

四、 參與心得

（一） 林〇德

很榮幸有機會參與這樣的國際會議，能夠了解當今在亞洲各國家對於資訊的審查、監控、仇恨言論以及聽到他們分享如何走向自己的解決辦法的過程。仇恨言論的限制往往與言論自由的權利有著很大的衝突，但又像 S7 會議所揭露的，部分言論的限制宣稱是要解決恐慌、達到平等，卻常常變成政府權力操控立場的手段，面對這樣的狀況需要人民與組織不斷的對話及反省。

聽到各國的分享，更加意識到自己身處在一個民主自由的國家，享受著豐富的權利，因為享有這樣的權利，當遇到歧視性言論時，往往難以對抗言論自由派的反抗，是否要限制歧視／仇恨言論？限度在哪？怎樣界定？有沒有相關申訴管道？這樣的限制是不是反而造成壓迫？我想在這條路上，我們也是需要時時警惕並審視這個議題。

身為一名老師，我不斷的跟學生對話並反思自己對於這兩個價值的平衡，就像講者說的，我們必須不斷關注，並將這樣的經驗運用在自己的經歷上，了解自己所支持的觀點，究竟是奠基在什麼樣的論述上。也必須隨時提醒自己保持開放，接受多元的聲音，找到差異性的優勢。必須全面了解消息，不能去脈絡的聽信片面的資訊，造成假新聞的發展，在當前科技及媒體發展如此蓬勃的社會中，我們更有義務要好好的看著自己手上擁有的，不浪費任何一個為自己發聲的權益。

（二） 陳○耀

我在這次的 APrIGF 會議參加了 Opening Plenary、【S5】開放且可交互運作的網路基礎建設為何是網路持續成功的關鍵，以及【S14】COVID-19 技術對人權的影響與對企業的作用。

在 S5 當中，講者最常提到的是「網路為去中心化」這個概念，然而，我認為網路並不是真正的去中心化，正確來說應該是「多個中心」的概念，只是我們在教導新鮮人「中心化」與「去中心化」時，沒有提過「多個中心」這樣的概念而已。

具體而言像是比特幣，號稱去中心化的貨幣，也是可以透過禁止種子節點（seed node）的解析來被控制。而各國通常對於一類電信商或是主要的 ISP 也會有力度不一的監管措施，因此各國政府透過監管行為確實還是有可能影響到網路世界，這點在中國是十分廣為人知的狀況，但卻沒有在會議中被提到有點可惜。

實際上去中心化的傳播我認為 COVID-19 疫情與不實訊息當之無愧，在傳播時很難找到源頭、尋找傳播路徑沒有那麼簡單、沒有一個有效的監管方式可以控制它的傳播，目前唯一證實有效的做法，只有所有的節點（民眾）都能意識到這個東西的危害，並且有意識的停止傳播，才有可能成功。

相較於此，網際網路並不是這樣的東西，一般民眾要上網還是必須透過 ISP 幫忙，ISP 需要向當地的網路資訊中心（Network Information Center，NIC）取得被分配的 IP 位址，再者，ISP 需要有其他的「中心」願意和他做邊界閘道器協定（Border Gateway Protocol，BGP）會話（Session）的交換，如此一來網際網路才得以發生。

而在 S14 這場主要討論到 COVID-19 疫情對於人權的影響，不過實際上討論時沒有把電子腳鐐納入，實在有點可惜。我認為到底特定國家居家隔離的「電子圍籬」系統侵犯人權狀況是否可以和該國電子腳鐐相比其實是個有趣的問題。首先，電子圍籬建立在使用者生活離不開手機的前提，因此如果某個人他完全不使

用手機時，電子圍籬對他是無效的（例如 S5 提到的孟加拉？），再來電子腳鐐會有較重的不適感,但是電子圍籬感覺不大,然而電子圍籬感覺不大的缺點在於，電子腳鐐被監控者可以在解除腳鐐時很明確的知道他的個人資料不再被搜集，但是電子圍籬的被監控者在使用者介面上是不知道他是不是被停止監控了。

不知道是否被監控或是不知道是否被停止被監控，最嚴重的問題在於沒有證據指控政府侵犯其權利，在沒有證據證明權利被侵害的前提下，自然無法進入司法程序來討論個人資料的使用是否合理，也就完全沒有討論權利被侵害後的賠償問題了，我認為這點應該會是在討論個人隱私的人權問題中，最迫切需要被討論的問題。

（三） 湯○樺

首先,我個人相當榮幸能夠受到NII的邀請來參加APrIGF 2021的線上會議，與來自亞太地區各個國家的優秀人士共襄盛舉，一起討論網路治理的相關議題。

說來慚愧，身為一名軟體工程師，平日工作與網路密不可分，但這卻是我第一次聽到 APrIGF 這個活動，當初看了 APrIGF 的議程表，讓我嘆為觀止，不是因為它都是以英文方式呈現,好歹平日與技術為伍的我還是需要些許英文程度去閱讀新知，而是它的議程探討範圍相當廣，但確實都是以網路為出發點，所以有些議題讓人非常感興趣，因為它可能相當貼近我們的生活，但我們卻忽略了它的存在。

我依照 NII 的規定，挑選了兩個感興趣的議程，一個是我在工作上接觸過的AI，另一個則是我不太熟悉，但卻令我感到興趣的開幕會議。在進入視訊會議的時候，內心其實是相當興奮的，因為整個會議就像是一個小型的聯合國，你可以聽到來自不同國家的英文口音，這不僅是一個關於網路議題的會議，也是一場文化上的饗宴，根據每個議題中的討論，每個人一定會有不同的想法論述，更何況是來自不同國家文化的人們，這之間所擦出的火花可想而知。

在會議過程中，我發現雖然每個人所表達的想法理念可能有衝突，但最終都會透過溝通來達成共識，我想這也是 APrIGF 這個活動的宗旨，經由大家的討論來解決現今網路上所遇到的問題，或是想辦法讓它變得更好，這無疑對未來的網路環境是有幫助的，因此我個人相當推崇這個活動能夠一直舉辦下去，也希望能夠讓更多國內的有志人士知道這個活動，相信從中能夠學習到許多新知，並有機會與國際人士共同參與討論，所以我很感謝 NII 讓我有機會參與這次的會議，如果下一次還有機會的話，相信我也不會輕易錯過的。

（四） 楊〇楷

這是我第一次線上參加 APrIGF 會議，也剛好選到自己有興趣的題目，探討網路中介者的責任，進行方式是主持人引言後，由四位講者介紹，最後綜合討論。好處是可以聽到印尼、印度、馬來西亞等亞洲國家對於中介者責任的看法，但可能是每位講者分配到的時間太短（只有各 5 分鐘左右），對於法律、管制爭議不一定能表達得很完整。

有趣的是，韓國高麗大學法學教授 Kyungsin Park 是介紹歐盟的架構，他以德國的 NetzDG 為例，認為這樣的管制可能讓平臺產生不透明、非正當程序的審查制度來管制用戶的言論，容易對言論自由產生負面影響。這個主題恰巧是我的碩士論文內容之一，我的立場與講者相反，一方面是，正因為平臺現有的審查制度不透明、非正當，讓平臺上違法言論的問題難以解決，才可能會有立法的需求，所以講者指出的批評很可能是未立法的現狀而不是立法後的結果；另一方面，NetzDG 框架所關注的，除了「我國言論自由保障是否容許要求平臺管制言論」外，更有「要求平臺在言論管制上賦予一定的正當程序」，若後者超越憲法框架要求，自然可能違憲，但這應不能一概而論。

我的觀察是，這個會議上的參與者，似乎對政府介入有較大的不信任感，不知道是否基於亞洲脈絡對國家權力的不信任？或是基於網路發展時的自由不干涉主義，認為公權力相對而言還是較不好的解方？

（五） 蔡○安

數位識讀確實是現代公民社會生活最重要的能力之一，也是防制不實訊息、網路危害內容過程中必做的功課。我國教育部也多年推廣媒體識讀素養教育，由部長召集組成「媒體素養教育推動會」，推動「媒體素養教育行動方案」，以分齡、分眾、分管道之方式，透過學校、社區大學、圖書館，以課程、活動、公眾資源分享推廣媒體識讀教育。從澳洲、尼泊爾、新加坡講者的分享中，發覺圖書館是很重要的推廣數位識讀能力的場域，因為與民眾很接近、受到信賴，圖書館員也對於大量資訊的處理及索引具備專業，不過講者也強調，需要 ICT 人員與圖書館員合作，給予圖書館員足夠的科技知識支援，才能提供民眾好的服務。

有關網路安全部分，我認為 DC-ISSS 計畫提供了很好的工作架構，應該先對公私部門進行全盤調查以了解需求，再彙整現有關於網路安全的指引或最佳做法、進行諮詢及修正，最後是規劃落實方案。讓我最有興趣的是第三組的採購供應鏈安全性議題，如今我們的生活及產業多被數位科技所涵蓋，確保這些數位媒介的安全性是無比重要卻容易被忽視的問題，我國產業界同樣缺乏重視網路安全的風氣，在未實際遭受損害前沒有誘因對網路安全建立制度及投入資源，我覺得 DC-ISSS 的概念非常好，希望藉由納入公私部門的回饋，建立共通做法及指引，讓產業形成風氣，也對政策提出建議。

附件：APrIGF 2021 完整議程表

Time (UTC)	27 Sep (Mon)	Time (UTC)	28 Sep (Tue)	Time (UTC)	29 Sep (Wed)	Time (UTC)	30 Sep (Thu)
				03:00 – 04:00 (60 mins)	S5. Why open and interoperable Internet infrastructure is key to the Internet's continued success Details	03:00 – 04:00 (60 mins)	S7. Internet Rules: Judicial and Regulatory developments impacts digital rights in Asia Details
					S8. Building digital information literacy skills for trust and well-being Details		S14. Human rights impact of Covid-19 technologies and the role of businesses Details
04:00 – 07:00 (3 hours)	Capacity Building Program for Fellows and Newcomers	04:00 – 05:30 (90 mins)	Opening Plenary	04:00 – 04:20 (20 mins)	Break / Social	04:00 – 04:20 (20 mins)	Break / Social
				04:20 – 05:20 (60 mins)	S4. Decrypting the encryption debate in Asia-Pacific Details	04:20 – 05:20 (60 mins)	S12. MANRS for Policy Makers to improve global routing security Details
					S13. Weaponization of surveillance amod a pandemic in South Ease Asia Details		S11. Digitally-led, Inclusive Growth in the Age of COVID-19 Details
		05:30 –	Break / Social	05:20 –	Showcase 2: Internet's	05:20 –	Showcase 3: Is the internet

Time (UTC)	27 Sep (Mon)	Time (UTC)	28 Sep (Tue)	Time (UTC)	29 Sep (Wed)	Time (UTC)	30 Sep (Thu)
		05:50 (20 mins)		06:10 (50 mins)	Technical Success Factors Details	06:10 (50 mins)	trusted forever? — The issue about the pirate site on “Manga” and freedom of expression in Japan Details
		05:50 – 06:50 (60 mins)	S1. Critical Times: Impact of Digitalization on Climate Change Details	06:10 – 06:30 (20 mins)	Break	06:10 – 06:30 (20 mins)	Break
			S3. Helping kids learn in times of pandemic Details	06:30 – 07:30 (60 mins)	S6. Citizen-Centered Approach on Tackling Hate Speech, Hindering State Authoritarianism and Algorithmic Censorship of Tech Platforms Details	06:30 – 07:30 (60 mins)	Special Session by UN IGF DC-ISSS: A workplan for greater online security and safety
		06:50 – 07:40 (50 mins)	Showcase 1: Transnational conversations on reclaiming freedom of expression online Details		S15. The Impact of the Global Pandemic on Schools on Internet Governance Details		Rapporteur Session by the Fellows

Time (UTC)	27 Sep (Mon)	Time (UTC)	28 Sep (Tue)	Time (UTC)	29 Sep (Wed)	Time (UTC)	30 Sep (Thu)
		07:40 – 07:50 (10 mins)	Break	07:30 – 07:50 (20 mins)	Break / Social	07:30 – 07:50 (20 mins)	Break / Social
		07:50 – 08:50 (60 mins)	S2. Don't shoot the messenger, intermediary liability principles under threat Details	07:50 – 08:50 (60 mins)	S9. More than wor(l)ds : Can AI effectively monitor online harms?Details	07:50 – 09:20 (90 mins)	Closing Plenary
			Session by the Fellows		S10. Advancing Internet Freedom in Asia-Pacific via applying UNESCO's Internet Universality ROAM Principles and Indicators Details		
		08:50 – 09:10 (20 mins)	Break / Social	08:50 – 09:10 (20 mins)	Break / Social		
		09:10 – 10:00 (50 mins+)	Townhall session	09:10 – 10:00 (50 mins+)	Townhall session		