

國家通訊傳播委員會

「強化我國網路治理交流與人才培育」

委託研究計畫

期末報告



財團法人中華民國國家資訊基本建設產業發展協進會

中華民國 109 年 12 月 25 日

目 錄

摘 要	vi
第一章 計畫簡介	1
第一節 緣起與目標	1
第二節 計畫架構與內容	2
第三節 執行時程及進度	3
第四節 預期成果與績效指標	4
第二章 通傳政策案例研析	6
第一節 數位主權：歐洲觀點與政策發展	6
第二節 科技防疫的網路治理議題	32
第三節 聯合國數位合作藍圖的擘劃與挑戰	52
第三章 大專院校講座	70
第一節 執行概況	70
第二節 中興大學場次	70
第三節 臺灣大學場次	74
第四節 高雄科技大學場次	77
第四章 人才培訓課程	81
第一節 活動內容與辦法	81
第二節 學員招募與評選	88
第三節 課程摘要紀錄	94

第四節 圖文影音紀錄	112
第五節 活動成效評估	114
第六節 學員獎勵活動	117
第五章 精華短片製播.....	122
第一節 短片內容	122
第二節 觀眾意見回饋	128
第三節 流量統計分析	130
第六章 國際會議參與.....	135
第一節 IGF 會議簡介.....	135
第二節 開閉幕場次	136
第三節 會議討論	138
第四節 IGF 2020 公報.....	146
第五節 心得與建議	152
第七章 總結建議.....	154
附件	160

圖 目 錄

圖 1. 計畫架構圖.....	2
圖 2. 歐盟執委會主張建立歐盟的科技主權.....	7
圖 3. 全球百大科技公司（154 家）來源國統計	9
圖 4. 全球主要平臺的地理位置分布.....	10
圖 5. COVID-19 爆發的數位政策議題.....	32
圖 6. 網域名稱含 COVID、CORONA、及 VIRUS 字串累計註冊量.....	36
圖 7. COVID-19 對全球網路服務的影響.....	38
圖 8. 全球上網普及率（依地區和開發程度統計）	54
圖 9. IGF Plus 模式生態系統	61
圖 10. 中興大學講座照片	73
圖 11. 臺灣大學講座照片	77
圖 12. 高雄科技大學講座照片	80
圖 13. 研習營講師簡介.....	84
圖 14. 研習營報名表.....	85
圖 15. 研習營活動網站.....	88
圖 16. 研習營宣傳圖文.....	89
圖 17. 研習營學員組成概況.....	91
圖 18. 研習營課前預習線上檢測答題結果.....	93
圖 19. 研習營布置與印刷品.....	112

圖 20. 研習營活動剪影.....	113
圖 21. 研習營課程簡報資料與錄影檔.....	114
圖 22. 研習營「課程內容」滿意度.....	115
圖 23. 研習營「行政會務」滿意度.....	115
圖 24. 研習營學員課後自我評估.....	116
圖 25. 優秀學員評選及 APrIGF 線上會議網站.....	118
圖 26. 研習營「TWIGF 2020 座談申辦」活動辦法.....	120
圖 27. 研習營「APrIGF 2020 線上特派員」活動辦法.....	121
圖 28. 網路安全議題短片畫面截圖.....	123
圖 29. 網路內容議題短片畫面截圖.....	125
圖 30. 網路人權議題短片畫面截圖.....	127
圖 31. 網路安全議題短片留言截圖.....	128
圖 32. 網路內容議題短片留言截圖.....	129
圖 33. 網路人權議題短片留言截圖.....	129
圖 34. 精華短片的觀看次數與時間.....	130
圖 35. 精華短片的流量來源.....	132
圖 36. 精華短片的觀眾性別與年齡.....	134
圖 37. IGF 2020 線上會議「對抗新冠肺炎的可信賴網路科技」.....	141
圖 38. IGF 2020 線上會議「新冠肺炎危機時期的信賴、媒體道德和治理」.....	144

表 目 錄

表 1. 計畫時程表（契約變更版）	3
表 2. 計畫查核項目（契約變更版）	4
表 3. 預期量化與質化成果	5
表 4. 歐盟官方說明數位主權（科技主權）內涵彙整表	13
表 5. 《塑造歐洲數位未來》戰略之目標與主要行動措施	18
表 6. 歐美專家對於歐盟尋求數位主權的評論	21
表 7. COVID-19 各國非藥物管制措施	34
表 8. 數位合作建議模式比較	59
表 9. 大專院校講座活動辦理概況	70
表 10. 研習營課程表	82
表 11. 研習營學員成果報告彙整表	110
表 12. APrIGF 2020 場次資料列表	118
表 13. IGF 2020 線上參與場次	136

摘 要

本計畫透過辦理大專院校校園講座、舉辦培訓課程、製播精華短片等工作，以提升大專青年對網路治理議題的認知、培養我國網路治理的多元人才，以及吸引大眾關心網路治理議題。另一方面，本計畫也挑選當前重要的治理議題進行研析，並（線上）參與相關國際會議進行政策交流，以協助我國掌握通傳政策的議題動向，促使我國網路治理發展符合國際趨勢。

本計畫如期完成契約（經契約變更）指定的所有工作，包括：

- 研析 3 個通傳政策案例，主題為「數位主權：歐洲觀點與政策發展」、「科技防疫的網路治理議題」，以及「聯合國數位合作藍圖的擘劃與挑戰」。
- 辦理 3 場次大專院校校園講座，包括臺大、中興、高雄科技大學，每場時間為 2~3 小時，出席人數分別為 102 人、120 人、56 人。
- 辦理 8 小時的培訓課程，共計 29 人結業，且選拔 1 位優秀人才線上參與網路治理國際會議。
- 製播 3 支精華短片，主題為網路安全、網路內容、網路人權，YouTube 觀看次數分別為 2.4 萬、3.3 萬，以及 7,200 次。
- （線上）參與 1 場國際網路治理會議（IGF 2020），並提供重要議題報告。

綜合以上工作項目，本計畫提出下列結論與建議：

一、通傳政策案例研析

1. 數位主權：歐洲觀點與政策發展

歐盟於今年（2020）2 月發布維護數位主權的政策方案，強調要讓歐盟

整體社會受益於數位轉型，同時保有公平競爭、開放、民主等歐洲基本價值，但也引發興起數位保護主義、和中俄獨裁政權為伍、政策方向錯誤且阻礙創新、破壞歐美雙方關係等負面抨擊。其實中俄等專制政權實施網路主權已經多年，且美國近來推出「乾淨網路」計畫也被視為是實施網路主權並採取中國大陸的干預控制模式，因此，目前探討相關議題會面臨定義不明確及帶有專制獨裁色彩的問題。儘管如此，現階段我國可先行評估是否也面臨歐盟所擔憂的數位風險，同時也要掌握歐盟相關政策進展，以即時因應具有域外效力的歐盟新規。

2. 科技防疫的網路治理議題

AI、大數據等新興技術被用於預測、監控和預防新冠肺炎疫情，網際網路更是疫情因應措施的重要基礎，網路治理議題也因此受到影響，範圍包含網路安全、網路發展、法律與人權、數位技術、資訊社會，以及數位經濟等層面。我國因防疫有成社會正常運作，反而缺乏數位轉型的實務經驗及迫切需求，未來需加速推動數位轉型與數位包容，以免落後於國際社會。此外，個資是此次科技防疫最重要的資源及決策依據，因此出現許多相關治理問題，如我國個資法對於「為增進公共利益所必要」有過度空白授權的疑慮，又如《實聯制措施指引》引發許多商家過度蒐集個資等情況。因此，後續仍需檢討改善科技防疫相關法規措施，以法制建立社會信任，民眾才會願意持續配合防疫措施，我國防疫成效才得以延續下去。

3. 聯合國數位合作藍圖的擘劃與挑戰

聯合國於2020年6月發布《數位合作藍圖》，數位合作並獲得聯合國193個會員國的承諾推動，且全球網路治理社群也普遍支持以IGF Plus模式作為全球數位合作的模式，因此，未來IGF可望訂定具體的網路治理政策規範或標準，惟其非強制性國際規範。儘管如此，藍圖對於我國的數位政策仍有重要參考意義，例如聯合國將研擬具體量化的數位包容等指標，我國可用於檢視上網資費的合理性、弱勢族群的上網權益保護、資訊素養

的教育成效等施政。此外，未來聯合國還將針對新科技的使用進行人權盡職調查，我們對於涉及使用數位科技的公共政策如《科技偵查法》草案、數位身分證計畫等措施，應該進行更審慎的評估，並和整體社會充分溝通，以真正落實保障數位人權。

二、大專院校講座

本年度於臺灣大學、中興大學、高雄科技大學共計辦理 3 場講座活動，場合皆為學分課程，學生涵蓋大學生與研究生，系所包括電工所、資工所和資管系，出席人數分別為 102 位、120 位、56 位。整體而言，3 場講座的大學生和研究生對於網路治理議題的興趣並無明顯落差，但如綜合上年度的執行經驗，顯然是上年度行政管理所學生的表現最為突出，他們積極提問至課後 45 分鐘才結束。惟本年度礙於地區不得重複、每場 2 小時以上、出席人數 50 人以上等規定，於活動安排受到較多限制，例如北部大學佔全臺大學 47% 但只能選擇 1 所、有些系所的專題演講課程只有 1 小時、許多文法系所的學生人數遠不及 50 人等。因此，建議未來將大專院校實際情況納入規格考量，以保留執行彈性，安排於學生可能對網路治理議題更感興趣的學校系所演講。

三、人才培訓課程

本年度共 29 位學員參與全日培訓課程並順利結業。學員對於課程內容整體設計的滿意度達 100%，且大多數學員表示課後的網路治理知識和興趣增加，並樂於參與座談交流活動，顯示本次課程達到柯氏（Kirkpatrick）學習成效的「學習層級」（第二層級）。然而本計畫在有限的資源下，僅能獎勵 1 名優秀學員參與國際會議（雖然本年度國際會議皆因疫情影響而改成線上會議）。面對網路治理的重要性提升，需要更多的多方利害關係人參與政策討論，未來除了應該持續辦理培訓課程外，也需要一併投入更多資源，提供學員更多的參與機會和舞臺，以鼓勵持續且長期地參與網路治理。

四、精華短片製播

本年度分別以網路安全、網路內容、網路人權為主題，和 YouTuber 合作製播 3 支精華短片。截至 12 月 1 日的觀看次數分別為 2.4 萬、3.3 萬，以及 7,200 次，並有 230 則、190 則和 77 則留言，內容大多是對影片表達肯定之意。精華短片製播旨在做為增進大眾認識網路治理議題的教材，惟全球每天有 72 萬小時的影片上傳到 YouTube，且本計畫培訓課程或大專講座的内容皆有一定難度，即使經剪輯也不易吸引大眾觀看，進而完成計畫所要求的流量分析。適逢 IGF 2020 國會議員場次建議各國推動網路安全、對抗假訊息等治理議題的大眾認知宣導，因此，未來如有充足預算，可為大眾量身訂做合適的影片內容並於合適的頻道推廣播放。

五、國際會議參與

受到 COVID-19 影響，IGF 2020 首度全面以虛擬會議方式進行。而為了展現會議的具體成效，本年度的會後公報 (Messages) 將所有會議的討論重點彙整成 12 個總體政策問題和建議，可說具有相當政策參考價值。例如消除數位落差的建議包含將「有意義的數位包容」列為政策指導原則，也就是讓使用者有合適的「設備」和「能力」可持續且快速地「連接」到符合他們需求的「內容和服務」，這些要素可作為檢視我國剩餘約 1 成未上網民眾的障礙因素，進而予以改善。近年來 IGF 力求轉型，未來如能依《數位合作藍圖》規劃，進一步提供治理常規、原則或標準，不但 IGF 的地位和影響力都將顯著提升，而且這些規範建議更可成為各國的政策決策參考，進而有助於減少跨國法規的衝突問題。

Abstract

Through organizing campus lectures, training courses and video clips, this project aims to raise the awareness of Internet governance among youth and college students, and to cultivate diversified professional talents of Internet governance in Taiwan. In the meantime, participation in international virtual forums and analysis of governance issues were to understand the trends of communication policy and to ensure the development of Internet governance in Taiwan in line with international trends. In light of the above-mentioned tasks, conclusions and recommendations are proposed as follows:

1. Governance issues analysis

- EU's digital sovereignty policy. Giving that factors such as digital dependence on other countries, falling behind in digital economic competitiveness, and the emergence of the new tech cold war, the EU has proposed a digital sovereignty policy to strengthen its digital autonomy as a way of self-protection. Therefore, we could also make a risk assessment on digital dependence, and identify EU's digital regulations with potential extraterritorially impact.
- Internet governance issues of technologies against COVID-19. The pandemic widens the digital gap and accelerates the digital transformation in various countries. With the success in combating coronavirus to keep life normal, however, Taiwan loses its practical experience and urgent needs for digital transformation. So we need to accelerate the digital agenda to link up with the world. In addition, reviewing and completing covid-related technological regulations and measures involving personal data are also needed so the public trust could be developed based on the rule of law and

the pandemic success story could be continued.

- UN's roadmap for digital cooperation. In order to connect, respect, and protect all people in the digital age, UN Secretary-General António Guterres calls for actions for global digital cooperation. Among the long list of tasks, quantitative indicators in relation to Internet connectivity and digital human rights will be defined, which can be used to review the effectiveness of Taiwan's digital policies and combine with existing plans to assist in bridging the digital gap for international community in the future.

2. Campus lectures in universities

- Three campus lectures were held this year with audience from college students and graduate students. Giving that courses dedicated to Internet governance are rare in Taiwan, continuous efforts in campus lectures are suggested so the youth have the opportunity to learn and care about Internet governance, and further participate in governance policy discussions.

3. Training courses

- The result of the courses matched the learning level (some of the second level) of Kirkpatrick's Training Evaluation Model. Due to the increasing importance of Internet governance, continuing training courses and more investment in creating long-term and stable participation incentives are recommended.

4. Video clips production and publication

- Three video clips were produced and published and have received many positive responses from the audience. Awareness raising on cybersecurity and combating disinformation online were advised to all governments

(though specified national parliaments) in the IGF 2020 Parliamentary Roundtable. Therefore, the authority in Taiwan could organize tailor-made videos for the public and to broadcast on appropriate online platform channels with sufficient budget.

5. International forums participation

- The IGF strives to transform to provide policy recommendations to the international community. It may develop concrete policy guidance, norms or standards with the implementation of the UN's digital cooperation in the coming years. Not being mandatory requirements, however, these outputs could be taken up by government agencies as useful references to establish related policies or regulations.

第一章 計畫簡介

第一節 緣起與目標

一、計畫緣起

網路治理的三層次架構，包括（一）經濟及社會層（Economic and Societal Layer）：含雲端應用等數位經濟相關行為，網路用戶衍伸出的網路隱私、犯罪、智財侵權、言論/內容審查等；（二）邏輯層（Logical Layer）：含根伺服器、網域名稱、IP 位址、通訊協定參數等，為網際網路名稱與號碼分配機構（Internet Corporation for Assigned Names and Numbers，簡稱 ICANN）的核心職掌，是連接基礎設施層與經濟及社會層的關鍵；（三）網路基礎設施層（Infrastructure Layer）：含網際網路交換中心、陸纜、海纜、衛星、無線通訊系統、寬頻網路、5G、IOT 等。

國際間探討網路治理公共政策議題範圍相當廣泛，從技術、經濟、法律、社會與文化、發展之角度，由多方利害關係人共同討論網際網路的開放、安全、普及上網（Access）、多元文化及關鍵網路資源保護等主題。隨著科技不斷演進，網際網路的快速發展之下，所衍生的問題層出不窮，包括網路安全、網路分裂、網路主權，甚至全球即將面臨從網路治理到 AI 治理的跨越，世界各國網路政策終將迎來莫大的挑戰，為能有效建立開放、包容、信任、創新的數位社會，是以，通傳會應掌握國際網路治理發展趨勢、強化與各國交流及學習，並培育更多元且廣泛的多方利害關係人具備參與國內外網路政策研討能力，進而凝聚我國網路政策議題共識，以前瞻觀點因應數位轉換所帶來的衝擊。

在開放、連結、創新為基礎的網路環境下，為建構有利數位創新之基礎環境，並配合「數位國家・創新經濟發展方案（DIGI+方案）」辦理措施「1.5.1.2 強化通傳與網路治理相關機關與國際之合作與交流」及「1.5.1.4

網路治理發展趨勢研析」之體現，期產出內容契合我國數位經濟社會與產業發展之需求。

二、計畫目標

本計畫將辦理大專院校校園推廣及培育我國網路治理多元專業人才，以提升大專青年對網路治理議題之認知，吸引更多大眾對於網路治理議題的關心，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，使我國網路治理發展符合國際趨勢。

第二節 計畫架構與內容

本計畫的委託辦理工作項目包括「國際趨勢及我國現況分析」、「校園講座及人才培育」、「國際網路治理交流」等 3 大項，並可再細分為通傳政策案例研析、大專院校講座、專業培訓課程、精華短片製播、國際會議參與等 5 個子項目，計畫工作架構如下圖 1 所示。此外，本計畫亦將配合通傳會需求，於履約期間分享計畫成果。



圖1. 計畫架構圖

第三節 執行時程及進度

本計畫執行時程為「自契約生效次工作日（109 年 4 月 30 日）起，至提交完整期末報告等文件」止。由於受新冠肺炎疫情影響，大專校園講座不易安排於 108 年下學期進行，且國際網路治理論壇包括 APrIGF 與 IGF 亦陸續宣布將改為線上會議，因此，本計畫申請並完成辦理契約變更。各項工作的時程規劃、查核項目暨時程，依契約變更更新如下表 1 與 2 所示。

表1. 計畫時程表（契約變更版）

項次		4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
(一)	國際趨勢及我國現況分析									
	1. 通傳政策案例研析			案例1、案例2		案例3				
(二)	校園講座及人才培育									
	1. 大專校園講座		安排聯繫		安排聯繫、備簡報		場次1、2、3			
	2. 專業培訓課程	*準備	自我預習	開課	*續 1	學員線上參與APrIGF			*續 1	
	3. 精華短片製播			企劃、製作		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								IGF 線上	
	專案管理									
	報告與審查					期中報告			期末報告	
*準備：活動規劃、網站建置、課程安排、講師聯繫、活動宣傳、報名作業、評選作業、學員聯繫、布置印刷、場地設備餐點安排等 *續 1：結業學員申辦 TWIGF 座談活動（7~8 月申請，11 月辦理） *續 2：結業學員參加 APrIGF 線上特派員活動										

表2. 計畫查核項目（契約變更版）

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（經契約變更延至工作日 230 日內） • 1 支精華短片成果	契約生效次工作日起 150 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 230 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、英文版 • 全文電子檔光碟片 1 式 2 份	指定期限內

第四節 預期成果與績效指標

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

表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	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	• 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 通傳政策案例研析

第一節 數位主權：歐洲觀點與政策發展

一、歐盟宣布數位主權政策

數位主權 (Digital Sovereignty) 或科技主權 (Technological Sovereignty) 被形容是歐盟近來的政治流行語，從布魯塞爾、巴黎到柏林的政界都在談論。雖然目前這兩個常被交替使用的詞彙尚無統一定義，不過，歐盟執委會 (European Commission, EC) 主席馮德萊恩 (Ursula von der Leyen) 已經將維護歐洲的數位主權列為任期內 (2019 ~ 2024) 的一大施政重點。

馮德萊恩於上任前，即提出將強化歐盟的數位能力列為未來施政優先項目，並表示「現在實現科技主權還不算太晚…我們必須掌握歐洲關鍵技術…包括量子計算、AI、區塊鏈、關鍵晶片技術等」(Propp, 2019)。其執政團隊進一步於2020年2月19日發布《塑造歐洲數位未來》(Shaping Europe's Digital Future) 戰略，以及該戰略中的2項政策方案--《人工智慧白皮書》(The White Paper on Artificial Intelligence) 與《歐洲資料策略》(The European Data Strategy)，以確保歐洲的數位轉型能讓所有民眾、企業及整體社會受益，同時保有公平競爭、開放、民主等歐洲基本價值。

馮德萊恩於發布會上強調，這些政策可以總結為科技主權，這是「歐洲必須擁有的自主選擇的能力，且是基於自我價值觀及尊重自我規範」(Leyen, 2020)。政策的說明資料也指出，《歐洲資料策略》就是要建立一個能夠充分尊重歐洲規範和價值的資料經濟空間，這將可以確保歐洲在全球化世界中的科技主權，並釋放AI等新興科技的巨大潛力 (EC, 2020 a)。

本節將探討歐洲的數位主權概念發展、其各種定義內涵、政策規劃，以及國際間對歐盟尋求數位主權的看法，以掌握國際重大網路治理政策議題趨勢，提供我國相關政策參考。



資料來源：Irish examiner；European Interest（左圖為歐盟執委會主席，右圖為執委會委員）

圖2. 歐盟執委會主張建立歐盟的科技主權

二、歐洲的數位主權發展

（一）法德兩國的率先警覺與推動

歐洲數位主權概念的起源，並無統一說法。例如歐洲的政治雜誌——新聯邦主義者（The New Federalist）指出，網路主權（Cyber-sovereignty）概念出現於 2000 年期間有位法國議員將其定義為「國家得以在網路空間施展作為的能力」（Paris, 2020）。法國的戰略研究基金會（Fondation pour la Recherche Stratégique）報告則認為，法國早在 2004 年於航太和國防工業等領域即主張科技主權（Darnis, 2020）。

但無論起源為何，2013 年史諾登（Edward Snowden）揭露美國國安局暗中監視各國領袖通訊的事件，對歐洲追求數位主權帶來重大影響。當年法國參議院的報告隨即示警「法國和歐盟淪為數位殖民地」，之後法國政界就開始主張法國的數位主權，相關詞彙也被用於警惕歐盟在政治、經濟和科技主權問題上面臨來自美中兩國的威脅（Kelly, 2018）。而德國也是因為史諾登事件觸動政治圈對於政權監控言論的歷史恐懼，才喚醒數位主權意識，進而促成與法國的相關合作計畫（Darnis, 2020）。雙方的合作立場並

有官方文件為證，例如法國國家網路安全局（ANSSI）2016 年的新聞稿載「法德兩國共同承諾推動歐洲的數位主權…包括從網路安全、數位能力、數位產業等層面進行」。另外，法德各自或共同的政策方案亦有如下案例：

- 2018 年法國部分政府單位宣布使用法國的 Qwant 作為預設的搜尋引擎，以取代 Google，並強調這是恢復數位主權。
- 2018 年德國率先提出 Gaia-X 雲端計畫，2019 年法德兩國宣布共同推動此計畫，以降低對美國廠商的依賴，宣示維護歐洲的數位主權。
- 2019 年 7 月法國通過《數位服務稅》（Digital Service Tax, DST）法案，並表明「法國是主權國家，有權決定國家的稅務規範」。

（二）GDPR 已行使數位主權但仍無資料掌控權

歐盟於 2016 年通過、2018 年實施的 GDPR（General Data Protection Regulation，通用資料保護規範）被視為歐盟已經行使其數位主權。資訊教育網站 Techopedia（2020）指出「常被引用的行使數位主權例子，就是歐盟 GDPR…且將資料主權原則擴展到全球…」。

美國智庫——大西洋理事會（Atlantic Council）的報告也認為，GDPR 進一步控制歐洲個資流向其他的司法管轄區，正是歐盟行使數位主權的一個雄心壯志案例。尤其是第 48 條「未獲歐盟法授權之移轉或揭露」，禁止在歐盟營運的公司基於遵循第三國的單方面要求而提供個資，更是行使主權的明確證據（Burwell & Propp, 2020）。

儘管如此，英國的科技媒體 Digit 報導認為，美國 2018 年賦予美國執法機構（經法院同意後）存取美國業者境外資料合法權力的雲端法案（Cloud Act），以及同年爆發 Facebook 默許劍橋分析（Cambridge Analytica）公司不當取得 5 千萬用戶資料的醜聞等事件，都日益加深歐盟國家對於資料掌握在他國手中的疑慮，並追求數位主權，因為其影響層面不只是個資掌控權，更是涉及歐盟國家的國防資安和數位經濟競爭力（Kelly, 2018）。

（三）數位經濟競爭力相對落後

歐美不同智庫如歐洲外交關係協會（The European Council on Foreign Relations, ECFR）和大西洋理事會的報告皆指出，歐盟尋求數位主權的其一主因，在於歐洲數位經濟的競爭力相對落後。雖然歐洲的科技表現不佳和其政策缺點亦有關聯，但是歐洲論述普遍認是因為歐洲市場長期被美國及近年崛起的中國大陸科技公司所主導，才會阻礙歐洲科技和大型公司的發展。也因此，反映在富比士（Forbes）全球前 20 大科技公司排行中，人口多達 5 億的歐盟，和人口僅有千百萬計的香港、南韓和臺灣一樣，皆為 1 家公司進榜¹，但美國卻高達 12 家，中國大陸和日本也各有 2 家；即使放眼至全球前百大科技公司（圖 3），歐洲也只有 14 家公司上榜，低於臺灣的 17 家（Klein, 2020; Burwell & Propp, 2020; Forbes, 2019; Ponciano, 2020）。

Location of the world's largest tech companies

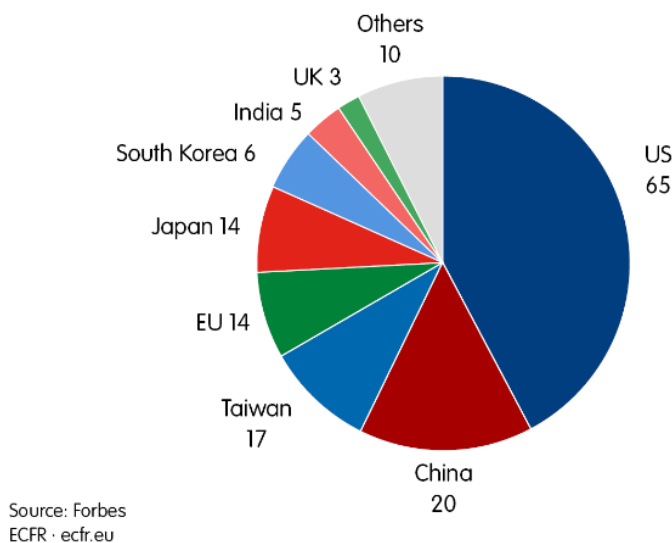
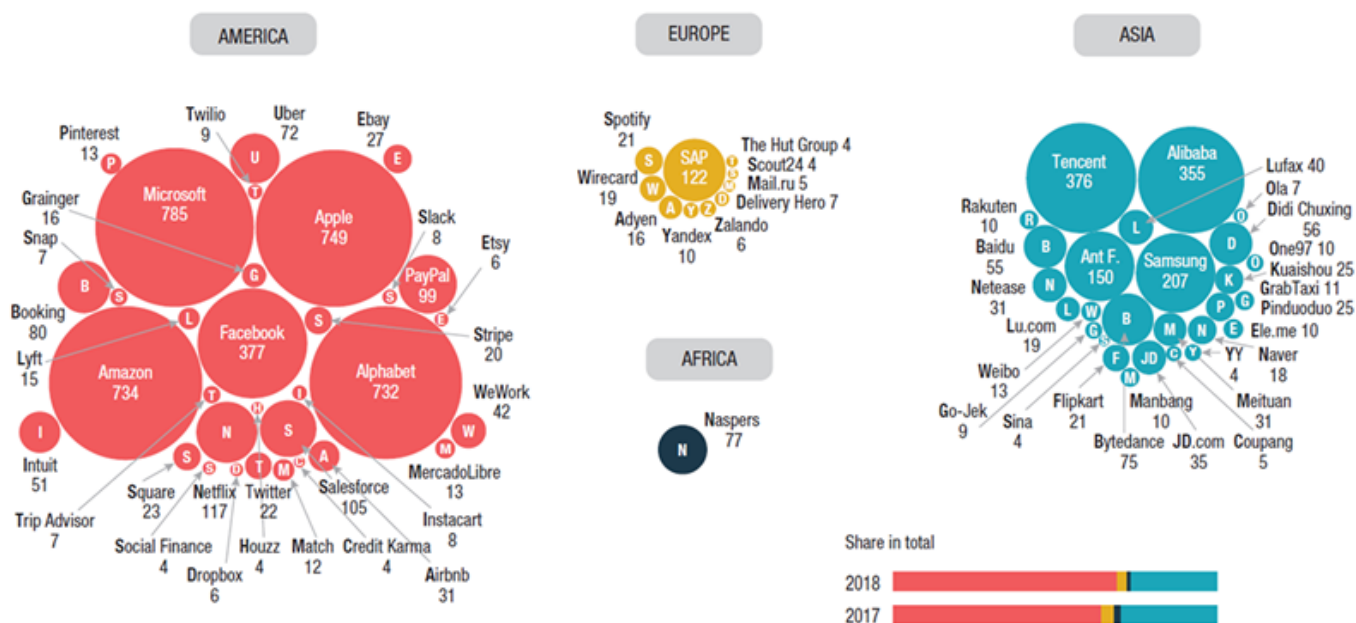


圖3. 全球百大科技公司（154 家）來源國統計

聯合國 2019 年數位經濟報告（Digital Economy Report）亦顯示，全球主要平臺高度集中於美洲，其次為亞洲，皆和歐洲有懸殊落差（圖 4），而且即使是歐洲最常使用的網站也仍是美洲的網站（Burwell & Propp, 2020）。

1 歐盟為德國電信，香港為中國移動通信，南韓為三星電子，我國為台積電。



資料來源：UNCTAD（數字代表各平臺 2018 年的市值，單位為 10 億美元）

圖4. 全球主要平臺的地理位置分布

（四）近來歐盟領袖的呼籲

近來頻頻呼籲建立數位主權的歐盟領袖，除了前述的歐盟執委會主席馮德萊恩外，還有法國總統馬克宏（Emmanuel Macron），以及德國總理梅克爾（Angela Merkel）。

馬克宏於 2020 年 2 月在法國軍事學院的演說中即表示，「必須尋求歐洲層級的政策主權，如 5G 基礎建設、雲端儲存、維運系統和海纜網路都是這類議題…歐洲的行動自由須有經濟和數位主權為基礎…定義自己要實施的法規架構是歐洲自己的工作…我們還需要強化歐洲的科技獨立…」（Macron, 2020）。再如他於 2019 年 9 月會晤工商界高層時也強調「我們所進行的戰鬥之一是主權…如果我們不在所有新領域（數位化、AI）成為冠軍…我們的選擇…將由其他人所主宰」（AFP, 2019）。

目前擔任歐盟理事會（the European Council，或稱歐盟高峰會）輪值主席的德國總理梅克爾於 2020 年 7 月在歐洲議會演說時，亦提倡數位主權。

她表示，「當前歐洲面臨的其一挑戰為數位轉型，過去幾個月來的疫情再次彰顯歐洲對其他國家的數位依賴，因此，讓歐洲成為數位主權國家很重要，並希望在 AI、量子計算、可信賴且安全的數位基礎建設領域，能有所進展」(Merkel, 2020)。此外，梅克爾於 2019 年 10 月和 11 月的國會施政報告和企業領袖會議致詞，也都呼籲歐盟各界要團結起來，降低對美國科技的依賴，以強化數位主權（林國賓，2019）。

（五）美中科技戰及新冠肺炎疫情的催化

美中兩國科技衝突的日益白熱化，也被許多專家視為是推升歐盟爭取數位主權的因素。由於歐洲從電信設備到平臺等數位化各層面同時依賴美中兩國，例如中國大陸的華為已於歐洲 5G 建設扮演要角，但是美國川普總統強迫盟國對華為 5G 實施禁令，凸顯美中雙方將歐洲市場視為爭奪全球技術和工業主導地位的關鍵戰場。不過，歐盟執委會委員布瑞頓(Thierry Breton)已於公開演說時強調「歐洲不會淪為美中緊張情勢下的戰場，也不會只當個旁觀者，而是要將命運掌握在自己的手中…維護歐盟的數位主權」。再者，作為長期盟友的歐美雙方，近來頻頻於數位稅、規範跨境資料傳輸的《隱私盾協議》等數位政策上，持對立立場，而美中科技戰又讓歐盟對於「美國將科技做為壓迫對手的武器」作法，有所警覺，也因此強化歐盟尋求數位主權及數位獨立的戰略思維（Shapiro, 2020；Darnis, 2020；Breton, 2020）。

此外，如前述梅克爾「疫情彰顯歐洲對他國數位依賴」演說，也凸顯新冠肺炎疫情催化歐盟發展數位主權的立場。大西洋理事會報告亦指出，疫情肆虐更凸顯數位化在當前世界的日常運作及因應病毒危機所扮演的關鍵角色，歐盟 2 月發布的 AI 和資料政策正巧呼應科技防疫的相關政策需求（利用 AI 分析大量資料以追蹤病毒傳播途徑，同時需確保這些資料的安全與隱私）。另外，視訊會議系統 Zoom 爆發嚴重的安全和隱私弱點，讓歐盟再次體會對美中科技依賴的風險，德國政府甚至限制使用 Zoom。這些發展促使歐盟在後疫情時代環境下，重新定義數位主權(Burwell & Propp, 2020)。

（六）政治、國安等層面需求

除了上述事件或情勢發展的驅動外，歐盟尋求數位主權還有政治面和國安面的因素。英國專家表示，由於資料已經成為地緣政治和地緣經濟的問題，但歐盟體認到過去做法無法保護其政治、國安和經濟利益，因此，轉向發展數位主權的能力，包括從國安角度要減少對國外科技的依賴，以及從經濟競爭力角度要取回資料主權並發展資料經濟（Zaccari, 2020）。

歐洲智庫--歐洲外交關係協會（ECFR）的報告指出，面對競爭日益激烈的地緣政治、美國關注狹隘的自身利益，以及歐盟缺乏數位獨立性等情勢，對歐洲決策者來說，數位主權概念能讓他們展現維護施政的能力和保護歐洲公民的努力，歐洲必須保護自己的數位主權並與其他人競爭，才能獲得數位經濟的利益、避免政治被假訊息分裂，以及擁有資訊的自主權和掌控權（Shapiro, 2020）。

三、歐洲的數位主權內涵

（一）專業報告和報導

雖然歐盟已經將數位主權或科技主權列為施政重點，但是目前各界對其定義或是內涵，仍是眾說紛紜。以下舉例 3 份報告和報導的闡述說明：

- 歐洲國際政經中心（The European Centre for International Political Economy, ECIPE）

有些人認為科技主權或數位主權是經濟策略，有些人則從價值、歷史或國際公法來看待...還有很多人談論整個歐盟的戰略自主權（Strategic Autonomy）...這意味歐洲的政策制定者保有滿足歐洲企業和促進歐洲經濟利益的能力（Bauer & Erixon, 2020）。

- 美國智庫——大西洋理事會

數位主權是個廣泛的概念，包括一個有足夠資安保護的強大且創新

的工業基礎，以及保障歐盟在數位化影響方面成為規則「制定者」而非「接受者」的能力（Burwell & Propp, 2020）。

- 美國期刊雜誌——外交政策（Foreign Policy）的報導支持數位主權者所持的 2 個定義為「每個公民對自己的資料擁有個人自主權」，以及「每個國家在其領土內擁有無爭議的權力壟斷」（Barker, 2020）。

（二）歐盟領袖談話和官方文件

當然，歐盟領袖的談話和官方文件，亦對數位主權的內涵有不少著墨，相關內容彙整如下表 4，從中除了顯示歐盟官方亦無統一的用詞和定義外，並且可歸納出以下歐盟數位主權的內涵特點：

- 建立自主能力：建立捍衛自我權益的能力，包括歐盟公民的個資自主權、歐盟產業的戰略自主權，以及歐盟政府的政策自主權。
- 堅守歐盟價值：須以歐盟價值觀和法律規範為依歸。
- 發展關鍵技術：掌握量子計算、AI、區塊鏈、晶片等關鍵技術發展，並維護網路關鍵基礎建設的安全。
- 扭轉當前頹勢：降低對他國的數位依賴，強化數位科技和數位經濟的國際競爭力。

表4. 歐盟官方說明數位主權（科技主權）內涵彙整表

歐盟官員或文件	對數位主權（科技主權）的說明
歐盟執委會 主席 馮德萊恩	科技主權是歐洲必須擁有的自主選擇的能力，且是基於自我價值觀及尊重自我規範（Leyen, 2020）。…現在實現科技主權還不算太晚…我們必須掌握歐洲關鍵技術…包括量子計算、AI、區塊鏈、關鍵晶片技術等」（Propp, 2019）。

歐盟官員或文件	對數位主權（科技主權）的說明
歐盟執委會 內部市場委員 布瑞頓	主權或稱戰略自主權…是關於歐洲捍衛其戰略利益，堅持歐洲的價值觀和抱負…。這是為了確保任何在歐洲投資、運營和競標者都遵守歐洲規則和價值觀；為了保護歐洲企業免受掠奪性…和政治性的外國收購；是關於多樣化和降低經濟性和技術性的依賴；是關於發展正確的技術項目，進而讓歐洲在關鍵策略技術上有替代方案（Breton, 2020）。
歐盟執委會 《塑造歐洲數位未來》戰略	歐洲的科技主權始於確保我們資料、網路和通訊的完整性與應變能力。這需要創造正確的條件，讓歐洲得以發展自己的關鍵能力，並因此降低對其他國家最關鍵技術的依賴。此能力能讓歐洲強化訂定自己數位時代的規則與價值…歐洲的科技主權不是針對他人定義的，而是聚焦於歐洲人和歐洲社會模式的需求。歐盟向任何願意遵守歐洲規則且符合歐洲標準的人開放（EC, 2020 b）。
歐盟執委會 參加歐洲網路治理論壇（EuroDIG） 會後訊息	數位主權是未來幾年歐盟於數位科技領域的優先推動項目，它具有雙重且互補含義：用戶在充分尊重歐盟民主原則下，可以對自己的線上個資和活動進行控制；研究、創新投資和政策將確保歐洲在技術供應鏈中的戰略自主權（O'Donohue, 2020）。
歐洲議會 《歐洲數位主權》 內部研究報告	科技或數位主權的概念，是促進歐洲在數位領域領導地位和戰略自主權的一種方法。非歐盟科技公司所帶來的經濟和社會影響…威脅歐盟公民對其個資的控制、壓抑歐盟高科技公司的成長，以及束縛歐盟政策制定者的執法。為此，數位主權是指歐洲在數位世界中獨立行動的能力，應從強化數位創新的保護性機制和主動性工具來加以理解（Madiega, 2020）。
歐盟理事會（或稱 歐盟高峰會） 輪值主席、德國總理梅克爾	當前歐洲面臨的其一挑戰為數位轉型，過去幾個月來的疫情再次彰顯歐洲對其他國家的數位依賴，因此，讓歐洲成為數位主權國家很重要，並希望在 AI、量子計算、可信賴且安全的數位基礎建設領域，能有所進展」（Merkel, 2020）。

*本表依據原文呈現「數位主權」、「科技主權」、「戰略自主權」用詞

資料來源：本計畫彙整

（三）其他相關看法

此外，西班牙的皇家國際與戰略研究所（the Elcano Royal Institute）和歐洲智庫——歐洲外交關係協會（ECFR）的研究員則是提出談論歐洲數位主權所涉及的「歐洲主權」問題。前者表示，對歐洲人來說，這是一種將命運掌握在自己手中的情況，是無法等待且必須贏得勝利的；對法國總統馬克宏而言，則意味「獨立行動的能力與自由」，例如在對華政策和對第三方國家實施制裁方面，但這最好稱為「自治」而非「主權」。而後者更形容它是「有問題的用語」，因為這似乎是要移除各會員國的主權，好讓布魯塞爾或法蘭克福重建一個主權（Ortega, 2020）。

四、歐盟的數位主權政策方案

根據被歐盟執委會主席馮德萊恩稱為「科技主權政策總結」的《塑造歐洲數位未來》戰略，未來5年歐盟的數位發展將以「為民服務的科技」、「公平競爭的經濟」、「開放民主和永續的社會」為3大目標，並提出23項主要行動措施，同時在國際上，還要成為數位轉型的全球領導者，和數位經濟的全球模範（EC, 2020 a）。

上述主要行動措施彙整如下表5，其範圍涵蓋關鍵技術發展、網路基礎建設和安全、數位教育和技能、產業策略和市場競爭、民主和媒體及環境永續等層面。當中又以《人工智慧白皮書》、《歐洲資料策略》，以及著重於規範網路平臺內容責任的《數位服務法案》（Digital Services Act），和一般稱為數位稅的《21世紀商業課稅通告》（Communication on Business Taxation for the 21st Century），還有檢討評估既有的競爭法規等措施，最受關注。以下簡介部分重大政策和法規（草案）。

（一）人工智慧白皮書

《人工智慧白皮書》旨在建立可信賴AI的框架，針對不同風險的AI

系統建立不同規範，以促進歐盟企業使用 AI，以及歐盟民眾信賴 AI，並成為全球可信賴 AI 的領導者。其主要政策措施包含增加研發投資（每年 200 億歐元）、吸引 AI 人才等。監管規範則依據 AI 系統的風險高低而有所差異，如高風險 AI 系統（健康、警務、運輸等）須為透明的、可追蹤、不歧視、有人為監管，甚至主管機關可以驗證演算法所使用的資料（涉及化妝品、汽車、玩具的查驗時）；低風險 AI 系統則擬以非強制性標章方式，鼓勵企業自我提高 AI 道德標準。

此外，《人工智慧白皮書》還提到人臉辨識技術的使用問題。白皮書指出，歐盟原則上禁止將人臉辨識技術用於處理生物資料，但是在有安全措施且於法有據的特殊情況下，可為例外。因此，歐盟執委會將廣泛討論潛在具正當性的例外使用情況（EC, 2020 b）。

歐盟執委會後續還將建立 AI 立法框架，第一版草案預計延到 2021 年第一季度完成²。

（二）歐洲資料策略

《歐洲資料策略》旨在建立歐盟資料單一市場，使歐盟成為資料驅動社會的領導者。在這個歐洲資料空間內，個資和非個資都是安全的，公私部門可輕易存取大量高品質資料以做開發和創新，且所有的資料驅動產品和服務都充分遵守歐盟的規則和價值觀。其執行層面的策略包含下列 4 項（EC, 2020 a）：

1. 建立資料存取和利用的跨部門治理框架

歐盟執委會於 2020 年 11 月 25 日公布《資料治理法案》（Data Governance Act）草稿，此法案旨在透過整個歐盟及各部門之間的

2 立法框架原訂於 2020 第 4 季公布，但根據國際法規資料網站 LEXOLOGY 於 2020/12/01 文章，此框架草案第一版將延至 2021 年第一季度完成。

<https://www.lexology.com/library/detail.aspx?g=d9f74ab9-139c-49e1-9d82-70de718af80f>

資料共享，為社會創造財富、增強民眾和企業對資料的控制和信任，並為主要科技平臺的資料處理措施提供基於歐洲價值的歐洲模式（如重視個資和消費者保護、競爭規則等）³。

2. 投資於強化歐洲能力和基礎建設項目

如整合會員國的雲端相關計畫（如德法 Gaia-X 歐洲雲端計畫）等。

3. 賦權於個資主體

如強化 GDPR 的個資可攜權，並賦予個資主體更多個資掌控權等。

4. 發展策略性產業和公益領域的歐洲共同資料空間

包括工業製造、運輸、醫療衛生、金融、能源等 9 項領域。

（三）數位服務包裹式草案

歐盟執委會於 2020 年 12 月 15 日提出《數位服務法案》(Digital Services Act, DSA) 和《數位市場法案》(Digital Markets Act, DMA) 的草案⁴，以保護消費者及其線上基本權利，並為所有人創造更公平與開放的數位市場。歐盟執委會表示，2 個包裹草案以歐洲價值觀為核心，對數位空間進行重大改革，為在歐盟營運的所有數位服務制定一套全面性的新規則。

《數位服務法案》的特點包括業者所須承擔的義務，依其服務規模和影響而有所不同，並將數位服務和業者分成以下 4 類：

1. 中介服務：提供網路基礎設施者，如 ISP 或網域名稱註冊商。
2. 代管服務：如雲端和網路代管服務。
3. 線上平臺：如線上市集、App 商店、協同經濟平臺（如共享經濟）、社群媒體平臺。

3 資料來源 https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2102

4 可詳歐盟新聞稿 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347，及法案介紹網頁 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

4. 超大型線上平臺：可能會因傳播非法內容而帶來重大社會傷害的平臺，尤其是在歐盟擁有超過 4,500 萬用戶（歐盟人口 10%）的平臺。

法案規範項目則如移除線上違法商品及服務和內容、為內容被平臺誤刪的用戶提供保障、超大型平臺須採取風險措施以預防其系統遭到濫用、實施廣泛的透明度措施（包括線上廣告，及向用戶推薦內容的演算法）、須能追蹤線上市場的商業用戶以協尋非法商品和服務的賣家、歐盟具有徹查平臺工作方式的新權力（包括協助研究人員取得主要平臺的資料）等。

《數位市場法案》則被視為網路世界的反托拉斯法，旨在解決平臺扮演數位「守門人」角色所引發的負面後果，例如它們享有牢固的市場地位、成為規則的制定者、擁有強大的商業媒合力量，甚至可控制整個平臺的生態系統。法案規範項目則如禁止採取明顯不公平的做法（如禁止用戶移除預裝的軟體或 Apps）、必須能夠連結到平臺外的第三方軟體、對違規者最高可處全球年營業額 10% 罰鍰甚至是分拆業務、歐盟可於調查評估後新增條款規則等。

兩項法案後續還需經由歐盟成員國的討論和歐洲議會的投票表決，一旦獲得通過，即可在整個歐盟地區實施。

表5. 《塑造歐洲數位未來》戰略之目標與主要行動措施

目標	主要行動措施	時程	說明
為 民 服 務 的 科 技	《人工智慧白皮書》的後續立法框架	已發布白皮書 立法框架從 Q4 2020 延後	為實現可信賴的 AI 建立立法框架，以及後續的安全、責任義務、基本權利等規範
	建立並部署尖端的聯合數位能力	Q2 2020	包括發展 AI、網路、超級和量子計算、量子通訊和區塊鏈；推出歐洲量子與區塊鏈策略；修正超級電腦規範
	加速投資歐洲的超高	2021	修正《寬頻成本降低指令》、更新《5G 與 6G

目標	主要行動措施	時程	說明
	速（Gigabit）網路		行動方案》、推動新的無線頻譜政策等
	歐洲網路安全策略	已發布策略 ⁵	建立網路安全聯合部門、檢討《網路與資訊系統安全指令》、推動單一市場的網路安全
	《數位教育行動方案》	Q2 2020	提升各級教育的數位素養及能力
	強化《技能議程》	Q2 2020	加強整體社會的數位技能，並強化確保青年於早期職業生涯轉換的數位技能
	改善平臺工作者的勞動條件	2021	--
	強化歐盟政府間互通性的策略	2021	確保公部門資料跨境與安全傳輸的協調和通用標準
公平競爭的經濟	《歐洲資料策略》	已發布策略、法案草稿	建立歐洲成為資料經濟的全球領導者、發布資料治理的立法框架，及《資料治理法案》
	檢視歐盟競爭法規	2020-2023 2020	持續檢討評估歐盟競爭法於數位時代的合宜性、啟動行業調查
	研議《數位服務法案》包裹	已發布法案草稿	探討包裹法案的事前規則，以確保由大型平臺業者扮演守門員角色且具有重大網路效應的市場特色，對創新者、企業和市場新進者而言，仍是公平且可競爭的
	提案《產業策略包裹法案》	--	提出一系列措施，以促進歐盟產業（包括中小企業）轉型成為乾淨、循環、數位化、具有全球競爭力的產業，並強化單一市場規則
	建立更方便、有競爭力且安全的數位金融架構	Q3 2020	包括針對加密資產、金融數位化營運和網路彈性的立法提案，旨在支持泛歐數位支付服務和解決方案的整合性歐盟支付市場策略
	《21 世紀商業課稅通告》	--	將視 OECD（經濟合作暨發展組織）協商進展，因應經濟數位化衍生的課稅問題
	提出新的《消費者議	Q4 2020	促使消費者能做出明智的選擇，並在數位化

5 歐盟執委會於 2020 年 12 月 16 日發布 EU Cybersecurity Strategy。請詳
https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

目標	主要行動措施	時程	說明
	程》		轉型中扮演積極角色
開放民主和永續的社會	全新及修正深化《數位服務市場》法規	已發布法案草稿	增加並調和線上平臺和資訊服務提供者的責任，並強化對平臺內容政策的監管（為《數位服務法案》包裹的一部分）
	修正《電子身分認證與信賴服務規章》(eIDAS)	Q4 2020	改善 eIDAS 效能，將其好處拓展到民間部門，並向所有歐洲人推廣可信賴的數位身分識別
	《媒體與視聽行動方案》	Q4 2020	支持視聽與媒體產業數位轉型和競爭力，促進使用有品質的內容及媒體多元化
	《歐洲民主行動方案》	Q4 2020	改善民主體系的韌性，支持媒體多元化，並因應境外干擾歐洲選舉的威脅
	《目標地球》	2021 開始	開發一個高精準度的地球數位模型，以改善歐洲的環境預測和危機管理的能力
	循環電子倡議	2021	為即將到來的循環經濟行動計畫中的產品持續性，動員新舊工具和政策，以確保設備的設計具有耐用性、可維護性、可拆卸性、重複利用性和可回收性，包括電子設備可透過維修或升級，以延長使用壽命
	永續環保的資料中心	--	於 2030 年前完成氣候中立、高效節能且可永續發展的資料中心，以及完成電信運營商環境足跡的透明化措施
	電子健康資料空間	2022 開始	推動基於歐洲通用交換格式的電子健康記錄，使歐洲公民可以在歐盟內安全地訪問和交換健康數據。一個安全的歐洲健康資料空間可提供更快速的研究、診斷和治療

資料來源：歐盟執委會；本計畫彙整

五、相關評論

歐盟宣示尋求數位主權引發不少大西洋兩岸專家的評論，尤其美國的情況更被形容為「許多美國外交政策界人士聞訊後表示憤慨，並質疑究竟

是要從何人手中奪回主權？又要如何拿取？」(Burwell, 2020)。

整體來看，給予歐盟數位主權的正面評價例如讚揚形同歐洲的「數位獨立宣言」、將吸引民主國家仿效、支持歐盟「增加研發投資以成為科技強權」的政策方向，甚至認為歐洲有機會充當美中爭端的調解人。

而負面評價則包括抨擊歐洲興起數位保護主義（技術民族主義）、和中俄獨裁政權為伍、認為歐盟模仿美國矽谷產業的政策方向是錯誤的且監管框架還會阻礙創新，以及呼籲歐盟勿成為美國的「戰略威脅」且雙方反而應共同合作對抗最大威脅——中國大陸。相關論述的重點彙整於下表 6。

表6. 歐美專家對於歐盟尋求數位主權的評論

	贊同支持論述	反對質疑論述
數位主權政策發布	形同歐洲的「數位獨立宣言」 - 歐洲政策研究中心（the Centre for European Policy Studies） 歐盟繼實施 GDPR 而提升數位形象後，再度發布志向遠大的數位未來政策方案，猶如是歐洲的「數位獨立宣言」，其 2 大政策目標就是要將利益和資料，從美中科技巨頭的手中還給歐洲，同時也彰顯歐盟對於「凡是在歐洲立足，就得遵守歐洲遊戲規則」的堅定立場⁶（Renda, 2020）。 歐洲必須保護數位主權以維護其權益 - 智庫--歐洲外交關係協會（ECFR） 如果歐洲想從新興的數位科技中獲	歐洲興起數位保護/技術民族主義 美國前貿易代表 Charlene Barshefsky 近來歐洲打出確保數位主權的旗幟，從歐盟執委會主席馮德萊恩強調要掌控關鍵技術的就職演說、法國總統馬克宏的主權戰鬥談話，甚至歐洲議會的報告建議仿照中國大陸建立「歐洲防火牆」，凸顯歐洲興起技術民族主義（techno-nationalism），要保護本地公司，且對數位經濟進行更大國家控制。具體證據如《數位服務稅》涉及歧視、《數位服務法案》涉及操弄競爭法、AI 政策對外國的 AI 應用系統設下不合理的障礙、歐洲雲端計畫將提

6 但此篇分析也指出，歐洲的「數位獨立宣言」應是為了提升歐洲在全球舞台建立數位信任所扮演角色的重要性，而非只在歐洲單一市場上築起圍牆，進而讓已經散亂的全球秩序更加隔閡且分歧。

	贊同支持論述	反對質疑論述
	得經濟利益，確保其政治免於假信息的分裂，並決定誰能知道他們最私人的資訊，則必須保護數位主權，並與其他地緣政治參與者競爭（Shapiro, 2020）。	供大規模補貼（Barshefsky, 2020）。 • 智庫—歐洲國際政治經濟學中心（ECIPE） 歐盟爭取數位主權一旦採取保護主義的做法，反而將不利歐洲的國際競爭力、減少獲得尖端技術的機會，且降低對國際投資和研發的吸引力（Bauer & Erixon, 2020）。
國際看待歐洲模式	將吸引民主國家仿效 • 智庫--歐洲外交關係協會（ECFR） 全球網路即將形成三種型式，包括由民間企業自訂規則所治理的「美國網路」、由國家全面監控且為國家利益服務的「中國網路」，以及以公共利益來規範數位市場和企業營運的「歐洲網路」。由於人們普遍認為，美國模式促進美國企業的自身利益，而中國模式主要由威權政府採用，因此，對於希望能兼顧數位市場開放和保護公民利益的民主政府而言，歐洲模式最具吸引力（Puddephatt, 2020）。	中俄獨裁政權樂於與歐盟為伍 • 美國期刊雜誌《外交政策》 歐盟正忙於奔波追求數位主權，想要擺脫對美中的科技依賴，並將此作為地緣戰略的優先事項。然而卻於戰略和道德模糊的數位主權標題下，奉行監管政策。獨裁者已將數位主權發揮得淋漓盡致，中、俄樂見歐洲的數位主權言論，一旦執法過度，歐盟可能無意間淪為有利於全面國家控制的體系（Barker, 2020）。
監管角色和科技產業政策	裁判不會贏得比賽，歐盟必須增加投資以成為科技強權 • 智庫--歐洲外交關係協會（ECFR） 儘管歐盟因為推出 GDPR 等法規的成功經驗，而以「監管的超級強權」自居，但現實情況是「裁判不會贏得比賽」。所以，即使歐盟的數位發展仍然依賴美中兩國、即使當前歐盟和	矽谷產業非歐盟強項，發揮裁判角色才能掌握數位命運 • 美國期刊雜誌《外交政策》 歐盟誤以為政府挹注巨額投資，就可以推動技術創新，但其實美國科技研發資金大多由民間企業自行支出，只有微幅金額來自美國政府的國防和航太業，如國防高等研究計畫署

	贊同支持論述	反對質疑論述
	成員國面臨龐大的預算壓力、即使歐盟 200 億歐元的 AI 投資預算遠不如 Google 一家公司的每年研發經費，但是如果歐洲不想淪為美中的數位戰場，就至少要達到某種數位主權或自治，並從監管超級大國轉變為技術超級大國。而這可以透過鼓勵更多的公共和民間投資達成，包含投資下世代 AI、資料和網路服務、半導體和 6G 等，且必須成為歐盟工業和商業戰略的一部分 (Klein, 2020)。	(DARPA) 投資 20 億美元於 AI，但科技巨頭每年的研發經費即高達 1500 億美元。又歐盟還誤以為需要發展矽谷般的科技產業，但 AI 和雲端都非歐洲強項，即使現在德國投入雲端發展，仍會錯過自動駕駛和電動汽車的時機。建議歐盟改弦易轍，才能掌握自己的數位命運。也就是以龐大的歐盟市場為基礎，透過發揮制定全球重大標準的經驗與力量，同時和志同道合的國際盟友合作（如於 2020 年元旦實施消費者隱私法保護的加州），以打贏這場建立「隱私、民主、公平、透明、法治」的科技價值大戰歐盟 (Barker, 2020)。 監管框架可能阻礙創新 • 美國智庫--大西洋理事會 歐盟執委會正在發展一個廣泛的數位監管框架，但它同時也會使歐洲的數位領域淪為更受管控的經濟空間，進而阻礙歐洲數位經濟所需的創新和可擴展性 (Burwell, 2020)。
與美中關係	歐洲有機會充當美中爭端的調解人 • 智庫--歐洲外交關係協會 (ECFR) 面對美中數位監管方式的南轅北轍——無政府狀況 vs. 國家嚴控，部分歐洲專家認為，歐洲可以充當美中爭端的調解人，並可從中獲得塑造未來	勿成為美國的「戰略威脅」，歐美應共同合作對抗最大威脅——中國大陸 • 美國前貿易代表 Charlene Barshefsky 如果歐洲執意推動數位主權，美國決策者只能將其視為「戰略威脅」，恐怕影響雙方多年來希望優先推動的貿易協議。因此，歐洲應重新考慮其數位

	贊同支持論述	反對質疑論述
	發展的機會。但這不代表歐洲會和美中保持等距的三角關係，而且歐盟能否找到和中國大陸的和解之道也令人懷疑（Shapiro, 2020）。	主權議程，應與美國進行更多的監管合作，以因應數位經濟最嚴峻的挑戰——中國大陸，因其保護主義融合國家和共產黨的控制權，並以空前規模補貼和竊取知識產權，對數位經濟構成生存威脅，例如它正在力推歐美都反對的新型中央控制網路（Barshefsky, 2020）。 • 美國約翰霍普金斯大學—美國當代德國研究所 AICGS 若歐盟希望中國的「以國家為中心」AI 方法（和歐盟的以人為本對立）不會成為國際主流，則應和美國合作，至少白宮的 AI 監管思考和歐盟相容，且行使科技主權可和夥伴合作以強化成效（Rashish, 2020）。 • 美國期刊雜誌《外交政策》 歐洲誤以為自己陷入了日益激烈的美中科技競爭之中，但科技衝突的核心實為價值之爭，而歐洲和中國大陸的價值是相反的，因此，歐洲的首要任務應是推動美國和其價值觀保持一致（Barker, 2020）。

資料來源：本計畫彙整

六、結論與建議

本節探討為什麼數位主權成為歐盟近來的焦點議題，其發展脈絡和內涵為何、政策方案有哪些重點，又引發什麼正反兩面評論。但其實中俄等

專制政權實施網路主權（Cyber Sovereignty）已經多年，中國大陸更自 2014 年開辦「世界互聯網大會」後大肆向國際宣傳網路主權，且於 2017 年實施正式提出網路空間主權的《網路安全法》；俄羅斯則是 2019 年底實施「主權網路法」（Sovereign Internet）。兩國皆是進一步藉由立法將國家對網路的監控審查合法化，因此，網路主權一詞也容易引發專制獨裁的聯想，這也是歐盟的數位主權遭抨擊為「和獨裁政權為伍」的原因。

無獨有偶，美國近來也形同是實施網路主權。其針對中國大陸業者推出的「乾淨網路」（Clean Network）計畫——排除不可靠的 5G 網路、電信商、應用程式商店、應用程式、雲端儲存及海底電纜等項目，即被視為是川普版的網路主權（Internet Sovereignty），並被抨擊為美國採用中國大陸的干預控制模式來治理網路，而且還會破壞全球網路的自由、開放與互連（Mackinnon, 2020; Zakaria, 2020）。

跨越國界且開放及互連，是網路的本質。Alexa Internet 的流量統計顯示，除了實施網路長城的中國大陸外，包括我國在內的各國民眾最常造訪前 10 大網站皆包含 Google、YouTube、Facebook 等美國企業網站，形成各國網民隨時都在網路上跨越國界和主權的情況。因此，要將傳統實體國家組成要素「人民、領土、政府和主權」的概念，套用在虛擬且自由連結的網路空間，並不容易，以致目前國際間對於 Digital Sovereignty、Technological Sovereignty、Cyber Sovereignty、Internet Sovereignty 等相關詞彙尚無統一定義，而且專家們也無法確定大家所談論的究竟是否為同一件事，或是存在多少差異。

由上顯示，目前各國主張或探討網路空間的主權議題時，首先會面臨定義不明確，以及帶有專制獨裁色彩的問題。儘管如此，在歐盟尋求建立數位主權的過程中，就實務面來看，現階段我們至少可先行評估我國是否也面臨歐盟所擔憂的數位風險，同時也要掌握歐盟相關政策進展。相關建議進一步說明如下：

（一）評估我國是否面臨歐盟數位風險疑慮，進而研議因應策略

歐盟要建立數位主權的主因，在於從國際地緣政治變化中，體認到美中兩國皆不可靠，導致歐洲的數位風險升高，包括無資料掌控權、數位依賴，以及數位競爭力落後，並因此提出建立歐盟資料單一市場、發展關鍵技術、強化網路基礎建設和安全與數位教育、打造公平的市場競爭機制等因應策略。

在國家社會和經濟發展皆仰賴網路運作的數位時代，雖然我國部分數位發展情況可能較歐盟為佳⁷，不過，同樣也面臨來自美中雙方對峙的壓力和高度依賴國外數位平臺等問題，況且我國還礙於市場規模太小而難以透過建立市場公平競爭秩序加以因應。因此，暫且撇開數位主權語意上和政治上的爭論，就實務面來看，我們可先評估是否也面臨歐盟所擔憂的數位風險疑慮，進而針對我國數位發展現況研議相關因應策略。

（二）掌握歐盟數位主權政策進展，即時因應具域外效力新規

專家們認為，歐盟的數位主權政策方案顯示歐盟正在建立一個廣泛的數位監管框架，且不排除當中的資料法案、AI 管理規範、《數位服務法案》等規範，可能如同 GDPR 一樣具有域外效力，並成為各國的立法借鏡，以及將會影響相關國際法規的發展（Burwell & Propp, 2020）。

對我國來說，以 2018 年上路的 GDPR 為例，相較於日韓分別已經和即將取得 GDPR 適足性認定以利個資的跨境傳輸，我國迄今仍在為雙邊的技術性協商、修改我國個資法、成立個資保護專責機關等工作而努力。因此，面對歐盟正加速推動新一波涵蓋多面向的數位規範，相關部會除了宜密切掌握歐盟 23 項主要行動措施（表 5）進展，以作為數位政策的參考（例

7 例如相較於歐盟的資料幾乎都儲存在美國業者的雲端，我國政府資料多存在國內業者的雲端；相較於歐盟的數位設備和數位科技皆高度依賴美中兩國，我國則是 ICT 產業重鎮且於全球半導體產業具有關鍵地位；相較於整個歐盟在全球百大科技公司中佔 14 家，我國則有 17 家上榜（圖 3，共 154 家公司）。

如其中甫公布的《數位服務法案》草稿已將數位服務業者進行分類且依其服務規模和影響力課以不同的責任，可以做為通傳會監理方向的參考)，同時也可從中盤點出具有域外效力的法規，以利我國及早準備因應措施。

七、參考文獻

- 林國賓 (2019)。梅克爾籲歐盟宣示數位主權 減少依賴美科技大廠。中時新聞網，14-11-2019。
<https://www.chinatimes.com/newspapers/20191114001139-260203?chdtv>
- 吳旻洲 (2020)。學者：台灣應建網路主權 才能抵抗中共銳實力。大紀元，05-06-2020。
<https://www.epochtimes.com/b5/20/6/4/n12161354.htm>
- 新華網 (2015)。习近平在第二届世界互联网大会开幕式上的讲话（全文）。16-12-2015。
http://www.xinhuanet.com/politics/2015-12/16/c_1117481089.htm
- 駐西班牙台北經濟文化辦事處 (2020)。歐盟外交暨安全政策高級代表 Josep Borrell 於 8 月 27 日發表專文：辛納屈主義。
<https://www.taiwanembassy.org/es/post/12887.html>
- AFP (2019). France Pledges Billions in Fight to Stop French Start-Ups Heading to United States. *The Daily Star*, 19-09-2019.
<https://www.thedailystar.net/business/global-business/news/france-pledges-billion-s-fight-halt-start-drain-1802107>
- ANSSI (2016). The European Digital Sovereignty – A Common Objective For France and Germany. 07-04-2016.
<https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany/>
- Barker, T. (2020). Europe Can't Win the Tech War It Just Started. *Foreign Policy*, 16-01-2020.
<https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/>

- Barshefsky, C. (2020). EU digital protectionism risks damaging ties with the US. *Financial Times*, 02-08-2020.
<https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103>
- Bauer, M & Erixon, F.(2020). Europe’ s Quest for Technology Sovereignty: Opportunities and Pitfalls. *ECIPE*, May 2020.
<https://ecipe.org/publications/europes-technology-sovereignty/>
- Breton, T. (2020). Speech by Commissioner Thierry Breton at Hannover Messe Digital Days. 15-07-2020.
https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1362
- Burwell, F. G. & Propp, K. (2020). The European Union and the Search for Digital Sovereignty: Building “Fortress Europe” or Preparing for a New World? *The Atlantic Council*, 22-07-2020.
<https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/>
- Darnis, J.P. (2020). European Technological Sovereignty: a Response to the Covid-19 Crisis? *Fondation pour la recherche stratégique*, 29-05-2020.
<https://www.frstrategie.org/en/publications/notes/european-technological-sovereignty-response-covid-19-crisis-2020>
- EC (2020 a). Shaping Europe's digital future. 19-02-2020. Strategy.
https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en. Press Release. Commission presents strategies for data and Artificial Intelligence.
https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273. Questions and Answers. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_264
- EC (2020 b). A European Strategy for Data. 19-02-2020.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX:52020DC0066>

- Forbes (2019). Top 100 Digital Companies 2019.
<https://www.forbes.com/top-digital-companies/list/>
- Jung, C. (2020). The New US Cyber Policy Has Serious Bite for Chinese Firms. *The Diplomat*. 07-08-2020.
<https://thediplomat.com/2020/08/the-new-us-cyber-policy-has-serious-bite-for-chinese-firms/>
- Kelly, R. (2018). Au Revoir, Google! Why France is Securing its Digital Sovereignty. *DIGIT*, 22-11-2018. <https://digit.fyi/france-digital-sovereignty/>
- Klein, A. O. (2020). The view from Spain: The EU's bid for digital sovereignty. *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry*, ECFR, Essay Collection, 30-07-2020.
https://www.ecfr.eu/publications/summary/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry
- Leyen, U. (2020). Shaping Europe's digital future. 21-02-2020.
<https://moderndiplomacy.eu/2020/02/21/shaping-europes-digital-future/>
- Mackinnon, R. (2020). It's Not Too Late to Save the Internet. *Slate*, 19-08-2020.
<https://slate.com/technology/2020/08/save-the-internet.html>
- Macron, E. (2020). Speech of the President of the Republic Emmanuel Macron on the Defense and Deterrence Strategy. 07-02-2020.
<https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/news-about-defence-and-security/article/speech-of-the-president-of-the-republic-emmanuel-macron-on-the-defense-and>
- Madiega, T. (2020). Digital Sovereignty for Europe. *European Parliamentary Research Service (EPRS)*, 02-07-2020.
[https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI\(2020\)651992](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651992)
- O'Donohue, P. (2020). Messages from EuroDIG - the European Dialogue on

Internet Governance. EC, 23-06-2020.

<https://ec.europa.eu/digital-single-market/en/blogposts/messages-eurodig-european-dialogue-internet-governance>

- Ortega, A. (2020). Europe's 'sovereignty fever'. *The Elcano Royal Institute*, 03-03-2020. <https://blog.realinstitutoelcano.org/en/europes-sovereignty-fever/>
- Paris, C. (2020). Digital and Technological Sovereignty: Europe's new Battle. *The New Federalist*, 30-03-2020. <https://www.thenewfederalist.eu/digital-and-technological-sovereignty-europe-s-new-battle?lang=fr>
- Ponciano, J. (2020). The Largest Technology Companies In 2019: Apple Reigns As Smartphones Slip And Cloud Services Thrive. *Forbes*, 15-05-2019. <https://www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/#1142235a734f>
- Propp, K. (2019). Waving the Flag of Digital Sovereignty. *The Atlantic Council*, 11-12-2019. <https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/>
- Puddephatt, A. (2020). Governing the Internet: the Makings of an EU Model. *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry*, *ECFR, Essay Collection*, 30-07-2020. https://www.ecfr.eu/publications/summary/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry
- Rashish, P. S. (2020). The Good, the Bad, and the Unknown of EU "Technological Sovereignty. 20-02-2020. <https://www.aicgs.org/2020/02/the-good-the-bad-and-the-unknown-of-eu-technological-sovereignty/>
- Renda, A. (2020). Europe's Digital Independence Day. *The Centre for European*

Policy Studies, 19-02-2020.

<https://www.ceps.eu/europes-digital-independence-day/>

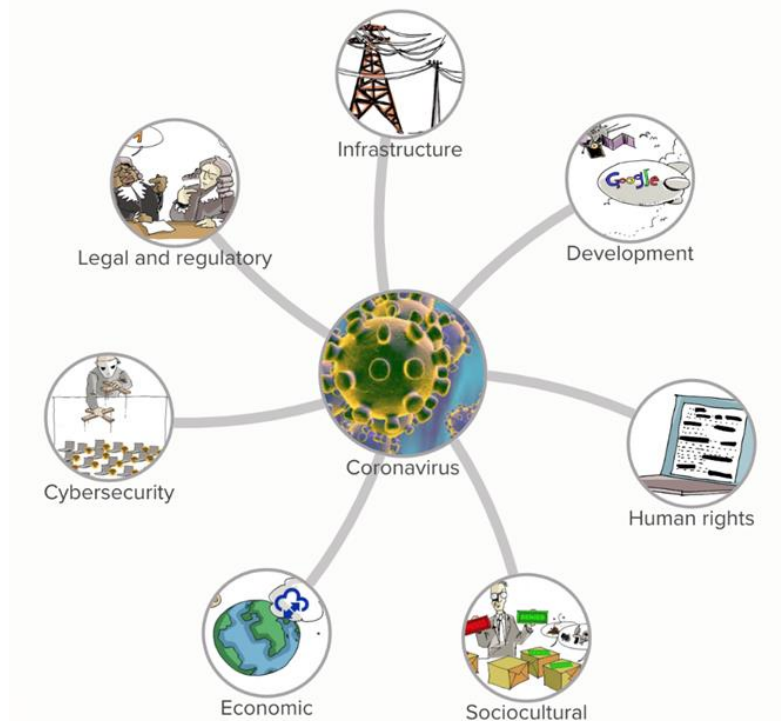
- Shapiro, J. (2020). Introduction: Europe's digital sovereignty. *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry*, ECFR, Essay Collection, 30-07-2020.
https://www.ecfr.eu/publications/summary/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry
- Techopedia (2020). Digital Sovereignty.
<https://www.techopedia.com/definition/33887/digital-sovereignty>
- Zaccaria, E. (2020). European Digital Strategy and the Global Race for Digital Sovereignty. *Computer Business Review*, 2-07-2020.
<https://www.cbronline.com/opinion/europes-digital-strategy>
- Zakaria, F. (2020). When it comes to the Internet, Trump prefers the Chinese model. *The Washington Post*, 7-08-2020.
https://www.washingtonpost.com/opinions/when-it-comes-to-the-internet-trump-prefers-the-chinese-model/2020/08/06/a9298236-d823-11ea-9c3b-dfc394c03988_story.html

第二節 科技防疫的網路治理議題

一、新冠肺炎與網路治理

(一) COVID-19 與網路治理

新冠肺炎（COVID-19）造成全球疫情危機，公共衛生安全成為人們關注焦點。許多新的數位技術、數位政策不斷出爐，試圖從不同方向探尋可能的解決方案。隨著疫情爆發，數位流行病學也迅速崛起，許多技術專家探索與利用 AI、大數據，及其他新興技術來預測、監控及預防疫情惡化衝擊。世界衛生組織（WHO）和全球其他衛生組織因應新冠肺炎疫情也加速數位化工作。瑞士的日內瓦網路平臺（Geneva Internet Platform, GIP）將 COVID-19 與數位政策相關議題歸納如下圖 5 的不同構面，包含基礎設施、發展、人權、社會文化、經濟、網路安全及法律構面（Digital Watch, 2020）。



資料來源：GIP

圖5. COVID-19 爆發的數位政策議題

（二）非藥物管制措施與我國科技防疫措施

COVID-19 疫情發展迅速，在尚無疫苗藥物的情況下，各國被迫於短時間內提出如下表 7 所示的各項非藥物管制措施（Non-Pharmaceutical Interventions, NPIs）來因應疫情的衝擊，包含政府宣布緊急狀態、教育宣導、偵測與隔離病毒、去除污染源、整備醫療資源、維持社交距離、經濟因應方案、旅遊限制、關閉學校與聚會場所等。當中各國尚未執行的以紅色區域呈現，已執行的以綠色區域呈現。

以臺灣、中國大陸、新加坡、韓國為例，初期 NPIs 措施導入時間較早，病毒防疫能及早因應，包含政府疾管單位啟動協調機制；教育方面提供宣導；隔離措施包含發熱隔離、居家隔離等。而相較於亞洲國家，美國未能及時推動早期 NPIs，造成疫情快速散播。由於疫情過度嚴重，後期應避免的 NPIs 又無法有效防疫，所以，政府不得不採取高密度措施，如關閉學校、餐廳、交通等，致使整體社會因疫情造成重大損害。

我國在疫情初期即超前部署並運用科技防疫，包括在偵測隔離方面有納入旅客入境健康聲明的「入境檢疫系統」、彙整入境相關資料的「防疫追蹤系統」、透過電信定位訊號協助落實居家隔離和檢疫的「電子圍籬智慧監控系統」、結合健保資訊以追蹤旅遊史的「即時警示系統」；以及在醫療資源方面也有同樣運用健保資訊及健保 IC 卡支援「口罩實名制」等措施。因此，我國防疫成功經驗也成為全球焦點，至少有 10 國與我政府洽談整套大數據與 AI 防疫的技術移轉（衛福部疾管署，2020）。

網際網路成為疫情期間各國社會運作不可或缺的基礎建設，網路治理也因此受到疫情衝擊所影響，層面包含網路安全、網路發展、法律與人權、數位技術、資訊社會，以及數位經濟等構面，將分別於下列章節分析與探討。

表7. COVID-19 各國非藥物管制措施

COVID-19 各國非藥物措施 (Non-Pharmaceutical Interventions, NPIs)		台灣	中國	新加坡	韓國	義大利	西班牙	法國	美國	英國
非藥物措施 (Non-Pharmaceutical Interventions, NPIs)										
政府	政府疾病管制中心CDC協調	○	○	○	○	○			X	○
	宣告國家緊急狀態		○		○	○	○	○	○	○
	提供匿名細部資料以避免公眾臆測			○	○	X			X	
教育	提供個人非藥物措施的教育宣導	○	○		○	○	○		○	○
偵測與隔離	密集檢測	○	○	○	○	○	○		X	○
	補充的檢測方法	○	○	○	○	○	○		X	○
	監視系統 (所有可疑的死亡或患病個案)		○	○	○	○			X	○
	免下車檢測站			○	○	X			X	○
	行動app追蹤交流	○			○	X			X	X
	嚴格之聯絡人追蹤	○		○	○	X			X	X
	溫度與健康檢查(機場、車站等)	○	○	○	○	○	○		○	○
	大規模發熱檢查 (溫度掃描)	○	○	○	○	○	○		X	○
	個案隔離	○	○	○	○	○	○	○	○	○
	家庭檢疫	○	○		○	○	○	○	X	○
去除污染	可疑個案居家隔离	○	○		○	○	○	○	○	○
	可疑個案居家檢疫	○	○		○	○	○	○	○	○
醫療資源	消毒 (大眾運輸、街道等)	○	○			X			X	X
	危險廢棄物管理									
醫療資源	緊急醫療病床供給量	○	○			X	X		X	X
	提供供給品(肥皂、消毒劑、口罩等)	○		○	○	X	X		X	X
	提供專業醫護人員額外津貼補助	○	○						X	X
	招募志工(醫學院學生)	○				○	○		○	X
社交距離與案件隔離	年長者及其他高風險病患之社交距離	○	○		○	○	○	○	○	○
	自願居家檢疫	○	○		○	○	○	○	○	○
	高風險鄰居隔離		○		○	○	○	○	X	X
	基於檢疫隔離需求撤離城市		○		X	○	○	○	X	X
	返國居民或持長期居留身份者之檢疫隔離	○	○	○	X	○	○		X	X
經濟	緩繳所得稅或帳單以避免需外出工作	○			X		○		○	X
	居家檢疫隔離補助方案	○		○					X	X
	延長呼吸器病患之病假			○		○			X	X
旅行禁止	停止非必要之國際旅行	○	X		X	○	○	○	X	○
	特定國家旅客入境管制	○	○	○	○	○	○	○	○	○
	封閉邊境	X	X	X	X	○	○	○	X	○
	封閉城市	X	○		X	○	○		X	X
關閉	關閉公立學校	X	X	X	X	○	○		X	○
	關閉私立學校與大學	X	○		X	○	○	○	○	X
	關閉寺廟、教會等宗教聚會場所	X			X	○	○	○	X	X
	關閉餐廳及社交場所	X			X	○	○	○	X	X
	禁止超過 250 人之集會	○(室內)	○		○	○	○	○	○	○
	禁止超過 50 人之集會	X			X	○	○	○	X	○
	關閉所有非必需之商業活動	X	X		X	○	○	○	X	X

source: Matt Bell, Elena Baillie, Genevieve Gee, Tomas Pueyo; revised by Dr. Kenny Huang

儘早實施

初期執行失敗

執行不足

應避免發生

被迫實施

最終付出代價

二、網路安全

（一）網路犯罪

網路安全沒有真空期，網路犯罪分子利用 COVID-19 疫情流行期間的混亂試圖從中獲利，金融產業特別是網路攻擊的首要對象之一。歐洲央行對金融機構提出警訊，銀行需要對疫情期間增加的網路攻擊做好準備（Barreira, 2020）。

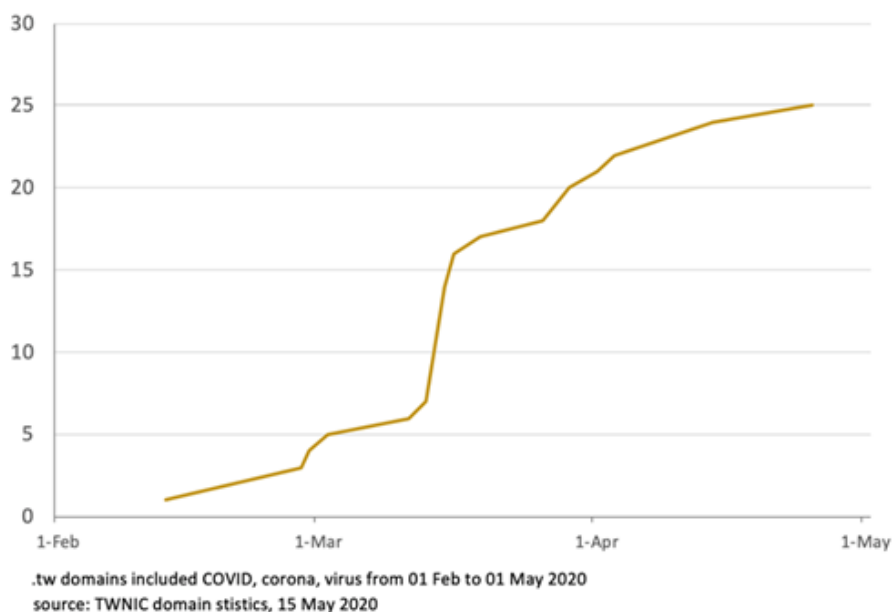
歐洲央行（European Central Bank, ECB）致函歐洲金融機構需訂定緊急應變計畫以因應病毒大流行的影響，包含員工無法上班或患病危及公司營運。歐洲央行監事會主席 Andrea Enria 表示如果員工無法執行日常任務，在受災地區的銀行運營能力將會受到挑戰（Shaun Lintern, 2020）。

除了潛在網路攻擊增加外，客戶與銀行間網路安全相關的詐欺行為與風險也同時增加，尤其是利用網路釣魚電子郵件等方式。在疫情流行階段，銀行員工採遠距在家工作模式也大幅度加重銀行資訊系統的壓力。遠距工作者可能使用開放與不安全網路，致使受到網路犯罪分子攻擊的風險很高。在家工作對員工而言可能更方便，但對於遠距提供之服務和資料而言並不安全，尤其是處理敏感個人資料面臨的網路安全威脅較高，因為遠距工作並沒有透過安全的工作場所網路連接，這些開放性網路沒有足夠的安全措施，例如 Web 過濾、防火牆或資料加密措施。事實上如果使用不安全網路來接取敏感資料，這種連線可能會被攔截，或資料被擷取及破壞。

世界衛生組織（World Health Organization, WHO）表示，網路犯罪者利用新冠肺炎病毒緊急情況發送釣魚郵件或 WhatsApp 信息，誘使閱讀者點選信件惡意網站連結或打開附件檔案。閱讀者依照此操作可能導引揭露個人帳號及密碼，犯罪者再利用獲取之帳號密碼資訊來竊取個人金錢或機敏訊息（WHO, 2020）。

（二）對域名的影響

台灣網路資訊中心（Taiwan Network Information Center, TWNIC）為評估 COVID-19 疫情對網域名稱的影響，收集 2020 年 2 月 1 日至 5 月 1 日期間新註冊域名，分析網域名稱包含 COVID、CORONA、及 VIRUS 三組字串。經過統計結果，在量測週期內包含此三個字串的新註冊網域名稱總計有 25 組。其註冊時間與累計註冊數量參考下圖（TWNIC, 2020）。



資料來源：TWNIC

圖6. 網域名稱含 COVID、CORONA、及 VIRUS 字串累計註冊量

同一時間內 TWNIC 資料庫全體新註冊網域名稱數量為 11,313 組域名，表示具有 COVID 三組字串域名僅佔同時期新註冊網域名稱的 0.22%。

TWNIC 量測註冊域名之網站回應資訊。經過量測正確回應網站內容者有五組，即是僅 20%註冊域名之網站可正確回應網頁查詢請求。網站回應此為域名保護訊息有 9 組，無法正常接取網頁有 4 組，回應網站建置中有 2 組，回應域名出售中有 2 組，DNS 設定錯誤有 1 組（TWNIC, 2020）。

今日網路世界無法杜絕網路安全與網路犯罪行為，所有公私部門都共同面臨網路安全威脅。尤其在疫情期間，以病毒為名進行各類網路犯罪行為不斷增加，企業採取遠距在家工作模式對網路安全威脅更加嚴峻。所有人都應該共同合作打擊網路犯罪，各機構都需要訂定緊急應變計畫，讓所

有員工了解可能面臨的資安威脅，並且了解網路安全不再是資安工程師的責任，而是所有員工都必須共同面對的問題與承擔的責任。

三、網路發展

（一）對網路流量的影響

COVID-19 疫情期間各國採取在家上學或在家工作措施，使網路整體通訊量增加。隨著越來越多的企業和學校在家工作或上學，電信業者必須擴充網路來承載增加的流量。許多企業受疫情衝擊無法繼續營業造成失業人口增加。失業者無法外出工作，缺乏收入支付生活的支出。疫情期間網路是不可或缺的服務，有基於此，電信業者也提出紓困措施，以減少失業者使用網路的負擔。

美國聯邦通訊傳播委員會（FCC）與電信業者共同推動「保持美國人連網誓約（Keep Americans Connected Pledge）」（FCC, 2020）。CenturyLink 電信公司是參與保持美國人連網誓約的公司之一，CenturyLink 公司在疫情期間提出延長免收滯納金的承諾，CenturyLink 承諾在 2020 年 6 月 30 日前不會切斷無法支付電信費用的住宅區用戶或小型企業用戶的網路連線，同時取消住宅區用戶及小型企業用戶網路流量上限直到 2020 年 8 月 1 日為止。此外，CenturyLink 特別為符合條件的用戶訂定新的付款計畫，讓用戶有較長時間來分期支付未繳納的帳單（CenturyLink, 2020）。

美國 Cloudflare 公司表示在 2020 年一月到三月之間，美國各主要城市的網路增加約四分之一流量，許多網路服務需求增加特別明顯。如視訊會議軟體、視訊電話服務。多數人被限制留在家中，家庭娛樂服務網路流量大量增加，電腦遊戲商店 Steam 曾經高達 2400 萬玩家在同一時間上線，由於平台無法支撐流量激增，許多準備參與的玩家必須在虛擬隊伍中等候數小時以遊戲競賽（Cloudflare, 2020）。

全球網路因為疫情使得流量攀升到歷史最高點，許多人好奇全球網路

是否有能力負擔因疫情所激增的訊務？許多資料顯示，使用者可能偶爾經歷網路速度變慢、或少部分網站速度稍慢、或少部分網路電話中斷，整體而言，網路仍維持相當好的品質。在 COVID-19 疫情激勵下，全球網路正產生前所未見的擴充與成長。威斯康辛大學 Paul Barford 教授負責一項網路 Mapping 計畫，他表示當使用者使用網路越多，就更加關注網路產生的小障礙，網路在部分地區也會發生些許局部故障，但影響範圍不大，這就是網路分散式網路系統的優點（Heaven, 2020）。

（二）對網路串流服務的影響

除了網路流量受到疫情影響外，使用者的網路使用行為也發生改變，尤其是因居家管制而激增的網路媒體串流服務。激增的媒體串流服務雖不會造成全球網路癱瘓，但間接影響整體網路使用品質。Sandvine 公司分析，全球網路流量已有超過一半以上是網路媒體串流服務（Sandvine, 2020）。為保障遠距上班工作者所必須的網路品質，歐盟與 Netflix、Youtube、Facebook 及新推出的 Disney+ 等眾多媒體串流公司協商，這些媒體串流平台同意降低媒體串流的影像品質，以減緩串流影像造成 Internet 整體運作壓力。另外，網路遊戲包含 Sony、Microsoft、Value 也降低網路影像遊戲更新頻率，或遊戲軟體更新限制在非高峰時段進行。



資料來源：Sandvine

圖7. COVID-19 對全球網路服務的影響

COVID-19 除了增加網路流量外，流量來源也更加分散，網路公司不得不處理同時來自多地點的流量。例如，當 Dropbox 服務連接到一個大學或一間辦公大樓，Dropbox 可以輕鬆管理數千個用戶。當成千上萬的用戶遍佈全球並且以高速網路連接時，Dropbox 必須耗費更多資源來處理不同來源的訊務請求。

儘管網路仍持續有一些小問題發生，全球網路表現仍相當優異。歐洲網路協調中心（Réseaux IP Européens Network Coordination Centre, RIPE NCC）觀察全球各地網路連接速度顯示，雖然網路速度略有降低，但總體變化不大（Speedtest, 2020）。媒體串流平台 Netflix 或 Youtube 雖降低媒體串流影像品質，但這並不表示全球 Internet 無法承載串流訊務，而是網路平台公司基於全球網路良善治理理念而採取自願性降速措施。

四、法律與人權

COVID-19 疫情威脅生命與經濟，各國政府因應疫情需求修訂或執行相關法律。各國政府在打擊病毒方面運用法律與憲法權力在程度上有很大差異。2020 年 3 月匈牙利議會通過 Orban 獨裁權力法（Spectrum, 2020），允許 Orban 總理有權中止任何法律的執行，並有權制止宣傳不實信息干擾公共秩序者。違反隔離命令者將受到長期監禁罪罰，更令人不安的是，這些基於緊急狀態賦予政府特殊權力並沒有訂定終止期限。

絕大多數現代憲法允許國家在緊急狀態採取特殊措施，但這種巨大特殊權力如果缺乏監督機制很有可能造成濫用，領導者可以發動緊急狀態獲得特殊權力規避國會對政府權力審查機制。只要政府提出 COVID-19 必要措施，由於公眾恐慌心態，幾乎所有人都願意放棄憲法賦予公民權利配合政府管制措施。涉及憲法的問題是：由誰決定國家進入緊急狀態，以及採取何種措施及何種監督機制。

緊急狀態另一個特徵是時間有限，只要緊急狀態結束，國家立即恢復

常態。某些國家或地方政府利用手機追蹤人民的位置以強制執行居家命令。以美國為例，在加州執行這樣的措施必須取得搜索票，德州則不需要取得搜索票。當各州都實施相關措施造成公共安全與隱私衝突時，就交由法院處理相關爭議。COVID-19 管制措施還包含影響公民其他權利行使，例如集會人數限制 10 人之內則違反公民集會自由權。在緊急狀態，法院會尊重行政機關的作為，但當緊急措施時間延長時，也將牽動法院對行政機關行為的判斷。

以色列憲法要求立法機關批准行政機關宣布緊急狀態，並定期更新緊急狀態情況。緊急命令措施甚至包含停止不必要法院程序，包含不起訴被告的刑事案件審判。儘管如此，最高法院仍持續運作並提供重要的審查。以色列是少數如新加坡、韓國、德國、與臺灣等國家利用手機追蹤感染者。以色列內閣通過一項行政命令，利用 Shin-bet 收集的大數據來隔離與感染者接觸的任何人。以色列最高法院判決此行政命令必須獲得立法授權與監督（Magid, 2020）。法院在緊急狀態具重要意義，它確保緊急命令遵循正當程序與具備充分監督機制。例如科索沃憲法法院駁回政府要求因疫情採取緊急狀態，憲法法院認為政府一般機構仍可繼續正常運作。義大利即便疫情導致相當高的致死率，法院及議會仍持續運作與開放。

許多民主制度具備有效工具來對抗病毒，並且不會讓民主制度陷於危險之中。某些國家的法院也發揮積極作用，確保防疫措施遵守法律程序。相反地，公眾卻普遍願意遵守政府對其基本自由的侵犯。當時間隨著疫情擴散而延長，當政府限制措施變得更加繁重，治理框架可能與疾病類似，它可能必須變得更糟之後才能變得更好。

五、數位技術

（一）人工智慧

AI 技術無疑是新冠肺炎 COVID-19 疫情爆發以來最受到關注的技術之

一，許多科技公司、醫療機構、研究機構都對 AI 應用於疫情控制充滿期待。以中國科技公司為例，阿里巴巴、百度和騰訊-免費開放研究人員使用他們的 AI 和雲端運算技術，希望加速新藥和疫苗的研發。阿里巴巴的阿里雲服務免費提供雲端運算技術以用於病毒基因測序，蛋白質篩選和其他研究工作，幫助研究機構免費研究 COVID-19 的潛在治療方法（Henan, 2020）。

阿里雲並與全球健康藥物研發中心（Global Health Drug Discovery Institute, GHDDI）合作研究以 AI 為基礎的藥物研發和大數據平台，此平台將分析整合其它冠狀病毒如 SARS（嚴重急性呼吸道症候群）、MERS（中東呼吸症候群冠狀病毒感染症）病毒歷史醫學資訊，作為為新冠肺炎研究。

中國百度公司免費提供防疫中心，基因檢測機構和全球研究機構其 LinearFoldAI 演算法，它可將病毒基因組二級結構的預測速度提高 120 倍，提升研究效率以更快尋求病毒解決方法。騰訊公司則與北京清華大學、廣東中山大學研究團隊合作提供免費雲端運算解決方案。

WHO 發布新冠肺炎警報的幾天前，加拿大的 BludDot 已經提出新冠肺炎的警報。BlueDot 是加拿大一家從事 AI 研究公司，BlueDot 的 AI 演算法每天可處理 65 種語言、100,000 條新聞文章的大量非結構化資料。它的巨量資料包含動物疾病、溫度與氣候資訊等所有有助於預測病毒傳播方式的資料（Prosser, 2020）

AI 也有助於新冠肺炎的治療，英國帝國學院與 BenevolentAI 公司合作，使用 AI 軟體找到一種現有已批准藥物，可能可限制病毒對人體的感染能力（Lemonick, 2020）。利用 AI 技術可以節省藥物研究人員的時間與資源，加強人員能力，使用現有的醫療數據進行分析。解決迫切的公共衛生問題而不需要重新部署整個公衛團隊，AI 技術的應用對於研究工作者產生很大的助益。

AI技術雖然令人期待，但是它也可能產出令人失望的結果，尤其是AI數量模型並不了解所有因素。AI是真實狀況的模擬（AI-powered simulation），輸入AI神經網路的數據與條件隨時在改變，可能導致計算後結果產生大幅度變化。以COVID-19疫情模型為例，傳播率、死亡率等參數細微的改變，都可導致全球總死亡率產生重大變化。儘管科學家嘗試使用AI或神經網路來解決或預測疫情，但無可避免地必須增加其他變數來微調模型，否則會嚴重影響預測的可信度。

（二）大數據

新冠肺炎疫情爆發後，從預警識別、疫情監測及風險評估，大量資料收集與分析一直都是決策的首要任務。尤其是AI公司BlueDot將預警資訊提供給WHO後，社會更加關注疫情資料收集。資料收集能夠預測與識別流行病毒，醫療中心可以根據患者地理位置與感染情況的資料建立傳染病監測大數據資料庫，這樣的大數據資料庫可以協助政府識別疫情散播情況。約翰霍普金斯大學系統科學與工程中心（CSSE）開發了病毒疫情監測系統（CSSE, 2020）即是重要的大數據資料庫，其大數據來源包含世界衛生組織WHO、疾病控制中心、各國衛生主管機關等巨量資料，建立疫情地圖情資系統以供研究人員使用。

COVID-19疫情爆發後，疫情資料共享的呼籲和倡議也逐漸產生。WHO邀請成員國衛生部長提升新冠肺炎的資料共享措施。學術界和私部門也參與資料共享，如美國哈佛醫學院和風險分析公司Metabiota將COVID-19相關資料於Github平台分享（McDonnell, 2020）。

（三）區塊鏈

區塊鏈技術也是受人關注的因應COVID-19數位技術。在疫情大流行期間，資金不斷投入來強化公共衛生系統或購置個人防護設備，政府投入大量資金於醫療準備、物資與支援系統。大量採購情況下對設備的價格、

品質、技術與來源驗證形成很大的挑戰。同一時間，數千萬人失去工作與收入，許多國家啟動相關補助計畫，在被封鎖與旅行限制期間提供個人補助支援。資金濫用、設備定價過高、假冒商品所造成的腐敗風險幾乎難以避免，區塊鏈技術成為這種情境下適當的技術工具。

區塊鏈技術可以記錄和追蹤流行病的所有捐款，並提供所有利害關係人資訊所需求的透明度。適合使用區塊鏈場域包含醫療供應鏈管理、加密醫療紀錄工具、聯絡人追蹤軟體等。在醫療供應鏈管理方面，醫院可部署區塊鏈技術來確保醫療設備的品質與來源。區塊鏈技術具有不可變更與訊息加密的特性，可以作為保存與共享醫療紀錄的工具。區塊鏈可應用於聯絡人追蹤應用軟體，當手機用戶與病毒感染者近距離接觸，系統產生通知以儘速採取正確的保護措施。當政府或捐助者採用區塊鏈技術於資金補助計畫，區塊鏈技術具防篡改交易紀錄、提供資料透明度，這些是防止貪腐並對利害關係人重要的屬性。決策者需要熟悉區塊鏈核心功能，才有能力做出明智決定，了解何時何地使用區塊鏈工具。數位基礎設施、使用者數位素養、法律制度及社會政治環境等因素都是構成區塊鏈服務是否可以成功的重要因素。

六、資訊社會

疫情大流行迫使全球多數企業將辦公場所從公司遷移到家中（Work From Home, WFH），企業在疫情流行期間比過去任何時候都更加依賴遠距工作工具來保持企業業務不中斷。對許多公司而言，這是員工首次持續密集地使用數位技術進行業務的虛擬協作、經營業務與商業交流。

在全球疫情仍不斷發展，許多人已經為未來可能演變之社會型態超前部署（Parungao, 2020）。以遠距在家工作為例，它是企業因應疫情採取的臨時應變措施，但實施的結果卻出乎預料的受到許多企業與員工歡迎。許多公司認為從辦公室上班移轉為在家工作很可能是永久的改變，而不是暫時性的改變。事實上，全球研究公司 Gartner 與 317 位首席財務長和企業財

務負責人進行一項調查發現（Gartner, 2020），74%的公司計畫在疫情結束後將部分員工職缺轉換為永久性在家工作職缺。促成這永久改變的最大因素是在家工作可節省公司成本，這是所有企業在本次疫情中意外發現的事實。員工減少停留辦公室可降低企業技術支援成本，降低租賃辦公室租金支出，同時為員工帶來經濟利益。網路招募平台 FlexJobs 研究發現，遠距在家工作的員工每年可節省超過 4000 美元支出（Pelta, 2020），包含通勤交通費用、辦公室用餐費用及其他雜項支出等。綜合這些因素，即使疫情結束，沒有太多理由讓企業運作完全回復到傳統的工作模式。

COVID-19 的發展也促使數位技術發揮重要作用，企業依賴數位技術使得員工即便在不同地點上班，員工的工作仍可無縫接軌地執行。虛擬工作場所解決方案的需求大幅度增加，幫助員工達成遠距工作協作、交流和業務執行。辦公室會議逐漸改變為電話視訊會議、辦公空間改變為工作管理系統、業務流程改變為工作資訊流程，越來越多人感受到工作改變為虛擬線上程序所帶來的效率、便利與透明。

員工過去在公司社交場所聊天的場景同樣可以被網路虛擬服務所取代，例如即時通訊軟體。今日數位技術幾乎可以完全取代在傳統辦公室執行的工作，企業有了 COVID-19 與數位技術實際運作經驗後，會更確認數位科技是長期解決方案與工作方法，並將它視為企業運作的新常態（New Normal）。

部分在家上班者考量家中其他干擾因素，因而選擇通勤至公司上班。紐約時報指出許多公司採用混合模式，例如團隊 A 及團隊 B 分別在不同天到公司上班（Miller, 2020）。企業可以規劃適合自己的遠距工作策略，在人員分散式工作架構下，維持健全的工作文化及有效率的產出。當企業遠距策略超越防疫需求，企業仍可善用此過程所學習的經驗與知識，持續回饋與提升企業未來遠距策略。

七、數位經濟

新冠肺炎疫情危機將全球經濟加速朝數位經濟推進，當經濟開始復甦時，病毒流行後對經濟的改變可能會產生持久影響。但並不是所有人及所有企業都準備好接受數位經濟的衝擊。

2020 年 4 月聯合國數位貿易發展會議（United Nations Conference on Trade and Development）報告指出，新冠肺炎加速數位解決方案產出、數位工具與服務的使用，且加速全球數位經濟推動的速度。雖然如此，但疫情迅速數位發展也擴大不同地區、不同國家的數位落差（UNCTAD, 2020）。

數位落差的不平等現象妨礙了全球多數地區使用數位技術的能力，這些技術可以協助人們在家中因應疫情。在大流行期間，越來越多企業與政府將業務與服務轉移到網際網路，透過實體隔離來遏制病毒的傳播。隨著消費者在疫情期間的娛樂、購物和改用網路視訊方式接觸，網路數位平臺也蓬勃發展。數位化發展使得遠距醫療、在家上班、遠距教學需求激增，這包含病毒擴展的更新資訊、研究者透過相關資訊交流進行公衛研究

在家上班與遠距教學等型態擴大網路即時通訊軟體的需求，例如 Microsoft Teams、Skype、Cisco Webex 和 Zoom 等即時通訊軟體。微軟表示，使用 Microsoft Teams 軟體的使用者在一週內上升了將近 40%（New York Times, 2020）。科技公司利用 AI 尋找病毒治癒方式，電子商務在疫情期間快速成長，許多企業更積極的利用電子商務平臺提供產品或服務。

然而，並非所有科技公司都因全球加速數位化而獲利，大量使用者湧向大型網路平臺也會帶來嚴重後果。例如惡化的網路安全及隱私問題、網路服務平臺更加集中化與寡占化、全球的數位落差日益嚴重。聯合國 2019 年數位經濟報告顯示，全球排名前 7 大的數位平臺已經佔全球數位平臺價值的三分之二（UNCTAD, 2019）。大型數位平臺受益於網路效應，他們提取、控制、分析使用者數據，並具備用戶資料商品化的能力。

隨著越來越多的人上網時間增加或被迫上網，全球數位落差情況也越來越嚴重，尤其是開發中國家。缺乏數位化資源或數位化能力的國家在數

位轉型過程可能面臨落差擴大的危機。最不發達國家（least developed countries, LDCs）的生命與經濟受到病毒疫情衝擊最大，在數位化準備度方面也最落後。最不發達國家只有 20%人口連接網際網路。

缺乏網路接取能力可能也限制其他領域的發展。例如學校關閉，無法上網可能導致教育差距擴大，社會不平等情況更為惡化。行動上網費用對開發中國家仍是昂貴支出，不良網路品質可能限制利用網路會議工具的能力。另一方面，疫情也迫使政府與企業更積極探索電子商務與新興數位化解決方案，這些新興數位化解決方案將有助於社會因應未來挑戰與衝擊。政府也應持續檢視新的政策與法規，確保數位轉型產生的效益可以公平分配。從數位經濟發展方面，COVID-19 與其他可能的挑戰一樣，政府與企業應積極探索可行數位化解決方案並消彌數位落差，共同因應數位轉型的挑戰。

八、結論與建議

COVID-19 對全球造成巨大衝擊，在此次危機中分析網路治理議題，可以從社會如何因應以及如何使用網路等方面，吸取教訓與經驗。這些經驗可能有助於我們面對未來的危機，即使在正常情況下，這些經驗可能也會影響我們的工作和互動方式。長期來看，這些經驗有助於我們發展更包容性的治理方法來應對網路治理的挑戰。

因應 COVID-19 所實行的措施可視為有史以來最大規模的實驗，而網路本身對於這些措施具有無可取代的重要性，甚至可說網路對於當今社會的重要性，獲得更廣泛的認可與理解。網路基礎設施與網路數位技術在疫情階段經歷了高速的發展。當全球開始進行封鎖，人們面臨的第一道課題就是如何使用網路來確保企業的持續運作、延續學生的課程學習。而除了使用網路來延續服務，另一方面也要保障網路安全，防止更多利用疫情的不實資訊進行網路駭侵行為。

在疫情階段最令人驚訝的是視訊會議技術的普及性。雖然視訊會議技術已有多年的發展，但企業從未認為視訊會議具有實體會議的可行性，尤其是面對面討論一直是傳統工作模式的一環。在疫情與社交距離管制措施下，大規模與高密度的視訊會議已成為防疫的必要措施。實施的結果也讓所有人肯定視訊會議的普及與可行性。

我國因為超前部署且運用數位科技成功阻止疫情蔓延，而成為全球的防疫模範。然而，這並不代表我國的科技防疫相關政策或法規制度已經完備，因此，本計畫從網路治理角度提供以下建議：

(一) 我科技防疫有成社會正常運作，但仍須加速數位轉型與數位包容

我國因為防疫成效良好，非藥物管制措施相較其他國家輕微，社會得以正常運作，公私部門和學校等機構對於數位工具的需求不若國外迫切與必要，遠距視訊服務沒有產生突發性成長。然而，正如我國因為歷經 2003 年 SARS 重創而能於 COVID-19 超前部署，或是韓國因為 1997 年亞洲金融風暴破產而勵精圖治成為科技和文化產品的輸出強國，此波疫情也被視為是各國加速推動數位轉型的一大契機，我國反而缺乏利用數位遠距工具完全取代實體業務運作的實務經驗。因此，在持續進行防疫工作的同時，我國需要全面強化數位社會發展，避免數位化進程反而相對落後。而這當中也包含需正視數位包容問題，許多研究發現重大疫情擴大社會健康的不平等和數位落差，所以，政府規劃實體和網路防疫資源時，應優先考量弱勢和年長族群，並以無障礙環境思維進行政策規劃，確保他們能夠取得必要的資訊與服務。

(二) 檢討改善科技防疫相關法規措施，建立社會信任以延續防疫成效

資訊可說是此次科技防疫最重要的資源及決策依據，過程中不論是疫情的通報、調查、監視、預警，其實都是在蒐集使用民眾的個資，因此，也出現許多個資相關的治理問題。例如雖然政府要求各機關防疫時須落實

《個人資料保護法》，但我國個資法對於「為增進公共利益所必要」賦予很大的授權空間，且《嚴重特殊傳染性肺炎防治及紓困振興特別條例》對於「中央流行疫情指揮中心指揮官」也賦予很大的行政權力；相較於歐盟對於是否符合公共利益是由個資專責機關認定，就我國現行制度可能是由疫情指揮中心全權決定，因此，產生過度空白授權的疑慮。又如疫情指揮中心也推動《實聯制措施指引》，但因缺乏後續的監督稽核機制，發生許多商家過度蒐集個資等情況。此外，政府授權超商接受健保卡購買振興三倍券，也引發不符合任何醫療和公衛使用目的等質疑（衛福部疾管署，2020；李崇僖，2020；中央社，2020）。

在疫情爆發的緊急狀態下，社會大眾會因為防疫的急迫性而同意政府蒐集較多個資，但在非緊急狀態時，資料保護措施應趨於嚴謹，民眾才能信任防疫制度並願意持續配合。因此，我國應檢討改善科技防疫的相關法規和措施，以法制建立社會信任，才能讓科技防疫的成效得以延續。

（三）網路治理重要性提升，鼓勵更多利害關係人參與

疫情之後我們認知的暫時性措施很可能會成為一個常態持續性的生活方式，社會進入一個未知的「新常態」，這些都將構成社會或商業的新挑戰。例如企業有更豐富的視訊遠距會議經驗後，可能對員工差旅有更多限制，或是不願支出更多差旅費用等。COVID-19 已經驗證現在社會需要高度依賴網路，這種依賴程度使得網路治理比起過去任何時候都更加重要。因此，我國應該鼓勵更多利害關係人參與網路治理、提升良善治理成效，讓網路治理可以更敏捷地適應後疫情社會的「新常態」。

九、參考文獻

- 中央社 (2020)。防疫實聯制被刷身分證 蒐集個資亂象多。聯合新聞網，2020-06-14。 <https://udn.com/news/story/120940/4634970>。
- 李崇僖 (2020)。專題演講 1：科技防疫與隱私保護。台灣網路講堂，

2020-06-02。 <https://www.ihub.tw/highlights/20200602>

- 衛福部疾管署 (2020)。建立健康安全防護網，持續優化科技智慧防疫。新聞稿，2020-06-01。
https://www.cdc.gov.tw/Bulletin/Detail/Mtrg60_RrPSBQP4kuO_snQ?typeid=9
- Barreira, V. M. (2020). ECB testing banks ability to deal with the second wave of COVID-19. CentralBank.com
- CenturyLink. (2020). How is CenturyLink supporting customers that are impacted by COVID-19. COVID-19 Support, CenturyLink News.
- Cloudflare. (2020). How has the coronavirus pandemic impacted Internet traffic. From <https://www.cloudflare.com/builtforthis/insights/>
- CSSE. (2020). COVID-19 Dashboard. From <https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6>
- Digital Watch. (Mar 2020). The COVID-19 crisis: A digital policy overview. Geneva Internet Platform. From <https://dig.watch/trends/covid-19-crisis-digital-policy-overview>
- FCC. (2020). Keep Americans Connected Pledge. FCC. From <https://www.fcc.gov/keep-americans-connected>
- Gartner. (Apr 3 2020). Gartner CFO survey reveals 74% intend to shift some employees to remote work permanently. Gartner news room. From <https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2>
- Heaven, W. D. (Apr 07 2020). Why the coronavirus lockdown is making the Internet stronger than ever. MIT Technology Review.
- Henan, S. (Jan 31 2020). Chinese tech giants open cloud computing to

researches amid coronavirus emergency. KrASIA media company.

- Lemonick, S. (Feb 04 2020). Two groups use Artificial Intelligence to find compounds that could fight the novel coronavirus. Computational Chemistry Volume 98 Issue 6.
- Lintern, S. (Mar 03 2020). Coronavirus: UK officials told to create extra mortuary space as government warns of surge in deaths. The Independent news & media, UK.
- Magid, J. (Mar 25 2020). High court lets Shin Bet continue phone tracking now Knesset oversight in place. The Times of Israel.
- McDonnell, T. (Feb 01 2020). Coronavirus is a proving ground for scientific transparency. Quartz Media. From <https://qz.com/1795103/coronavirus-is-a-proving-ground-for-scientific-transparency/>
- Miller, C.C. (Jul 2 2020). Is the five days office week over. New York Times.
- New York Times. (Mar 23 2020). Big Tech could emerge from coronavirus crisis stronger than ever. New York Times.
- Parungao, A. (2020). The future of remote work after COVID-19. From <https://www.ekoapp.com/blog/the-future-of-remote-work-after-covid-19-3-common-predictions>
- Pelta, R. (Jun 25 2020). 6 Ways working from home will save you \$4000 or more annually. Flexjobs. From <https://www.flexjobs.com/blog/post/does-working-remotely-save-you-money/>
- Prosser, M. (Feb 05 2020). How AI helped predict the coronavirus outbreak before it happened. SingularityHub. From <https://singularityhub.com/2020/02/05/how-ai-helped-predict-the-coronavirus-outbreak-before-it-happened/>

- Sandvine. (2020). COVID-19 global Internet phenomena report highlight.
From <https://www.sandvine.com/phenomena>
- Spectrum, H. (2020). Kim Lane Scheppele: ORBAN’S Emergency.
Retrieved August 08 2020, from
<https://hungarianspectrum.org/2020/03/21/kim-lane-scheppele-orbans-emergency/>
- Speedtest (2020). Tracking COVID-19 impact to global Internet performance.
From
<https://www.speedtest.net/insights/blog/tracking-covid-19-impact-global-internet-performance/>
- TWNIC Blog (May 22 2020). 新冠病毒 COVID-19 對網域名稱之影響。
TWNIC BLOG。From <https://blog.twNIC.tw/2020/05/22/7227/>
- UNCTAD (2019). Digital Economy Report 2019. United Nations.
- UNCTAD (2020). The COVID-19 Crisis: Accentuating the need to bridge digital divides. United Nations.
- WHO (2020). Beware of criminals pretending to be WHO. World Health Organization. From
<https://www.who.int/about/communications/cyber-security>

第三節 聯合國數位合作藍圖的擘劃與挑戰

一、聯合國數位合作藍圖與宣言

（一）數位合作藍圖

聯合國秘書長古特瑞斯（Antonio Guterres）於 2020 年 6 月發布《數位合作藍圖》（Roadmap for Digital Cooperation），提出全球連網、數位公共財、數位包容、數位能力建構、數位人權、人工智慧（AI）、數位信賴與安全、數位合作等 8 項有賴全球共同採取行動的關鍵領域，以建立連結、尊重、保護所有人的數位時代。

古特瑞斯表示，數位科技讓我們在新冠肺炎疫情蔓延下，能夠運用科技抗疫，並以遠端方式維持社會運作，但同時也帶來威脅生命、破壞人權和隱私權的網路攻擊和假新聞散佈等危害。因此，我們正處於科技治理的關鍵時刻，如果現在大家不團結一起善用科技，我們將失去管理科技影響力的重大機會，且網路可能進一步分裂，這將損害所有人的利益。

《數位合作藍圖》源自古特瑞斯於 2018 年 7 月成立的「聯合國數位合作高階專家小組」（High-level Panel on Digital Cooperation, HLPDC），由蓋茲基金會創辦人 Melinda Gates 和阿里巴巴集團創辦人馬雲，共同領導來自不同專業領域、多方社群、地理區域、性別、年齡層的 20 位專家組成。HLPDC 於 2019 年 6 月發布《數位相依時代》（The Age of Digital Interdependence）報告供全球討論。而經彙整全球超過上百個回饋意見，以及主題專家的圓桌論壇建議後，古特瑞斯發布《數位合作藍圖》（UN, 2020；HLPDC, 2020）。

（二）數位合作宣言

數位合作還更進一步獲得聯合國 193 個會員國的承諾。聯合國第 75 屆大會於 2020 年 9 月 21 日通過《紀念聯合國成立 75 周年宣言》，當中的 12

項承諾即包括「加強數位合作」。此外，紀念宣言也強調聯合國是唯一擁有獨特合法性的全球組織，及實施多邊主義(Multilateralism)是毋庸置疑。

紀念宣言的 12 項全球性承諾為：不棄任何人於不顧、保護地球、促進和平、遵守國際法規、重視女性權益、促進信賴、加強數位合作、改造聯合國、確保持續財源、增進夥伴關係、與青年合作，以及為未來做好準備。當中**加強數位合作**的條文（第 13 條）如下：

我們將加強數位合作。數位科技深刻改變社會，帶來前所未有的機會和新挑戰，一旦遭到不當或惡意使用，就會助長國家內部和國家間的分歧、危害安全、侵犯人權、加劇不平等。打造數位合作和數位未來的共同願景、展現善用科技的全部潛力，並解決數位信賴和安全問題，仍是必須持續的優先事項，因為當前世界比任何時候都更加依賴數位工具來實現連結和社會經濟繁榮。數位科技具有加速實現 2030 年議程（指聯合國永續發展目標，簡稱 SDGs）的潛力，我們必須確保人人都能安全且無負擔地上網，而聯合國可以為所有關係人提供一個參與商議的平臺。

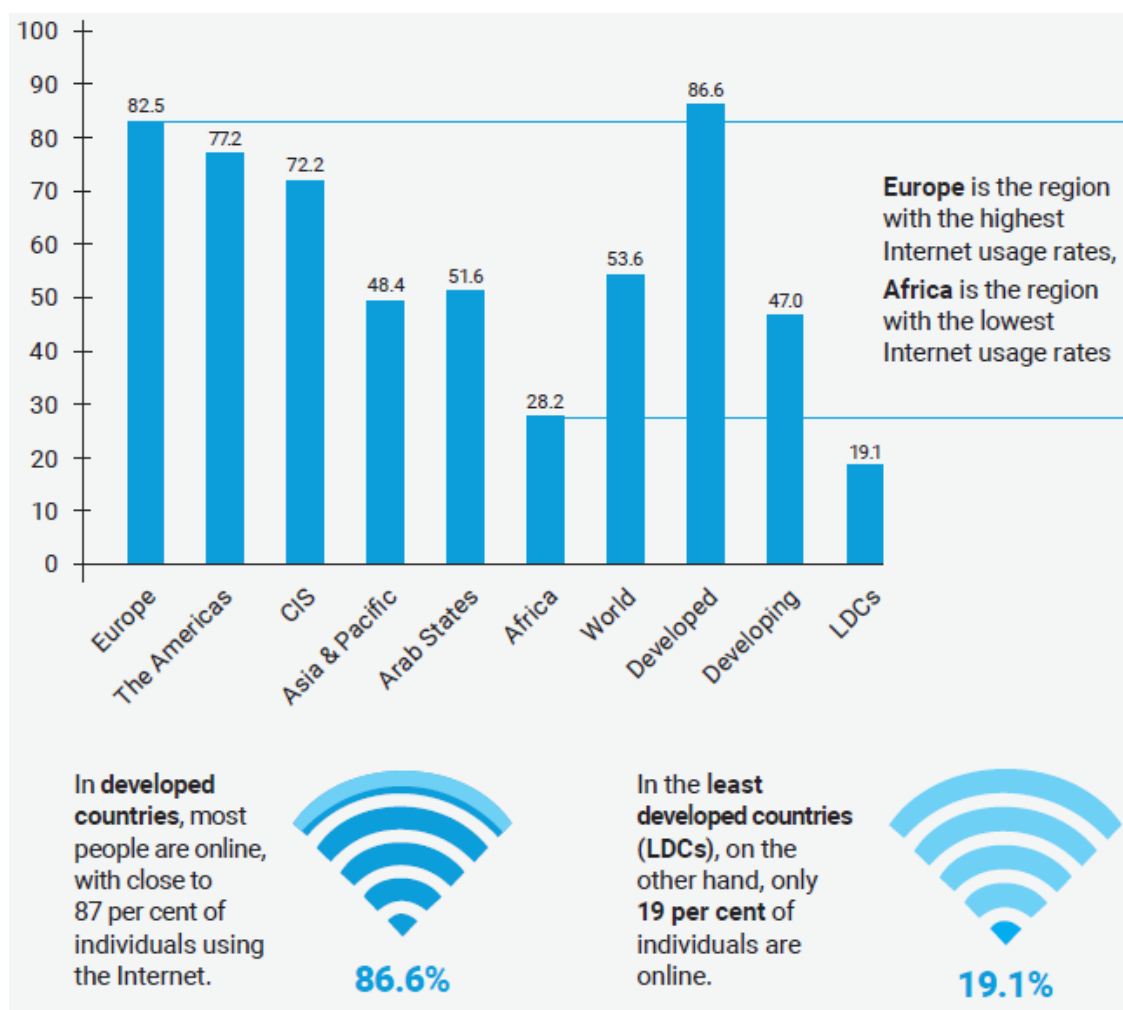
此外，紀念宣言還著墨於聯合國的地位和多邊主義。宣言指出「沒有任何其他全球性組織擁有聯合國的合法性、號召力、制訂規範的影響力（第 1 條）…我們面臨的挑戰是相連的且只有倚賴改善多邊主義才能因應…多邊主義不是一種選擇，而是我們建立一個更公平、強韌和永續世界的毋庸置疑，且聯合國必須成為全球努力的核心（第 5 條）」(UNGA 75, 2020)。

二、全球網路發展當前問題

根據《數位合作藍圖》引用「聯合國數位合作高階專家小組」的分析 (HLPDC, 2018)，目前全球網路發展面臨上網普及率偏低、數位公共財不足、數位落差顯著、數位能力建構未符合需求、數位科技遭濫用於侵犯人權、AI 治理缺乏國際協調、網路威脅不斷升高、數位合作未獲重視且缺乏成效等問題，相關重點簡述如下。

（一）上網普及率偏低

目前全球人口約 78 億，但上網普及率只有 53.3%，意即全球仍有 36 億人無法上網。以地理區域而言，上網普及率最高的是歐洲 82.5%，最低為非洲 28.2%；再就發展程度來看，已開發國家的上網普及率已達 86.6%，但最低度開發國家只有 19.1%（圖 8）。而導致全球數位落差的因素除了傳統寬頻的建置成本高昂、最低度開發國家的人民購買力薄弱無法吸引業者投資網路建設外，缺乏數位能力也會阻礙數位工具的採用。



資料來源：ITU 2019

圖8. 全球上網普及率（依地區和開發程度統計）

（二）數位公共財不足

利用大數據和 AI 創造出即時可行和前瞻性見解的數位公共財，對於達

成永續發展目標相當重要，例如可用於辨識新疾病的爆發、對抗假新聞、追蹤弱勢族群所承受的衝擊等。雖然網路開始是從具有開放資源精神的公共管理方式發展，但演變至今，開放資源和公共性的網路已降至很低的比例，數位解決方案的取得往往受限於著作權和財產權，即使仍存有部分的數位公共財，但也礙於語言、內容、基礎建設等障礙而無法取得或使用。

（三）數位落差顯著

數位落差不只反映而是更強化既有的社會、文化及經濟不平等。網路使用人口的性別落差就是最明顯的例子，世界上每 3 個國家中就有 2 個國家的男性網路使用率高於女性。此外，移民、難民、流離者、老人、年輕人、小孩、殘障人士、偏鄉民眾和原住民等，也都面臨相同的挑戰。COVID-19 的爆發凸顯數位工具已經成為數百萬人的生活命脈，因此，需要即時採取行動，彌補數位落差的鴻溝。

（四）數位能力建構未符合需求

研究顯示，非洲撒哈拉沙漠以南地區於 2030 年前可產生 2.3 億個數位工作，但這需要投入 6.5 億個訓練機會。有效的能力建構方式需要考量政治、經濟和社會環境的差異，甚至需要為各別國家和人民量身訂做方案。然而，目前大多數的數位能力建構計畫是以「供給」而非以「需求」為導向。此外，對數位能力建構的投資不足，也是長期面臨的問題。

（五）數位科技遭濫用於侵犯人權

數位科技日益被用於侵犯人權、深化不平等和強化既有的社會歧視。例如鎖定目標的通訊監控和臉部辨識軟體，可能導致任意逮捕和拘役人民；對特定少數族群的錯誤自動辨識，深化既有的社會偏見；女性、維權人士、同性戀等族群面臨持續性的線上騷擾或暴力和破壞名譽等威脅；有些數位身分計畫缺乏隱私和資料保護架構；2019 年全球遭外洩資料高達 150 億筆，但是社群媒體平臺的財務獎勵模式卻鼓勵為商業目的而蒐集個資。此外，網路全面封鎖和常態性阻斷或過濾網路的服務，也被聯合國視為侵犯國際人權法規。

（六）AI 治理缺乏國際協調

AI 應用可能為工商業和社會開啟新機會，但它也帶來重大的安全危害，例如致命性自動化武器系統自動定奪生死、深偽（deepfakes）工具被用於操弄公眾意見等。為此，目前全球已有超過 160 個組織型、國家型或國際型的 AI 倫理和治理規範，但這也凸顯全球的 AI 治理缺乏一個共同平臺進行國際協調與合作，且討論時亦有代表性和包容性不足的問題。

（七）網路威脅不斷升高

當前全球網路飽受各種威脅，例如全球每天超過 2.4 億封疫情相關的垃圾郵件、全球資料外洩造成國家和企業數億美元的損失、惡意軟體攻擊已對重要經濟和社會功能的資訊系統造成數十億美元的持久損害、破壞政治參與和散播仇恨的假訊息攻擊層出不窮、政府和非政府組織加速發展尖端的網路兵工廠等。雖然國際間也出現「巴黎籲請網路空間信賴與安全」（Paris Call for Trust and Security in Cyberspace）、「網路合約」（the Contract for the Web）等倡議，但是這些努力的普遍性或廣度無法涵蓋全球。

（八）數位合作未獲重視且缺乏成效

目前全球數位合作存在許多問題，包括數位合作議題在國家、區域和全球議程中都未受到重視（直到近期才有 G20 開始討論數位經濟問題）；國際技術機構和標準制定組織對於數位合作的包容性安排不足；涉及數位政策議題的機制過度重疊，以致數位合作架構非常複雜、分散，又不見得有效，且讓預算短少和缺乏專業的開發中國家、中小企業、邊緣化族群難以參與；數位科技日益橫跨不同領域，但是政策制定卻仍然由單一部門各別進行；缺乏可靠的資料、指標和證據，用以制定可行的政策介入措施；政府、民間企業和公民社會之間缺乏信任。

三、需採取行動的關鍵領域

《數位合作藍圖》進一步提出需要全球共同採取行動的 8 項關鍵領域行動，以建立連結、尊重、保護所有人的數位時代。

（一）2030 年前完成全球普及上網

為了確保 2030 年前人人都能享有安全且可負擔的網路連線，包括能實際使用數位服務，聯合國將依據 SDGs 採取以下措施：

1. 支持建立個人需要接取線上空間的上網基準線，以及定義包括通用目標和指標在內的可負擔能力。
2. 召集全球投資者和融資專家小組考慮開發一個融資平臺，並尋找其他投資網路連線的新模式，尤其是在難以到達的地區和鄉下地區。
3. 推廣新的和可能具有變革性的模式，以加速網路連線，如 ITU（國際電信聯盟）和聯合國兒童基金會的全球學校連網倡議（GIGA）。
4. 為規模較小的網路供應商促進有利的法規環境，並同時評估在地和區域的連網需求。
5. 加速討論將連網作為急難準備、因應和援助的一部分，包括透過跨機構間的急難電信通訊群組（ETC）進行討論。

（二）推動數位公共財以建立更公平的世界

如果要實現增加網路連線的好處，所有利害關係人應共同推廣開放原始碼軟體、開放資料、開放 AI 模型、開放標準和開放內容等數位公共財，且這些數位公共財是遵循隱私權及其他適用的國際和國內法規、標準、最佳做法，並且不造成任何危害。聯合國秘書長樂見成立「數位公共財聯盟（Digital Public Goods Alliance）」，以加速推動此倡議。

（三）確保數位包容涵蓋所有人以加速發展

為了確保未能充分受益於數位機會者的意見也能被聽到，聯合國秘書長將建立一個由多方利害關係人組成的非正式網絡「數位包容聯盟」，制定數位包容的年度計分卡，並建立衡量數位包容和素養的計量指標，以加速包容性數位生態系統的推廣。聯合國秘書處還將針對數位包容的倡議、機制和方案，進行比對調查。

（四）強化數位能力建構

在媒合聯合國既有能力建構計畫的基礎下，聯合國秘書處將啟動一個廣泛的多方利害關係人網絡，推動以全面性和包容性的方法進行永續發展的數位能力建構，包括由聯合國開發計畫署(UNDP)和國際電信聯盟(ITU)領導成立一個新的推動數位能力發展聯合機制。

（五）確保保護數位人權

為了因應數位相依時代保護人權、尊嚴和自主性所面臨的各種挑戰和機遇，聯合國人權事務高級專員辦事處(OHCHR)將製定指南，針對新科技使用的人權層面進行盡職調查(due diligence)和影響評估。聯合國秘書長呼籲會員國，將人權放在數位科技發展和使用的監管框架和立法中心；並呼籲科技領導者，儘快從企業面採取明確行動以保護數位隱私和人權。

（六）支持可信賴 AI 的全球合作

為了因應會員國提出的 AI 包容性、協調和能力建構等問題，聯合國秘書長將設立一個全球 AI 合作的多方利害關係人諮詢機構，由會員國、聯合國相關單位、民間企業、學術單位、公民團體等共同組成，提供有關可信賴、基於人權、安全、永續和促進和平的 AI 發展諮詢，並作為 AI 最佳典範、標準化和法律遵循等議題的資訊分享和意見交流平臺。

（七）推動信賴和安全的數位環境

一份闡明理解數位信賴和安全是共同要素，且由所有會員國皆認可的總體性聲明（尤其獲得國家最高層級的體認），有助於塑造基於全球價值觀的數位合作共識。因此，聯合國秘書處將與會員國持續探討是否以及如何推動這項聲明，包括將聲明開放給其他多方利害關係人簽署。

（八）建立更有效的全球數位合作架構

聯合國數位合作高階專家小組(HLPDC)已為全球數位合作提出 3 個建議模式（將於下段介紹），雖然全球利害關係人仍在就此進行討論，但

聯合國秘書長已表示擬推動下列強化 IGF 因應當前數位議題的相關措施。

1. 建立一個策略性且賦權的多方利害關係人高階組織，以解決迫切問題、協調 IGF 討論的後續行動，並將 IGF 相關建議提供給合適的規範制定決策組織。
2. 促使 IGF 議程更聚焦於幾個策略性的政策議題。
3. 建立高階、部長級或議員級議程，確保產出更具體可行的會議結論。
4. 強化全球 IGF 和區域 IGF、國家 IGF 及青年倡議的連結。
5. 針對本報告提及的優先領域，強化整合 IGF 議程和閉會期間的政策制定工作。
6. 以創新可行的籌資戰略，解決論壇長期運作和促進參與所需資源。
7. 透過強化組織識別（Corporate Identity）等方式提升 IGF 知名度。

四、數位合作的可能模式

（一）高階專家小組建議模式

如前所述，全球數位合作究竟將採取什麼模式，目前相關利害關係人正針對 HLPDC（2019）建議的 3 種模式——IGF Plus、分散式共同治理、數位共同體，進行討論。這些模式的概述、特色和共同性彙整如下表 8。

表8. 數位合作建議模式比較

HLPDC 建議模式	概述	特色	共同性
IGF Plus 模式 (IGF+)	在現有 IGF 基礎上，強化研議具體的政策建議或常規，以供公眾討論或供各國政府及決策單位參考或採用	強化既有且經聯合國授權的多方利害關係人論壇 IGF	• 參與方式：多方利害關係人、包容性 • 共同原則：共識決導向、客製化的解決方
分散式共同治理模式	將數位規範的設計與實施分離，採取如 ICANN 等組織的由下而	新的專家網絡和多方利害關係人	

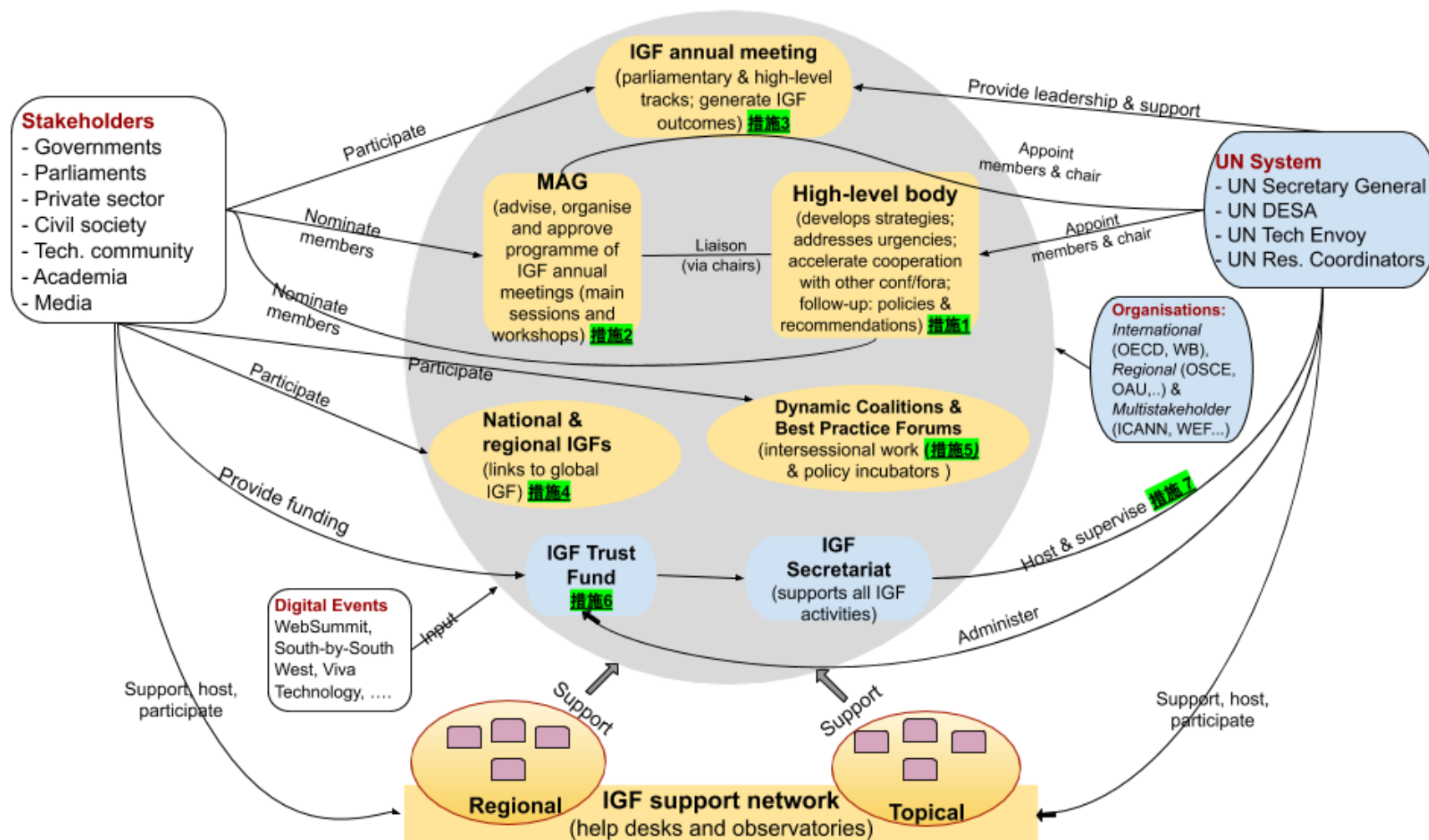
HLPDC 建議模式	概述	特色	共同性
(the Distributed Co-Governance, COGOV)	上運作方式，但訂定的是非強制性的常規或規範，以供各國政府參考或採用	治理將扮演更重要角色	案、敏捷因應新興議題、角色權責明確、可量測的結果和問責制、權力平衡、過程開放透明、創新且由下而上的合作方式、公平和全球最大公共利益的結果
數位共同體模式 (the Digital Commons Architecture, DCA)	旨在創造利害關係人的溝通對話以解決數位問題，雖然不會制定規則，也可能不會指定技術解決方案，但會提供實施指南、技術模型和可信賴的全球性標準	同時從「多邊」和「多方利害關係人」的途徑，相互學習治理	

資料來源：HLPDC；本計畫彙整

《數位合作藍圖》指出，現階段以 IGF Plus 模式的呼聲最高；惟也有人認為需要再檢視、擷取其他 2 種模式的互補性優點；此外，還有些國家正在考慮以國家或地區為範圍，進行 GOGOV 模式的試驗。而彙整全球多方利害關係人對於數位合作模式意見，且於 2020 年 9 月呈交聯合國秘書長的《選項報告》(The Options Paper)，亦提出相似的共識建議，也就是以 IGF Plus 模式為基礎，並採用其他 2 種模式優點，包括 COGOV 模式的由下而上運作方式，以及 DCA 模式的提供可實施的結果。

由上顯示，未來全球數位合作採取 IGF Plus 模式的可能性很高，日內瓦網路平臺 (GIP) 進一步將此模式和前述《數位合作藍圖》中聯合國秘書長擬推動的 7 項強化 IGF 措施，繪製成下頁圖 9 IGF Plus 模式生態系統。

圖 9 顯示，未來 IGF Plus 模式仍是在聯合國系統的領導下運作，雖然如何與國際組織合作尚不明確，但多方利害關係人除了可參加既有 IGF 年度會議、國家型和區域型 IGF、IGF 閉會期間持續進行的動態聯盟 (Dynamic Coalitions, DCs) 和最佳典範論壇 (Best Practice Forums, BPFs)、提名或角逐 MAG (Multistakeholder Advisory Group, 多方利害關係人諮詢小組) 委員之外，還有機會進入新成立且負責推動政策發展和合作事務的高階組織，另外也可提供財務協助，或加入支援性工作。



圖片來源：GIP（本計畫微調）

圖9. IGF Plus 模式生態系統

（二）「多邊」和「多方利害關係人」

HLPDC（2019）將政府、民間企業和公民社會之間的缺乏信任，列為當前數位合作的其一問題。HLPDC 強調，政府間（Intergovernmental）國際組織應該讓更廣泛的關係人加入，且實際上「多方利害關係人」和「多邊」方式已經共同存在了，當前挑戰是如何運用彼此來強化各自的效用。

《數位合作藍圖》則指出，數位合作是「多方利害關係人」的共同努力，雖然政府仍處於核心地位，但是民間部門、科技公司、公民社會和其他利害關係人的參與亦是必要的，且需從一開始就參與才能訂出切實有效的決策和政策。而聯合國已經準備好成為新興科技的政策對話平臺，且將於 2021 年任命一名「科技特使」擔任諮詢顧問及協調人，以指導聯合國內部高層就關鍵科技趨勢採取策略方針，並於數位合作事務協助會員國及多方利害關係人對廣泛聯合國系統的聯繫。

聯合國秘書長古特瑞斯亦有相關說明。他於聯合國第 75 屆會議上表示，樂見紀念宣言承諾要改善「多邊主義」，因為「雖然國家主權是聯合國的支柱，但沒有人會想要一個世界政府，而是大家必須共同來改善世界治理。在此互連的世界中，我們需要聯合國大家庭、國際金融機構、區域組織、經貿集團等更緊密有效合作的『網絡化』多邊主義，以及公民社會、城市、企業、地方當局，以及更多年輕人加入的『包容性』多邊主義」（UN Secretary-General, 2020）。

五、數位合作的機會和挑戰

目前各界專家對於《數位合作藍圖》究竟能否帶領我們邁向更美好的數位未來，尚且無法定論。以下綜整相關情勢和專家意見，並從中歸納全球數位合作的機會和挑戰。

（一）數位合作的機會

1. 藍圖方向獲得支持肯定

《數位合作藍圖》線上發布會除了由聯合國秘書長為藍圖內容揭開序幕外，還有瑞士聯邦總統 Simonetta Sommaruga、全球資訊網（WWW）創辦人 Tim Berners-Lee、世界經濟論壇（WEF）創辦人暨主席 Klaus Schwab、國際商會（ICC）副主席 Ajay Banga、網際網路協會（ISOC）總裁 Andrew Sullivan 等國際政商和民間團體領袖，對藍圖表達支持之意（GIP, 2020）。

負責共同彙整《選項報告》的德國政府和阿拉伯聯合大公國政府，更是樂觀看待全球數位合作的前景，因為他們在徵詢全球意見的過程中，不但看到全球利害關係人的積極參與討論，而且還能進一步針對當前問題的識別和解決方案形成廣泛的共識（Options Paper, 2020）。

英國民間智庫漆咸樓（Chatham House）指出，這份藍圖是截至目前最具雄心壯志的一個數位願景，不但辨識全球科技治理方式的一些關鍵缺口，還據此提出全球數位合作的具體措施，例如定義數位連線的基準線（基本流量）和可負擔的能力（網路費）、制定數位包容的年度計分卡等（Buchser and Mandal, 2020）。

丹麥奧胡斯大學（Aarhus University）榮譽教授 Wolfgang Kleinwächter（2020）表示，當前數位合作問題是有太多的政府和非政府的談判或政策制定機構，但是卻未能反映全球網路治理生態體系的高度複雜性，資安專家、經貿專家、外交官、人權專家、技術人員等，都在各自場域內產出可能導致網路分裂的法規。因此，藍圖要促進議題溝通和政策對話，且對複雜的網路問題採取全面性的整體方法，是正確的方向與做法，

公民團體如 Access Now 和 RESET 也表示，藍圖識別出當前數位發展的重要問題，並嘗試著手解決，因此也呼籲國際社會共同努力實現藍圖的願景（Micek and O'brien, 2020; Röller-Siedenburg, 2020）。

2. 識別出合適的政策對話平臺——聯合國

Kleinwächter（2020）表示，全球有數十個組織或平臺在討論、談判或

制定網路治理相關的國際規範，如聯合國轄下的 ITU、人權理事會（UNHRC）、開發計畫署(UNDP)等，以及其他如 WTO(世界貿易組織)、WEF（世界經濟論壇）、ICANN（網際網路名稱與號碼分配機構）、IETF（網際網路工程任務小組）、MSC（慕尼黑安全會議）等。但是網路治理議題非常複雜，如業者的商業模式會引發安全、資料保護、言論自由等問題，需要跨領域關係人以全面性方法共商解決之道。因此，藍圖不是要讓聯合國成為「網路的世界政府」，而是做為「多方利害關係人的政策對話平臺」，且未來任命的「科技特使」也不是「網路世界的總統」，而是「議題溝通的促進者」。

《網路治理導論》(An Introduction to Internet Governance) 作者暨外交基金會（DiploFoundation）創辦人 Jovan Kurbalija（2020）亦贊同聯合國是合適的政策對話平臺。他表示，目前國際間缺乏以全球為範圍，且由多方利害關係人共同進行政策討論和制定規範的空間。雖然國際間有 WEF 等具影響力的專業組織存在，但是在重視合法性、象徵性、公平性的時代，聯合國是唯一可以成為「所有人數位之家」的地方，可以作為「多方利害關係人的政策對話平臺」，讓大家依各自的關係人角色進行討論，否則一旦角色錯置混用，例如企業界開始立法、公民團體承包所有業務…，將會導致亂象叢生且引發危機。

（二）數位合作的挑戰

1. 聯合國為具官僚陋習的國際組織

國際公民團體 Access Now 表示，權力、階級、政治、種族和財力，都是阻礙連網、永續發展、人權和數位合作的因素。由於聯合國常處於政治僵局，且是具有官僚作風陋習的國際組織，加上過去承諾的增加網路連線和資通訊科技使用的目標，不但沒有實現且還遠遠落後。因此，他們對於未來聯合國推動增進數位權益並不樂觀，但仍會密切關注公民社會參與等相關問題（Micek and O'brien, 2020）。

2. 聯合國須面對政治立場迥異的現實問題

漆咸樓認為，藍圖引領推動數位公共財、建立數位包容聯盟、協調 AI 治理等倡議，凸顯聯合國想要重新建立其制定規範的權力，並扮演全球科技治理的核心和協調角色，但它也因此必須面對民主政府和專制政府作法（處理數位科技的方式）迥異的現實問題，並須巧妙地融合各方權力，而目前藍圖是暫時擱置這些核心問題（Buchser and Mandal, 2020）。

3. 聯合國體系內實施多方方式將是一大挑戰

關於上述的政治分歧，Kleinwächter（2020）有進一步的說明。他表示，15 年前網路治理的主要爭議正是中國大陸主張「政府掌控」方式，而美國主張「自由市場」方式；由於當時大家以為治理方式只會適用於網路而非實體世界，以致最終得以妥協接受多方利害關係人方式。然而，今天的網路世界已和實體世界畫上等號，治理議題也從「有些政治意涵的技術問題」轉變成更複雜「具有技術成分的政治戰場」，加上抱持傳統主權原則的國家擔憂一旦聯合國為政府以外的利害關係人敞開大門，將有危害聯合國體系核心原則，意即侵犯國家主權的風險，因此，未來要在聯合國體系內以由下而上、開放、透明的方式，發展治理政策和談判協議，將是一大挑戰。

4. 藍圖缺乏穩定財源和強制力

Kleinwächter（2020）以「沒有牙齒和預算的許願清單」來形容藍圖缺乏穩定財源和強制力，但他也強調，這是反映現實的問題，也就是儘管設定了正確方向，但不保證可以成功航向目的地。Kleinwächter 並表示，有鑑於美中科技強權的衝突加劇、聯合國秘書長的禁止自動化武器提案被忽視、歐美雙方可能因為課徵數位稅而出現數位貿易戰、俄國於聯合國的對抗網路犯罪新倡議可能破壞安全與言論自由、中國大陸在 ITU 提議發展新的網路架構（New IP）可能將去中心化的網路變成新型集中控制的網路等

情勢，未來 10 年我們可能要面對更加衝突的網路空間，同時也要習慣數位合作與網路衝突的共存。

5. 藍圖如何實施尚待闡明

德國公民團體 RESET 指出，藍圖還有諸多未說明的問題。例如各種新措施的確切作用和功能尚未闡明；也不清楚誰是利害關係人且會真正參與計畫；還有聯合國成員國的角色、參與方式，及如何確保決策被推行、又如何解決民主和專制政府的治理歧見也都不確定。總之，目前尚不清楚聯合國將如何實施這份藍圖（Röller-Siedenburg, 2020）。

六、結論與建議

加強全球數位合作已於《紀念聯合國成立 75 周年宣言》中，獲得聯合國 193 個會員國的承諾，且聯合國《數位合作藍圖》也提出 8 項行動關鍵領域，期能建立連結、尊重、保護所有人的數位時代。而不論是紀念宣言強調的聯合國獨特合法地位及規範影響力，或是合作藍圖對於行動關鍵領域的規劃，都凸顯聯合國有意扮演全球網路治理的核心角色。再者，網路治理專家也認同聯合國是合適的「政策對話平臺」，加上全球網路治理社群也普遍支持改革既有聯合國 IGF 的 IGF Plus 模式，因此，未來全球數位合作應是會在聯合國系統的領導下運作，且 IGF 的重要性和影響力也將隨著更多政策決策者的參與（規劃部長級、議員級的議程），以及產出具體的政策規範或常規，而顯著提升。

不過，正如 Kleinwächter（2020）形容藍圖是「沒有牙齒和預算的許願清單」，未來不論是採取 IGF Plus 模式或融合其他模式，所提出的規範或標準都沒有強制性；且在後續的推動時程和細節方面，目前尚無任何進一步消息，包括聯合國秘書長古特瑞斯於 11 月 17 日的 IGF 2020 閉幕致詞也未提及，因此，各界對於藍圖究竟將如何實施仍有諸多疑問。例如聯合國會員國的角色和參與方式為何、如何解決民主政府和專制政府的治理對立歧見、哪些國際組織是網路治理議題合適的規範制定決策組織、如何在盛

行傳統多邊主義的聯合國體系下實施多方利害關係人由下而上且開放透明的政策發展方式等問題。

儘管如此，藍圖的發布和行動關鍵領域的規劃，對於我國的數位政策發展仍具有啟示，也就是行動關鍵領域所規劃的數位合作多項措施及現況問題分析，可做為我國檢視相關政策實施成效和評估調整政策措施的重要參考。例如在普及上網和數位包容方面，聯合國將定義上網基準線（基本流量）、可負擔費用，以及訂定包含數位素養在內的數位包容年度計分卡等指標。我國可藉由這些具體量化的國際指標，檢視國內上網資費是否合理、弱勢族群的上網權益是否受到保護，以及資訊素養教育是否成效良好等施政結果。

此外，為了保障數位人權，未來聯合國將針對新科技的使用進行人權盡職調查，雖然調查項目尚未公布，但藍圖已指出，鎖定目標的通訊監察和人臉辨識軟體、缺乏保護設計的數位身分計畫等政策措施，都可能涉及侵犯國際人權法規。又聯合國秘書長古特瑞斯也強調，各國應將「人權」放在數位科技監管框架和立法的中心。我國《科技偵查法》草案、即將試辦的數位身分證等措施，都引發國內各界的不同論戰。因此，我們對於涉及使用數位科技的公共政策應該進行更審慎的評估，並和整體社會充分溝通，以真正落實保障數位人權。

七、參考文獻

- Buchser, M. and Mandal, R. (2020). Can the UN Roadmap on Digital Cooperation Improve our Digital Future? Chatham House, 12-06-2020. <https://www.chathamhouse.org/2020/06/can-un-roadmap-digital-cooperation-improve-our-digital-future>
- GIP (2020). Roadmap for digital cooperation. <https://dig.watch/process/roadmap>
- HLPDC (2019). The Age of Digital Interdependence. UN Secretary-General's

High-level Panel on Digital Cooperation.

<https://digitalcooperation.org/panel-launches-report-recommendations/>

- HLPDC (2020). UN Secretary-General launches a Roadmap for Digital Cooperation. 11-06-2020.
<https://digitalcooperation.org/un-secretary-general-launches-a-roadmap-for-digital-cooperation/>
- Kleinwächter, W. (2020). UN Secretary General's Roadmap on Digital Cooperation: Creative Navigating in Stormy Cyberwaters. CircleID, 13-06-2020.
<http://www.circleid.com/posts/20200613-un-secretary-generals-roadmap-on-digital-cooperation/>
- Kleinwächter, W. (2018). Internet Governance Outlook 2018: Preparing for Cyberwar or Promoting Cyber Détente? CircleID, 06-01-2018.
http://www.circleid.com/posts/20180106_internet_governance_outlook_2018_preparing_for_cyberwar_or/
- Kurbalija, J. (2020). Digital Roadmap: The realistic acceleration of digital cooperation. DiPLO, 16-06-2020.
<https://www.diplomacy.edu/blog/digital-roadmap-realistic-acceleration-digital-cooperation>
- Micek, P. and O'brien, L. (2020). New U.N. “Roadmap” on tech: only useful if we drive “digital cooperation” forward. Access Now, 23-06-2020.
<https://www.accessnow.org/new-u-n-roadmap-on-tech-only-useful-if-we-drive-digital-cooperation-forward/>
- Options Paper (2020).
<https://www.global-cooperation.digital/GCD/Navigation/EN/The-Options-Paper/the-options-paper.html>
- Röller-Siedenburg, K. (2020). The UN Roadmap for Digital Cooperation - Where Could It Take Us? RESET, 13-08-2020.

<https://en.reset.org/blog/un-roadmap-digital-cooperation-where-could-it-take-us-08132020>

- UN (2020). Report of the Secretary-General Roadmap for Digital Cooperation. June 2020. <https://www.un.org/en/content/digital-cooperation-roadmap/>
- UN Secretary-General (2020). Secretary-General's remarks at General Assembly Ceremony marking the 75th Anniversary of the United Nations. 21-09-2020. <https://www.un.org/sg/en/content/sg/statement/2020-09-21/secretary-generals-remarks-general-assembly-ceremony-marking-the-75th-anniversary-of-the-united-nations-bilingual-delivered-scroll-down-for-all-english-and-all-french>
- UNGA 75 (2020). Declaration on the commemoration of the seventy-fifth anniversary of the United Nations. 21-09-2020. <https://undocs.org/en/A/RES/75/1>

第三章 大專院校講座

第一節 執行概況

本計畫依據委託辦理工作項目規定，完成 3 場次各 2 小時且出席人數達 50 人以上的大專院校講座活動，包括北部的臺灣大學、中部的中興大學，以及南部的高雄科技大學。演講場合皆為學分課程，學生涵蓋大學生與研究生，系所包含電工所、資工所和資管系，出席人數最少為 56 人，最多高達 120 人。各場次的辦理概況彙整如下表 9。

表9. 大專院校講座活動辦理概況

場次	時間	學校	系所 / 活動名稱	講題與講者	人數
1	9/18 (五) 14:00~16:00	國立 中興大學	資訊科學與工程學所 專題演講課程	美國電子商務網領預告全 球通信產業變革及爭議 (吳國維)	120
2	10/5 (一) 13:20~15:20	國立 臺灣大學	電信工程學研究所 專題討論課程	淺談「數位主權」與「網 路分裂」(吳國維)	102
3	10/8 (四) 13:30~16:20	國立高雄 科技大學	資訊管理系企業資訊網 路課程 (大三、大四)	轉變中的網路世界規則 (陳文生)	56

第二節 中興大學場次

一、活動訊息

- 系所：資訊科學與工程學所
- 場合：專題演講課程
- 時間：109 年 9 月 18 日 (五) 14:00 ~ 16:00
- 地點：資訊科學大樓地下一樓致平廳

- 人數：120
- 講題：美國電子商務綱領預告全球通信產業變革及爭議（簡報詳附件 1）
- 講師：本計畫主持人吳國維

二、演講內容摘要

（一）電信產業的定義與風險

股票市場已將電信產業視為傳統夕陽產業。過去 15 年來，各國大電信公司的股價低迷，但網路公司的股價成長卻超過百倍，且所有社群媒體如 Google Hangout、Facebook Messenger 都提供原本屬於電信業者的即時通訊服務，因此，產業凋零化和被取代，是電信產業面臨的風險。電信產業因為涉及國家安全而受到法規管理且肩負許多責任和義務。但是現今網路業者已提供相同服務，因此，如何定義電信產業值得思考。

（二）美國《全球電子商務綱領》與治理議題

美國於 1997 年柯林頓總統時代，由當時白宮科技顧問 Ira Magaziner 研擬擘劃下世紀的經濟框架《全球電子商務綱領》（The Framework for Electronic Commerce），當時已預知網路發展的潛力和問題，並建議網路政策的原則，可謂真正的超前部署。

當年 Magaziner 即指出，「人性」是制訂網路和電子商務政策的要素，但政府因官僚體系不宜過度介入網路發展，且網路政策應由利害關係人共同制訂。他並認為網路將成為推動民主、個人自由和人民賦權的力量，果真於 2010 年至 2012 年發生「阿拉伯之春」民主運動，且近年網紅也確實展現強大的號召力量。此外，Magaziner 還提出課稅、隱私、內容限制、數位簽章、著作權、網路管理、加密、電信自由化等 8 個問題，當中有許多是當前重要的網路治理議題。例如當年 Magaziner 努力和歐盟及日本溝通，促成跨國電子商務不課稅的共識，但是現在法國要推動課徵數位稅；還有隱私一直是歐洲和美國的爭議問題，奉行資本主義的美國將隱私視為

使用者和業者之間的合約問題，並因此質疑歐盟透過法律 GDPR 保護隱私的作法。

不過，Magaziner 卻誤信市場力量會給予人們最大的自由度和選擇權。網路產業發展至今，全球網路市場呈現高度集中化（或歐盟認為的壟斷），世界各國的前幾大網站幾乎都由 Google、YouTube、Facebook 等公司囊括，而且我們沒有什麼選擇的權利，手機作業系統只有 Android 和 iOS 兩種，即時通訊軟體更是不得不使用，因為親友都集中在某幾個大平臺上，一旦我們選擇退出，就形同斷絕社會聯繫。

（三）我國《電信管理法》

我國於今年（2020）7 月 1 日實施新版《電信管理法》，廢除第一類及第二類電信事業分類，並從過去高度管制的特許制度改為登記制度。依據該法第 5 條，只要配有無線電頻率、網路識別碼、用戶號碼等，就要辦理登記為電信業者，且須繳稅並承擔偏鄉地區網路建設的責任和費用，但是電信事業普及服務基金的補貼遠不及實際支出。

然而，同樣提供即時通訊服務的網路業者（例如 Google 在美國紐約市廣設的網路連線服務亭 LinkNYC，提供免費 Wi-Fi 並可藉此撥打網路電話；還有提供全球超過 200 個國家語音和網路漫遊的 Google Fi 電信方案），因為不需要使用第 5 條的頻譜和號碼資源，而不用登記成為電信業者，也沒有連帶的責任和義務。因此，我們應該重新思考電信業者的定義和監管。

三、現場交流 (Q&A)

（一）請問對於美國網路中立法規不斷修改的看法？

「網路中立」(net neutrality) 概念是美國哥倫比亞大學法學教授吳修銘 (Tim Wu) 於 2003 年所提出，意旨網路傳輸要公平，不能因為網站、內容、平臺、使用者或裝置等不同，而有差別收費或是不同的傳輸速度。例如曾有影音公司向 ISP 業者提出願意支付更多費用，以確保獲得最大最穩定的

頻寬，進而提供高品質的影音服務。Tim Wu 認為，由於頻寬大小是固定的，此舉將會排擠其他用戶的使用權益。

「網路中立」論述引起美國社會正反兩方意見，支持者認為網路的公平使用為公共利益，不應為了少數人而犧牲多數人的權益；反對者如 ISP 則主張將會導致限制競爭和不利創新投資。相關法規曾於歐巴馬總統時期通過，但是川普總統時期改為廢除。直到今日，美國社會仍持續爭論而無法取得共識。

四、活動剪影



圖10. 中興大學講座照片

第三節 臺灣大學場次

一、活動訊息

- 系所：電信工程學研究所
- 場合：專題討論課程
- 時間：109 年 10 月 5 日 (一) 13:20 ~ 15:20
- 地點：博理館 112 教室
- 人數：102
- 講題：淺談「數位主權」與「網路分裂」
- 講師：本計畫主持人吳國維

二、演講內容摘要

(一) 從資料中心談「網路主權」

資料中心是雲端運算的重要基礎建設，Google 於 2013 年啟用的臺灣彰濱工業區的資料中心，規模為當時亞洲最大，儲存許多亞洲國家的資料，如果其他國家想要索取這些資料，即涉及「網路主權」問題。「網路主權」本來是極權國家提倡的，它們還實施「資料在地化」措施，但此政策和透過資料自由流通的雲端運算是有衝突的。另一方面，2013 年爆發史諾登（Edward Snowden）揭露美國國安局暗中監視各國領袖通訊的事件後，德國總理梅克爾也轉為提倡建立歐洲自己的網路。

近年來，歐洲對於沒能在全球網路發展扮演要角而感到震驚。例如全球前 20 大網路公司都是來自美中兩國，沒有 1 家是歐洲企業；又每個國家（除了中國大陸以外）的網路流量都高度集中於 Google、YouTube、Facebook 這 3 家美國公司等。因此，歐洲最近也開始主張「數位主權」，並且要加強發展 5G、AI 和 IoT（物聯網）等領域。不過，究竟「數位主權」

和傳統的「國家主權」有什麼異同，國際間仍在討論中。

(二) 美國《全球電子商務綱領》與治理議題

美國於 1997 年柯林頓總統時代，由當時白宮科技顧問 Ira Magaziner 研擬擘劃下世紀的經濟框架《全球電子商務綱領》，當時許多專家認為政府政策不宜過度介入網路，且網路將成為推動民主、個人自由和人民賦權的力量，果真於 2010 年至 2012 年發生「阿拉伯之春」民主運動。

《全球電子商務綱領》還提出課稅、隱私、內容限制、數位簽章、著作權、網路管理、加密、電信自由化等 8 個問題，當中有許多是當前重要的網路治理議題。例如當年 Magaziner 努力和歐盟及日本溝通，促成跨國電子商務不課稅的共識，但是現在法國要推動課徵數位稅。

除了和國際對話外，Magaziner 於國內的政策溝通更不在話下，對象涵蓋美國 18 個部會。因此，面對網路的發展與爭議，我國擬成立新的「數位發展部」並無法解決問題，最需要的反而是許多的跨部會協調與溝通。

(三) 全球網路技術標準、網路關鍵資源，以及「主權」

訂定全球網路標準的 IETF（網際網路工程任務小組）沒有在任何國家註冊，所以不屬於任何法律架構，也沒有真正的「正統性」或「合法性」，這與人類數百年的「主權」和司法體系有很大差異。

ICANN（網際網路名稱與號碼分配機構）則是 1997 年美國白宮決定成立的，當年歐盟曾主張網路空間屬於公共利益，IP 位址與網域名稱是公共財，但是美國共和黨仍基於網路源起於美國國防部計畫，而認為美國政府應該擁有網路關鍵資源的所有權。也因此，歐巴馬政府因史諾登事件而訂於 2016 年交出 IANA（網路號碼指派機構）監管權且改由國際共管模式時，有美國議員發起阻止交出監管權行動，並認為這是非法轉移美國政府財產。

(四) 「主權」與「網路分裂」

「數位主權」意味在網路空間實施「國家主權」。但是網路是全球單一的網路，而中國大陸於 1998 至 1999 年期間即開始推動網路長城計畫，這是否代表全球網路「分裂」成「中國網路」和「其他網路」呢？其實每個國家都有實施網路過濾，只是範圍和程度有所差異而已。例如我國就將宣傳中國大陸「惠臺 31 項措施」的網站封鎖下架，但這其實有爭議性，因為它的網址 www.31t.tw 是向我國 TWNIC 申請取得的，且有繳交註冊費。另外一個案例是新加坡，它禁止民眾在網路上討論政治和宗教問題。

國際專家對「網路分裂」持不同看法，網路之父 Dr. Cerf 等專家認為「網路分裂」可從為技術、政府、商業等三個層面來探討，但是美國學者 Milton Mueller 主張「網路分裂」的爭辯其實是對未來「國家主權」的權力鬥爭。

三、現場交流 (Q&A)

(一) 對於「網路主權」的爭議問題能否訴諸於國際法庭？

由於聯合國認為國際法庭不能凌駕於「國家主權」之上，因此，國際法庭的決議文只是建議性質，不太可能因為不履行決議文就動員聯合國出兵，跨國爭議問題主要還是需由雙方彼此協商退讓。

(二) 請問對於法務部推動《科技偵查法》的看法。

此法讓檢調人員不需經由法律程序，即可對嫌疑人的手機、平板或電腦進行監聽，甚至可以透過植入木馬等駭客手法進行，所以，這是大家都應該關心的問題。

四、活動剪影



圖11. 臺灣大學講座照片

第四節 高雄科技大學場次

一、活動訊息

- 系所：資訊管理系
- 場合：企業資訊網路課程（大三、大四）

- 時間：109 年 10 月 8 日 (四) 13:30 ~ 16:20
- 地點：管理學院 1 樓 C120 電腦教室
- 人數：56
- 講題：轉變中的網路世界規則（簡報詳附件 1）
- 講師：本計畫顧問陳文生

二、演講內容摘要

（一）生活中的網路治理議題

在數位化時代，網路治理議題無所不在。例如今年最熱門的治理議題是電子監控防疫與隱私權保護，不論是臺灣或是各國，大家都希望透過科技提高防疫成效，但同時也伴隨侵犯隱私的疑慮。還有複雜的中美科技戰或我國 OTT 影音監管措施，及這 2 個議題所交織的國家安全和市場經濟等問題，更是引發各方不同觀點的激烈論戰。另外，在打擊犯罪方面也有法規侵犯隱私權的問題；而假訊息防治或仇恨言論的監管，也帶來危害言論自由等問題。這些議題和我們的數位生活息息相關，而且經常面臨各種權益、價值觀或立場的難以權衡，因此，需要所有利害關係人共同參與討論，才能找出符合最大公共利益的的解決之道。

（二）什麼是網路治理？

網路治理是一種藉由政府、民營部門和公民社群，也就是多方利害關係人，各自發揮角色、共享原則、規範、規則、決策程序及計畫，以形塑網際網路的發展與應用的過程。過程中採取多元、公開、透明、平等參與、當責（Accountability）原則，期能達到維持網路的安全穩定和互連等目標。

網路治理的範圍相當廣泛，涵蓋基礎建設、法規、安全、發展、經濟、社會文化、人權等各層面，而且治理的觀念、要素、模式、議題和生態系統也隨著網路發展而轉變，例如過去許多人主張網路不宜受到政府和法律

的監管，但是隨著網路濫用問題日益嚴重、科技巨頭不但富可敵國還主宰人類的生活，各國紛紛推出各種立法，於是網路發展的主導力量也從過去的程式碼（Code）變成法規（Law），被形容為 Law is Code。此外，網路無國界互連的特性在近年來許多國家開始主張網路主權並實施相關的禁用措施下，也逐漸朝向巴爾幹化的分裂發展。

（三）多方利害關係人模式典範：ICANN

ICANN 是一個全球性的非營利機構，1998 年 10 月成立於美國加州，負責監督管理域名系統（DNS）、IP 位址的分配暨指派、根伺服器系統等。為確保所有人皆能平等參與決策，ICANN 制定複雜的治理流程，各利害關係人團體（技術社群、公民團體、公司企業、使用者、學術界、政府）大致分為負責制定政策的支援組織（SO）和負責提供建議的諮詢委員會（AC），大家不但能參與 ICANN 技術決策，也可以監督並參與 ICANN 組織的營運規劃。

ICANN 作為多方利害關係人模式的奉行者，採取由下而上方式制定政策，且內部的政策發展流程皆遵循「界定議題→發起工作小組→制定政策→共識決通過政策→執行」的基本架構，並以共識（非投票）做成決策。

（四）如何參與網路治理？

國內外皆有許多網路治理會議活動開放大眾參與，例如國內有網路治理研習營、TWIGF 年度論壇及平日的臺灣網路講堂等活動；而國際則有 APrIGF、IGF（可線上參與）、ICANN、APNIC 等國際相關會議，且有獎助津貼可供申請。網路治理需要也非常歡迎大家的參與。

三、現場交流 (Q&A)

本場講座的現場交流以線上投票方式，讓同學思考 4 個網路治理問題，共計有 44 人投票，參與率約 8 成，投票結果摘錄如下。

- 您願意為了新冠肺炎的防疫成效，而接受如手機定位的電子監控嗎？
「願意」為了防疫而接受電子監控的比例約 48%，較「不願意」多 2%。

- 您認為臺灣應該禁止本地業者經銷來自中國的 OTT 相關服務嗎（如愛奇藝）？

超過 52%認為「不應該」，原因包括如同收看美劇、仍可透過跨境收看；但也有 36%認為「應該」，主要是因為對方沒有對等開放市場。

- 您認為政府應為了打擊犯罪，而以「植入程式」監看 LINE 等通訊軟體嗎？
84%認為「不應該」，因為檢警調容易擴權，進而侵害自由和人權；只有 14%認為「應該」，因為通訊軟體內有許多罪證。

- 誰該負責移除網路上的不當內容？

高達 66%認為內容平臺業者應該負責移除，21%認為是執法當局或法院，只有 9%認為網路內容根本不應該被審查。

四、活動剪影



圖12. 高雄科技大學講座照片

第四章 人才培訓課程

第一節 活動內容與辦法

一、活動簡介

電子監控的防疫成效與人權隱私如何兼顧？網路訊息的真實正確與言論自由如何取捨？網路科技引領我們邁向智慧化的數位生活，但同時也衍生破壞安全、侵犯人權、製造社會衝突等新型態的濫用行為。網路是我們所有人共同擁有的珍貴資源，唯有透過所有多方利害關係人（multi-stakeholder）的溝通對話，才能找到治理網路的最佳方案。因此，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。

「2020 網路治理研習營」為一日免費研習活動。透過專題講習與模擬演練，帶您認識網路安全、人權、數位經濟、新興科技等重要議題，以及如何參與這些議題的政策討論。優秀學員還有機會出國參加 2020 APriGF（亞太區網路治理論壇）。本活動名額有限，敬請把握報名良機！

- 名稱：2020 網路治理研習營
- 時間：109 年 6 月 6 日（六）
- 地點：IEAT（台北市進出口商業同業公會）會議中心 8F 綜合教室（臺北市中山區松江路 350 號）

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，以及 1 日（8 小時）實體課程。上課方式有課堂講習暨問答，以及分組演練；課程主題涵蓋網路人權、經濟與新興科技、網路治理與國際關係、網路安全與基礎建設、網路內容與平臺。課程表如表 10 所示。

表10. 研習營課程表

6/4 (四)前		課前預習	
1. 影片		(1) 網路治理發展史 (2) 網路治理與政策模式 (3) 當前網路治理重要法規 (4) 媒體與內容	
2. 文章		(1) What is... internet governance? (2) “Father of the internet” Vint Cerf says we need to be less naive if we’re going to fix it	
3. 線上測驗		將以 email 通知錄取學員線上測驗的網址連結	
6/6 (六)	項目	課程	講者/主持人
08:40 - 09:00		報到	
09:00 - 09:50	專題 講習	網路人權議題	台灣人權促進會 何明諄 副秘書長
10:00 - 10:50		經濟與新興科技議題	理律法律事務所 熊全迪 律師
11:00 - 12:00		網路治理與國際關係	NII 產業發展協進會 吳國維 董事 禮騏法律事務所 謝佩芬 (前) 顧問
12:00 - 13:00		午餐	
13:00 - 13:50	專題 講習	網路安全與基礎建設議題	台灣網路資訊中心 (TWNIIC) 黃勝雄 董事長暨執行長
13:50 - 14:40		網路內容與平臺議題	理律法律事務所 曾更瑩 律師
14:40 - 15:00		午茶	
15:00 - 16:30	分組 演練	議題討論 / 角色扮演	各主題講者帶領學員進行演練
16:30 - 17:10		小組成果報告	學員推派代表
17:10 - 18:00	結業式	參與分享和機會、結業	優秀學員、秘書處

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，同時也請前任優秀學員分享參與經驗。講師群依姓氏筆畫簡介如下：



吳國維
NII產業發展協進會 董事

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）多方利害關係人指導委員會主席（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



曾更瑩
理律法律事務所 合夥律師

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）多方利害關係人指導委員會副主席（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



熊全迪
理律法律事務所 初級合夥人

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、交易平台、監理沙盒等）
個資保護
一般商務及公司法務



黃勝雄
台灣網路資訊中心 (TWNIC) 董事長暨執行長

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) 多方利害關係人指導委員會委員 (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



何明諄
台灣人權促進會 副秘書長

經歷

臺灣網路治理論壇 (TWIGF) 多方利害關係人指導委員會委員 (現任)
台灣人權促進會之台灣網路透明報告專案經理

專長

網路人權議題
言論自由
個資隱私保護



謝佩芬
禮騏法律事務所 顧問

經歷

臺灣網路治理論壇 (TWIGF) 多方利害關係人指導委員會副主席 (現任)
TechGirls 主持人 (現任)
台灣網路資訊中心 (TWNIC) 國際事務委員會委員 (現任)
2020年立委選舉台北市選區候選人
國家安全會議政策研究人員
吐瓦魯常駐聯合國代表團外交官
台灣／美國紐約州律師

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

薛福仁
網路治理研習營 優秀學員代表

經歷

橙迅科技公司工程師

圖13. 研習營講師簡介

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（部分課程以英文授課，現場不提供口譯）

（二）報名時間

自即日起至 2020 年 5 月 20 日 23:59 截止（臺灣時間）。

（三）報名方式

本次活動一律透過本網站線上報名，報名時須完整填寫報名表。



第1個區段，共3個

2020網路治理研習營報名表1

【重要聲明】您參加本次活動所填寫的個人資料（姓名、任職單位、職稱、email、手機等），將由NII產業發展協會於本次活動與未來相關活動通知之目的範圍內使用。我們將依個人資料法規定保護您的個人資料，您也可以隨時通知我們刪除您的個人資料。

第2個區段，共3個

一、基本資料

1. 姓名（同身分證件）*
2. 年齡*
3. 單位類別*
4. 單位與部門 / 學校與科系*
5. 職稱 / 年級*
6. 縣市（居住地）*

第1個區段，共3個

2020網路治理研習營報名表2

【重要聲明】您參加本次活動所填寫的個人資料（姓名、任職單位、職稱、email、手機等），將由NII產業發展協會於本次活動與未來相關活動通知之目的範圍內使用。我們將依個人資料法規定保護您的個人資料，您也可以隨時通知我們刪除您的個人資料。

第3個區段，共3個

二、參與情況

1. 請問您有什麼想參加本研習營（單選）？*
2. 請問您最關心什麼網路政策議題（單選）？*
3. 請問您曾參加哪些網路政策議題相關事務或活動（複選）？*
4. 如果錄取成為學員，是否將進一步參加優秀學員甄選（全程補助出國參加 APiGF 2020）？*
5. 補充說明（200字內），若有自我介紹短片，請在此提供YouTube連結；如有英文能力證明等補充資料，請email至 igcamp@nii.org.tw，謝謝。

圖14. 研習營報名表

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 30 名學員。

（三）結果公布與通知

評選結果訂於 2020 年 5 月 26 日（二）於本活動網站公布，並以 E-mail 個別通知錄取學員。

六、學員義務

（一）活動前夕

- 繳交「出席保證書」：為避免浪費學習資源，錄取學員須填寫「出席保證書」（未滿 20 歲者須經家長或監護人同意），並於 2020 年 5 月 28 日（四）前 email 主辦單位，先回傳者可優先選取分組組別。相關表單及說明將檢附於錄取通知中，未於期限內繳交視同無條件同意放棄本次活動參與資格。
- 完成預習課程（3 小時）：錄取學員須於 2020 年 6 月 4 日（四）前，完成預習及線上測驗，請詳「學習資源」。

（二）研習營期間

全程出席並積極參與討論；注意自身安全，並遵守活動規範。

七、交通與住宿補助

本研習營提供宜花東及新竹以南學員（全程參與課程者）交通與住宿補助，憑收據與票根核實報銷，並於課程結束後統一匯款作業。若有憑據不齊者，將無法獲得補助。

（一）交通補助

限 2020 年 6 月 5 日至 7 日期間的長途大眾運輸工具（客運、臺鐵和高鐵，且限標準車廂）一次往返，且須檢附來回車票票根。

（二）住宿補助

限 2020 年 6 月 5 日至 6 日單日住宿，補助上限為新臺幣 2,000 元整。

八、學員獎勵

（一）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。

（二）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，並於會後提供記錄摘要（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。徵稿時間延長至 8 月 31 日下午 3 時止，詳情請至 TWIGF 網站。

（三）APrIGF 線上特派員獎學金（5 名）

結業學員可申請擔任 APrIGF 特派員，透過線上參與方式，於會後提供 1 場座談記錄摘要（以中文撰寫；將刊載於本網站的【學習資源】），即可獲頒新臺幣\$2,000 元整獎學金。

（四）參與國際會議全額補助（1 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 1 名本國籍優秀學員參加 9 月 27 日~30 日於加德滿都舉辦的 2020 APriIGF（亞太區網路治理論壇），並提供機票、住宿與餐費。評選項目包括學習熱忱、論述與表達能力、英文程度等。獲選學員須配合主辦單位的相關安排參與會議，並於會後提供出國報告，且分享國際參與經驗。

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、交通資訊、線上報名、錄取名單、學習資源等 8 個項目選單，網站首頁如下圖 15 所示。



二、活動宣傳

本年度研習營的活動宣傳方式包括協請臺灣網路治理論壇（TWIGF）於其臉書社團發布活動公告，及發 email 邀請年度論壇的與會者；協請通傳會發文政府相關部會；本計畫發文全國大專院校、台灣電信產業發展協會，以及發 email 且致電邀請立法院跨黨派「數位治理委員會」。



圖16. 研習營宣傳圖文

三、報名與評選

本次研習營活動共收到 80 份報名表，扣除 5 份重複，計有 75 人合格報名。本次評選作業由本計畫 2 位成員及來自學術界與公民團體的 2 位外部專家，組成 4 人評審小組，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、英文程度等項目做綜合評估。評選方式採兩階段進行——個別評分及評選會議討論，最後選出 30 位正取學員及 15 位備取學員。

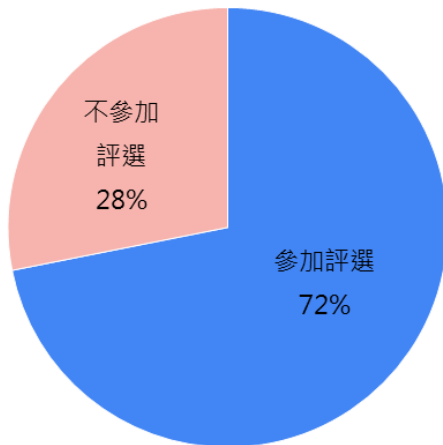
四、學員組成概況

經通知聯繫正備取學員後，共計 32 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 12，包含 18 位大專青年（56%）、7 位公部門人員（21%），以及 7 位來自民間各界的人士。大專學員的就讀科系橫跨文法商和理工科系，且有 8 位是碩博士班學生；公部門則包含通傳會、外交部、國防部和立法院人員；民間各界人士則來自公民團體、企業和學研單位。

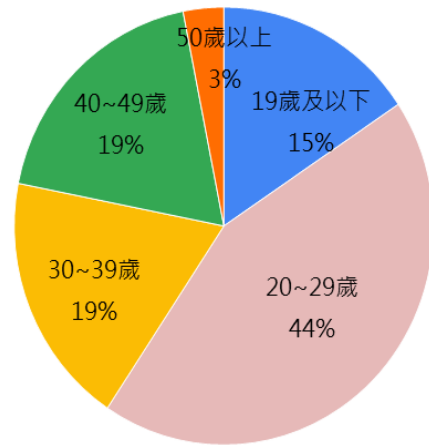
對應至年齡層，亦以 20~29 歲年輕人居多（44%）；參與經驗為高達 75% 都曾參加網路治理相關會議或社群；參與目的以單純「對網路治理議題有興趣」者為最多（56%），遠高於「與工作和學業相關」者（25%）；至於最關心的網路治理議題前 3 名依序為網路安全（35%）、網路人權（28%）、新興科技（16%），沒有任何學員表示對數位包容議題有興趣。此外，還有 72% 學員表示願意參加可獲得全額補助參與國際會議的「優秀學員甄選」。

而課程當日的報到學員共計 29 位，他們除了全程出席外，課程中也相當積極地提問及參與演練課程的討論，最後皆獲頒結業證書和獎學金（公務人員除外）。

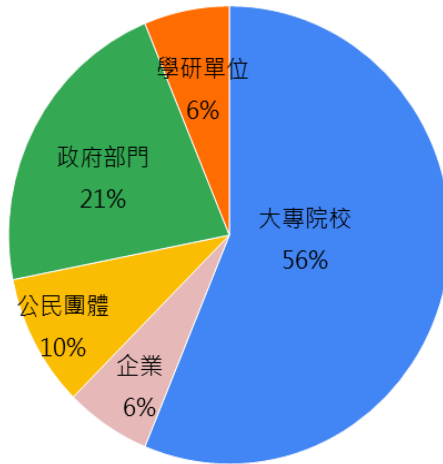
優秀學員評選 (補助參加 APrIGF)



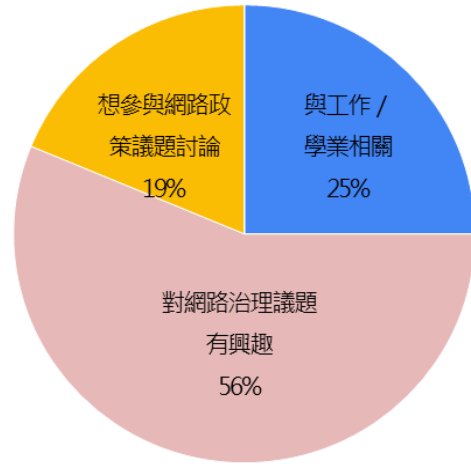
年齡



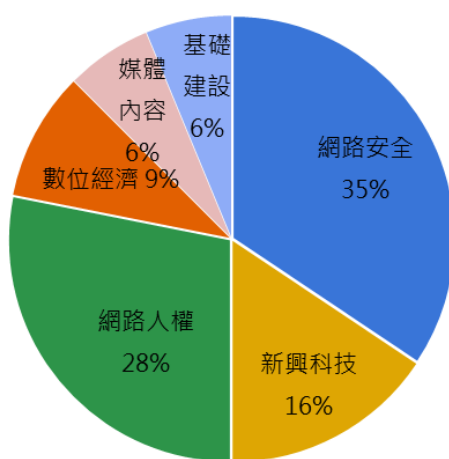
單位



參與本次活動目的

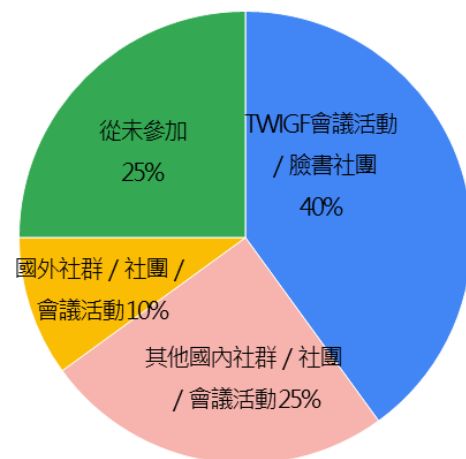


最有興趣議題



想改變目前網路政策 0%

相關參與經驗



數位包容 0%

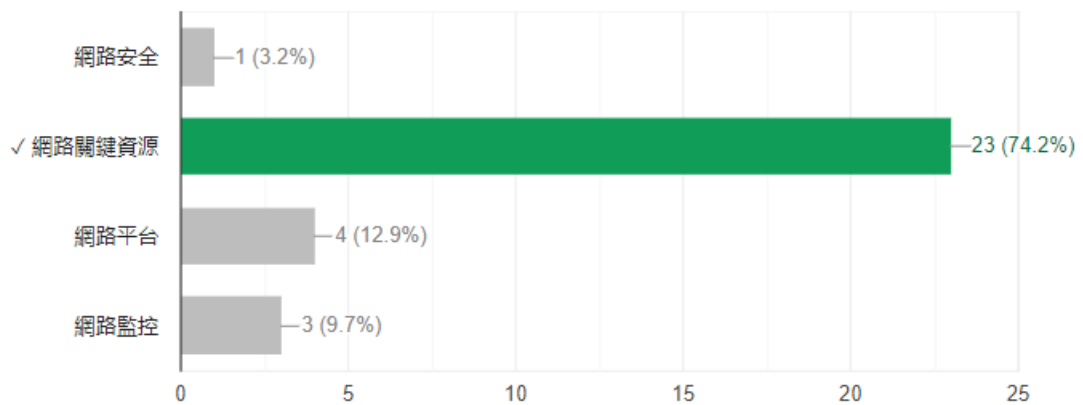
圖17. 研習營學員組成概況

五、學員課前預習線上測驗

本次活動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。結果共有 31 位學員作答，平均分數為 82.6 分，當中有 14 人滿分，8 人低於 60 分。各題答題結果如下圖 18 所示。

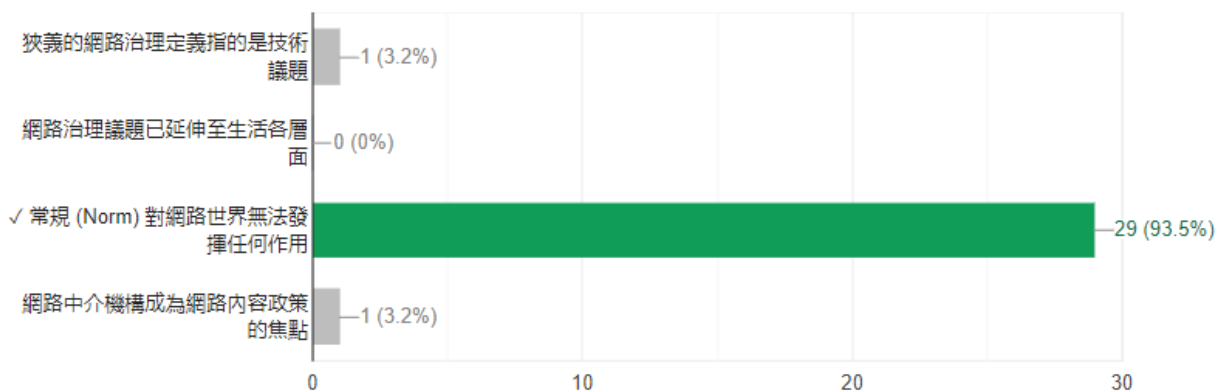
1. 網路治理「早期」的國際爭論焦點是？

答對次數：23 (作答總數：31)



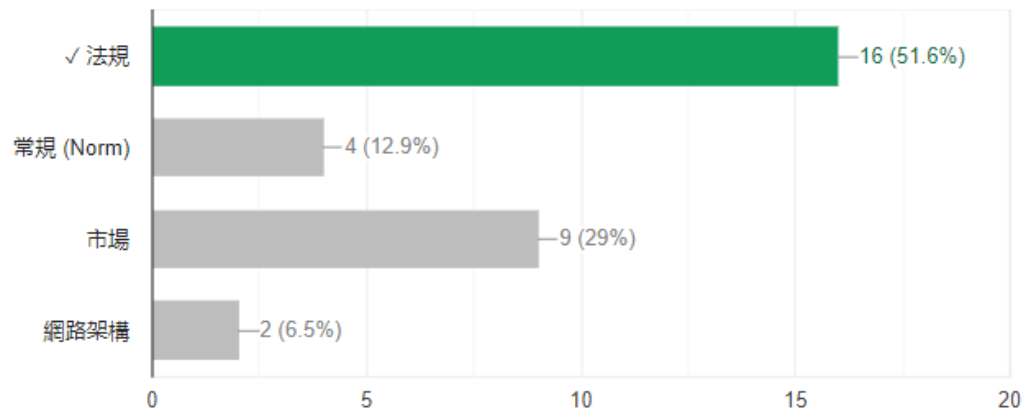
2. 有關網路治理的敘述，下列何者錯誤？

答對次數：29 (作答總數：31)



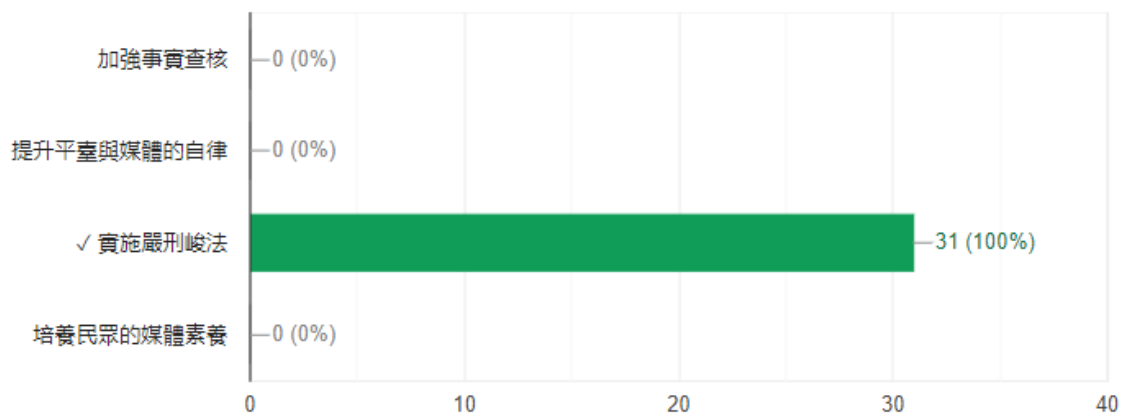
3. 影響網路空間的4個要素包括法規、常規、市場、網路架構。隨著時代演進，現今網路空間最重要的驅動力是？

答對次數：16 (作答總數：31)



4. 下列何者「不是」國際普遍認同的防制假訊息作法？

答對次數：31 (作答總數：31)



5. 有關網路之父Vint Cerf於專文中的描述，下列何者錯誤？

答對次數：29 (作答總數：31)

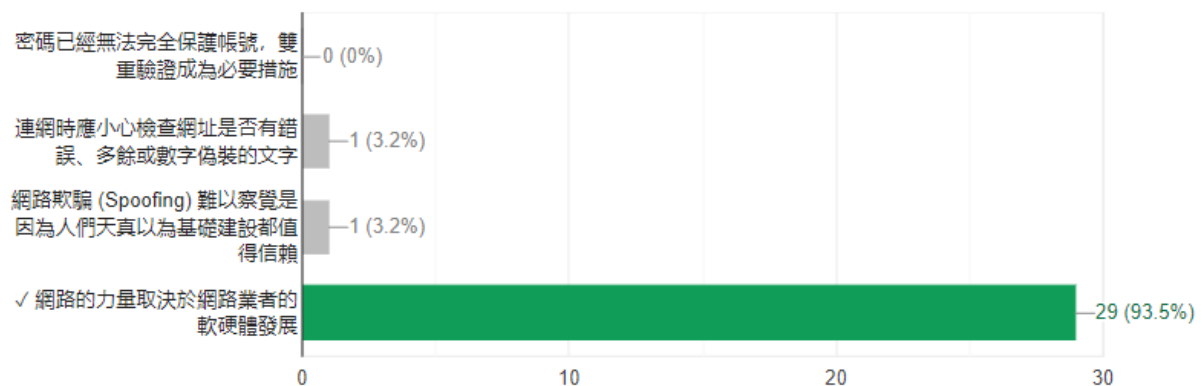


圖18. 研習營課前預習線上檢測答題結果

第三節 課程摘要紀錄

一、專題講習

(一) 網路人權

1. 演講摘要

講者：台灣人權促進會／何明誼 副秘書長

(1) 為何數位人權很重要？

全球市值前 10 大公司大多是網路公司（2019 年 8 月 1 日資料），例如美國的 Microsoft、Apple、Amazon、Alphabet、Facebook，以及中國大陸的騰訊、阿里巴巴。再以 Microsoft 為例，其市值超過 1 兆美元，比全球 GDP 排名二十多的臺灣還高，凸顯這些網路公司是富可敵國；加上它們提供的服務為大家每天使用，顯見對全球與人類都有巨大影響力。

現代人從起床甚至是睡覺都離不開網路（例如以 APP 監控睡眠品質），以致數位時代的我們猶如生活在圓形監獄，監獄管理員位處監獄的中心，可隨時在囚犯不知情下，監看他們的行為，這是以最少的資源與成本，做到最大有效管理。總之，數位人權攸關我們要如何生活在數位社會。

(2) 什麼是數位人權？

近年來國際社會逐漸形成使用「數位人權」(Digital Right)一詞的共識。國際網路人權組織 Access Now 將數位人權分成資料治理與保護、民主投票、媒體自由、人工智慧與演算法等 18 個面向。另外，《經濟社會文化權利國際公約》(ICESER) 第 15 條亦明列每個人都享有科學進步及應用的權利，臺灣也將相關權利融入國內法規，因此，常說上網是人權，也推動偏鄉的基礎建設。而在保障權利的同時，也表示要避免科技帶來的負面影響，因此，台權會並不是主張禁用晶片身分證、人臉辨識等科技應用，而是提倡要避免科技帶來的負面衝擊。

(3) 數位人權中的隱私權

隱私可說是一個呼吸的空間，它允許形塑自我發展及界定和世界的連結，例如我們希望所接收的資訊是由自己決定，而不是由 Facebook 或 Google 操弄。其實 1960 年代《公民政治權利國際公約》即有任何人的私生活與通信不得無理或非法侵擾等規範。而我國憲法雖然沒有「隱私權」這 3 個字，但 2005 年大法官釋字第 603 號解釋令即載明憲法第 22 條保障個人資訊自主權，人民可以決定自己的資料於何時被何人以何種方式使用。

另外，隱私權也不完全等同資訊安全，雖然有時候兩者會重疊，但有時候是單獨發生。例如日前傳出臺灣 2 千萬筆個資遭外洩且拍賣，即屬於侵犯隱私暨資安事件；而 Facebook 利用個資優化演算法並進行推播，則是侵犯隱私事件。

(4) 如何思考個資保護？

現在蒐集巨量資料的成本低廉，運算能力又強，可透過不同活動資料建構出一個人的剖析（profile），因此，大家要小心警覺。而這些資料大多屬於後設資料（metadata），例如 email 的寄件者、收件者、寄件時間、路由資料、信件或附件大小、使用的瀏覽器 etc.，即使不知道通訊內容，也能從中推斷出許多個人剖析。因此，對於政府進行通訊監察時，主張通訊紀錄不敏感故應不需經由法官同意即可取得通訊紀錄，實則不然。

(5) 以保障隱私權為基礎的個資處理原則

以保障隱私權為基礎的個資處理原則包括合法、目的特定、具正當利益等。當中有關資料主體的權利，如知情同意、資料的更正或刪除等，我國《個人資料保護法》皆有相關規範，但沒有拒絕剖析或自動化處理、資料可攜性等權利，因為這些也是歐盟近年才新增的權利。

大家可思考晶片身分證（eID）問題。臺灣每 10 年更換一次身分證，這次要改成果片，還具有電子簽章功能。因此，很多人擔心資安風險更

高，以及遭到國家監控。

2. 提問與回覆

- (1) 民眾普遍對於資訊安全認知薄弱。面對隱私權同意條款的萬言書，民眾常常在不甚瞭解的情況下就將權利讓渡出去，究竟該如何消弭企業與民眾之間因資訊不對稱所產生的誤會？
- (2) 有別於人權工作者對於網路人權的捍衛與維護，部分民眾似乎不在意自己的個資被蒐集使用，甚至認為企業依個人喜好投放廣告或資訊，是客製化服務的表現。鑒於一般民眾與人權工作者對於網路人權的態度大相逕庭，人權工作者是否應該繼續努力，或是該如何取得平衡？

回覆（兩題一起回答）：民眾對於個資安全的認知普遍薄弱，而目前的知情同意書又淪為一個形式，內容往往太過艱澀難懂，以致使用者無法清楚瞭解自己的個資將會被如何使用。先前歐盟 GDPR 修法已針對知情同意書明確規範了企業或政府應該使用清楚易懂的語言，告知使用者個資被蒐集利用的風險。另一個問題是，企業或政府沒有真正落實告知責任，例如政府在疫情期間利用電信業者所提供的個資來評估景點的人數，卻沒有清楚告知人民如何使用或使用哪些資料。清楚的告知行為可以讓民眾瞭解自己身處的情況，或是在權利受損時可以明確主張那些權利主體受到侵害。

- (3) 目前網路治理領域大家較關心的是來自政府的監控，還是企業的監控？政府該如何應對或是監督個資安全，又企業與使用者權力不對等的問題該如何改善？

回覆：不管是政府或是企業的監控，對於個資安全議題的思考框架都是相同的。在面對個資安全被侵害時，政府可採取法律行動來加以制裁（如愛爾蘭政府控告 Google 的個資蒐集政策），但對於個人來說，面臨受到侵害的情況是相對無能為力的。

（二）經濟與新興科技

1. 演講摘要

講者：理律法律事務所／熊全迪 律師

（1）共享經濟

共享經濟即是國父所主張的「物盡其用、貨暢其流」概念。以 Uber 為例，早年主要的法規爭議在於它是屬於資訊媒合平台或是特許的計程車客運業，後來 Uber 依據《公路法》改為和國內小客車租賃業合作，但交通部又修改相關管理規則，要求租賃時間至少 1 小時且須從車行出發等，影響 Uber 營運。而 Airbnb 也差點面臨挑戰，交通部 2019 年預告修法，將違法經營旅館業，或平台刊登非法旅宿資訊，皆分別處以 200 萬元罰鍰，後來法規沒有通過。外送平台則是出現承攬或雇傭關係的爭議，平台業者主張和外送員是平等的承攬關係，因此未替外送員投保勞健保等，但外送員須穿制服且使用特定外送箱，具有組織從屬性，又接近雇傭性質。這些案例也顯示，政府於共享經濟上，面臨同時需要保護既有產業和發展創新的兩難局面。

（2）人工智慧（AI）

人工智慧的治理議題首先是責任歸屬，以全自動的自駕車為例，車主其實猶如乘客，一旦發生事故，究竟該由負責設計製造的車商或是由購買的車主負責？又如果 AI 決策造成歧視該由誰負責？這些問題有待思考。而在智慧財產權上，目前 AI 的作品尚且無法取得專利或著作權。至於法規方面，我國曾有立委提出「人工智慧發展基本法」，未獲得通過，但科技部訂有《AI 科研發展指引》、金管會亦有《金融科技發展與創新實驗條例》（金融監理沙盒）、經濟部推出《無人載具科技創新實驗條例》（無人車沙盒），而在歐盟則有《人工智慧道德準則》等規範。

（3）區塊鏈

區塊鏈的主要應用為虛擬貨幣，其他應用如農業、食品安全等。區塊鏈的最大問題為個資保護，因為歐盟 GDPR 對於資料跨境傳輸是採原則禁止，但區塊鏈是無國界的記帳本，理論上資料一定會傳到境外，此點和法規有衝突。另一問題是我國個資法可以要求刪除個資，歐盟 GDPR 還有被遺忘權，但區塊鏈具有不可竄改的特性，可能會因此違法。

區塊鏈的應用還有智能合約，也就是當滿足一定條件時，程式就會自動執行。但它也涉及國家管轄權爭論、無法移轉登記所有的權利、無法確認使用者是否具法律行為能力、無法呈現法律意義上的契約內容完整性等問題。

(4) 虛擬貨幣

虛擬貨幣中的加密貨幣，最知名的是比特幣、以太坊等。其主要爭議在於它究竟是屬於資產、財產，或是有價證券。瑞士主管機關以代幣稱之，並將代幣分成支付型、使用型、資產型（證券型），共 3 種。我國金管會 2019 年擬定證券型代幣（STO）監理規範架構，採取分級管理方式。

(5) 物聯網（IoT）

物聯網需思考個資保護與資安問題，但資安問題不一定涉及個資，也可能是國安資料遭外洩等問題。

2. 提問與回覆

(1) 近期社會關注外送員的工作權益是否應該由勞基法來保障，又外送員與業者之間為雇傭還是承攬關係的相關討論眾說紛紜。目前較少從承攬關係的方向來討論。請問從承攬關係做規範會有甚麼問題嗎？

回覆：對於勞務工作不應該只有二分為雇傭關係或是承攬關係。也許可以將勞工保險、雇傭關係以及承攬關係之間的關聯性分開來規範，折衷找出解決的解決方法。

(2) 請問身為非技術背景的法律工作者，在面臨技術不斷改變時，如何從中發覺法律上的不足或是政策上的修正？又是如何看待經濟與新興科技議題？

回覆：以開放的心態多吸收不同的資訊，當新興科技應用於社會活動而產生法律相關的議題時，身為法律人士便能快速掌握內容，進而做出建議或詮釋。

(三) 網路治理與國際關係

1. 演講摘要

講者：NII 產業發展協進會／吳國維董事

(1) 網路運作與唯一識別碼

任何裝置連上網路，必然會涉及 IP 位址、域名（Domain Name）、根伺服器（Root Server）等網路底層架構，而且不需經過實體世界的海關，就可以連到世界各國的網站，因為它是全球通用的架構。IP 位址與域名也稱為「唯一識別碼（Unique Identifier）」，當使用 IP 位址時，它必須是唯一的（類似電話號碼），也就是同一時間不能有 2 個人使用同一個 IP 位址，否則技術上會有衝突，無法辨別資料究竟要傳輸給誰。域名也是「唯一識別碼」，如果有 2 個域名完全相同，在網路上將無法解析。早期網路只有 IP 位址，但因為這些數字很難記憶，於是 Jon Postel 發明網域名稱系統（DNS），將 IP 位址與域名做逐一對應。

(2) gTLD 與 ccTLD 的治理議題

不論是 IP 位址、域名，或根伺服器，都是在 IETF（Internet Engineering Task Force，網際網路工程任務小組）定義，它是全球網路技術標準的來源。Jon Postel 創造 DNS 時，通用頂級域名（Generic Top-level Domain, gTLD）只有 .com、.org 等 6 個，後來大家覺得不敷使用，所以，2006 年開放 new gTLD 申請，以致目前全球約有 1,500 個 gTLD。還有另一種是國碼

頂級域名（Country code top-level domain, ccTLD），它是根據 ISO 3166 列表制定，但 IETF 從未指 ccTLD 是國家擁有，且全球一半以上的 ccTLD 是由商業公司營運而非國家。不過，大約從 1999 年後，許多國家開始認為 ccTLD 屬於政府所有，一些太平洋島國的 ccTLD 也是國家外包給商業公司管理維運。臺灣的.tw 是由台灣網路資訊中心（TWNIC）負責，大家可以思考政府是否有透過公開招標程序委託 TWNIC 管理.tw 等問題。

(3) IANA 與 ICANN 監管權的國際爭議

由於網路是美國國防部於 1970 年代所發明，所以，全球 IP 位址與域名事務在 2016 年之前，是在美國商務部的監管下，由網路號碼指派機構（Internet Assigned Numbers Authority, IANA）負責，且其業務自 1999 年起外包給位於美國加州的非營利組織——網際網路名稱與號碼分配機構（Internet Corporation for Assigned Names and Numbers, ICANN）。此和美國的「政府不插手民間能做的業務」文化有關。不過，歐洲於 1996 年曾主張 IANA 應該改設立於瑞士且由國際共管，但美國基於網路屬於美國資產的立場而拒絕交出 IANA。直到 2016 年歐巴馬政府才正式將 IANA 監管權移交給 ICANN 且改為國際共管模式。

此外，聯合國於 2003~2005 年期間也曾於美國的反對下，討論 ICANN 的管轄權，並提出 4 種國際共管模式。原本歐洲擬從中挑選 1 個模式並支持，但後來考量聯合國的官僚與低效率問題，轉為支持美國，此爭論迄今仍懸而未決。

(4) IP 位址的治理議題與國際爭議

全球 IP 位址由五大洲的區域網際網路註冊機構（Regional Internet Registries, RIRs）負責管理與發放，中、俄、印等國早於 1997 年即質疑此管理機制，並主張應將 IP 位址分配到各國且自行管理。相關爭議性問題如為什麼由這 5 個 RIRs 負責、它們又該由誰管理、RIRs 採會員制是否合理（需先加入會員才能申請購買 IP 區段）、除購買費用外每年還需另外繳費

是否合理等。不過，由於當年 IPv4 位址已經發出 6 成，且接管程序複雜，之後 IPv4 又於 2016 年發放完畢，因此，此問題就不了了之。

此外，全球 13 顆根伺服器中有 10 顆在美國，也是國際間爭論不休的問題，因為每個國家都想要擁有，於是演變成現今全球有近千顆鏡像伺服器情況。

講者：禮騏法律事務所／謝佩芬（前）顧問

(1) 聯合國是官僚制度嚴重的組織？

聯合國大會由 193 個會員國組成，規模愈龐大的組織，科層制度就愈複雜。為了整合、管理來自眾多會員國的需求與意見，聯合國的科層制度必然比單一國家要來得複雜許多，也因此在各項事務的推動上，複雜的制度導致效率的低落，常常招來對聯合國辦事效率的批評。雖然如此，但聯合國在國際間佔有舉足輕重的地位。

(2) 聯合國的運作機制

聯合國分為六大組織，分別為大會、安理會、經濟及社會理事會、秘書處、國際法院以及託管理事會。主要事務的推動與決策通常由大會以及安理會來主導。加入聯合國除了要是一個主權獨立的國家外，還必需經過安理會 9 票的同意才得以加入。而臺灣遲遲無法加入聯合國的原因，就是受到身為常任理事國中國大陸的長期阻撓結果。

聯合國大會下分為六個委員會（裁軍和國際安全委員會、經濟和金融委員會、社會、人道主義和文化委員會、特別政治和非殖民化委員會、行政和預算委員會及法律委員會），分別針對各項議題召開定期會議，且全程網路轉播，即使是非會員國也能線上參與。對於國家外交而言，重要的並非這些定期會議，而是在正式議程以外的非正式磋商，以及更機密、只在各國使節之間的非正式討論。透過這些非正式的討論，有助於更加瞭解國際間的生態。

(3) 聯合國設置常任理事國的原因

第一次世界大戰結束後，國際秩序尚待重建之際，國際聯盟的出現試圖整頓國際秩序，維護世界和平。無奈當時的大國如美國等不願加入，其他組織內的大國因維護自身的利益，不願配合國際聯盟的運作，導致國際聯盟的瓦解。二戰之後，考量到國際聯盟的前車之鑑，為了吸引各方大國加入，特別設立安全理事會以及常任理事國制度，以擴張大國在組織內的權力，增強其加入聯合國的誘因。

(4) 加入聯合國的重要性

透過加入聯合國，除了享有與其他會員國相同的權利外，在正式議程以外的非正式磋商和非正式討論，在外交過程上扮演非常重要的角色。非正式磋商有助於國家之間的交流，並能夠瞭解他國對於各項議題的立場，進而尋求合作互利的機會，以達到提升國家利益的效果。

2. 提問與回覆

(1) 針對外交方面的資安議題，政府還有甚麼改善空間？ccTLD 若交由民間主導管理，政府該如何去監督規範？

回覆（謝佩芬）：蔡政府上任後，清楚定調資安即是國安的一部分。資安議題不一定由政府主導，通常是由私部門為因應其產業需求，協同學術界共同研擬，進而推動資安的相關措施。鑒於全世界的資安人才不足，日益精進的駭客攻擊防不勝防，政府只能被動地回應，無法積極地全面預防，因此，透過多方利害關係人的共同應對是很重要的。

回覆（吳國維）：假新聞、垃圾郵件是否為資安議題？又定義為何？兩者的定義因為立場不同而有所差異，如垃圾郵件對於政府、民眾是困擾的行為，但對於業者而言卻是成本低廉又有效的行銷手段。由此可知假新聞、垃圾郵件該如何去定義是值得討論的。從 ICANN 結構的角度來看，資安議題就是 IP 位址、域名、根伺服器三者所組成。其中令

人擔憂的是 IP 位址被冒用，因此，需透過 RPKI (Resource Public Key Infrastructure，資源公鑰基礎建設) 去驗證使用者身分。而域名同樣也有被冒用的風險，需透過 DNSSEC (DNS security extensions，域名系統安全擴充) 確保使用者有獲得充分的授權。上述資安議題可藉由 ICANN 的政府諮詢委員會 (GAC) 集結各國政府的意見，並對 ICANN 提供相關議題的建言。最後也建議臺灣參與國際會議或組織發言時，應該提出國際間通用的議題，而不是只針對自身立場提出單方面的需求，可以試圖將自身問題擴張為國際議題，不僅在解決問題時能使自己受益，同時國際也能跟著受益，國際議題更能得到國際的共鳴與關注。

(四) 網路安全與基礎建設

1. 演講摘要

講者：台灣網路資訊中心 (TWNIC) / 黃勝雄 董事長暨執行長

(1) 網路基礎建設的發展

A. 網路封包與動態路徑

1969 年美國 3 個實驗室的網路串接，第一次使用 TCP/IP (Transmission Control Protocol / Internet Protocol，傳輸控制協定/網路協定) 封包傳遞訊息。從當時一直到今天，封包傳遞都是動態的，沒有規定路徑。目前全球網路每天約有 90 萬筆路徑，當中有 20 萬筆會更新，顯示每天約 20% 的路徑是持續變動中，這是網路的特性，但也衍生出網路安全問題。

B. 全球網路根伺服器的治理議題

全球共有 13 顆根伺服器，且主要由美國維運，此點長期引發許多國家不滿。由於網路世界日益和實體世界融合，網路受控於某國形同是重大國安議題，所以，中國大陸於 2016 年通過《網路安全法》，俄羅斯於 2019 年實施網路獨立法案，其目的都是希望獲得更多的網路主導權，避免過度依賴由美國掌控的全球網路。但這些立法是否有效，可再另外討論。

C. 網路市場主導者的演變

網路市場過去由電信業者主導，但現在電信業者變成笨水管，改由內容業者稱王，因為網路流量來自網路內容透過內容傳遞網路（Content Delivery Network, CDN）遞送訊息。以北美地區為例，預估 2021 年 91% 網路流量是由 CDN 傳送；臺灣目前則約佔 70~80%，這也代表很多資料不是在網路上讀取，而是在本地儲存設備下載，所以大家覺得追劇速度很快。又過去內容業者曾向電信業者要求網路中立，但現在連興建海纜都由內容業者主導。也因此，當環境演變時，我們要思考法規是否應該跟著調整，否則耗費大量資源訂定電信管理規範，結果卻只管到 9% 的網路訊務。

D. 資料跨境流通的問題

現在各種商業活動都在網路上執行，數位貿易即將超越實體貿易，但也產生資料落地、跨境傳輸、資料自由流通與違法資料控制等問題，且很多議題及各國相關法規彼此衝突，有賴更高的國際原則加以調解。

E. 海纜的重要性

全球超過 95% 流量由不到 200 條海纜傳送，所以海纜成為未來戰爭的攻擊目標。海纜也是數位經濟的主要戰場，Facebook、Google、Amazon 等內容業者都大量投資網路基礎建設，逐漸取代傳統電信業者的角色。此外，SpaceX 公司將在全球發射 2 萬顆衛星，一旦完成，也將成為全球重要的網路基礎設施。

(2) 網路安全的治理

A. 利用 IP 位址與域名的犯罪行為

IP 位址與域名都會遭到仿冒或篡改。若從網路犯罪行為來看，利用 IP 位址的犯罪行為如 SSH（Secure Shell，安全外殼協定）暴力攻擊、DDoS（Distributed Denial-of-service，分散式阻斷服務）攻擊、寄發垃圾郵件等；利用域名的則如釣魚網站、惡意網站、惡意程式或勒索軟體的幕後操作網

站等。此外，這些非法行為也透過分散方式運作，以致查緝非常困難，例如商業登記於巴拿馬，但從歐洲網路協調中心（RIPE NCC）取得 IP 位址，而實際營運則在俄羅斯。

B. 跨國查緝網路犯罪的方式

網路無國界，但網路犯罪通常是跨越國境，且犯罪軌跡資料猶如大海撈針，還要面臨跨境司法管轄權問題，因此，案件難以偵破。目前解決方案有 3 種，首先是《司法互助協定》（MLAT），現在已較少使用，且和臺灣簽署的國家有限。第 2 是《布達佩斯公約》（Budapest Convention），全世界有 30 多個國家簽署，締約國可以跨越彼此國境調查網路犯罪，但速度仍緩慢且過程複雜。第 3 是透過司法機關彼此合作取得資料，不過，合作方式與內容不透明。

C. 網路空間主導元素的轉變

根據新芝加哥學派理論（New Chicago School Theory），網路空間是由法律、常規、市場、網路架構等四個元素管理。20 年前的情況為「程式碼就是法律」（Code is Law），它決定網路空間的使用行為。但自 2018 年歐盟實施 GDPR，變成「法律即（市場）規則」（Law is Code）。不過，常規也可以規範網路空間的使用行為，例如網路的通訊協定、號碼、域名的分配與監管機制，皆不是政府單位主導，而是由利害關係人共同訂定政策。

(3) 網路攻擊肇事者認定調查（Cyber Attribution）的重要性

網路 IP 位址可以造假，且難以追蹤，例如 2017 年肆虐全球的電腦勒索病毒 WannaCry，原本依據查得的 IP 位址以為是源自北韓，但後來發現此 IP 位址是假造的。由於無法追蹤真正的 IP 位址，就無法追查真實的所在地，進而找出肇事者，並依法論處，因此，連發明網路的美國國防高等研究計畫署（Defense Advanced Research Projects Agency, DARPA）都對外尋求協助，期能改善網路攻擊肇事者的調查方法。另一方面，也正因為 IP 追蹤困難，所以，很多國家於入境時，要求繳交社群網站帳號，以從中取得

情資，這也成為資安偵防的重要一環。

網路攻擊肇事者的認定調查對國家安全而言，是至關重要。因為根據《塔林手冊》(Tallinn Manual)，遭受網路攻擊或武力威脅的國家後續可以採取的措施不只是防守，而是可以行使自衛權，或是「先發制人」，主動發動預防性的武力或網路攻擊措施。

2. 提問與回覆

- (1) 各國規範網路的法律不盡相同，假設甲國的人民在乙國違反當地法律，甲乙兩國都主張對於該行為人擁有管轄權，當兩國的法律有衝突時將會如何解決？是否有實際案例？

回覆：就國際的準則而言，不論行為人國籍為何，犯罪行為所在國家都具有管轄權。問題的核心在於域外效力，而執行力取決於國家的實力。例如針對網路侵權行為，臺灣的法律罰則僅有罰款，但如有來自國外的侵權行為，而違法的機構沒在臺灣境內登記設立，就無法處罰國外的行為人。臺灣法律的域外效力相當薄弱，所以，法規應清楚訂定違法者將停止網路內容的接取、移除或瀏覽，以增強法律的執行力。

- (2) 請問您是否支持政府基於維護主權或防制犯罪等理由，而接掌網路的管轄權？大型企業的實力富可敵國，來自企業的監控漸漸地與政府的管制抗衡，請問兩者之間該如何取得平衡？

回覆：當國家遭遇緊急狀態或重大事件，政府有權依法進行管制措施，所實行的管制必須經過立法機關的監督並符合比例原則。若是遇到衝突狀況，要在法律的框架之下，使用上位原則來整合。

(五) 網路內容與平臺

1. 演講摘要

講者：理律法律事務所／曾更瑩 合夥律師

(1) 現實生活法律亦適用網路內容

現實生活中和「內容」有關的法律，都會適用到網路上的內容。例如高雄市長韓國瑜罷免案於6月6日進行投票，中選會根據《公職人員選舉罷免法》指出，投票日當天零時起，即禁止於網路上發表或轉貼支持或反對罷免的資訊，否則將處新臺幣50萬元以上罰鍰。

網路內容無所不包，不論是社交聯絡、食衣住行、育樂、查資料，大家都會接觸到網路內容。它們的共同特徵就是內容大多是由用戶提供，平臺只是彙整呈現。

(2) 網路平臺是否應為用戶所張貼的內容負責？

A.《著作權法》案例

小強於部落格上的照片遭大強盜貼於Instagram (簡稱IG)，小強因此要求IG刪除大強的侵權貼圖，並賠償損失。依據《著作權法》，小強須證明照片是他原創且遭大強盜用。而IG如要主張免責，則須提出相關證明，例如已警告用戶不得侵權、具有保護著作權及侵權的處理措施、IG沒有從侵權內容獲利等。

B.《兒童及少年福利與權益保障法》案例

媽媽發現小明沉溺於網路且玩的遊戲過於血腥暴力色情，因此向主管機關投訴，認為遊戲廠商應為提供限制級遊戲給青少年，負起法律責任。依據《兒童及少年福利與權益保障法》，父母應禁止兒少沉溺於網路，任何人也不得販賣或提供對兒少有害的物品或內容。再依《遊戲軟體分級管理辦法》，遊戲業者須進行內容分級，如有侵害兒少身心健康內容，則須限制接取瀏覽或移除該內容。

C.《動物傳染病防治條例》案例

小華從電商平臺訂購食品，收到貨物後才發現成分含有非洲豬瘟疫區的豬肉。依據《動物傳染病防治條例》，此廣告刊登者、平臺提供者、應

用服務提供者或電信業者，應採取加註防疫宣導警語、保存相關業者與訂購者的資料，以及限制接取、瀏覽或移除相關網頁內容等措施。

(3) 平臺是否應過濾或監控用戶所張貼的內容？

平臺一旦採取管制措施，必會涉及言論自由問題。雖然我國憲法明文保障基本人權，但也列出可採法律限制的例外情況，如為了防止妨礙他人自由、避免緊急危難、維持社會秩序、增進公共利益等。因此，對於公然侮辱和毀謗、國家安全、兒少保護、商業廣告、網路霸凌、假訊息等都有相關法規，至於仇恨和種族歧視問題，臺灣則較少見。

其實國際公民團體早已訂定《馬尼拉中介者原則》，他們認為一旦要求網路中介者（ISP、社群網路平臺、搜尋引擎等業者）為內容負起法律責任，將會破壞言論自由和隱私權，因此，主張網路中介者應免於對第三方內容承擔責任。

(4) 各國內容法規趨勢

A. 美國

美國於 1996 年制定《通訊規範法》，用以管控兒童接觸到低俗淫穢言論。當中第 230 條保障網路服務供應商免責於使用者所張貼的言論，同時也賦予它們（審查）限制冒犯性內容的權力。不過，美國總統川普於 2020 年 5 月 28 日簽署行政命令，要求聯邦通訊委員會（FCC）審查第 230 條中，對社交網站的保護，以阻止社交網站進行言論審查。

B. 德國

德國於 2018 年實施《社交網路強制法》，要求大型社群網站必須在接到檢舉後的 24 小時內，移除「明顯」違反德國刑法的仇恨言論，對於「較不明顯」或「有爭議」的仇恨言論，也須於 7 天內決定是否移除。屢次失責的業者最高將面臨 5 千萬歐元的罰鍰。而 2020 年 2 月 19 日梅克爾內閣進一步提出加重社群網站責任的新方案，並提交國會商討。

C. 法國

法國於 2020 年 5 月 13 日通過一項法律，規定網路平臺業者必須在 1 小時內，刪除戀童癖和恐怖主義等相關內容，否則最高可處全球營收 4% 罰鍰；對於其他「明顯違法」內容，則給予 24 小時處理。另一方面，法國法院將設立專門的數位檢察官，且政府也將成立專責單位，負責觀察網路仇恨言論。此法引發不切實際、干涉言論自由等批評。

D. 臺灣

我國有關散播假訊息的法規，過去只有《社會秩序維護法》第 63 條，現在則有很多，例如《傳染病防治法》第 63 條、《嚴重特殊傳染性肺炎防治及紓困振興特別條例》第 14 條、《災害防治法》第 41 條、《食品安全衛生法》第 46-1 條、《總統副總統選舉罷免法》第 90 條、《公職人員選舉罷免法》第 104 條等，這些法規對於散播者都祭出刑事處罰。但我國對平臺業者目前是採取自律方式，Facebook 和 Line 等主要業者於 2019 年發布「不實訊息防制業者自律實踐準則」。

各國對於規範網路內容有不同做法。究竟平臺業者是否該為用戶張貼的內容負責或進行監控，值得大家思考。

2. 提問與回覆

- (1) 在德國、法國，哪些人可以要求平臺業者下架仇恨言論？仇恨內容又如何定義？

回覆：只要是公民皆可以去投訴、要求言論下架，一旦接獲投訴，平臺就必須做出處理。

- (2) 約束內容的實體法為社會秩序維護法。當內容違法接受司法機關審判時，程序法會如何處理？

回覆：民事庭的法官無強制執行力，若當事者或其他第三人不願配合提供資料，僅會受到罰鍰處分；刑事庭法官則可根據刑法處以拘提、

搜索、扣押等動作，具有強制力。但司法審判都是非常曠日耗時。

(3) 根據《遊戲軟體分級管理辦法》，遊戲必須針對內容進行分級，但是業者該如何辨別使用者是否真正成年？法律是否真正發揮作用？

回覆：業者可以透過要求用戶輸入出生年等資訊確認其年紀，或是透過信用卡等付款資訊，判斷使用者並非未成年人。在發生爭議時，如遇到刻意隱匿年紀的個案，也應該積極處理，以絕後患。

二、分組演練

分組演練課程將學員分成「網路人權」、「經濟與新興科技」、「網路治理與國際關係」、「網路安全與基礎建設」、「網路內容與平臺」5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。分組方式係由學員依個人興趣自行選擇，每組 5~6 位學員。最後再由各組指派代表上臺報告討論結果，主要重點彙整如下表 11。

表11. 研習營學員成果報告彙整表

組別	1. 網路人權
題目	企業提供個人化服務與數位人權
共識	- 企業提供個人化服務時，應該提供消費者查詢個資的管道，並且讓消費者了解會如何處理、利用個資。此外，雖然消費者有權選擇其他企業的服務，但特定企業所提供的服務在現代生活中扮演著關鍵角色，使得消費者不得不繼續使用該服務，因此，企業或許可依消費者同意個資的比例，提供相對應的服務，而不是單方面強硬要求蒐集個資。 - 政府的管制應尊重企業與消費者的締約空間。唯有在特定情況下（如涉及基本民生設施、國安），政府才適時介入管制，以維護使用者權益。
組別	2. 經濟與新興科技
題目	共享經濟下的勞工權益應如何保障？以外送平臺為例
共識	外送平臺與外送員之間的權利義務不對等，外送員的工作性質不受勞基

	法的保障，當權益受損時，在沒有工會及勞基法的保障下，難以向資方爭取權利。因此，應由政府主導協調勞資雙方訂定定型化契約。 ● 解決外送員權益受損的方法，不應只限縮於承攬關係或雇傭關係的認定上，而透過定型化契約明文規範雙方的權力義務，不僅能夠保障外送員的權利，也能促進共享經濟的發展。雖然平臺和餐廳的成本將因此增加，但政府可透過節稅獎勵等方式，減輕它們的負擔。
組別	3. 網路治理與國際關係
題目	RIRs 會費機制、域名管理、根伺服器分布等國際網路規則是否合理？
共識	● 雖然 RIRs 因地制宜的會費機制屬合理，但是合法性（legitimacy）問題需進一步討論。 ● ccTLD 不一定象徵國家，如港澳等地皆有 ccTLD。這有賴於網路治理機制的獨立運作，讓各地能夠自由使用各種域名。 ● 目前全球共有 13 顆根伺服器，當中只有 3 顆位於美國以外區域。從自由競爭角度來看，美國因資金和技術優勢而擁有 10 顆也是合理，但過度集中會有連線中斷的風險。此問題已可透過 Anycast 技術設置多個鏡像伺服器加以解決，且各國都可以申請設置。
組別	4. 網路安全與基礎建設
題目	New gTLD 的政策規範
共識	● 經評估 ICANN 仲裁域名爭議的四大規則—混淆字串、侵害合法權益、違反善良風俗、侵害社群利益，本組認為可以申請的 New gTLD 包括.台派、.媽祖、.civil society、.中華民國、.辣台妹、.public policy 以及.XDD 等名稱；而不宜申請的名稱如.gov 與.g0v，以免產生字串混淆的爭議。
組別	5. 網路內容與平臺
題目	網路平臺與政府是否應該為內容負責？
共識	● 基於保護網路使用者的安全，網路平臺應適時監控平臺上的內容，尤其涉及人身安全、公共危險的言論，不應無限上綱地被保護。 ● 民眾雖然期待政府扮演主持公道的角色，但也不願意政府過度介入。不過，政府仍然應該監督網路平臺的審查行為，必須透過法律以維持最低度的監控界線，進而因應科技的潛在風險。

第四節 圖文影音紀錄

一、 布置與印刷品

本次課程的布置與印刷品包括議程版、講桌版、識別證（3款），以及研習證明書，成品如下圖 19 所示。



圖19. 研習營布置與印刷品

二、活動剪影



專題講習與 QA



分組演練



小組成果報告

圖20. 研習營活動剪影

三、課程簡報與錄影檔

本次專題講習課程的簡報資料與錄影檔（限講師同意的課程）彙整於活動網站「學習資源」（<https://www.igcamp.tw/resources/>）以供開放使用。



圖21. 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）。

本次問卷調查於結業式前進行，共計發出且回收29份問卷，回收率為100%。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」、「其他建議」4個部分，統計結果說明如下。

一、課程內容滿意度

本年度學員對於課程內容的整體設計給予 100% 滿意的高度評價（非

常滿意及滿意)，且不論是分組演練、專題講習或預習教材的滿意度都超過 9 成以上（分別為 90%、97%、93%）。

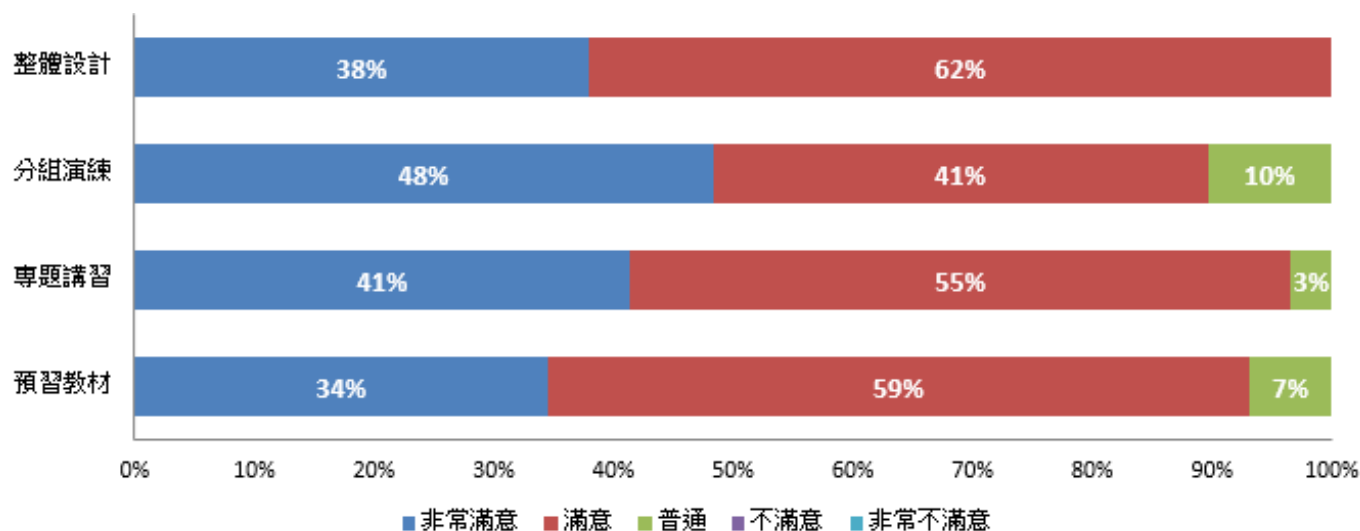


圖22. 研習營「課程內容」滿意度

二、行政會務滿意度

本年度學員對於行政會務同樣給予高度肯定，對餐飲和活動地點的滿意度（滿意及非常滿意）都達 100%；對行政服務的滿意度也有 93%。

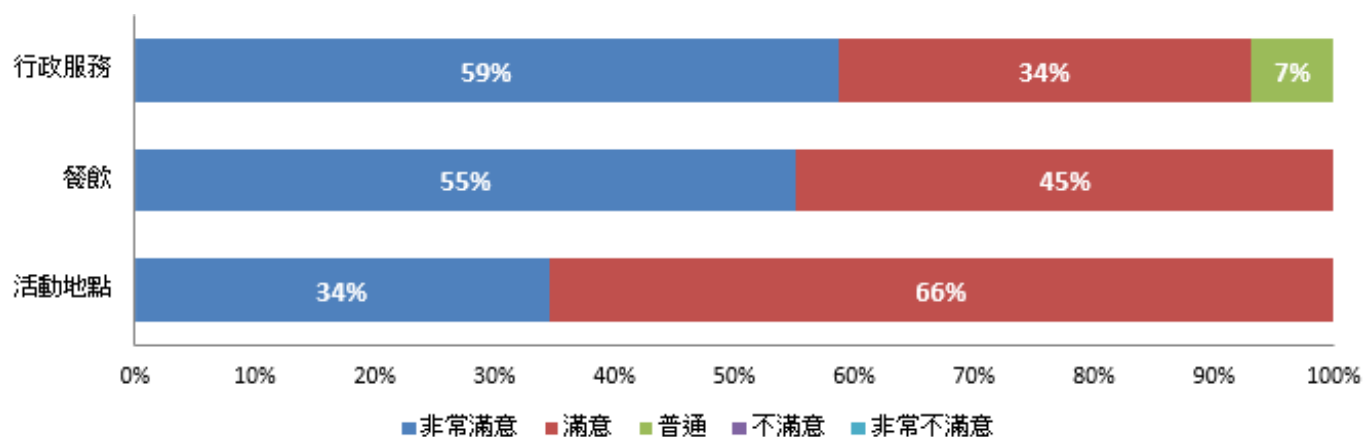
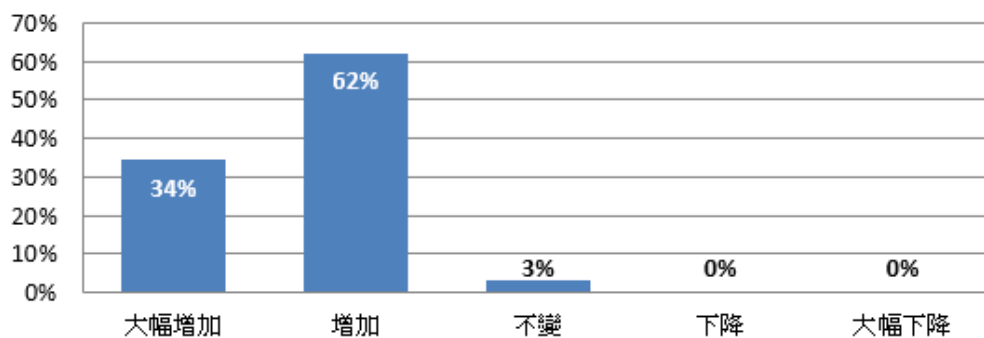


圖23. 研習營「行政會務」滿意度

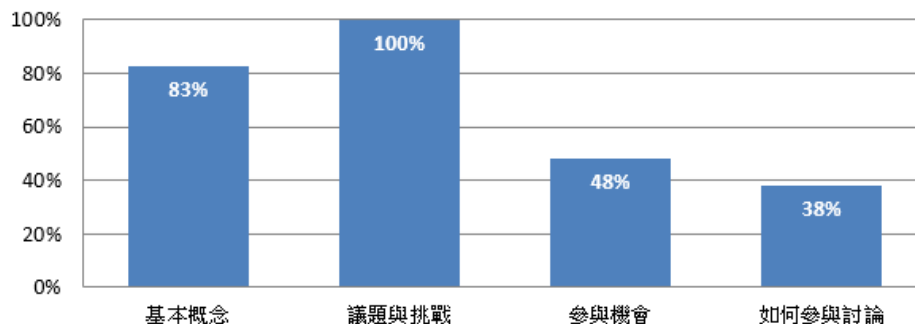
三、學員自我評估

高達 97% 學員表示對於網路治理的興趣增加（增加與大幅增加，並以四捨五入合計）；且所有學員都認為本次課程學習到網路治理的議題與挑戰，還有 83%認為學到基本概念，至於參與機會及如何參與討論的比例較低，應是和課程時間不足有關（介紹參與機會為 15 分鐘，分組討論演練為 90 分鐘）。此外，86% 學員表示未來願意參加 TWIGF，願意參加國外論壇（線上參與）的比例也不低，APrIGF 為 76%，聯合國 IGF 為 66%。

課後對網路治理的興趣



本次課程學習到網路治理的 (複選)



未來願意參加的網路治理活動 (複選)

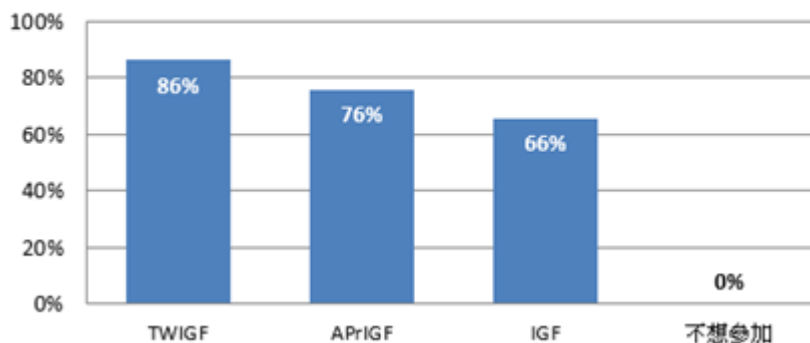


圖24. 研習營學員課後自我評估

四、其他建議

本次問卷並詢問學員「對本課程的相關建議或參與感想」。許多學員除了表達謝意，或表示課程內容令他們收穫良多或引起對網路治理的興趣外，也針對整體活動提出如下的建議：

- 增加課程時間

有些建議增加「專題講習」時間，有些建議延長「分組演練」時間。

- 增加提問管道

有些學員建議增加 slido 等線上提問管道，讓學員可以匿名提問（本次課程的提問方式係比照網路治理國際會議，須於指定點透過麥克風發言，並先表明姓名和單位職稱，讓大家可以了解其所屬的多方利害關係人的類別）。

- 增加課程內容

學員建議增加的內容包括國內外案例的數量、資料治理、AI 倫理等。

第六節 學員獎勵活動

一、選拔優秀學員參與國際會議

本屆 29 位結業學員中，有 22 位表達參加優秀學員甄選的意願。本次評選小組由 5 位講師組成，從角逐學員中遴選 1 位優秀學員參加 9 月 27 日至 30 日於加德滿都（尼泊爾）舉辦的 APrIGF 2020（全額補助）。

本次評選會議於研習課程結束之際於講師休息室舉行（圖 25 左側）。評選小組針對學員於課堂上所表現的學習熱忱、論述與表達能力、英文程度等項目，進行綜合評估，最後推選並決議 1 位正取與 5 位備取人選。

本屆優秀學員為政大公共行政學系的張同學（正取），評選結果並公布

於活動網站上。惟受到新冠肺炎疫情影響，APrIGF 2020 宣布改為線上會議（圖 25 右側），而優秀學員亦表示配合改以線上方式參與會議。



左圖：評選會議；右圖：APrIGF 2020 公布改採線上會議

圖25. 優秀學員評選及 APrIGF 線上會議網站

APrIGF 2020 共有下表 12 所列的 14 場座談，本計畫考量議題重要性，以及和通傳會的業務相關性，將請優秀學員參與編號 1、4、9、10、12 共 5 場座談，並於會後提供線上參與摘要報告（請詳附件 3）。

表12. APrIGF 2020 場次資料列表

場次名稱 (入選提案)	申辦單位	子類	主要內容
1 Do cybernorms help or hinder incident response activities?	APNIC	資安與信任	何種網路常規有助於網路事件管理
2 Combating Live Streaming of Online Child Abuse Content	公民團體 (尼泊爾)	資安與信任	打擊虐童線上內容
3 Not just 0s and 1s : discussing the increasing role of technology in ‘women’s safety’	Point of View (印度)	資安與信任	科技促進女性安全
4 Breaking Encryption: Is it the Panacea for addressing security issue online?	ISOC (印度)	資安與信任	加密是促進或阻礙資安?
5 New approaches to technical capacity building: an action-oriented dialogue	APNIC	包容... 多元化	開發中國家網路維運的能力建構
6 Access to information: a holistic approach to	國際圖書館	包容...	連網的價格、弱勢、

場次名稱 (入選提案)	申辦單位	子類	主要內容
meaningful digital inclusion	組織	多元化	操作技能
7 Bridging the digital gender divide: Learnings from the digital gender gap audit scorecard	媒體組織 (菲律賓)	包容... 多元化	數位落差的性別問題
8 Promoting internet and human rights: Challenges in Establishing Multistakeholder Collaborations	新聞學組織 (馬來西亞)	人權與 道德	東南亞國家的網路治理對話分享
9 Jack and the Tech Giants: Freedom of Expression and Information in the Tech Era	DigitalReach (泰國)	人權與 道德	科技巨頭於言論自由和安全的角色
10 The digital rights landscape in Asia Pacific after COVID19	Access Now (印度)	人權與 道德	疫情對亞太地區數位人權的影響
11 The Single, Global Internet – A Technical Discussion	ICANN	創新與 發展	提升域名和 email 全球通用
12 The Internet's Environmental Impact: an action-oriented dialogue	APNIC	創新與 發展	降低基礎建設對社會面、環境面的影響
13 Learn from Home During COVID-19	NetMission (香港)	創新與 發展	數位教學的經驗交流與討論
合併 1 Accessible digital information, training and libraries: Reducing discrimination for persons with disability	ISOC (澳洲)	包容... 多元化	促進殘疾人士的平等上網機會

資料來源：APrIGF 2020；本計畫彙整

二、TWIGF 座談申辦活動

為鼓勵學員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，本計畫提供新臺幣 2 萬元整獎學金予成功申辦 TWIGF 2020 座談的學員（經 TWIGF 評選最高分者），學員可以獨自或組隊參加，活動辦法詳如下圖 26 之活動海報。

本計畫於 7~8 月共計發出 3 次活動通知，並個別邀請上課表現優異的學員參與活動，惟經與 TWIGF 秘書處確認，截至申辦期限 8 月 31 日截止，

沒有任何學員提出座談申請，推估原因可能是規劃座談須先進行議題研究，門檻相對較高所致。



圖26. 研習營「TWIGF 2020 座談申辦」活動辦法

三、APrIGF 線上特派員活動

同樣基於鼓勵學員持續參與網路治理相關活動，本計畫邀請所有學員申請擔任 APrIGF 2020 線上特派員，凡是於期限內交付 1 場次座談摘要報告，即可獲頒新臺幣\$2,000 元獎學金（共 5 個名額），且摘要報告將具名

刊載於研習營網站的「學習資源」。活動辦法請詳下圖 27 之活動海報。結果共有 4 位學員參與本活動並如期完成摘要報告，報告請詳附件 4。

號召
APrIGF 2020
線上特派員

亞太區網路治理的年度盛事 APrIGF 2020 將於 9/28 (一)~9/30 (三) 召開，今年首度以網路會議方式舉辦，您只要線上參加 1 場會議，並於會後做成摘要報告，就可獲頒新臺幣 2,000 元整獎學金，名額只有 5 名，額滿為止！

■ 申請方式

- 申請資格：「2020 網路治理研習營」結業學員
- 申請方式：即日起，填妥並 email 本申請表，即有機會擔任 APrIGF 線上特派員，最快回覆且屆時能「同步」線上參與者將優先獲選，其次為最快回覆但只能於會後觀看影片者，申請結果將以 email 個別通知。

■ 履行事項

- 請速至 APrIGF 2020 官網 <https://ap.rigf.asia/> 完成線上會議報名。
- 如能「同步」線上參與，請於報告檢附線上參與的螢幕截圖。
- 請於 10/15 (四) 23:59 前將摘要報告 email 主辦單位，報告格式請見附檔。您的摘要報告將會具名刊載於「2020 網路治理研習營」網站的「學習資源」，您參加本活動即代表您同意具名公開摘要報告。

■ 活動獎勵

- 如期完成所有「履行事項」的特派員，將獲頒新臺幣 2,000 元整獎學金。

「APrIGF 2020 線上特派員」申請表

■ 學員姓名：

■ 表格填寫

APrIGF 2020 完整議程請詳 <https://ap.rigf.asia/>，以下 5 場為線上特派員活動所挑選的場次，並請填寫：

- 優先順序欄：請以 1~5 標示您想參與場次的優先順序
- 同步參與欄：可同步參與的場次請打○，其餘請打 X

優先 順序	同步 參與	會議時間 (台北時間)	會議場次名稱
		9/28 (一) 16:00~17:00	Do cybernorms help or hinder incident response activities?
		9/29 (二) 13:15~14:15	Jack and the tech giants: freedom of expression and information in the tech era
		9/29 (二) 14:45~15:45	The internet's environmental impact: an action-oriented dialogue
		9/29 (二) 16:00~17:00	The digital rights landscape in Asia Pacific after COVID19
		9/30 (三) 13:15~14:15	Breaking encryption: Is it the panacea for addressing security issue online?

圖27. 研習營「APrIGF 2020 線上特派員」活動辦法

第五章 精華短片製播

第一節 短片內容

一、網路安全短片

- 片名：臺灣的網速世界最快嗎？但是...網路安全嗎？
- 片長：10 分鐘
- 網址：https://www.youtube.com/watch?v=_8D79LLgrgo
- 發布日期：2020 年 8 月 18 日
- 受訪者：台灣網路資訊中心（TWNIC）／黃勝雄 董事長暨執行長

本支短片藉由大家最有感的網速問題，先引發關注和興趣，再提醒大眾注意網路安全議題。主持人馮韋元首先於開場引言指出，臺灣的平均網速約為法國的 3 倍，甚至有新聞報導指稱臺灣的網速世界第一。但他也表示，很多每天長時間上網和享受快速網路服務的民眾，忽略了網路安全問題，所以，也藉此機會向專家請益學習。後續的訪談重點摘要如下：

（一）一般使用者的網路安全問題

網路並非為安全而設計的，所以一般大眾都會碰到勒索病毒、釣魚網站、駭客攻擊等問題，例如 2017 年全球超過 150 個國家遭受勒索病毒 WannaCry 感染。其實這些問題每天都上演，只是一般民眾往往不知道自己的裝置已經被入侵或感染。其後果就如最近有國外資安公司揭露臺灣 2 千萬筆個資在暗網兜售。

（二）網路安全的責任歸屬（多方利害關係人的角色）

假設有 100 % 安全的系統，但是使用者設定密碼為 123，則駭客便可於 1 分鐘內入侵此系統。所以，其實是所有的「利害關係人」都要為網路安全承擔一部分的責任，包括製造商要生產安全的軟硬體系統、電信商要確保連線的不中斷、政府要訂定產品的安全憑證和網路安全法規，而消費者也

要具備基本的安全防護觀念。

（三）一般使用者的安全防護措施

一般使用者的基本安全防護措施包括安裝防毒軟體（企業用戶還須安裝防火牆等防護設備），還有設定複雜的密碼、經常備份資料，以及汰換裝置時要確認刪除所有資料。

（四）下載 Apps 的注意事項

許多民眾不知道 Apps 其實是很多病毒的來源，現在查詢資料很方便，使用者要為自己的安全負責，下載前可先查詢該 Apps 的評價與使用者經驗，切勿下載來路不明的 Apps。



圖28. 網路安全議題短片畫面截圖

二、網路內容短片

- 片名：臺灣的網路自由嗎？網路上什麼都可以 po 嗎？
- 片長：9 分鐘
- 網址：<https://youtu.be/BMOsMxeilJs>
- 發布日期：2020 年 10 月 8 日
- 受訪者：理律法律事務所／曾更瑩 合夥律師

主持人開場提到臺灣是一個享有言論自由的民主國家，人民能夠自由上網表達自己的想法而不必擔心受到政府干預或懲罰。然而言論自由並不代表可以隨意分享可能會傷害他人的內容，言論自由仍需適度限制。後續的訪談重點摘要如下：

（一）不實內容的法律管制

目前臺灣已有多部法律如《社會秩序維護法》、《傳染病防治法》、《食品安全衛生法》及《公職人員選舉罷免法》等，對於不實謠言進行管制，散布謠言者將面臨刑事處罰或是巨額罰金。因此，發表內容或分享網路上的訊息時，應該三思而後行。雖然言論自由是《憲法》保障的基本人權，但行使權力的同時，不該妨害他人的權利及利益，所以，目前有愈來愈多的法律針對言論自由做出相關規範。

（二）內容管制應有法律授權

言論自由是《憲法》保障的基本人權，僅有在特定情況下，才能以法律加以管制。因此，對於內容的管制必須經由執法單位或是司法機關來執行，平臺業者並無正當權力做內容限制，但是可於接獲檢舉時將有問題的內容下架。

（三）網路內容的責任歸屬

網路內容的責任歸屬不容易界定，臺灣現行法律並沒有針對平臺的行為作出明確規範，但是未來可能會針對網路多方利害關係人的責任歸屬訂出更明確的法律規範，除了一般使用者及平臺需承擔責任之外，其他的利害關係人如搜尋引擎或電信商，也應該共同為網路內容負責。



圖29. 網路內容議題短片畫面截圖

三、網路人權短片

- 片名：參加抽獎活動不要再被騙！大家不要那麼容易分享個人的資料給全世界看！
- 片長：11 分鐘
- 網址：<https://youtu.be/0H9BXriHDjE>
- 發布日期：2020 年 10 月 30 日
- 受訪者：台灣人權促進會／何明誼（前）副秘書長

主持人開場引用《Digital 2020》報告，指出臺灣人平均上網時間近 8 小時，遠超過世界平均值 6 小時 43 分，顯示臺灣人對網路的高度依賴，但報告也提到臺灣人對於個人資料被濫用的警覺性比較低，因此，特地與專家共同探討個資隱私的重要性。後續的訪談重點摘要如下：

（一）敏感個資保護的重要性

先前風靡全球的 FaceApp，使用者只需上傳臉部照片就能使用各種特效。臉部是一種生物特徵，除非進行整容，否則一輩子都不會改變，也就是說一旦生物特徵遭到濫用，極有可能導致終生的傷害。因此，上傳敏感個資時，務必思考其導致的後果。

（二）留意 Apps 索取權限

在使用、下載 Apps 時，使用者應注意此 Apps 要求使用手機上哪些權限（如照片、通訊錄等）。使用者除了需要擁有保護個資的意識外，也應該具備基本的操作技術，能夠主動檢視哪些個資將被使用。

（三）eID 的正反論述

晶片身分證 eID 的爭議不斷，支持者認為使用晶片身分證能夠更方便存取電子化政府的服務，而且晶片身分證也比紙本身身分證更不易被偽造。

反對者則認為身分驗證的機制並無明確的規範，有可能導致人民的個資得以被公部門或私部門任意使用。反對論點還有未來網路上的使用者將逐漸喪失匿名性，提供網路服務的業者可能為了降低風險等因素而要求存取這些身分資料，慢慢地讓網路服務走向實名制。

（四）免費服務的代價

現代人享受著各式免費網路服務，但所付出的代價就是犧牲個資隱私。提供服務的業者藉由使用者所提供的個資，投放個人化服務及廣告，漸漸地使用者的喜好可能受到內容的影響而有所改變。究竟使用者的喜好是自己決定，還是由服務供應商引導所致，這是現代人值得思考的議題。



圖30. 網路人權議題短片畫面截圖

第二節 觀眾意見回饋

一、網路安全短片

本支短片有 230 則留言，雖然當中不乏與內容主題無關的粉絲支持留言，以及究竟哪一國才是全球網速第一的討論，不過，更多留言表示學習到新知識、肯定內容專業性、感謝分享網路安全觀念等。此外，還有部分留言拋出更多的網路安全議題，如網銀安全、竊聽、下載 Apps 個資遭竊等。



圖31. 網路安全議題短片留言截圖

二、網路內容短片

本支短片共有 190 則留言，許多留言表示肯定內容專業性、感謝分享言論自由的相關知識等。大部分觀眾留言認同言論自由必須有其規範，不該無限上綱而傷害到他人權益，但也有部分觀眾認為平臺亦須負責。



圖32. 網路內容議題短片留言截圖

三、網路人權短片

本支短片有 77 則留言，許多留言表示肯定影片主題，以及感謝提醒個資保護的重要性，並希望能夠多製作網路相關議題的影片。此外，還有不少觀眾分享自己的個資隱私保護相關經驗。

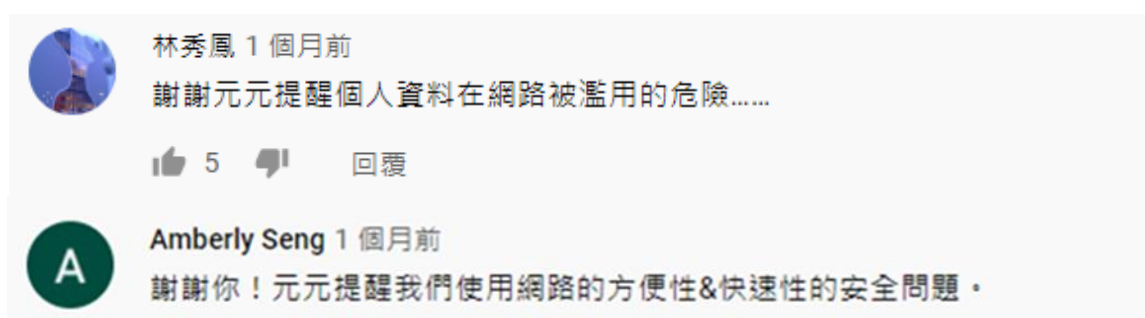


圖33. 網路人權議題短片留言截圖

第三節 流量統計分析

一、觀看次數與時間

3 支短片的觀看次數以網路內容為最高，約 3.3 萬次，觀看時數為 1,700 小時；其次是網路安全 2.4 萬次和同樣是 1,700 小時；最後是落差較大的網路人權 7,200 次，觀看時數 454 小時，推估主要原因可能是影片名稱以詐騙為標題，對於詐騙事件層出不窮甚至有「詐騙王國」不雅稱號的臺灣來說，此類影片或許已經無法引起觀看興趣。其次是此影片被 YouTube 自動曝光的次數較低，相關數據將於下段「觸及率」說明。



圖34. 精華短片的觀看次數與時間

此外，由於短片附有「網路治理研習營」同一主題的講習課程影片網址，因此，這 3 門課程影片的觀看次數 185 次、116 次和 91 次，也明顯高於其他課程影片的 30 多次。

二、曝光次數與流量

3 支短片獲得 YouTube 自動顯示的曝光次數分別為 30.5 萬、22.5 萬、12.1 萬，第 3 支網路人權短片的曝光次數只有其他 2 支短片的 4 成和 5 成，因此，對觀看次數亦有相當程度的影響。至於影片流量方面，3 支影片大約 7~8 成流量都是來自 YouTube 首頁的「瀏覽功能」，其他流量分別來自創作者的「頻道頁面」、YouTube 自動呈現的「建議影片」，以及使用者訂閱頻道的「通知」。

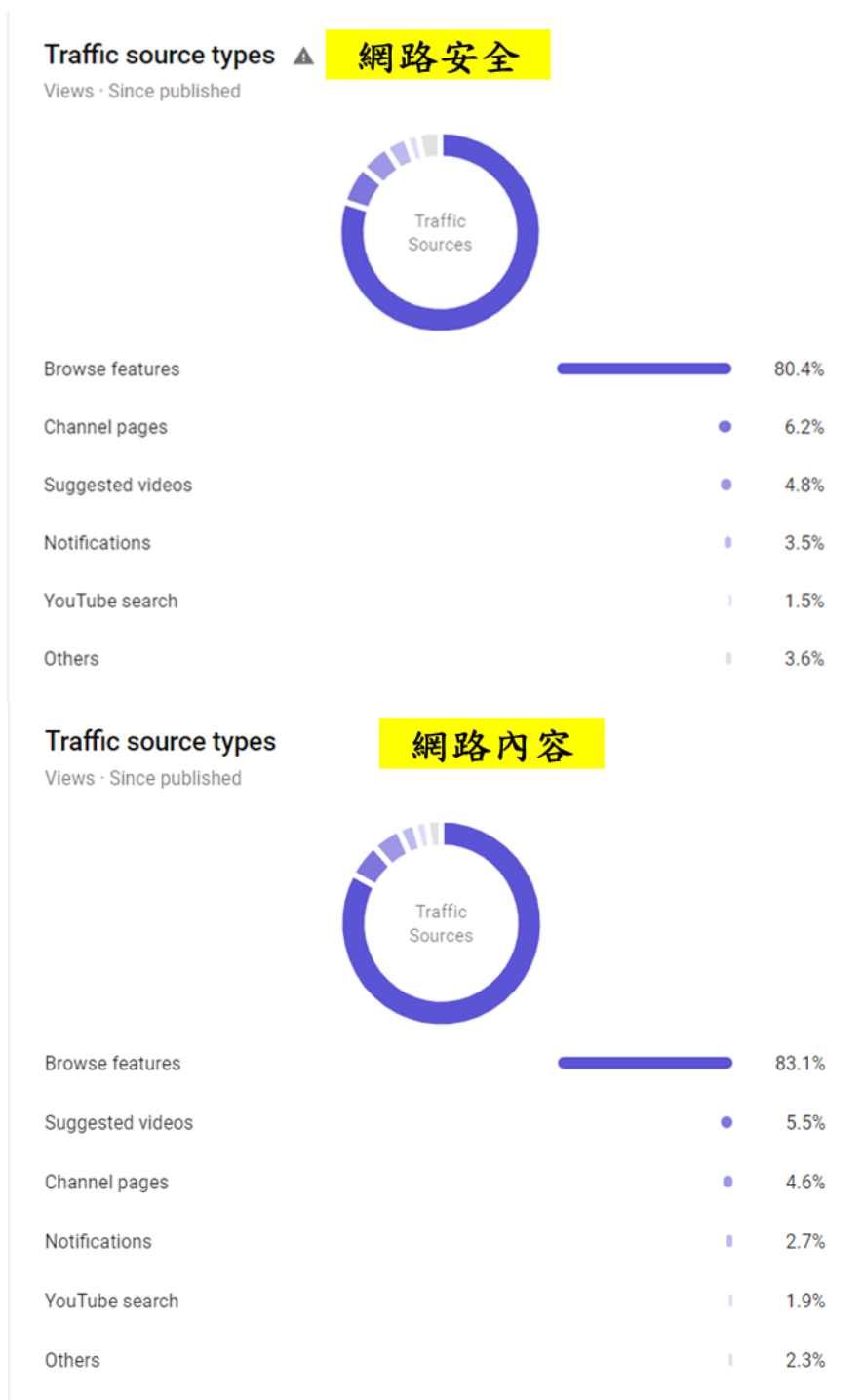




圖35. 精華短片的流量來源

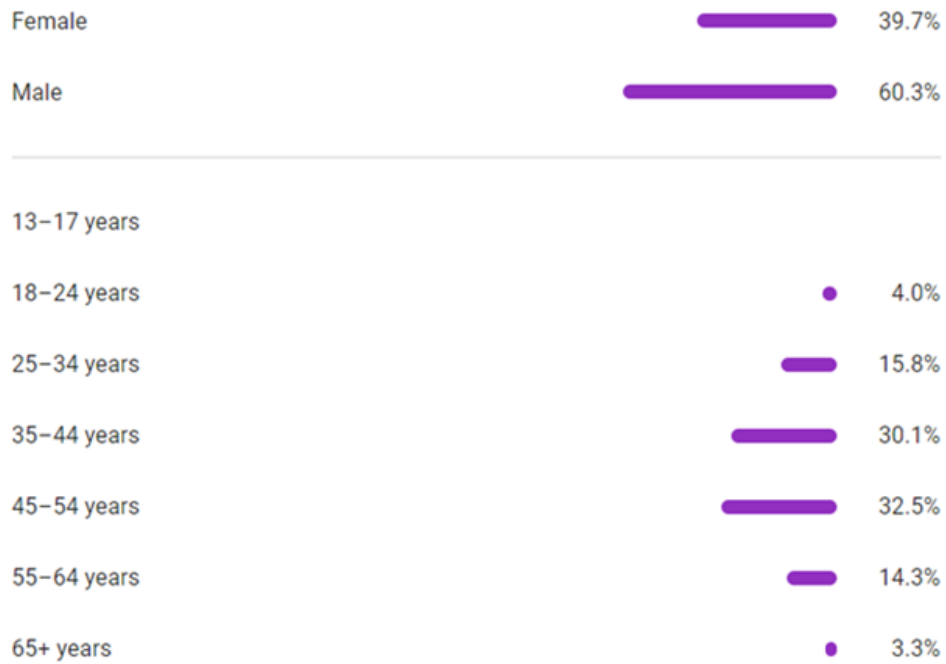
三、觀眾年齡與地區

3 支短片的觀眾年齡層皆以 45 歲~54 歲為最多，其次為 35 歲~44 歲，2 者合計超過 6 成，而 34 歲以下的年輕族群合計反而不到 2 成，顯示此頻道的中壯年以上族群較年輕族群更關心網路治理議題。另外，性別方面，網路安全和網路內容影片的男女觀看比例為 6:4，但網路人權的觀看比例則是女性（52.3%）略多於男性（47.7%）。至於地理區域，3 支短片的觀眾皆為 8~9 成來自臺灣，美國約佔 3%，其他還有來自加、英、澳、港、日等國家或地區。

Age and gender

Views · Since uploaded (lifetime)

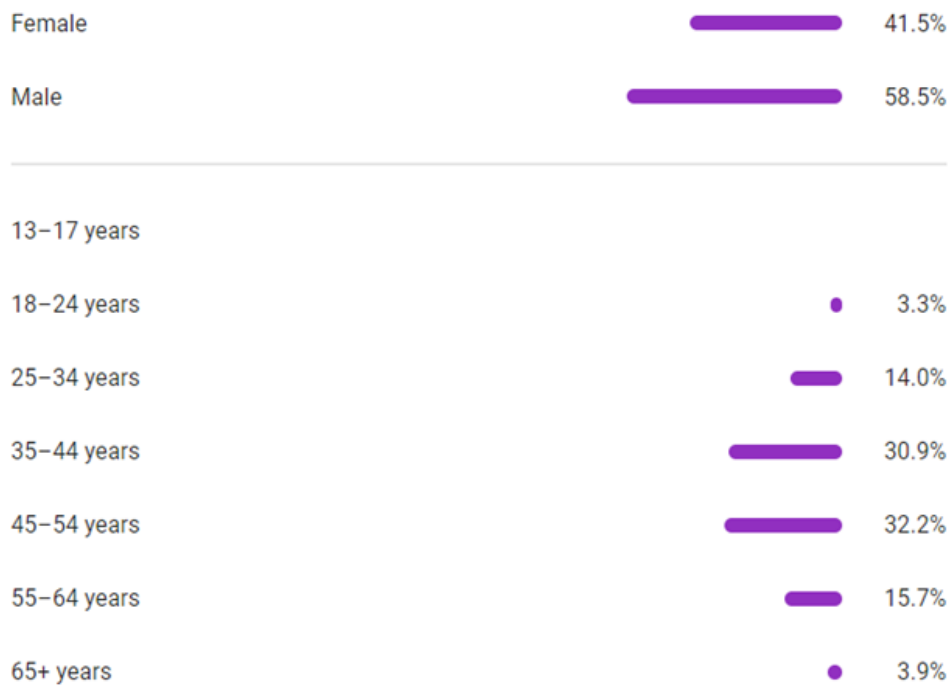
網路安全



Age and gender

Views · Since uploaded (lifetime)

網路內容



Age and gender

Views · Since uploaded (lifetime)

網路人權

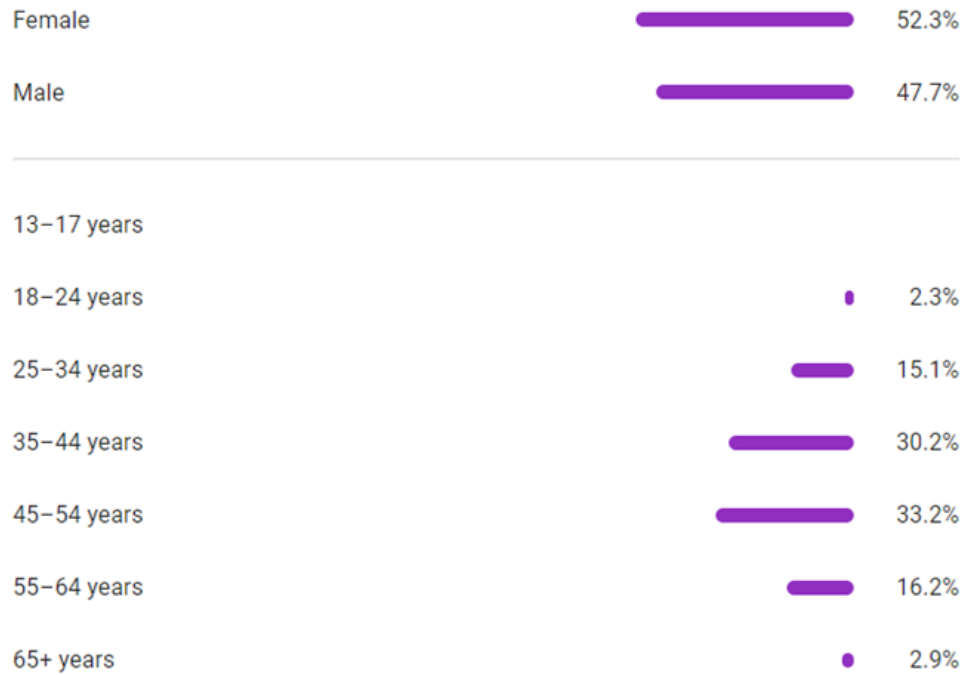


圖36. 精華短片的觀眾性別與年齡

第六章 國際會議參與

第一節 IGF 會議簡介

一、會議背景

有鑑於治理網路需要採取包容性和回應性方式，聯合國資訊社會世界高峰會（World Summit on Information Society, WSIS）於 2005 年決議，由當時聯合國秘書長召集成立一個多方利害關係人參與的新對話論壇，於是網路治理論壇（Internet Governance Forum, IGF）於 2006 年正式成立，主要討論網路治理的公共政策議題，以強化全球網路的持續運作、安全、穩定與永續發展。

IGF 於每年年底召開，儘管會後不會做成決策，但是卻能促進多方利害關係人社群對於如何善用網路機會和因應網路挑戰的討論互動、知識分享和實務交流，且對政策決策具有啟發性。因此，除了各大洲與各個國家紛紛見賢思齊地舉辦論壇，促成區域型 IGF 與國家型 IGF 的發展外，聯合國大會亦於 2015 年 12 月授權延長 IGF 再舉辦 10 年，象徵鞏固 IGF 作為全球多方利害關係人平等參與網路政策討論的平臺地位。

二、會議資訊

受到 COVID-19 影響，第 15 屆 IGF 於 2020 年 11 月 2 日至 6 日，以及 9 日至 17 日，首度全面以虛擬會議方式進行。本年度大會主題訂為「網路促進人類強韌和團結」（Internet for Human Resilience and Solidarity），討論主題分成「資料」、「環境」、「包容」、「信賴」四大類別。為期 12 天的會議共計有 275 個場次和超過 1,000 位講者，並吸引來自全球 173 國 6,136 人的線上參與。

IGF 有各種型式的會議，本次線上參與場次如下表 13 所示，包括開幕

和閉幕、由 MAG（多方利害關係人諮詢小組）規劃的主要會議（Main Sessions）、僅限各國政府部門和國際組織申辦的開放論壇（Open Forums）、開放全球多方利害關係人申辦的座談討論（Workshops）、特別為各國議員舉辦的議會圓桌會議（Parliamentary Roundtable）。

此外，本計畫也摘要集結本年度會議討論成果的 IGF 2020 公報，以提供政策參考。本年度論壇完整議程請詳

<https://www.intgovforum.org/multilingual/content/igf-2020-schedule-0>。

表13. IGF 2020 線上參與場次

會議種類	申辦單位	場次名稱
開閉幕	大會主辦	Opening Session、Closing session 開幕場次、閉幕場次
主要會議	MAG 主辦	Digital Cooperation 數位合作
開放論壇	歐盟執委會	Trustworthy Internet Technologies against COVID-19 對抗新冠肺炎的可信賴網路科技
座談討論	美、中大學	Overcoming the US-China Digital Cold War 克服美中數位冷戰
	APNIC 等	Trust, Media Ethics & Governance During COVID-19 Crisis 新冠肺炎危機時期的信賴、媒體道德和治理
議會圓桌會議	聯合國經濟和社會事務部	Building Trust in a time of COVID-19 response and post-COVID-19 recovery 在新冠肺炎因應和後疫情復原時刻建立信賴
(會後文件)	IGF 秘書處	IGF 2020 Message IGF 2020 公報

第二節 開閉幕場次

本屆 IGF 開幕典禮由聯合國負責經濟和社會事務的副秘書長劉振民致詞。他指出當前全球數位落差問題嚴重，最低度開發國家的民眾上網率只有 19%，還有無法負擔上網費用和缺乏數位能力等問題，這些都需要大家共商解決方案，讓尚未連網的人也能受益於數位科技。

接續進行的開幕座談亦聚焦於消弭數位落差和 COVID-19 對數位化的影響，與談人包括聯合國第 75 屆大會主席 Volkan Bozkir、聯合國經濟及社會理事會主席 Munir Akram、美國哥倫比亞大學永續發展中心主任 Jeffrey Sachs、瑞士前總統 Doris Leuthard、ITU 秘書長趙厚麟等人。討論重點可歸納如下：

- COVID-19 的毀滅性影響凸顯網路和數位科技對我們日常生活的重要性，並加速全球數位化進程，接下來也應持續推動數位化，且透過所有利害關係人參與的方式。
- 疫情的大流行同時彰顯數位不平等的嚴重現象。為了發揮網路作為全球公共財的功能以實現包容性和永續發展，普及上網是至關重要，但關鍵挑戰是決定如何落實及如何籌資。
- 應充分投資基礎設施，包括將一些道路和橋樑的投資移轉到網路，而且要提供可負擔的上網資費。
- 人力資本的投資同樣重要。投資於所有人（尤其是弱勢族群）的數位素養和能力發展，是確保有意義連網的關鍵。
- 應確保國家和全球的數位治理過程能跟上技術變革的步伐。有效的數位治理關鍵在於真正的包容性、參與性和多方利害關係人方法。
- 應加強全球數位合作機制。國際社群可以依據不同的角色、職責和專業領域，在平等的基礎上共同合作。此外，超越地緣政治的辯論以建立更有效的公私伙伴關係，也相當重要。

而閉幕典禮則是由聯合國秘書長古特瑞斯（Antonio Guterres）致詞，

除了同樣指出 COVID-19 對數位化的影響和消弭數位落差的重要性外，古特瑞斯還呼籲大家共襄盛舉他於今年（2020）6 月發布的《數位合作藍圖》，包括強化 IGF 功能及提升具體影響力，讓 IGF 的討論能進一步形成共同標準或原則，而他也會就涉及自己職責的項目，加速展開行動。

第三節 會議討論

一、主要會議：數位合作

本場會議由 MAG（多方利害關係人諮詢小組）主辦，主要探討 IGF 於全球數位合作所扮演的角色，主持人為聯合國副秘書長暨數位合作特別顧問 Fabrizio Hochschild，與談人包括德國和瑞士政府官員、歐美電信和網路業者代表，以及跨國公民團體組織代表等。

德國數位政策官員 Daniella Brönstrup 認為，討論是必要且重要的環節，因為它是良好政策建言的基礎，且高質量的討論正是 IGF 的價值。她並建議 IGF 成立一個高階委員會，但不是作為決策單位，而是協助將結論建議傳達給國際決策組織。瑞士通訊傳播局國際事務主任 Thomas Schneider 也表達相似看法，他表示，IGF 被定位為打造數位政策的地方，但討論結果要能傳達給決策者，而《數位合作藍圖》已提出相關作法，或許將可改善此問題。

ETNO（European Telecommunications Network Operators，歐洲電信網絡營運商協會）總監 Lise Fuhr 指出，建立多方利害關係人的合作架構有許多方式，但重要的是找到將解決方案化為行動的方法，如國會議員應協助將 IGF 討論帶回各國並加以活化運用。ISOC（網際網路協會）強韌網路計畫資深副總裁 Joseph Hall 則認為，要消除討論和解決方案的落差，需要大家能對網路抱持相同的理解，也就是維護網路的去中心化。而 Facebook 人權事務主任 Miranda Sissons 表示，現在有許多破壞網路開放的勢力，IGF

在確保網路的開放、包容和安全上扮演要角，因此，可以成為相關對話的核心。

綜合各與談人意見，主辦單位歸納本場會議的結論如下：

- 數位合作為當前關鍵課題，因為數位落差不只是存在而是更惡化。
- IGF 是傳播優良措施和推動能力建構的有效機制，與會者在 IGF 碰面、交換資訊，並商討可實施的解決方案。這正是多方利害關係人如何落實數位合作並產生可行結果的最佳範例。
- 網路發展或許始於自由開放地交換資訊，但近來趨勢日益顯示，除非我們推動有益於所有人的全球數位合作，否則網路分裂很可能成為一種新常態。
- IGF 不只是每年一度的會議，而是閉會期間也進行許多活動。所以，利害關係人應持續參與這些討論活動。
- IGF 具有促進政策討論的價值，並不是每個議題都必須有具體結果，而且沒有其他地方像 IGF 一樣，可以開放地分享意見和提出議題。其實 IGF 在尋求產出更具體結果的同時，也可以同時保持討論功能。

二、開放論壇：對抗新冠肺炎的可信賴網路科技

本場會議由歐盟執委會主辦，主持人為瑞士策略研究公司 Martel Media 主管 Giovanni Rimassa，與談人包括歐盟官員、荷蘭政府官員、歐盟消保團體代表，以及我國行政院資通安全處簡宏偉處長。

主持人開場表示，歐盟因應 COVID-19 推出歐盟工具箱 (EU Toolbox)，提供使用疫情追蹤示警 Apps 的指南，所列原則如 Apps 應為自願性安裝及提供資料、Apps 應有成效但不能追蹤民眾的行蹤、資料不可儲存超過 14 天、應完全符合歐盟資料保護及隱私原則、應可於歐盟範圍內互通等。

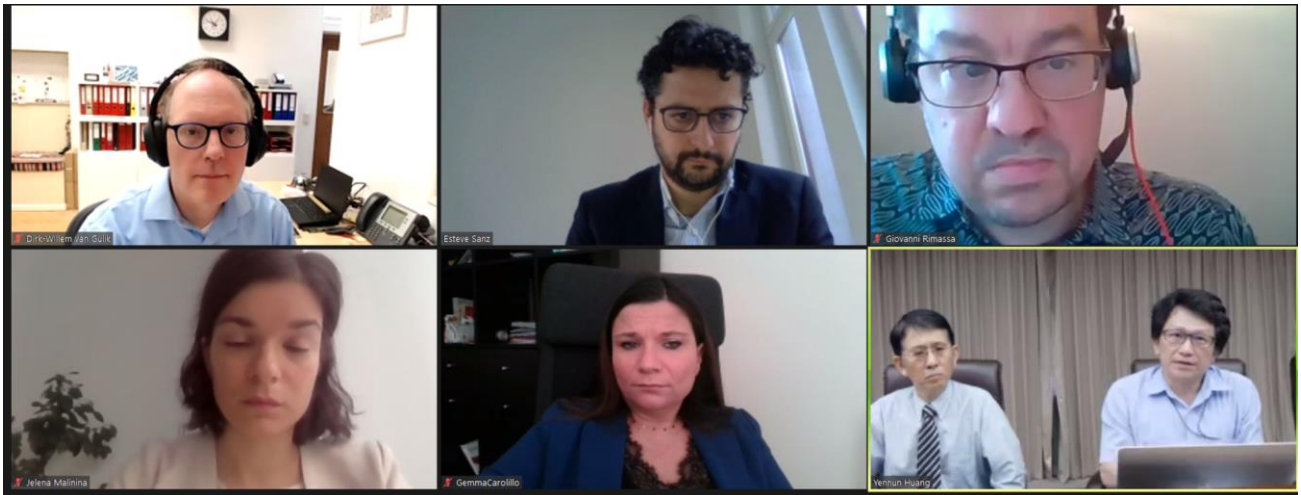
歐盟下世代網路計畫（Next-Generation Internet, NGI）副主任 Gemma Carolillo 指出，歐盟有緊急科技檢視中心（Emergency Tech Review Facility），由民間社群自主成立，提供 COVID-19 相關科技的安全隱私獨立分析，包含測試並給予基於安全隱私和法遵的開發接觸史追蹤 Apps 建議。

荷蘭政府特別顧問 Dirk-Willem van Gulik 提及荷蘭的接觸史追蹤 App（CoronaMelder）已有 5 百萬民眾安裝。有鑑於大眾對隱私的疑慮，此 App 一開始即採取隱私設計（privacy by design）概念及去中心化的方式開發。因此，調查也顯示，民眾對它的信任主要是因為使用開放原始碼軟體（open-source）且開發過程透明。

簡宏偉處長則是分享我國的科技防疫經驗。他表示，我國的智慧防疫系統包含從旅客入境健康聲明即開始彙整相關資料的「入境檢疫系統」，並將資料拋轉至「防疫追蹤系統」，提供第一線民政和衛政人員關懷防疫使用，再透過以電信訊號定位的「電子圍籬系統」協助落實居家隔離和檢疫措施，還有「疫止神通」系統方便居家檢疫民眾進行自主健康通報並取得防疫相關協助資訊。簡宏偉並強調，我國防疫策略兼顧維護人權和依法保障隱私，包括超前部署推出的「社交距離 App」以及「健康回報 App」也基於相同理念，且提供原始碼給各國防疫使用，前者並符合歐盟 GDPR 個資保護規範，但臺灣因為病例數少，這 2 款 Apps 的使用率並不高。

最後，主辦單位也歸納以下本場討論要點以供各界參考：

- 信任是民眾安裝接觸史追蹤 Apps 的關鍵，所以，技術的透明度和可公開取得相當重要。
- 歐洲的接觸史追蹤 Apps 有國家公共衛生單位管理，但很多國家沒有。此類 Apps 應有公共監督和資料保護措施，且最好有完全透明的資料模式。
- 人人都有權利使用此類 Apps，政府應確保身障族群和使用舊款手機民眾的使用可得性。



圖照來源：IGF 2020

圖37. IGF 2020 線上會議「對抗新冠肺炎的可信賴網路科技」

三、座談討論：克服美中數位冷戰

本場座談由美國喬治亞理工學院教授 Milton Mueller 等人共同主辦，並由 Mueller 主持，與談人包括美國國務院經濟和商業事務局國際傳播資訊政策副助理秘書長 Stephen Anderson 和中國大陸工業和信息化部首席工程師 Guo Feng（以下簡稱美國、中國官員）、香港立法會前議員莫乃光，以及南非 WITS 大學教授 Iginio Gagliardone、波蘭 Lodz 大學教授 Joanna Kulesza、印度網路治理計畫研究員 Jyoti Panday（以下簡稱某國學者）。

本場座談中，美中雙方代表數度針對治理議題針鋒相對，而包括主持人在內的學者也提出相關看法。討論重點如下：

- 網路治理模式和中國網路相關新倡議

美國官員表示，我們賴以生存的網路是開放、互通和安全的，網路協定也是據此邏輯設計，這也是多方利害關係人社群要確保的網路運作方式。然而，中國向 ITU 提出的新網路架構（New IP）提案是攻擊網路的根基，試圖將中國的數位獨裁植入管理全球網路的基礎協議中，一旦實施將賦予國家重大的控制權，威脅現有的多方利害關係人模式。但中國官員反

駁指出，中國不但沒有威脅現有的網路治理生態系統，而且還支持並參與 ICANN，也承諾維護網路治理的安全等傳統價值，如於 2020 年 9 月發布《全球數據安全倡議》，當中即禁止非法蒐集民眾資料，以及反對利用後門程式進行監控。而南非學者則認為，中國政府並沒有利用電信基礎設施將其網路治理模式強加於非洲，只是中國業者有時候會利用中國的監控成效來銷售產品。

• 網路主權與網路分裂

針對上述的中國《全球數據安全倡議》，主持人認為它過於強調網路主權和國界；美國官員也表示，網路主權概念就是對抗多方利害關係人模式，並指稱美國的「乾淨網路」計畫對於維護網路安全是必要的。但中國官員捍衛網路主權概念，強調這是正當存在，就如同每個國家在實體世界擁有主權一樣；他並表示，美國「乾淨網路」計畫將中國供應商排除在美國的電信網路之外，形同美國實施網路主權。而對於美中雙方陷入爭論，波蘭學者表示，歐洲尋求的是策略性自主權而非網路主權，並以人權和市場開放為原則，所以，歐洲或許可以發展出網路治理的第三條道路。此外，多位與談人認為，其實美中兩國政府都在限制和分裂網路。香港前議員莫乃光表示，如果我們不同意中國的防火長城，我們可能也應該反對美國的乾淨網路。

• 結論建議：以全球網路用戶為中心

主辦單位最後總結表示，儘管本場會議無法化解美中雙方的基本立場和政策歧見，但是與談人幾乎一致認為，本議題的討論起點應是全球網民的福祉，亦即以全球網路用戶為中心，而不是對一個國家或另一個國家施加限制，國家決策高層應該聚焦於「人民主權」，而非「國家主權」。

四、座談討論：新冠肺炎危機時期的信賴、媒體道德和治理

本場座談由本計畫主持人吳國維和中國蘇州西交利物浦大學講師錢憶

親等人共同主辦和主持，與談人包括中國大陸、英國、新加坡學者，印度公民團體以及中國網路業者等。

中國傳媒大學教授 Yun Long 表示，中國大陸在疫情爆發初期，由於疫情的不確定性和不可靠訊息的傳播，導致公眾輿論缺乏信任。微博副總編輯 Shu Wang 則強調，中國大陸新聞媒體的微博官方帳號發表 2 百萬則訊息向大眾通知疫情消息，而微博自己也積極對抗謠言訊息，包括發布示警標籤、增加 6 倍員工處理投訴謠言、刪除 74 萬則被標記為謠言的貼文等。

網際網路協會（ISOC）德里分會主席 Amrita Choudhury 表示，印度的疫情假訊息大幅增加，印度政府請平臺業者立即採取行動，優先刪除不實內容並傳播確實訊息，而平臺也者也配合實施相關措施，如通知收到疫情假訊息的用戶、限制未經證實訊息的發布、顯示 WHO 等可靠機構的資訊等。

英國諾丁漢大學資深研究員 Ansgar Koene 指出，疫情期間人們使用社群媒體的時間呈倍數成長，社群媒體也成為人們獲取疫情資訊的主要資源。而新加坡南洋理工大學教授 Ang Peng Hwa 表示，新加坡民眾對政府資助的追蹤 Apps（TraceTogether）有所疑慮，移除此強制性軟體的請願多達 480 次，但我們要思考的是，隱私考量是否比生命安全更加重要。

本計畫主持人吳國維則是認為「社群媒體」一詞會產生誤導，因為它並不是具有行為準則和發布流程的媒體，而是讓我們輕鬆且無需編輯和檢查地去共享一些訊息，因此，我們應該教育大眾「社群媒體」不是媒體。

綜合以上討論，本場座談的共識和政策建議可歸納如下：

- 社群媒體是 COVID-19 資訊的主要來源，若使用得當，可增強媒體信譽。因此，應該立即廣泛討論其定位問題，釐清社群媒體是否屬於媒體並受相關法規監管。

- 重建網路信賴需要政府和利害關係人共同努力。政府要重視民眾的媒體素養和如何治理媒體，因為這是建立線上信賴的要務；平臺業者則應有更透明的內容下架政策；而大眾也要了解平臺是如何獲利。



圖照來源：IGF 2020

圖38. IGF 2020 線上會議「新冠肺炎危機時期的信賴、媒體道德和治理」

五、議會圓桌會議：在新冠肺炎因應和後疫情復原時刻建立信賴

為了強化各國立法機關與 IGF 的連結性，繼 2019 年首度舉辦國會議員專屬的場次後，2020 年 IGF 再度辦理類似會議，讓各國議員討論如何在疫情時期建立對網路的信賴。

德國議員 Manuel Höferlin 建議設立一個全球議員網絡，以利整個年度都可以討論並相互學習最迫切的數位科技議題和政策，而非只是每年一度的 IGF 才討論。此建議也獲得義大利議員 Mattia Fantinati 支持，他並表示，網路屬於每一個人，它為人們提供發展自由和批判性思考的工具。

波蘭議員 Krzysztof Gawkowski 指出，疫情促使人人將生活的各層面都

移轉到數位空間，因此，具備使用數位工具的能力，將成為勞動市場的必要條件。歐洲議會議員 Marina Kaljurand 則強調，與數位科技相關的政策討論應該包括國會議員，所有利害關係人應該建立互信，在各層級展開合作，聯合國《數位合作藍圖》的三個重要支柱正是合作、安全和信賴，並應趁 COVID-19 疫情時刻將數位化放在政治議程的首要位置。

另一位義大利議員 Francesco Berti 表示，義大利將假新聞視為民主政治的威脅，議會並因此成立一個假新聞的委員會；而個資隱私也是當前網路治理的一大挑戰。總體而言，沒有監管的數位創新將無法提供信任，沒有控制的假新聞和平臺將使網路和傳播淪為操弄，因此，國會議員要重視數位相關的立法。

綜合以上討論，議員們的建議包括 IGF 每年舉辦高層、部長級和議員會議，並確保產出更具體成果；建立一個常設的非正式 IGF 議員小組，以促進各國議員交換網路政策議題的立法準備、採認和執法等相關資訊及經驗；評估建立一個全球網路公共政策和法規資料庫的可行性。

此外，本場會議還發布結論文件，提供以下建立網路信任的相關建議供各國議員參考：

- 宣傳數位科技促進永續發展的示範案例，以展現數位包容可以增強人們對科技的信任。
- 透過多方利害關係人的伙伴關係和倡議，推動有意義的網路連線。
- 鼓勵將數位素養融入所有公民的正式教育課程中。
- 積極參與並支持對抗錯誤或虛假訊息的認知宣導和能力發展。
- 推廣日常使用網路的網路安全和網路衛生新文化。
- 透過保護網路的公共核心，提高網路空間和其基礎設施的穩定性。

第四節 IGF 2020 公報

IGF 自 2017 年起嘗試將該年度的 2 百多場會議討論重點，精選彙整成公報（Message），提供包含決策者在內的各界人士參考。而 IGF 2020 公報（草稿版）更強調政策參考性，首度以年度主題（資料、環境、包容、信賴）的總體政策問答方式呈現。以下摘錄和通傳會執掌相關的主題內容⁸。

一、資料

1. 我們需要採取哪些政策和具體措施，以確保資料的蒐集和使用能使所有人（包括發展中國家、邊緣化族群、尚未連網者）受益？
 - 應該努力擴大資料集（data sets）的廣度和包容性，以免 AI 因為缺乏足夠的大數據而產生偏見、擴大落差、邊緣化和排他性，尤其在健康方面可能導致致命性後果。但另一方面，也要強化資料蒐集取得同意過程的透明度。
 - 全球仍有 30 多億人無法上網，他們的資料尚未被蒐集和處理，這也代表他們無法讓大數據和 AI 增進其發展和福祉。因此，普及上網和數位發展方案需要包含資料策略，且需要的是長期計畫而非一次性的倡議。
2. 在科技發展總是快於法規的世界，對於資料的蒐集和使用，如何兼顧民眾的權益保護（包括不被濫用於監控民眾、線上平臺的操弄）和資料處理所帶來的合法經濟及其他利益？
 - 個人資料的主要蒐集者，也就是政府和民間企業，應將邊緣化和少數族群納入資料集，這是改善代表性和能見度的重要環節，但同時不能

8 IGF 2020 首度將「環境」列為分類主題。環境永續和氣候行動是《聯合國 2030 年議程》的基本內容，此主題主要探討如何強化 ICTs 對環境永續的正面效益，以及如何將負面衝擊（例如資源消耗增加、製程產生環境污染、電子垃圾等）降到最低。由於此主題並非通傳會業務範圍，故本報告僅彙整其他 3 個分類主題的公報內容。

使他們受到不利的影響，例如有針對性的監控和限制連線服務。

- 資料在地化政策旨在保護公民的資料免於受到違反其國家法律的使用，然而卻也對缺乏資源遵循複雜法規的本地中小企業和初創企業帶來不利影響，從而阻礙經濟發展。因此，資料立法必須考量創新機制，在保護隱私和跨國共享資料的利益中間取得平衡。

3. COVID-19 相關資料的蒐集和使用政策，係採迅速且由少數關係人決策方式。我們可從中學到什麼經驗，又這些創新的資料政策如何應用於其他與疫情無關的情境？

- 已有開放資料政策和標準的國家，能夠快速建立尊重人權的 COVID-19 資料措施。因此，其他國家應該考慮制定相關政策或標準，這不只是為未來的危機做準備，而是也能為日常情況提供民主化和基於證據的決策。
- 接觸史追蹤 Apps 被快速下載，顯示只要能夠信任資料的安全、沒有蒐集不必要的項目、使用範圍沒有超出蒐集目的、不會被用於行為監控，民眾會願意基於公益目的而分享資料。因此，政府和民間企業應努力制訂這種透明標準，以確保民眾未來願意持續配合資料的蒐集。
- 近年來資料主權已成為趨勢，許多國家透過立法將公民資料保留在國內。但疫情的大流行顯示，限制資料傳輸不利於因應全球性的挑戰。
- 如何監管私有的線上公共空間（如社群媒體平臺）一直是近年來激烈爭辯的問題。疫情的大流行凸顯民間部門可以和政府緊密合作，以支持更準確的政策制定並賦予公民權力。此次經驗可成為未來共管模式的良好範例。

二、包容

1. 利害關係人如何實施持續性政策，以促進所有人有意義的數位包容，並消除所有形式的數位落差？

- 有意義和包容的網路連線應成為所有消除數位落差政策的指導原則。有意義的連線係指讓使用者有合適的設備和能力，可持續且快速地連接到符合他們需求的內容和服務（尤其是本地的）。
- 疫情凸顯數位不平等現象，因此需要即時進行基礎建設，政府應以更靈活創新的監管框架鼓勵電信公司行動，例如修訂通用服務基金辦法、促進頻譜使用、簡化基礎設施部署的核准流程等。
- 社區網路可以促進可負擔且有意義的連網。需要為當地社區進行技術能力建構，以確保他們具有技術和知識可以建立並維運安全、可持續的基礎設施。傳統運營商應該讓這些網路能夠互通互連。
- 財政資源是實現網路普及的關鍵，除了政府資金和電信業的投資外，應更關注的是找到創新的融資模式。調降基礎設施和設備的稅率也可以使上網費更可負擔。
- 需要採取更多持續性政策或措施來消除影響女性和多元性別族群的數位落差，包括賦權他們創造數位內容、打擊線上基於性別的暴力行為、加強立法和執法，以及平臺業者的持續作為。
- 科技公司和公部門等單位有責任確保數位產品、服務和內容能夠滿足殘疾人的需求。必須嚴格執行連網相關法規，並將無障礙設計的理念融入數位科技的開發中。還需要適當的法律框架來解決與生產和發行無障礙數位內容相關的智慧財產權障礙和市場失靈問題。
- 應該動員更多資源和財源推廣網路的多語化。公私部門和非營利單位應授權當地社群和原住民，以其母語製作數位內容。此外，政府和科技公司也應在其服務和技術中，實現國際化域名（IDN）和電子郵件地址的全球通用（Universal Acceptance, UA）。
- 公私部門應投入更多資源發展公民的數位技能，並賦予他們批判性思考的能力，且能以安全和有意義方式使用科技來增進自我權益。

- COVID-19 加速全球數位轉型，國際社會有責任透過能力建構方式，協助開發中國家利用數位科技推動社會和經濟發展。例如幫助他們制定法規和機制，以管理數位科技的開發、佈建和使用。
2. 我們需要什麼政策、法規和支援，來打造包容性數位經濟的有利環境，以使每個人都可從中受益？
- 政府應該加強「為未來工作做好準備」，如訂定且實施扶持性的政策和法規，以確保有意義的連網和使用科技、改革教育制度以更注重數位技能和軟實力，以及支持創新和企業家精神等。
 - 政府和大型企業應支援小型企業，以利它們能從數位市場獲益。支援方式如協助能力發展、提供指導、提供容易使用的電子商務平臺等。
 - 各國公私部門需解決女性、殘疾人士和其他弱勢族群於數位經濟所面臨的不平等問題，例如排除他們加入平臺經濟或其他數位商業的障礙、確保他們獲得公平的勞動權益等。
 - 協調的跨國政策有助於加速發展包容性和持續性的數位經濟，例如消除跨境數位貿易壁壘。
 - 安全可靠的數位支付有助於包容性數位經濟的發展，各國政府應和其他利害關係人合作，建立合適的數位支付基礎設施，並可透過稅金減免等方式鼓勵業者和消費者使用。
 - 維護數位經濟中的勞工權利和工作平等，需要法律框架，且方向上應著重於保護人員，而不是工作。
3. 我們如何確保數位包容的政策空間和流程具有包容性，並促進民眾積極且有意義地參與？
- 有效的數位包容政策需要有目標族群（青年、婦女、農民、殘疾人士等）積極參與政策的制定。數位不平等的問題並不同，政策應符合不同目標族群的需求。

- 利害關係人應該為青年、婦女、多元性別者，和其他代表性不足的族群創造更多機會，使他們能夠有效、持續且有意義地參與網路治理（包括決策）。要確保這些參與空間的安全可靠，避免刻板主義，並配置更多資源（包括財務）於能力建構。

三、信賴

1. 對於確保現今和未來網路的穩定和強韌運作，必要的構成要素是什麼？

- 疫情凸顯安全可靠的網路，是維持社會運作的解決方案，民眾和國家必需能夠信任受到良好保護的網路基礎建設。
- 訂有國家緊急通信計畫的國家，在災難時可以更有效地管理和應變危機。相關應對策略應確保各級政府之間的協調與一致。
- 疫情成為評估數位基礎建設落差和瓶頸的機會，並可開始訂定可負擔且可靠的連網行動計畫。
- 網路的設計初衷是鼓勵全球無國界地互通互連，因此，將更多的人、設備和網絡連接到全球網路，向來且持續是核心目標。
- 相較於公司網路受到較好的保護，員工因為疫情而在家上班增加新的網路風險，應該加強員工的安全教育和訓練，以提升網路安全能力。
- 家用 IoT 設備的快速成長，增加用戶的安全和隱私疑慮。各種指南、出版品和建議應以方便使用的格式呈現，並少用術語和技術詞彙。

2. 利害關係人可以做什麼，以打造一個安全可靠、尊重人權、保護兒少、消除歧視的網路空間？

- 網路是疫情期間民眾溝通和取得訊息的重要管道，政府應持續甚至加速推動數位轉型。
- 事實核查受到政治壓力、財源不足、法律威脅的阻礙，有賴地方和

國際合作，以及因應大量、各種來源和不同語言的訊息。

- 機器人工具可以自動執行打擊假訊息的任務，節省人力資源，但須重視透明度（例如此工具使用的標準和其影響、誰佈建此工具、其目的為何），以免機器人限制言論自由和資訊取得等基本權利。
- 教育、媒體素養、促進尊重事實和科學的公開對話，是打擊線上錯誤信息、恢復對新聞業的信任，以及增進社群媒體（及其算法）處理資訊透明度的核心措施。
- 利害關係人應該合作開發技術工具，以解決線上假訊息和假新聞的問題，例如如何應用 AI 和機器學習來識別仇恨言論。
- 打擊假新聞是每個人的共同責任，使用者在社群媒體分享或傳播資訊時要承擔責任，而不是將所有責任推給社群媒體。相關的認知宣導必須立即加強，並從小培養年輕人的批判性思考。
- 保護兒童上網需要在風險管理和最大機會之間取得平衡，此問題最好由兒童、父母、教育者、業者和政策制定者共同討論。

3. 如何營造有助於利害關係人互信和體諒彼此的對話環境，進而針對網路安全挑戰共同合作提出整體解決方案？

- IGF 應該促進利害關係人對於共同責任和行動的對話，包括在必要時進行監管，以確保使用者能夠持續在安全的網路環境中，進行互動和交流。
- 聯合國的網路安全對話已能納入多方利害關係人的觀點，但需要更努力地具體投入，包括支持跨越數位落差的能力建設。
- 保護兒童網路安全是所有利害關係人的責任，大家應該針對線上遊戲的治理進行系統化的實證研究，包括在國內和國際採取法規和業者自律措施。

- 建立網路空間的信任機制應基於責任、透明、尊重、相互協商、相互理解的原則，在主要的多方利害關係人之間建立開放性合作，並探索各種工具，例如法律和規範、IT 能力、社會責任、道德、監督和自律，以及常規和標準。
- 確保安全和隱私對於IoT生態系統的蓬勃發展非常重要，而指導方針和相關決策過程必須讓包括民間社會和政策制定者在內的各種利害關係人參與。目前缺乏IoT相關的風險知識，並且需要能夠呈現最佳典範和預防風險的能力建構行動，而 IGF 正好可以協調此需求。

第五節 心得與建議

今年（2020）IGF 首度於公報（Messages）中，將所有會議討論重點彙整成 12 個總體政策問題和建議，可說具有相當政策參考價值。例如對於 COVID-19 相關資料的蒐集和使用，公報建議措施包括制訂透明的標準以確保民眾未來願意持續配合防疫資料的蒐集，此點也呼應本報告第二章第二節「科技防疫的網路治理議題」第二點結論建議。而消除數位落差的建議，則包含將「有意義的數位包容」列為政策指導原則，也就是讓使用者有合適的「設備」和「能力」可持續且快速地「連接」到符合他們需求的「內容和服務」，這些要素可以作為檢視我國剩餘約 1 成未上網民眾的障礙因素，進而予以改善。又如對於如何打造安全可靠網路空間的建議，包括立即加強對民眾宣導在社群媒體分享資訊的責任，而本計畫製作的網路內容主題短片，正是向民眾宣導承擔責任及三思而後行的觀念。

除了公報的政策建議外，第二度舉辦的議員專屬會議也持續強化各國立法機關和 IGF 的連結性，並針對各國議員如何促進網路信任提出建議措施；加上幾乎每場會議於會後都附上討論重點或建議，甚至有些講者還自

願承諾將協助推動網路治理發展⁹，這些改變都凸顯 IGF 力求轉型，從過去定位為「不做決策的政策交流平臺」，逐漸轉變成「透過討論進而提供政策建議之處」，同時也呼應聯合國秘書長古特瑞斯於《數位合作藍圖》中提出的強化 IGF 功能及影響力。未來轉型後的 IGF 如能進一步提供相關的治理常規、原則或標準，不但其地位和影響力都將顯著提升，且這些規範建議更可成為各國的重要決策參考，進而有助於減少跨國法規的衝突問題。

9 例如在「克服美中數位冷戰」座談討論中，美國喬治亞理工學院教授 Milton Mueller 承諾將針對中國民眾提供多方利害關係人治理的教育課程；波蘭 Lodz 大學教授 Joanna Kulesza 承諾將於 ICANN 場合提倡以「使用者主權」為中心的觀念。

第七章 總結建議

本計畫透過辦理大專院校校園講座、舉辦培訓課程、製播精華短片等工作，以提升大專青年對網路治理議題的認知、培養我國網路治理的多元人才，以及吸引大眾關心網路治理議題。另一方面，本計畫也挑選當前重要的治理議題進行研析，並（線上）參與相關國際會議進行政策交流，以協助我國掌握通傳政策的議題動向，促使我國網路治理發展符合國際趨勢。

本計畫如期完成契約（經契約變更）指定的所有工作，包括研析 3 個政策案例、舉辦 3 場大專校園講座、舉辦 1 梯次培訓課程、製播 3 支精華短片，以及（線上）參與 1 場國際會議，並提出以下結論與建議。

一、通傳政策案例研析

（一）數位主權：歐洲觀點與政策發展

面對數位化發展高度依賴美中兩國且競爭力相對不足、國際地緣政治競爭日益激烈，以及新冠肺炎疫情危機催化數位轉型的迫切需求等情勢，歐盟於 2020 年 2 月發布維護數位主權的政策方案，強調要讓歐盟整體社會受益於數位轉型，同時保有公平競爭、開放、民主等歐洲基本價值。不過，也引發興起數位保護主義、和中俄獨裁政權為伍、政策方向錯誤且阻礙創新、破壞歐美雙方關係等負面抨擊。

但其實中俄等專制政權實施網路主權已經多年，甚至已經完成立法將國家對網路的監控審查合法化；無獨有偶，美國近來「乾淨網路」計畫也被視為實施川普版的網路主權，且採取中國大陸的干預控制模式。因此，目前探討網路空間的主權議題時，會面臨定義不明確及帶有專制獨裁色彩的問題。儘管如此，在歐盟尋求建立數位主權的過程中，就實務面來看，現階段我們可先行評估國內是否也面臨歐盟所擔憂的數位風險，同時也要掌握歐盟相關政策進展，以即時因應具有域外效力的歐盟新規。

（二）科技防疫的網路治理議題

AI、大數據等新興技術被用於預測、監控和預防新冠肺炎疫情，網際網路更是疫情因應措施的重要基礎，網路治理議題也因此受到影響，範圍包含網路安全、網路發展、法律與人權、數位技術、資訊社會，以及數位經濟等層面。我國因為防疫成效良好，社會得以正常運作，但反而缺乏利用數位遠距工具完全取代實體業務運作的實務經驗。此波疫情被視為是各國加速推動數位轉型的一大契機，因此，我國也要全面強化數位社會發展，包含因應數位落差問題，避免數位化進程反而相對落後。

此外，個資是此次科技防疫最重要的資源及決策依據，因而衍生許多相關治理問題。如我國個資法對於「為增進公共利益所必要」賦予很大的授權空間，且《嚴重特殊傳染性肺炎防治及紓困振興特別條例》對於「中央流行疫情指揮中心指揮官」也賦予很大的行政權力，以致產生過度空白授權的疑慮。又如《實聯制措施指引》因為缺乏後續的監督稽核機制而發生許多商家過度蒐集個資等情況。因此，後續仍需檢討改善科技防疫相關法規措施，以法制建立社會信任，民眾才會願意持續配合防疫措施，我國防疫成效才得以延續下去。

（三）聯合國數位合作藍圖的擘劃與挑戰

聯合國於2020年6月發布《數位合作藍圖》，提出全球連網、數位包容、數位人權等8項有賴全球共同採取行動的關鍵領域。數位合作並於《紀念聯合國成立75周年宣言》獲得聯合國193個會員國的承諾。不過，《數位合作藍圖》也被形容是「沒有牙齒的許願清單」，凸顯未來即使發布治理規範或標準，也不具有強制性，且目前尚未公布後續的時程和細節，因此，各界對於如何推動數位合作仍有諸多疑問。

儘管如此，《數位合作藍圖》對於我國的數位政策仍具重要參考意義。例如聯合國將研擬具體量化的數位包容等指標，我國可用於檢視上網資費的合理性、弱勢族群的上網權益保護、資訊素養的教育成效等施政。此外，

未來聯合國還將針對新科技的使用進行人權盡職調查，並表示鎖定目標的通訊監察、缺乏保護設計的數位身分計畫等措施，都可能涉及侵犯國際人權法規。我國《科技偵查法》草案、數位身分證計畫等政策，都引發國內各界的不同論戰，因此，對於涉及使用數位科技的公共政策應該進行更審慎的評估，並和整體社會充分溝通，以真正落實保障數位人權。

二、大專院校講座

本年度於臺灣大學、中興大學、高雄科技大學共計辦理 3 場講座活動，場合皆為學分課程，學生涵蓋大學生與研究生，系所包括電工所、資工所和資管系，出席人數分別為 102 位、120 位、56 位。講師則由本計畫主持人吳國維和顧問陳文生擔任，演講主題分別為淺談數位主權與網路分裂、美國電子商務綱領預告全球通信產業變革及爭議、轉變中的網路世界規則。

整體而言，本年度 3 場講座的大學生和研究生對於網路治理議題的興趣並無明顯落差，但如綜合上年度的執行經驗，顯然是上年度行政管理所學生的表現最為突出，他們積極提問至課後 45 分鐘才結束。惟本年度礙於地區不得重複、每場 2 小時以上、出席人數 50 人以上等規定，於活動安排受到較多限制，例如北部大學佔全臺大學 47% 但不得選擇第 2 所、有些系所的專題演講課程只有 1 小時、許多文法系所的學生人數遠不及 50 人等。因此，建議未來將大專院校實際情況納入規格考量，以保留執行彈性，安排於學生可能對網路治理議題更感興趣的學校系所演講。

三、人才培訓課程

本年度共 29 位學員參與全日培訓課程並順利結業。學員對於課程內容整體設計的滿意度達 100%、高達 97% 學員表示上完課後對網路治理的興趣增加，且所有學員都認為學到了網路治理的議題與挑戰，還有 86% 學

員表示願意參加 TWIGF、76% 願意線上參加 APrIGF、66% 願意線上參加 IGF。而從知識和興趣的增加，以及樂於參與座談交流的態度，也顯示本次課程達到柯氏（Kirkpatrick）學習成效的部分「學習層級」（第二層級）。

然而本計畫在有限的資源下，僅能獎勵 1 名優秀學員參與國際會議（雖然本年度國際會議皆因疫情影響而改成線上會議），並提供如 APrIGF 線上特派員等單次小規模的活動，期能儘量維繫學員對網路治理議題的持續關注，並為單日的培訓課程增添些許的延續性。面對網路治理的重要性提升，需要更多的多方利害關係人參與政策討論，未來除了應該持續辦理培訓課程外，也需要一併投入更多資源，提供學員更多的參與機會和發表舞臺，以鼓勵他們持續且長期地參與網路治理。

四、精華短片製播

本年度分別以網路安全、網路內容、網路人權為主題，排除萬難和 YouTuber 合作製播 3 支精華短片，截至 12 月 1 日的觀看次數分別為 2.4 萬、3.3 萬，以及 7,200 次。第 3 支短片觀看次數落差較大，推估主因可能是影片名稱為臺灣民眾過於熟悉的詐騙議題，以致不易引起觀看興趣。但無論如何，觀眾的意見回饋都相當正面，留言數分別為 230 則、190 則和 77 則，大多為對主題和內容表示肯定，以及感謝分享重要知識和觀念等。

精華短片製播旨在做為增進大眾認識網路治理議題的教材，惟全球每天有 72 萬小時的影片上傳 YouTube，且本計畫培訓課程或大專講座的内容皆有一定難度，即使經剪輯也不易吸引大眾觀看，進而完成計畫要求的流量分析。適逢 IGF 2020 國會議員場次建議各國（雖然是針對各國議員的建議）推動網路安全、對抗假訊息等治理議題的大眾認知宣導，因此，未來如有充足經費，可參考市場行情編列預算，為大眾量身訂做合適的影片內容且於合適的頻道（如知識型頻道）推廣播放。

五、國際會議參與

受到 COVID-19 影響，IGF 2020 首度全面以虛擬會議方式進行。而為了展現會議的具體成效，本年度的會後公報 (Messages) 將所有會議的討論重點彙整成 12 個總體政策問題和建議，可說具有相當政策參考價值。例如消除數位落差的建議包含將「有意義的數位包容」列為政策指導原則，也就是讓使用者有合適的「設備」和「能力」可持續且快速地「連接」到符合他們需求的「內容和服務」，這些要素可作為檢視我國剩餘約 1 成未上網民眾的障礙因素，進而予以改善。

此外，今年 IGF 也再次舉辦議員專屬會議，持續強化各國立法機關和 IGF 的連結性，並於每場會議結束後，提供討論重點或建議，這些改變都凸顯 IGF 力求轉型，未來如能依《數位合作藍圖》規劃，進一步提供治理常規、原則或標準，不但 IGF 的地位和影響力都將顯著提升，且這些規範建議更可成為各國的政策決策參考，進而有助於減少跨國法規的衝突。

六、未來工作建議

綜合前述本年度各工作項目的執行經驗與成果，本計畫所建議的後續研究議題與執行工作可歸納如下：

(一) 研究分析

- 評估我國數位風險疑慮

評估我國是否面臨如資料掌控權、數位依賴、數位競爭力等歐盟所擔心的數位風險，進而針對我國數位發展現況研議相關因應策略。

- 掌握歐盟數位法規進展並評估具域外效力者

追蹤歐盟數位主權政策 23 項主要行動措施 (表 5) 進展，尤其《數位服務法》草案等規範可供我國相關治理政策參考；並盤點且評估行動措施中可能具有域外效力的法規，以利我國及早準備因應措施。

- 檢視科技防疫相關法規措施

檢視並改善涉及個資隱私的科技防疫相關法規和措施，如個資法、傳染性肺炎防治特別條例、實聯制實施機制等，以透過法制建立社會信任。

- **追蹤《數位合作藍圖》指標進展**

追蹤聯合國《數位合作藍圖》有關訂定普及上網和數位人權等具體量化指標的進展，未來可用於檢視我國相關數位政策的成效，並可結合既有計畫協助國際社會縮減數位落差。

(二) 推廣宣導

- **持續辦理大專院校講座**

國外大學設有網路治理專屬的學分課程，國內則十分罕見，因此，可透過 1~2 小時的專題演講，讓大專青年有機會認識網路治理、對治理議題產生興趣，進而可能願意關心並參與治理政策討論。

- **視預算製播大眾認知宣導影片**

IGF 2020 國會議員場次建議各國推動網路安全、對抗假訊息等議題的大眾認知宣導。未來相關部會如有充足預算，可為大眾量身訂做宣導影片，並於合適的影音平臺與頻道播出。

(三) 人才培訓

- **持續培訓人才並協助創造長期參與誘因**

網路治理的重要性因為疫情爆發而顯著提升，未來除了持續辦理培訓課程外，也需一併投入更多資源，共同創造鼓勵長期參與的誘因和機會。

(四) 數位發展

- **加速推動數位轉型與數位包容**

COVID-19 擴大數位落差，也加速各國推動數位轉型。我國因防疫有成社會正常運作，反而缺乏數位轉型的實務經驗及迫切需求，未來需加速推動數位轉型與數位包容，以免落後於國際社會。

附件