

國家通訊傳播委員會

「推動我國網路治理發展與國際趨勢研析」

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 1 月 2 日

目 錄

摘 要	ix
第一章 計畫簡介	1
第一節 緣起與目標	1
第二節 計畫架構與內容	3
第三節 執行時程及進度	3
第四節 預期成果與績效指標	5
第二章 大專院校宣講	7
第一節 執行概況	7
第二節 宣講內容	9
第三節 國立成功大學場次	12
第四節 國立政治大學場次	14
第五節 世新大學場次	16
第六節 東海大學場次	19
第七節 國立高雄科技大學場次	20
第八節 靜宜大學場次	22
第三章 人才培訓課程	24
第一節 活動內容	24
第二節 活動辦法	28

第三節	活動網站與宣傳	31
第四節	學員評選與錄取	34
第五節	課程內容摘要	37
第六節	印刷與影音紀錄	52
第七節	學習成效評估	55
第八節	選拔優秀學員參與國際會議	60
第九節	TWIGF 特派員活動	61
第四章	國際專家訪臺	63
第一節	專家簡介與行程安排	63
第二節	拜會通傳會	64
第三節	TWIGF 專題演講：網路的自治與正統性	68
第四節	TWIGF 座談：如何因應市場鞏固問題?	70
第五節	TWIGF 座談：DNS 封鎖架構與問題	75
第五章	舉辦座談會議	80
第一節	申辦通傳議題座談會議	80
第二節	通傳議題座談：OTT 現狀、治理及未來展望	84
第三節	通傳議題座談：AIoT 時代的安全與隱私挑戰	94
第四節	國際參與分享會議：臺灣、亞太與全球的焦點議題	103
第六章	參與國際會議	116
第一節	2019 亞太區網路治理論壇 (APrIGF)	116

第二節 2019 聯合國網路治理論壇 (IGF).....	127
第七章 治理議題分析.....	142
第一節 全球主要討論議題.....	142
第二節 AI 治理：歐盟與 OECD 政策建議.....	151
第三節 內容治理：發展中的全球政策標準.....	173
第四節 5G 治理：公眾健康、資安與國安.....	189
第八章 結論與建議.....	199
附件	207

圖 目 錄

圖 1. 計畫架構圖.....	3
圖 2. 大專院校宣講活動海報.....	8
圖 3. 大專院校宣講內容簡介 1.....	9
圖 4. 大專院校宣講內容簡介 2.....	10
圖 5. 大專院校宣講內容簡介 3.....	11
圖 6. 成功大學宣講照片.....	13
圖 7. 政治大學宣講照片.....	15
圖 8. 世新大學宣講網路投票結果.....	18
圖 9. 世新大學宣講照片.....	18
圖 10. 東海大學宣講照片.....	19
圖 11. 國立高雄科技大學宣講網路投票結果.....	21
圖 12. 國立高雄科技大學宣講照片.....	22
圖 13. 靜宜大學宣講照片.....	23
圖 14. 研習營講師簡介.....	28
圖 15. 研習營活動網站.....	32
圖 16. 研習營宣傳截圖 (官網與 FB 社團).....	33
圖 17. 研習營宣傳截圖 (大專院校網站).....	34
圖 18. 研習營合格報名者的得分統計.....	35
圖 19. 研習營學員組成概況.....	36

圖 20. 研習營布置與印刷品.....	53
圖 21. 研習營照片.....	54
圖 22. 研習營課程簡報資料與錄影檔.....	54
圖 23. 柯氏學習評估模式.....	55
圖 24. 研習營「課程內容」滿意度.....	57
圖 25. 研習營「行政會務」滿意度.....	57
圖 26. 研習營學員課後自我評估.....	58
圖 27. 研習營優秀學員報告與評選會議照片.....	60
圖 28. 研習營「TWIGF 特派員活動」辦法與獎勵.....	61
圖 29. 研習營「TWIGF 特派員活動」摘要報告刊登頁面.....	62
圖 30. 國際專家拜會通傳會照片.....	67
圖 31. 國際專家於 TWIGF 專題演講照片.....	70
圖 32. 國際專家參與「Internet consolidation is here 座談」照片.....	74
圖 33. 阻止非法內容傳輸之尋求服務供應商順序.....	77
圖 34. 處理網路安全問題的政策順序.....	77
圖 35. 國際專家參與「CP/TPP ISP DNS Block 架構跟問題座談」照片 ...	79
圖 36. 2009 年與 2019 年網路流量架構比較.....	85
圖 37. 「OTT 現狀、治理及未來展望座談」照片.....	93
圖 38. 「OTT 現狀、治理及未來展望座談」媒體報導.....	94
圖 39. 「AIoT 時代的安全與隱私挑戰座談」照片.....	103

圖 40. 「臺灣、亞太與全球的焦點議題」分享會網站頁面	105
圖 41. 「臺灣、亞太與全球的焦點議題」分享會線上提問	112
圖 42. 「臺灣、亞太與全球的焦點議題」分享會照片	113
圖 43. 2019 APrIGF 會議剪影	126
圖 44. 2019 IGF 會議剪影	141
圖 45. 歐盟《可信賴 AI 的倫理準則》實施評估清單	158
圖 46. 歐盟 AI 倫理原則與日本 AI 社會原則	167
圖 47. 美國、歐盟、臺灣之 AI 策略重點	170
圖 48. 美、歐、印、中之網路法規強度	175
圖 49. 瑞士、澳洲民眾上街抗議 5G 建設	192

表 目 錄

表 1. 計畫時程表.....	4
表 2. 計畫查核項目.....	4
表 3. 預期量化與質化成果.....	6
表 4. 大專院校宣講活動辦理概況.....	7
表 5. 研習營課程表.....	25
表 6. 研習營學員成果報告彙整表.....	50
表 7. 學習成效層級一與二之評估方式與限制.....	56
表 8. 日本盜版漫畫網站討論中的因應措施.....	66
表 9. 「Internet Consolidation is here 座談」共識與歧見.....	74
表 10. 「CP/TPP ISP DNS Block 架構跟問題座談」共識與建議.....	79
表 11. 通傳議題座談會之議題挑選與提案規劃.....	80
表 12. TWIGF 首日議程表與本計畫申辦場次.....	81
表 13. 「OTT 現狀、治理及未來展望座談」共識與歧見.....	92
表 14. 「AIoT 時代的安全與隱私挑戰座談」共識與歧見.....	102
表 15. 「臺灣、亞太與全球的焦點議題」分享會議程.....	105
表 17. 2019 IGF 遠端參與場次.....	128
表 18. IGF 2019 專家精選的討論議題.....	143
表 19. IGF 2019 政府關切的討論議題.....	144

表 20. IGF 2019 各界關切的討論議題	145
表 21. IGF 共同研討議題	148
表 22. 全球關切議題 (IGF 2019) 彙整	150
表 23. 歐盟《可信賴 AI 的政策與投資建議》列表	159
表 24. 歐盟與 OECD 之 AI 政策建議比較	165
表 25. 內容治理實施標準(準則)之條文摘要	181

摘要

本計畫透過辦理校園演講、培訓課程、座談會議、國際專家訪臺等活動，並參與國際會議及彙整分析通傳政策議題，以提升大專青年對網路治理的認知，培育我國網路治理的多元專業人才及民間參與能量，促進國內多方利害關係人對話與凝聚政策共識，增進國際交流與相互學習，並掌握通傳政策議題動向，進而促使我國網路治理發展符合國際趨勢。

本計畫並針對上述各項工作，提出結論與建議：

- 大專院校宣講：於特定課程或全系所固定集會活動宣講，各有其深度交流或廣度宣傳的效果，值得持續辦理。
- 人才培訓課程：課程結果達到柯氏 (Kirkpatrick) 學習成效的學習層級 (第二層級)，但在缺乏責任歸屬的驅動要素下，只憑本計畫的短期誘因，難以將學員的興趣及知識技能，轉化成參與國內外議題討論的具體行動力，有賴社會各界共同創造長期穩定誘因加以改善。
- 國際專家訪臺：日本專家訪臺開拓我國網路治理議題視野，強化我國推動多方利害關係人參與的信念，並促進臺日治理政策交流。未來應持續邀請國際專家來訪。
- 舉辦座談會議：討論結果顯示，多方利害關係人皆認為，我國的 OTT 影音政策應採取低度管理，且 AIoT 的安全隱私有賴各方共同推動。
- 參與國際會議：相較於東南亞國家熱烈申辦 APrIGF 座談，我國更應展現積極參與。而在 IGF 部分，則需關注為了強化國際數位合作的 IGF Plus 模式發展；另也建議行政與立法部門，參考 56 國議員所提出有關制定網路法規的相關建議。
- AI 治理：發展以人為本、可信賴的 AI，已成為國際趨勢，且歐美日等

國皆以國家策略迎接 AI 時代的機會與挑戰。因此，我國除了應將偏向產業政策的《臺灣 AI 行動計畫》升級為兼顧因應社會衝擊的國家整體策略，並調和由立委提出且已獲立法院一讀通過的《人工智慧發展基本法》外，也要關注新任歐盟執委會主席是否推動 AI 立法並促其成為影響全球的下一個 GDPR。

- 內容治理：為了避免網路濫用行為惡化及各國法規衝突導致全球網路分裂，國際網路治理專家已提出旨在成為國際政策標準的《內容與管轄權計畫：實施方案》，與《全球資訊網合約》，我國可以據此盤點檢視國內的相關政策與措施，以確保我國的內容治理符合國際主流趨勢。
- 5G 治理：行動通訊技術涉及的公眾健康議題從未間斷，主管機關應著手準備公眾溝通方案，以因應我國即將於 2020 年啟動 5G 商轉。另外，在安全方面，建議政府了解 5G 網路的技術特性，並參考國際降低 5G 風險的措施，透過多管齊下方式，將可能的資安與國安衝擊降到最低。

Abstract

Through organizing campus lectures and training courses, this project aims to raise the awareness of Internet governance among youth and college students, and to cultivate diversified professional talents in the field of Internet governance in Taiwan, as well as to enhance the participation of private sectors. Panel discussions had also been held in order to promote multistakeholders dialogue within the country and to build policy consensus. In the meantime, the international expert paid a visit to Taiwan sharing international policy of Internet governance and enhancing international exchange and mutual learning. Last but not the least, participation in international forums and analysis of governance issues such as AI, Internet content, and 5G 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:

- Campus lectures in colleges: Participants include undergraduate and graduate students, whose majors cover liberal arts and science. Generally speaking, graduate students showed more interests in Internet governance. Lectures were organized in specific course or regular assembly for the whole department. Each venue has its advantage of in-depth communication or extensive publicity effect respectively, which deserves continuous investment of efforts.
- Training courses: All participants completed the full program of the training courses and their overall satisfaction was better than that of last year. The result of the courses matched the learning level (the second level) of Kirkpatrick' s Training Evaluation Model. However, due to the lack of the

drives of responsibilities, the short-term incentives of this project could hardly turn the interests and knowledge of participants into concrete actions for taking part in the discussions of domestic and international issues. It depends on the long-term and stable incentives (such as job opportunities, chances to keep on participating in international conferences, etc.) created by all sectors of society to improve this situation.

- A visit from the international expert: The Japanese expert, Mr. Maemura Akinori was invited to Taiwan sharing the issue of content blocking and the phenomenon of Internet consolidation that is of global concern at TWIGF. His visit to Taipei had broadened the horizon of Internet governance in Taiwan, strengthening the belief in promoting multi-stakeholder participation and encouraging policy exchanges between Taiwan and Japan. He also would be likely to share what a well-received event TWIGF was with his fellow Japanese. In the future, it is highly recommended that international experts should be invited continuously.
- Panel discussions: Based on the results of the panel discussions, multistakeholders all thought that OTT video service policy in Taiwan should be managed in light touch approach, and the improvement of security and privacy of AIoT depends on the joint efforts of all parties. However, panelists had different opinions on the degree of light touch approach, methods, and consumer protection practices on the governance of OTT video service. In addition, for the AIoT session, no consensus was reached on whether or not the government can detect people's devices or demand for the backdoor access to products for the sake of security concern. Nevertheless, these disagreements still helped improve mutual understanding and communication, and could serve as a basis for subsequent policy discussions.

- Participation in international forums: Compared with the enthusiasm of applying for workshops at APrIGF from the Southeast Asian countries, Taiwan should present even more active participation or apply for the role of panelists. In terms of Internet Governance Forum (IGF), we should focus on the development of IGF Plus model, which is to strengthen international digital cooperation. It is also recommended that the administrative and legislative sectors refer to the relevant suggestions proposed by parliamentarians from 56 countries (Message from the Meeting of Parliamentarians Participating in the 14th UN Internet Governance Forum) on the formulation of Internet regulations, which fully reflect the basic spirit needed for the current Internet policies and legislation.
- AI governance: The development of human-centric and reliable AI has become an international trend, and countries such as Europe, the United States, and Japan have all adopted national strategies to embrace the opportunities and challenges of the AI era. Therefore, we should upgrade the “Taiwan AI Action Plan,” which favored industrial policies, to a national overall strategy that takes social impacts into account, and reconcile it with the “Basic Law on Artificial Intelligence Development,” which was proposed by the legislators and has been approved on the first reading at the Legislative Yuan. Moreover, we should pay attention to whether the newly elected Commission President of the European Union will promote the legislation of AI and turn it into the next GDPR that affects the whole world.
- Content governance: In order to avoid the deterioration of online abuse and global Internet fragmentation resulting from the conflict of national regulations, international Internet governance experts have proposed “Content & Jurisdiction Program : Operational Approaches” and “Contract for the Web,” which aim to become international policy standards. Based on

these standards, relevant policies and measures in Taiwan could be reviewed and improved to ensure that the content governance is in line with trends of international mainstream.

- 5G governance: The public health issues involved with mobile communication technology have never ceased, and there have been cases of people protesting against 5G deployment on the streets in Switzerland and Australia this year. Therefore, the authority in Taiwan should get started for a public communication plan in response to the upcoming launch of 5G business in 2020. In addition, since the deployment of 4G, using China-manufactured equipment in critical facilities such as core networks was banned in Taiwan in accordance with relevant regulations. It is suggested that the government should understand the software-oriented technical characteristics of 5G networks, the legislation and legal system where 5G core equipment manufacturers are located, as well as refer to international policy measures that reduce 5G risks. Through a combination of simultaneous policies, we could minimize the possible impacts of 5G networks on national security.

第一章 計畫簡介

第一節 緣起與目標

一、計畫緣起

聯合國資訊社會世界高峰會議 (World Summit on the Information Society, WSIS) 曾提出「網路治理 (Internet governance)」的定義，指一種藉由政府、私部門和民間社群，各自發揮角色、共享原則、規範、規則、決策程序及計畫，以型塑網際網路演進與運用的發展和應用過程。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。

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。

面對數位科技、數位經濟模式的快速演變，以及各國網路政策走向變動等所衍生的網路治理挑戰，並因應我國將於 109 年邁向 5G 世代，以政策推動 5G 發展及網路治理有其重要性，是以，本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，提升本會主管數位匯流發展與網路治理之權責，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，本會於 107 年辦理「網路治理交流與人才培育」補助計畫(計畫之期末報告已公開於政府研究資訊系統 (GRB)，網址：<https://www.grb.gov.tw/>)，為延續該計畫推動之成果，爰於 108 年再廣續辦理「推動我國網路治理發展與國際趨勢研析」委託研究計畫，期產出內容契合我國數位經濟社會與產業發展之需求。

本計畫期藉由廠商在網路治理方面之豐富經驗，一方面赴大專院校推廣網路治理及國際趨勢發展等概念，另一方面舉辦專業課程(如研習營)培育我國優秀人才參與國際會議，強化我國與國際網路治理組織之交流合作，並以多方利害關係人參與模式，舉辦至少 2 場次與本會職掌有關之國內網路治理相關研討會、座談會或論壇，凝聚各方利害關係人之共識，尋求最佳網路治理方案，並提供國際議題或案例(包括 5G 相關治理議題)分析及建議等事項，俾利本會研擬提升我國網路治理環境之施政參考。

二、計畫目標

本計畫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及民間參與國內外網路治理會議研討之能量，並掌握通訊傳播有關之網路治理模式與議題動向，推動我國網路治理發展與國際同步，增加國內多方社群對話機會，促進凝聚網路治理政策共識，並進行跨國分享與相互學習，展現網路治理的雙向實質國際交流與合作，凝聚各方利害關係人之意見，尋求最佳網路治理方案，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「校園推廣及人才培育」、「國際網路治理交流」、「推動網路治理發展」、「國際趨勢及我國現況分析」4大項，並可再細分為大專院校宣講、辦理培訓課程、邀請國際專家訪臺、參與國際會議、舉辦國際參與分享會議、舉辦通傳議題座談會議、彙整全球主要議題、分析通傳政策議題等8個子項目，計畫架構如下圖1所示。



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 (108 年 4 月 24 日) 起，至提交完整期末報告等文件」止。各項工作的時程規劃、查核項目暨時程，如下表 1 與 2 所示。

表1. 計畫時程表

工作項目	4月	5月	6月	7月	8月	9月	10月	11月	12月
1. 大專院校宣講									
1.1 安排宣講	安排第1~3場			安排第4~6場					
1.2 製作海報&教材	2小時教材				更新教材				
1.3 執行宣講		5/2成大, 5/4政大	6/12世新			執行第4~6場			
2. 辦理培訓課程									
2.1 活動規劃&網站建置									
2.2 課程安排&講師溝通									
2.3 活動宣傳&報名	4/26~5/12								
2.4 布置印刷&行政庶務									
2.5 學員評選&公布聯繫		5/13~17; 5/20~							
2.6 活動執行&會後作業		5/31~6/1(40人)							
2.7 優秀學員選拔與出國			行前準備	APriGF 7/16~19		參加分享會議			
2.8 TWIGF特派員活動				7/5~6					
3. 邀請國際專家訪台									
3.1 邀請聯繫									
3.2 行程安排									
3.3 演講交流				7/4~6					
4. 參與國際會議									
4.1 參加APriGF			行前準備	7/16~19					
4.2 參加IGF								11/25~29	
5. 舉辦國際參與分享會議									
5.1 活動規劃&網站建置									
5.2 活動宣傳&報名									
5.3 活動執行&會後作業									
6. 舉辦通傳議題座談會議									
6.1 提案規劃	4/15								
6.2 講者邀請聯繫									
6.3 座談會議召開				7/5					
7. 彙整全球主要議題									
7.1 資料蒐集與彙整									
8. 分析通傳政策議題									
8.1 議題分析1~2									
8.2 議題分析3									
9. 期中期末報告									
9.1 期中報告初稿									
9.2 期中審查&報告修正									
9.3 期末報告初稿									
9.4 期末審查&報告定稿									包括增補IGF

表2. 計畫查核項目

查核項目	查核點	日期
期中報告	<p>1.完成赴大專院校或國立大學宣講網路治理發展與國際趨勢至少 3 場次，並提供宣講的學校名稱、時間、場地、規模(每場參加人數)、推廣內容與主題等資料。(參照 7-19 頁)</p> <p>2.完成至少 30 人的網路治理人才培訓課程(含入門及進階課程)，並選拔優秀人才參與國際會議。另提供培訓課程實施報告。(參照 24-62 頁)</p> <p>3.邀請通訊傳播有關之網路治理國際學者專家至少 1 人訪台交流，並提供國際學者專家名單及交流內容報告。(參照 63-79 頁)</p>	<p>契約生效 次工作 日 150 日 內</p>

	4.於國內具一定規模之非營利性網際網路治理論壇【例如：臺灣網路治理論壇(TWIGF)】舉辦至少 1 場次之研討會或座談會，聚焦討論涉通訊傳播之網路治理議題至少 3 項，共同推動我國國家型 IGF 發展，並提供重要議題報告。(參照 80-103 頁)	
期末報告 (初稿)	<p>1.累積完成赴大專院校或國立大學宣講網路治理發展與國際趨勢至少 6 場次(含期中報告前完成之場次)，並提供宣講的學校名稱、時間、場地、規模(每場參加人數)、推廣內容與主題等資料，以及執行成果與效益分析報告，並就未來網路治理人才培訓提出建議。(參照 7-23 頁)</p> <p>2.參與國際網路治理會議至少 1 場次【含 2019 年亞太區網路治理論壇 (APrIGF)】，並完成至本會發表出國心得分享及提供重要議題報告。(參照 116-141 頁)</p> <p>3.舉辦至少 1 場次之國際參與心得分享交流會議。(參照 103-115 頁)</p> <p>4.彙整全球網路治理主要討論議題，從中挑選至少 3 個與我國通訊傳播政策相關之案例(包括 5G 相關治理議題)，完成研析報告。(參照 142-198 頁)</p>	契約 生效 次工 作日 240 日 內
期末報告 (定稿)	<p>依審查意見修訂期末報告，並包含</p> <p>1.出席 2019 年聯合國網路治理論壇(IGF)之重要議題報告(參照 127-141 頁)</p> <p>2.中文摘要 (3,000 字至 3,500 字)(參照 ix-xiii 頁)</p> <p>3.英文摘要 (1,000 字左右)</p>	指定 期限 內

第四節 預期成果與績效指標

本計畫主要執行「校園推廣及人才培育」、「國際網路治理交流」、「推動網路治理發展」、「國際趨勢及我國現況分析」等 4 大項工作項目。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、推動輔導，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	人才培育	32. 培育人才情形, 含人數及內容	<ul style="list-style-type: none"> • 培訓課程人數≥ 30 • 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)	<ul style="list-style-type: none"> • 大專校園宣講場次≥ 6 (每場人數≥ 30) • 大專校園宣講簡報≥ 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	<ul style="list-style-type: none"> • 國際專家訪臺≥ 1 	引進國際網路治理第一手資訊，提供國內多方利害關係人與國際專家交流機會
		44. 學術活動互動(研討會、專題討論...等)	<ul style="list-style-type: none"> • 出席國際會議≥ 2 	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
	推動輔導	49. 輔導/推廣目標達成率	<ul style="list-style-type: none"> • 國際參與分享會議≥ 1 • 通傳議題座談會議≥ 1 	推動國內多方利害關係人對話，促進凝聚政策共識，促進我國國家型 IGF 發展
其他效益 (科技政策管理及其他) 己		56. 決策依據	<ul style="list-style-type: none"> • 彙整全球主要議題≥ 1 • 分析通傳政策議題≥ 3 	掌握全球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 大專院校宣講

第一節 執行概況

本計畫依據委託辦理工作項目規定，完成 6 場次各 2 小時且出席人數達 30 人以上的大專院校宣講活動，包括北部 2 場次（政治大學、世新大學舉辦，中部 2 場次（東海大學、靜宜大學）、南部 2 場次（成功大學、高雄科技大學）。宣講場合則於特定課程，或整個系所的固定集會活動，且系所橫跨文科與理科，出席者涵蓋大學生與研究生。至於出席人數單一場次最少為 31 人，最多高達 210 人。各場次的辦理概況彙整如下表 4。

表4. 大專院校宣講活動辦理概況

場次	時間	學校	系所 / 活動名稱	地點	人數
1	5/2 (四) 13:30~15:30	國立 成功大學	電腦與通訊工程研究所專 題研討	電機系繁城講堂	183
2	5/4 (六) 13:30~16:15	國立 政治大學	行政管理碩士學程 (在職 專班)公共管理課程	綜合院館南棟一樓 270113 教室	33
3	6/12 (三) 13:00~15:00	世新大學	資訊傳播學系(所)週會	大禮堂 A201 良彥講 堂	210
4	9/26 (四) 14:10~16:10	東海大學	資訊管理所專題討論課程	管理學院 M243 教室	31
5	9/30 (一) 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)	財金學院大樓地下 1 樓 E006 教室	51
6	10/21 (一) 13:00~15:00	靜宜大學	資訊管理學系資管生涯講 座 (大四)	資訊大樓 115 教室	80

本計畫並設計製作宣講活動海報與電子檔（下圖 2），以便校方於活動前宣傳使用，以及活動時張貼於現場合適的位置。



圖2. 大專院校宣講活動海報

第二節 宣講內容

本計畫以「網路世界誰來管？」為題，規劃製作2個小時的宣講簡報，內容從國內近期重大且生活化的實際案例切入，並從中帶入多方利害關係人的參與精神，期能藉此引發學生共鳴及對網路治理的興趣，進而願意關心並參與議題的討論。本計畫完成的宣講簡報共計51頁，詳「附件一」，內容分成5大部分，大綱與重點簡介如下：

1. 生活中的網路治理議題

- 3個近期重大議題案例 (以多方利害關係人的不同觀點呈現)
- 名人提及的網路治理議題
- 上列議題對照 2018 聯合國 IGF 主題&子題

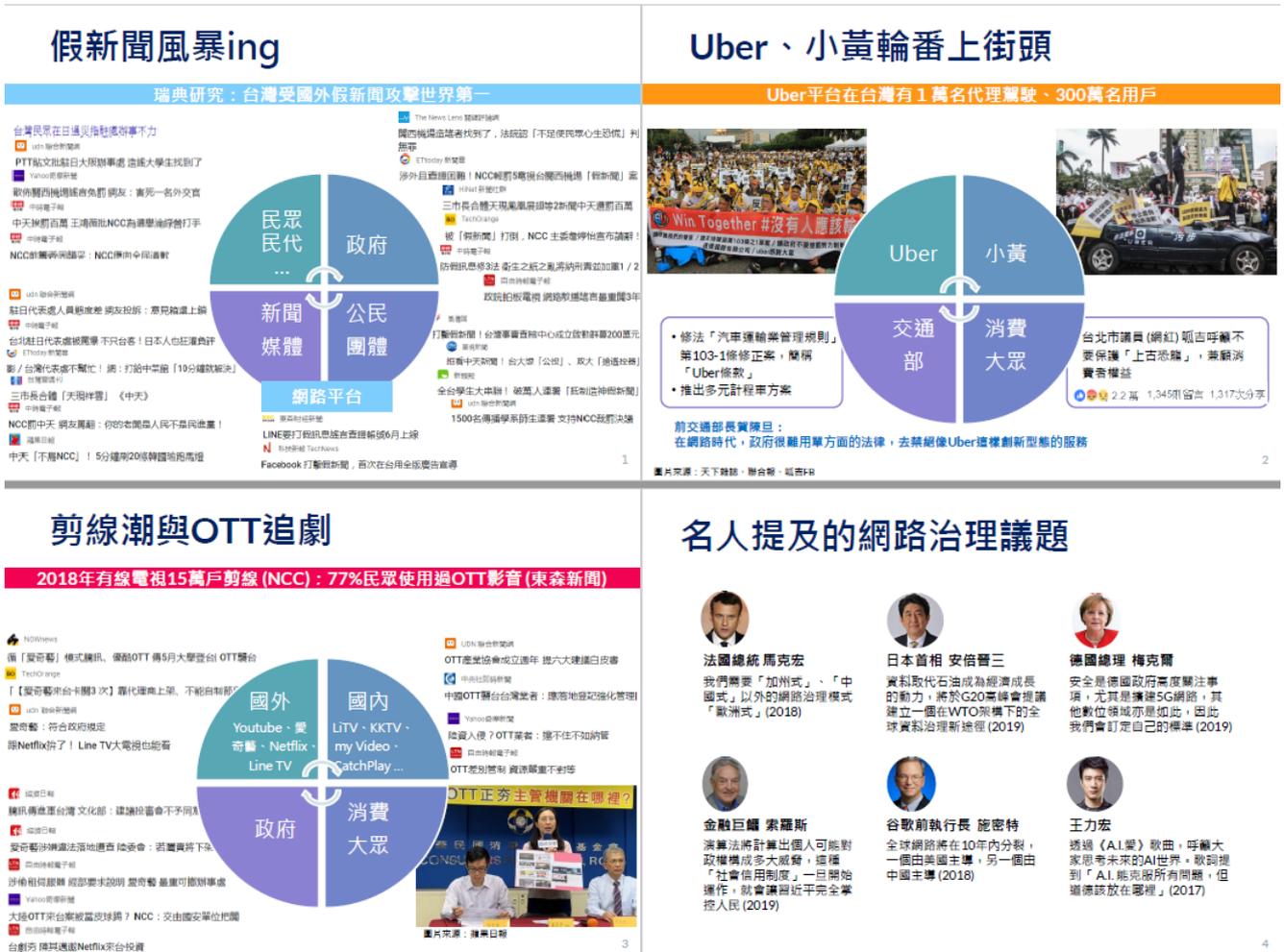


圖3. 大專院校宣講內容簡介 1

2. 什麼是網路治理

- 網路三層式架構及其參與者
- 網路治理觀念的轉變
- 網路治理的定義、目標、範疇、多方利害關係人模式
- 網路治理的模式與發展
- 腦力激盪：誰該負責移除網路上的不當內容？科技公司應該配合執法當局打擊犯罪要求而在產品植入後門程式嗎？誰該為中勒索軟體病毒 (如 WannaCry) 而負責？ (共 3 個問題)

網路世界誰來管？

No one person, government, organization, or company governs the digital space. Digital Governance may be stratified into the three layers... Solutions to issues in each layer include policies, best practices, standards, specifications, and tools developed by the collaborations of stakeholders and experts from actors in business, government, academia, technical, and civil society (ICANN, 2015)

參與者

- World Economic Forum
- ICANN
- International Internet Consortium
- ICG
- Regional Organizations
- Private Sector
- Non-Governmental Organizations
- Academia
- Law Enforcement Agencies

觀念的轉變 (2/2)

2010

2019

圖片來源：Dr. Andy Yen；Business Insider

網路治理的模式與發展

	1996~2005	2006~2015	2016~
多方模式 Multi-stakeholder	<ul style="list-style-type: none"> 1998年非營利組織 ICANN 於美國加州成立，採多方模式運作，受到美國商務部監督 (受外公約) 	<ul style="list-style-type: none"> 2006年聯合國開始每年召開 IGF，推動多方模式治理網路，並帶動全球 NRIs (國家型與區域型 IGF) 發展 2013年史坦登事件引發國際對美國不滿；2014年美國宣布交出 IANA 監督權，但美國內部有反對聲浪 2014年全球 90 多個國家「網路世界多方利害關係人聲明」(NETmundial) 	<ul style="list-style-type: none"> 2016年 ICANN 完成 IANA 移轉，象徵美國政府退出監督全球網路資源 2016~2025年聯合國持續舉辦 IGF 近幾年要求 IGF 改革聲浪高漲 2018年觀點：我們需要更強大的網路治理，且歡迎支持多方模式
多邊模式 Multi-lateral	<ul style="list-style-type: none"> 中國、伊朗等國：全球網路不該只由美國政府與 ICANN 掌管，而應由聯合政府管理 (intergovernmental) 的多邊模式來管理 	<ul style="list-style-type: none"> 2011年中、俄等國：聯合國應建立多邊的國際網路管理系統。ITU 2012年中國的 ITU 推動新協議授權電信振興 (ITR) 讓美國等多國拒絕 2013年 WTO 展開服務貿易協定 (TISA) 談判，包含電子商務條約 	<ul style="list-style-type: none"> 2018年法國總統馬克宏：呼籲建立包含所有利害關係人在內的新形態多邊合作，專家區強調新多邊主義 G7 - G20 - BRICS - NATO - WTO - ILO 等 intergovernmental 組織皆討論網路治理 2019年日地安供稱三：提議建立一個在 WTO 架構下的全球資訊治理新途徑
主權(中國)模式 Cyber sovereignty		<ul style="list-style-type: none"> 2010年《中國互聯網狀況》白皮書出現網路主權主張 2014年中國開始每年舉辦「世界互聯網大會」(海峽論壇)，宣傳主權模式 2015年習近平致詞：建立多邊...的國際網路治理體系 	<ul style="list-style-type: none"> 2017年中國實施新版《網路安全法》，為主權模式的代表作 2018年自由之家研究：中國連續4年為全球侵犯網路自由最嚴重國家，且積極對外出口數位威權主義，威脅全球網路的開放自由，並危及全球的民主原則 2019年專家：美國主張「美國第一」，和中俄等國皆聲稱主權的「新國家主權主義」

Q1：誰該負責移除網路上的不當內容？

- (1) 網路內容根本不應該被審查
- (2) 網路寬頻業者 (電信、ISPs)
- (3) 內容平台業者 (Google、FB 等)
- (4) 執法當局或法院
- (5) 不知道

圖4. 大專院校宣講內容簡介 2

3. 多方利害關係人模式典範：ICANN

- ICANN 執掌簡介
- ICANN 的多方利害關係人模式與社群
- ICANN 的政策發展流程、公眾意見徵詢與決策

ICANN

= Internet Corporation of Assigned Names and Numbers

Numbers
Internet Protocol
IP位址
電腦如何找到網站在網路上的位置

Names
Domain Names
網域名稱
人腦如何記憶網站

Unique Identifier

ICANN

= Internet Corporation of Assigned Names and Numbers

ICANN的工作：

- 管理 DNS (Domain Name System)
- 確保IP與DN相同且獨一無二

→ 當你輸入網址，電腦會幫你找到正確的網站

Coordinating with our partners, we help make the Internet work.

ICANN Multi-stakeholder Community

ICANN 員工，負責執行推動由 ICANN 社群制定之政策

負責就 ICANN 政策的技術面提出建議

4個諮詢委員會(AC)分別代表所屬團體，向 SOs 制定之政策提出建議

3個支援組織(SO)分別就權責範圍訂定相關政策

ICANN Policy Development Process

- ICANN 訂有複雜治理流程：各利害關係人團體不但參與 ICANN 決策，也監督並參與 ICANN 組織的營運規劃。
- ICANN 的多方利害關係人政策發展流程基本架構：

- GNSO 政策發展流程

圖5. 大專院校宣講內容簡介 3

4. 其他議題案例

- 韓國憲法法院宣布網路實名制違憲
- 法國判 Google 違反 GDPR (General Data Protection Regulation, 通用資料保護規範) 並重罰
- 美國陰謀論者 Alex Jones 頻道與發文遭 FB、YouTube 等網站刪除
- 金磚五國以國安為由擬另建獨立網際網路

5. 如何參與網路治理及結論

- 國內活動：網路治理研習營、TWIGF 年度論壇與其他會議活動
- 國際活動：APrIGF、IGF (可線上參與)、ICANN、APNIC 等國際相關會議與課程
- 網路之父 Dr. Vint Cerf 呼籲青年參與網路治理短片
- 參考資料：書籍、影片、文章

第三節 國立成功大學場次

一、活動訊息

- 系所：電腦與通訊工程研究所
- 場合：該所之定期專題研討會議
- 時間：108 年 5 月 2 日 (四) 13:30 ~ 15:30
- 地點：電機系繁城講堂
- 人數：183
- 講師：本計畫主持人陳文生執行長
(宣講內容請詳第二節簡介，或「附件一」之簡報資料)

二、現場交流 (Q&A)

1. 就老師的角色而言，要如何協助促進網路治理的觀念與參與？

老師可於課堂上宣傳網路治理相關觀念、談論生活上的相關議題，以協助與鼓勵學生了解網路治理，並產生更多興趣，進而參與政策討論。

2. 在網路上流傳的新聞有什麼管道可以釐清是否為假新聞呢？

Line 的謠言釐清官方帳號 MyGoPen (台語「麥擱騙」) 可以協助長輩和

有需要的朋友查證訊息，希望培養民眾警戒與查證的態度，而不是人云亦云地分享資訊，共同創造更乾淨的網路空間。

3. 在網路上如何平衡言論自由與假新聞？

這是最近大家都很關心的議題，需先定義何謂假新聞，每個人的定義可能都不一樣，先釐清此點才能避免影響言論自由。

三、活動剪影



圖6. 成功大學宣講照片

第四節 國立政治大學場次

一、活動訊息

- 系所：行政管理碩士學程（在職專班）
- 場合：公共管理課程
- 時間：108年5月4日（六）13:30～16:15
- 地點：綜合院館南棟一樓 270113 教室
- 人數：33
- 講師：本計畫研究員梁理旋副執行長
(宣講內容請詳第二節簡介，或「附件一」之簡報資料)

二、現場交流 (Q&A)

1. ICANN 的政策決策時間有多久？

沒有一定的時間標準，例如 GDPR 已經開始實施，為了因應新法規，ICANN 相關政策的調整只花一年，但是對於城市是否可以作為頂級域名的決策，則大約耗費十年。概括來看，平均約三到五年。

2. 如果各國都在基礎層與邏輯層建立網路，是否就能擁有各自獨立網路？

全球網際網路已先存在，然後一些國家才想獨立。以俄羅斯來說，因為擔心.ru 網路被美國從全球的根伺服器刪除，同時也為了監控網路封包，因此要自建網路。但當中還涉及複雜的技術問題，且目前看來是難以克服。

3. 針對假新聞，通傳會是否會仿效德、法等國，以立法處罰平臺業者？

目前政府對假新聞的抑制和懲處，主要是透過修改並落實既有法規，

並未傳出將仿效德法等國針對網路平臺祭出立法懲處。例如通傳會提出於《廣播電視法》修正草案增訂事實查證原則，且依據既有《衛星廣播電視法》的違反公序良俗、事實查證等條文，於2019年3月對中天電視的「市長合體天降祥雲」、「抹黑新加坡外交官」2則新聞開罰共100萬元。

4. 政府要如何遏止社群平臺和自媒體的假訊息，同時維護言論自由？

民主國家如法國是針對特定敏感時期，如選舉期間做管制。而對美國這種多元文化、種族的國家來說，要定義假新聞特別困難，也因此難以擬定相關解決方案。我國也是一樣，有些人對於中天被罰不以為然，有些人覺得是天經地義，所以，單是假新聞的定義就有很大的分歧。而常被提及的因應方式包括提升公民數位素養、支持高品質的新聞媒體、成立事實查核單位等。臺灣也有事實查核中心，但也不能過度倚賴單一的因應方式。

5. 網路的中介機構、平臺業者是否合適擔任守門員的角色？

平臺業者是以利益為導向，如果政府立法規定平臺業者要做假消息的控管且訂有罰則，業者的審查標準有可能會比政府更加嚴格。

三、活動剪影



圖7. 政治大學宣講照片

第五節 世新大學場次

一、活動訊息

- 系所：資訊傳播學系 (所)
- 場合：系 (所) 週會
- 時間：108 年 6 月 12 日 (三) 13:00 ~ 15:00
- 地點：大禮堂 A201 良彥講堂
- 人數：210
- 講師：本計畫主持人陳文生執行長
(宣講內容請詳第二節簡介，或「附件一」之簡報資料)

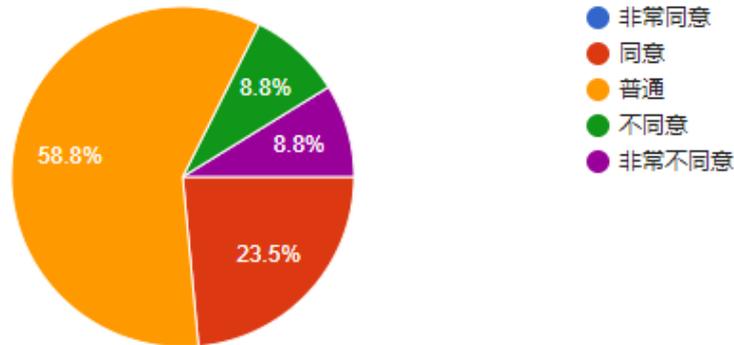
二、現場交流 (Q&A)

本場宣講活動的現場交流以透過 Google 表單投票功能進行。惟可能礙於當下來不及輸入網址等原因，最後僅有 34 人參與投票。投票結果摘錄如下，各題票數統計如圖 8 所示。

- 24% 同學願意提供個資以換取免費服務，比例高於不同意的 18%。
- 同學認為應該負責移除網路不當內容的，主要是內容業者 (85%) 與政府 (68%)。
- 50% 同學認為科技公司不應該配合打擊犯罪要求而在產品植入後門程式，認為應該的只有 15%。
- 同學認為應該為中勒索軟體病毒負責的，主要是軟體業者 (65%)、網路使用者 (53%)，和政府 (44%)。
- 50% 同學認為不應該讓 Uber 消失，認為應該消失的只有 9%。

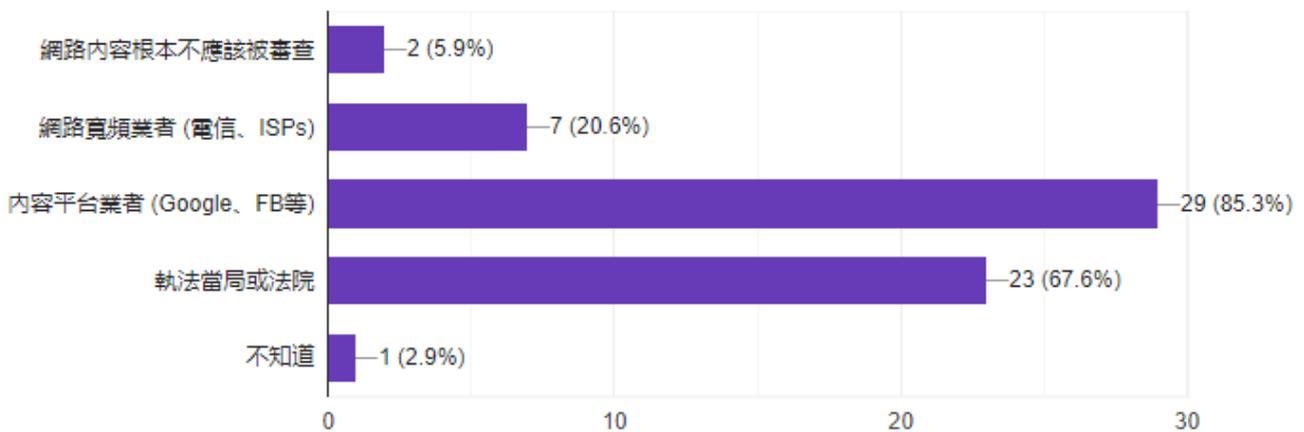
1. 你同意提供個人資料來換取免費網路服務之使用嗎(單選)?

34 則回應



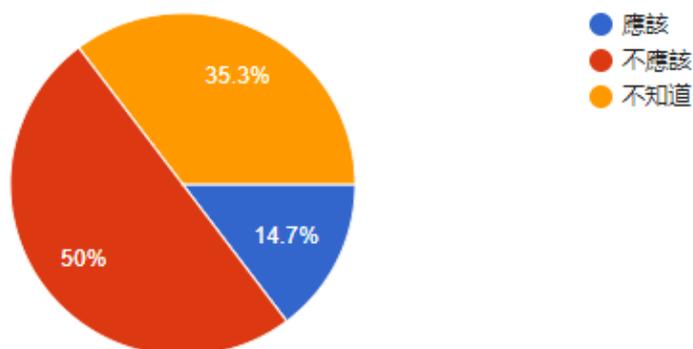
2. 誰該負責移除網路上的不當內容(多選)?

34 則回應

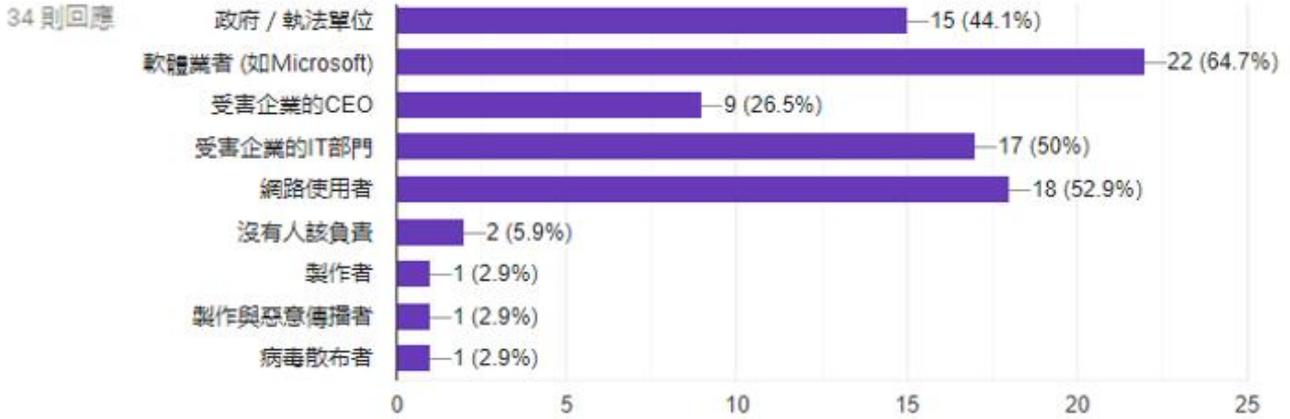


3. 科技公司應該配合執法當局打擊犯罪要求而在產品植入後門程式嗎(單選)?

34 則回應



4. 誰該為勒索軟體病毒(如WannaCry)而負責(多選)?



5. 您認為在台灣Uber應該被禁止而消失嗎?

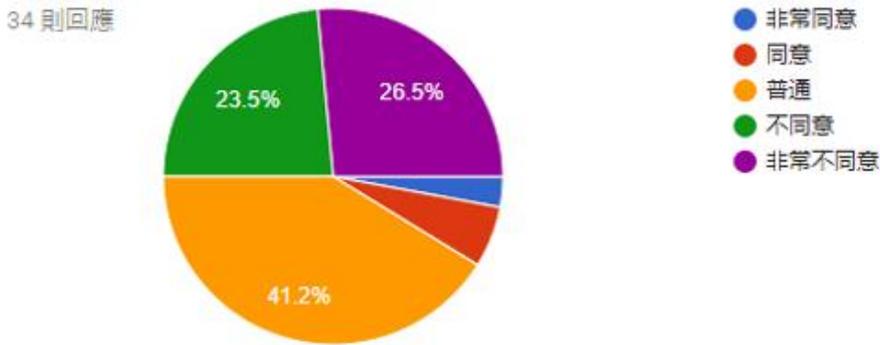


圖8. 世新大學宣講網路投票結果

三、活動剪影



圖9. 世新大學宣講照片

第六節 東海大學場次

一、活動訊息

- 系所：資訊管理所
- 場合：專題討論課程
- 時間：108年9月26日(四) 14:10~16:10
- 地點：管理學院 M243 教室
- 人數：31
- 講師：本計畫研究員梁理旋副執行長

(宣講內容請詳第二節簡介，或「附件一」之簡報資料)

二、現場交流 (Q&A)

本次宣講活動因剩餘時間不足，僅提供 1 位同學提問，其問題為是否有合適議題可做為碩士論文的主題。惟此課程教師認為同學應該自行探討論文題目，而非詢問本次講者。

三、活動剪影



圖10. 東海大學宣講照片

第七節 國立高雄科技大學場次

一、活動訊息

- 系所：資訊管理系
- 場合：企業資訊網路課程（大三）
- 時間：108年9月30日（一）13:30~16:20
- 地點：財金學院大樓地下1樓E006教室
- 人數：51
- 講師：本計畫主持人陳文生執行長

（宣講內容請詳第二節簡介，或「附件一」之簡報資料）

二、現場交流 (Q&A)

1. 是否有系統可以判定網路假訊息、假新聞？

雖然可以利用軟體機器人去判斷假訊息，但仍會發生錯誤，因此，需要第二道的人工審核程序。以 Facebook 為例，它在全球約有一至二萬人從事人工判別審核的工作。

2. 線上意見調查

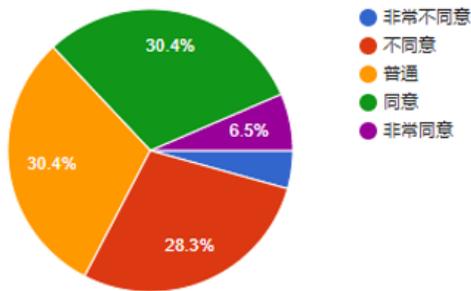
本次活動並透過 Google 表單投票功能進行線上意見調查，共有 46 位 (90%) 同學踴躍參與。投票結果摘錄如下，各題票數統計如圖 11 所示。

- 37% 同學願意提供個資以換取免費服務，比例高於不同意的 33%。
- 同學認為應該負責移除網路不當內容的，主要是內容業者 (78%) 與政府 (52%)。
- 22% 同學認為科技公司不應該配合打擊犯罪要求而在產品植入後門程式，認為應該的只有 6.5%。

- 同學認為應該為中勒索軟體病毒負責的，主要是軟體業者和網路使用者，比例皆為 62%；其次為政府和受害企業的 IT 部門，皆為 44%。
- 74% 同學認為不應該讓 Uber 消失，認為應該消失的只有 4%。

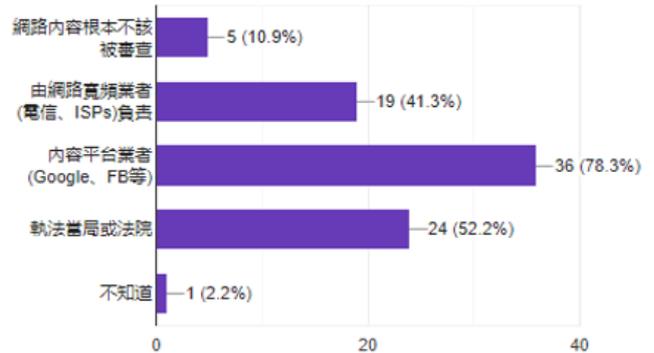
1. 你同意提供個人資料來換取免費網路服務之使用嗎(單選)?

46 則回應



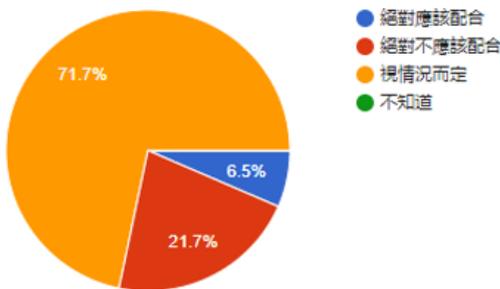
2. 誰該負責審查及移除網路上的不當內容(多選)?

46 則回應



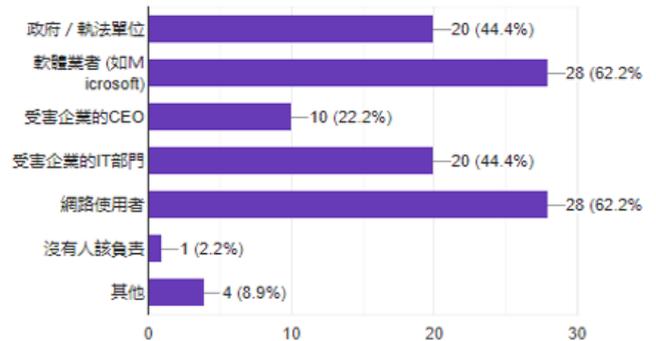
3. 科技公司應該配合執法當局打擊犯罪要求而在產品植入後門程式嗎(單選)?

46 則回應



4. 誰該為中勒索軟體病毒(如WannaCry)而負責(多選)?

45 則回應



5. 您認為在台灣Uber應該被禁止而消失嗎(單選)?

46 則回應

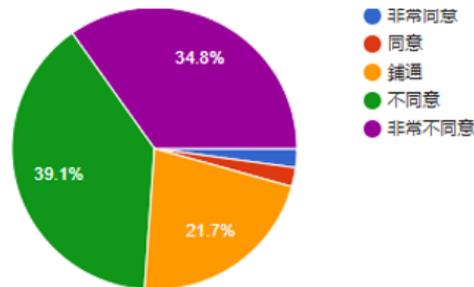


圖 11. 國立高雄科技大學宣講網路投票結果

三、活動剪影



圖12. 國立高雄科技大學宣講照片

第八節 靜宜大學場次

一、活動訊息

- 系所：資訊管理學系
- 場合：資管生涯講座 (大四)
- 時間：108 年 10 月 21 日 (一) 13:00 ~ 15:00
- 地點：資訊大樓 115 教室 80
- 人數：80
- 講師：本計畫研究員梁理旋副執行長

(宣講內容請詳第二節簡介，或「附件一」之簡報資料)

二、現場交流 (Q&A)

1. 個人參與網路治理的方式除了研習營與 ICANN 外，還有什麼其他管道？

最簡單的，就是參加臺灣網路治理論壇 (TWIGF)，除了每年舉辦年度大型會議外，平時也不定期辦理主題演講活動，而且還有 FB 社團提供全球網路治理相關政策的資訊。而網路治理研習營主要是提供 2 天的授課與演練課程，並選拔優秀學員參加國際網路治理會議。

2. 請問 NII 協進會的工作內容？

略 (本問題與網路治理無關)。

三、活動剪影



圖13. 靜宜大學宣講照片

第三章 人才培訓課程

第一節 活動內容

一、活動簡介

網路引領我們邁向智慧化生活的數位時代，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。

「2019 網路治理研習營」為兩天一夜的免費人才培訓活動。透過課堂講習與模擬演練，帶您認識網路安全、人權、數位經濟、新興科技、網路內容等重要議題，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 2019 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：2019 網路治理研習營
- 時間：108 年 5 月 31 日（五）至 6 月 1 日（六）
- 地點：IEAT（台北市進出口商業同業公會）會議中心 3F 第 2 會議室（臺北市中山區松江路 350 號）

二、課程簡介

本年度研習營課程共計 2 天，包含自我預習（0.5 天）、入門（0.5 天）、進階（1 天）三種課程，且皆屬必修；上課型式包括課堂講習暨問答，以及分組演練；課程主題涵蓋網路政策模式、重要法規、人權、安全、經濟、新興科技、基礎建設、媒體內容等。課程表如表 5 所示。

表5. 研習營課程表

入門課程		課前自我預習
2 小時 (影片)	1. 網路治理發展史 / 吳國龍(維)顧問 2. The History of Internet Governance / Wolfgang Kleinwächter 教授	
2 小時 (文章)	1. What is... internet governance? / IGF 2019 2. About IGF FAQs (10 個) / IGF 3. Vint Cerf: The father of the Internet reflects on what his creation has become / Noted 報導	
入門課程		5 月 31 日 (五)
13:30 - 14:00	報到	
14:00 - 14:30	開幕致詞 & 學員自我介紹	
14:30 - 15:30	自我預習課程討論	
15:30 - 15:50	休息	
15:50 - 17:20	演講 (1)：認識網路治理 網路治理與政策模式 當前網路治理重要法規 數位匯流下的言論管制	
進階課程		6 月 1 日 (六)
09:00 - 09:10	報到	
09:10 - 10:40	演講 (2)：網路治理的挑戰 網路人權 網路安全 經濟與新興科技	
10:40 - 11:00	休息	
11:00 - 12:00	演講 (3)：網路治理的挑戰 網路基礎建設 媒體與內容	
12:00 - 13:00	午餐	
13:00 - 13:40	分組演練 (上)：訂定主題	
13:40 - 15:10	分組演練 (中)：角色扮演	
15:10 - 15:30	休息	
15:30 - 16:00	分組演練 (下)：成果報告	
16:00 - 16:30	參與分享 & 未來機會	
16:30 - 17:00	結業 & 交流	

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、學術界等國內相關領域專家共 9 位擔任講師，同時也請上屆優秀學員回來分享參與經驗。講師群依姓氏筆畫簡介如下：



吳國龍(維)
NII 產業發展協進會 顧問

經歷

中華電信股份有限公司董事 (現任)
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)
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



周宇修
台灣人權促進會 會長

經歷

聯誠國際法律事務所律師 (現任)
民間司法改革基金會常務執行委員 (現任)
臺北市政府國家賠償委員會審議委員 (現任)
中華民國律師公會全國聯合會司法革新委員會、財經法委員會、消保法委員會委員
哥倫比亞法學院訪問學人
公益法律全球研究網成員
月旦法學雜誌企畫主編、憲政時代執行主輯
國際特赦組織台灣分會理事

專長

競爭法、行政救濟法
傳播媒體法
勞工、企業社會責任等法治議題



林克容
台灣網路資訊中心 (TWNIC) 網安組資深工程師

經歷

資策會資安所組長
數位聯合電信 (Seednet) 協理

專長

專案管理
資訊安全管理
應用系統規劃



邱文聰
中央研究院法律學研究所 副研究員

經歷

國立台灣大學國家發展研究所副教授（現任）
台灣人權促進會執行委員（現任）

專長

資訊隱私、憲法隱私權
醫學倫理（基因倫理）法律



胡元輝
中正大學傳播系 教授

經歷

台灣事實查核中心委員（現任）
優質新聞發展協會理事長（現任）
卓越新聞獎基金會董事長
公視基金會、台視總經理
中央通訊社、自立晚報社長
TVBS電視台新聞部總編輯

專長

傳播經營與管理
公共媒體與公民媒體
新聞製播與採寫



陳文生
NII產業發展協進會 執行長

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）
教育部電算中心組長、副主任等
高雄第一科技大學計算機中心主任、圖書館館長、資管系主任（所長）、教務長等
台灣網路資訊中心（TWNIC）執行長
中國科技大學資訊學院院長

專長

網際網路應用與管理
軟體專案管理
資訊安全
網路治理
資訊管理



曾更瑩
理律法律事務所 合夥律師

經歷

TWNIC國際事務委員會委員（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）
經濟部商品標示審議委員會委員

專長

電信、電子商務
網路法律
個人資料及隱私權保護



黃勝雄
台灣網路資訊中心 (TWNIC) 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)
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



熊全迪
理律法律事務所 初級合夥人

經歷

證券櫃檯買賣中心
台灣金融科技協會會員

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

圖14. 研習營講師簡介

第二節 活動辦法

一、報名資格、時間與方式

1. 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)

2. 報名時間

自即日起至 2019 年 5 月 12 日 23:59 截止 (臺灣時間)。

3. 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，並回覆以下問題：

- 請說明為什麼想參加本研習營。
- 請說明最關心的網路議題為何與為什麼。
- 請說明網路議題相關事務或活動 (社群/社團/會議等) 參與經驗。
- 其他補充說明，如英文能力證明、自我介紹短片 (請提供 YouTube 連結) 等。

二、評選與錄取

1. 評選標準

主辦單位將組成評選小組，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、英文程度等其他項目，進行綜合評估。

2. 錄取名額

本研習營預計招收 40 名學員。

3. 結果公布與通知

評選結果將於 2019 年 5 月 20 日(一) 於本活動網站公布，並以 E-mail 個別通知錄取學員。

三、學員義務

1. 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」，或「監護人(家長)同意書暨出席保證書」(未滿 20 歲者)，並於 2019 年 5 月 22 日 (三) email 主辦單位。表單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。
- 完成自我預習課程 (4 小時)：請詳學習資源。

2. 研習營期間

- 全程出席，並積極參與討論。
- 注意自身安全，並遵守主辦單位活動規範。

四、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。

1. 交通補助

- 限 5/30 ~ 6/2 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。
- 須檢附來回車票票根。

2. 住宿補助

- 住宿費限 5/31~6/1 單日住宿，補助上限為新臺幣 1,600 元整，憑收據核銷。
- 住宿同時補助雜費新臺幣 400 元整，此項目不須檢附憑據。

五、學員獎勵

1. 結業證書 & 獎學金

全程參與研習營的學員可獲頒結業證書，及新臺幣\$2,000 元獎學金。

2. TWIGF 特派員獎學金

結業學員可申請擔任 TWIGF 特派員，提供 2 場座談記錄摘要（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。

3. 參與國際會議（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 2019 APrIGF (7 月 16 日~19 日，於海參崴舉辦)，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。

第三節 活動網站與宣傳

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。



活動內容

「2019網路治理研習營」為兩天一夜的免費人才培訓活動。透過課堂講習與模擬演練，帶您認識網路安全、人權、數

最新消息

- [研習營課程錄影檔上線](#)
2019-07-12
- [2019網路治理研習營公布TWIGF特](#)

交通資訊

本研習營訂於IEAT會議中心舉辦，會場鄰近民權東路的行天宮，公車與捷運皆可到達。詳細資訊請見網頁說明。

圖15. 研習營活動網站

二、活動宣傳

本年度研習營的活動宣傳管道包括網路治理相關組織的官網與臉書社團、公務系統，以及本計畫的大專院校宣講活動。

1. 網路治理相關組織的官網與臉書社團

- TWIGF、台灣網路青年論壇、Taiwan GPS 海外人才經驗分享及國際連結計畫之臉書社團。
- TWNIC (台灣網路資訊中心) Blog。
- 網路治理議題支援平臺。



台灣網路治理論壇 (Taiwan IGF)
社團 · 2017年8月加入
台北市 · 台灣

由NII產業發展協進會主辦的「網路治理研習營」，活動報名已進入倒數三天的時間囉(截止日期為5月12日23:59)！今年的研習營在IEAT (台北市進出口商業同業公會)會議中心舉辦，日期為5月31日下午和6月1日，活動為免費參加，全程參與的學員除了獲得結業證書和獎學金之外，今年另新增TWIGF特派員獎學金，並選出一名優秀學員參加今年的APriGF，請大家把握機會，踴躍報名參加！
詳細活動內容與辦法請見官網說明。
<https://www.igcamp.tw/>



2019 網路治理研習營
5/31 (五) - 6/1 (六) | 台北市IEAT會議中心
線上報名

安全 人權 隱私 經濟 新聞



網路治理議題支援平臺
Internet Governance @ TW

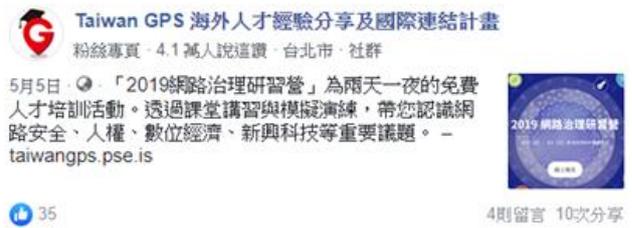


2019 網路治理研習營
線上報名

安全 人權 隱私 經濟 新聞

📅 2019-05-31 13:30 ~ 2019-06-01 17:00

2019年網路治理研習營 (報名截止時間為5月12日23:59)

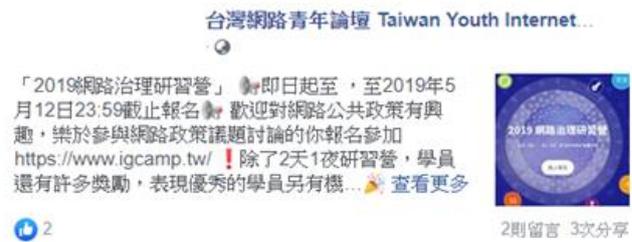


Taiwan GPS 海外人才經驗分享及國際連結計畫
粉絲專頁 · 4.1 萬人說這讚 · 台北市 · 社群

5月5日 · 🌐 · 「2019網路治理研習營」為兩天一夜的免費人才培訓活動。透過課堂講習與模擬演練，帶您認識網路安全、人權、數位經濟、新興科技等重要議題。 - taiwangps.pse.is

👍 35

4則留言 10次分享



台灣網路青年論壇 Taiwan Youth Internet...

「2019網路治理研習營」即日起，至2019年5月12日23:59截止報名，歡迎對網路公共政策有興趣，樂於參與網路政策議題討論的你報名參加 <https://www.igcamp.tw/>！除了2天1夜研習營，學員還有許多獎勵，表現優秀的學員另有機... 查看更多

👍 2

2則留言 3次分享



悠遊寰宇。在地識別
網路服務與技術的溝通交流平台

tw/台灣

活動訊息
**「2019 網路治理研習營」
開放報名!**



2019 網路治理研習營
線上報名

安全 人權 隱私 經濟 新聞

圖16. 研習營宣傳截圖 (官網與 FB 社團)

2. 公務系統

- 通傳會協助本計畫行文至交通部、經濟部、科技部等相關部會，及台灣網際網路協會、台灣電信產業發展協會等公協會，邀請報名及轉知。
- 通傳會並協請教育部發文轉知所屬大專院校。



圖17. 研習營宣傳截圖 (大專院校網站)

3. 本計畫大專院校宣講活動

- 搭配本計畫之大專院校宣講活動，於介紹「如何參與網路治理」時，一併宣傳研習營活動。

第四節 學員評選與錄取

一、報名與評選

本次研習營活動共 81 人報名，扣除 9 人資料填寫不齊，計有 72 人合格報名。又當中有 6 人為政府單位保留名額，因此，最後須經由評選的有 66 人，預計從中選出 34 人，加上政府單位保留名額，共計錄取 40 位學員。

本次評選作業由本計畫 2 位成員及來自學界與公民團體的 3 位外部專家，組成 5 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。評選採兩階段作業，進行方式如下說明：

- 個別評分：每位評審委員從 66 位合格報名者中，選出 34 位推薦者。獲得 1 位評審委員推薦即得 1 分，最高為 5 分。評分結果得分統計如下圖 18 所示。
- 評選會議：評審委員針對第一階段得分結果進行討論與調整，並依最後得分排序，選出 34 名正取學員與 20 名備取學員。

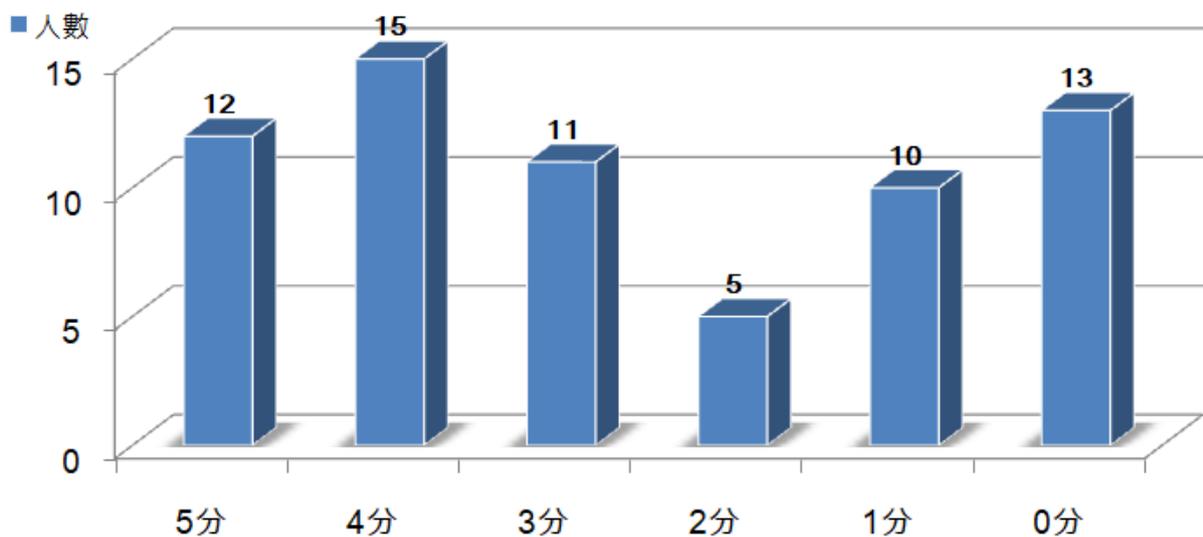


圖18. 研習營合格報名者的得分統計

二、學員組成概況及參與情況

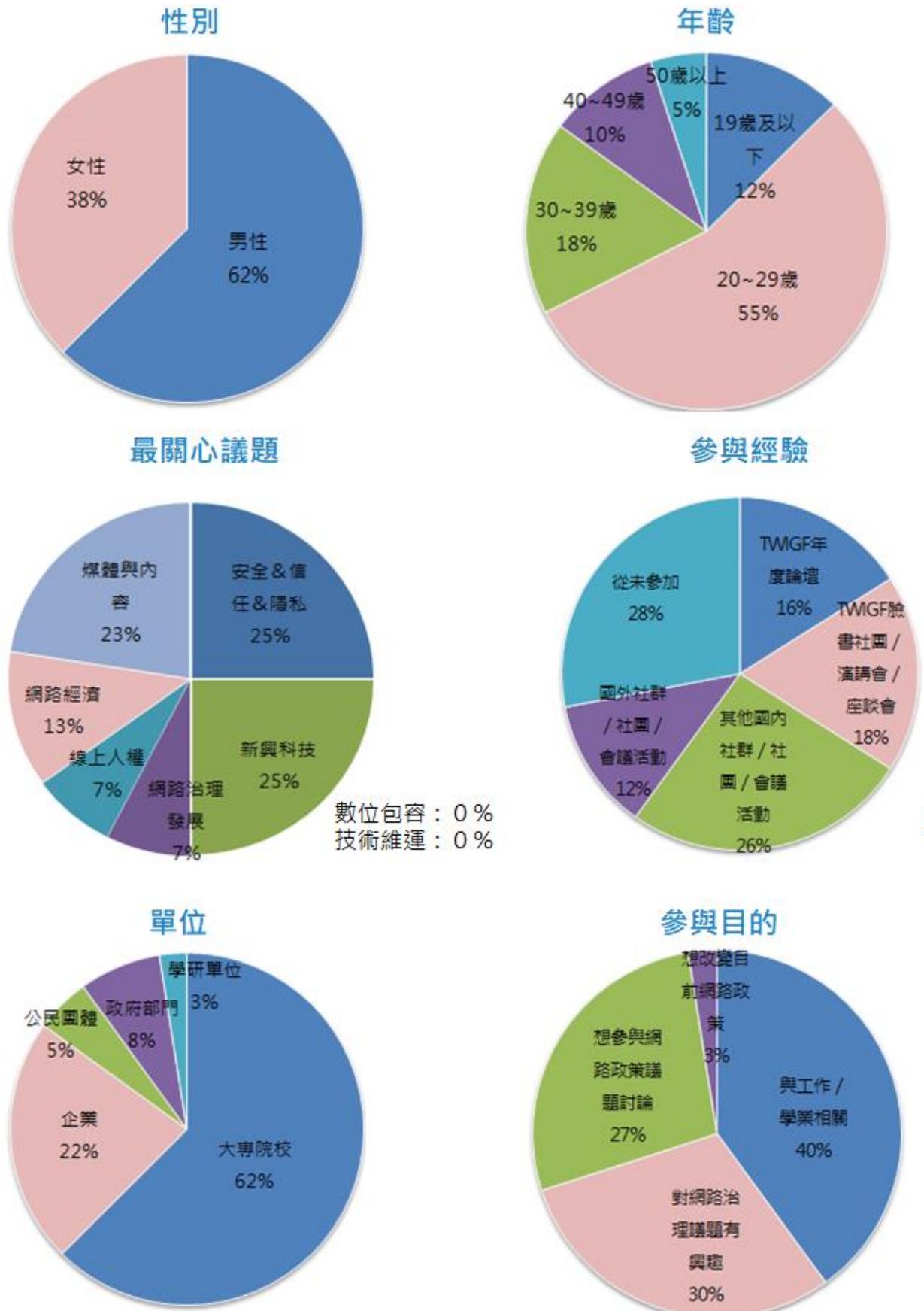


圖19. 研習營學員組成概況

上圖 19 為本年度 40 位學員的組成概況。經通知聯繫正備取學員後，本年度學員包含 25 位大專青年 (62%)、3 位公務人員 (8%)，以及 12 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學院，且有 3 位在海外就學；社會人士學員也有多位來自國內知名企業 (半導體、電信、資安等)。對應至年齡層，亦以 20~29 歲年輕人居多 (55%)。性別比例大致為男性 6 成，女性 4 成。參與經驗則是超過 7 成學員都曾參加網路治理相關會議或社群。參與目的以工作和學業相關為主 (40%)。至於最關心的網路治理議題，主要有安全與隱私 (25%)、新興科技 (25%)，以及媒體與內容 (23%)。

本年度 2 天研習課程所有學員皆全程出席，並獲頒結業證書與獎學金 (公務人員除外)，而且在課程中也相當積極地提問及參與演練課程的討論。

第五節 課程內容摘要

一、專題講習

1. 網路治理與政策模式

(1) 演講摘要

講者：黃勝雄／台灣網路資訊中心 (TWNIC) 執行長

(本場全程以英文進行，簡報資料詳「附件二」；錄影檔請至研習營活動網站「學習資源」igcamp.tw/resources/)

網路發展的重點已從 20~30 年前的基礎建設、10 多年前的網路技術創新和社群媒體的出現，邁向未來 10 年的政策規範制定及網路治理。網路治理的定義可從狹隘的技術層面 (IP 位址的分配、域名註冊、DNS 根區管理) 延伸到生活中的每個面向 (基礎建設和能力建構、電信法規、普及、隱私和言論自由、智慧財產權、網路犯罪、國家安全等)。

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所管理。20 年前的情況為網路架構改變市場和法律，一旦決定技術和架構，便可找出網路空間的行為模式，也就是用網路標準來管理網路空間的一切行為，因此有「程式即法律」(Code is Law) 的說法。而今出現「法律即 (市場) 規則」(Law is Code) 的範例，如去年歐盟實施 GDPR，改變了市場行為 (所有產品須符合 GDPR 規範)，顯示法律可以引領網路發展。另外，規範也可以改變結構和市場，例如 MANRS (Mutually Agreed Norms for Routing Security，路由安全共同協議規範) 是由業界發起的安全自我管制規範，業者自願承諾遵守 MANRS 基本措施，以維護路由安全。

當處理網路安全問題時，單一組織可採用國際標準 (如 ISO 270001)；若發生在國內，便可使用該國司法；若牽涉到其他國家，則可使用國際協議；而當國際協議不足以解決問題時，就可嘗試從網路治理尋求解方。

(2) Q&A

- 臺灣的網路規範是否較美國限制更多？

各國網路規範的程度不一，單就網路安全規範來看，臺灣今年初已正式實施《資通安全管理法》，但是網路安全不能只靠一種規範來維護，如《個人資料保護法》也間接與網路安全相關。

- 國際上如何處理網路相關法律問題？對於破壞法律的國家是否有處罰？

以網路安全來說，少有國際協議去規範國際間的問題，大多是由民間企業所發起和推動的相關規範，如前述的 MANRS。

2. 當前網路治理重要法規

(1) 演講摘要

講者：曾更瑩／理律法律事務所合夥律師

(簡報資料詳「附件二」；錄影檔請至研習營活動網站「學習資源」
igcamp.tw/resources/)

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，法律已成為現今網路世界中最重要之驅動力。由於網路科技發展迅速，當代社會中的網路相關法條，通常是跟在議題之後展開討論，進而著手訂定管制方式。如果我們將目前常見的網路議題與相關法條配對，可以歸納如下：

- 網路基礎建設相關：電信法、資通訊安全法
- 內容相關：言論自由、智慧財產權、兒少保護、通訊監察
- 經營管制相關：執照、廣告、公平交易、消費者保護、跨境電商
- 其他相關基本法律：隱私權保護、民法、刑法、司法管轄權等

綜觀網路治理相關法規的國際發展趨勢，以個資法為例，歐盟 GDPR 自 2018 年實施至今剛滿一年，各國政府、跨國企業、公民社會等有些額手稱慶，有些埋怨不滿；許多國家或地區更準備著手制定或修改相關法規。另一方面，近來歐美政府試圖管制跨國網路巨頭時，皆選擇以競爭法來處理，因此，未來各國的公平交易委員會可能成為網路最大的主管機關。還有，隨著網路管轄日益地變成有國界，政府也開始將實體產業的行業管制套用在網路產業上，如管理 Uber、Airbnb 和 OTT 等。這些議題未來如何發展值得持續關注。

(2) Q&A

- 在嚴格與放鬆管制之間，臺灣的網路相關法規應朝哪個方向發展？

比起由律師、法官等人或政府單方面決定，應廣納多方利害關係人團體意見，經充分且深入討論未來發展方向且達成共識後，才能開始制定相關法律。

- 政府擁有人民許多個資，如果因網路攻擊而導致個資外洩，人民是否能

向政府求償？

公務或非公務機關都有保護個資安全的義務，若違反此義務造成個資當事人的損害，必須負起賠償責任。因此，除非是天災或意外，否則人民可以向政府求償。

- 智慧手環蒐集使用者的生理數據，公司若拿這些數據做匿名運用，是否違反個資法？

要視公司與個資當事人所簽署的合約內容而定，如果超出當時預設的資料蒐集目的與使用範圍，則違反個資法。

3. 數位匯流下的言論管制

(1) 演講摘要

講者：周宇修／台灣人權促進會會長

(錄影檔請至研習營活動網站「學習資源」igcamp.tw/resources/)

從大法官釋憲的角度來看，憲法第 11 條所保障的「自由」一直在蛻變，因為法律並非一成不變，而是會隨著科技發展和社會變化衍生出不同內涵。司法院釋字第 613 號解釋即指出，言論自由還包括通訊和傳播的自由，除了廣播、電視，還有透過其他通訊傳播設施取得資訊和發表言論的自由。不過，司法院釋字第 678 號解釋也表示，目前法律只處理到無線電波的部分，尚未管制到網路，若真要管制網路，必須考量管制的方式、其必要性和正當性，以及管制後的效果。

過去不同媒體使用不同的技術傳輸，因此，管制者制定不同法規進行分類管制。但在數位匯流時代中，過往的分類已失去意義，同一市場的不同技術受到不同法律規範，導致競爭上產生問題。例如：科技業跨足金融業成為所謂的 FinTech (金融科技)，是否應受同樣的《銀行法》管制，值得探討。而有待探討的議題還有很多，以《數位通訊傳播法》(草案)為例，第 5 條規定通訊傳播業者應依法配合國安、資安等相關事項。雖然管制並非

永遠是負面的，但是必須考量管制產生的外溢效應。

此外，數位匯流時代還需關注傳播媒體演變對民主政治的威脅。數位匯流打破原先不同的傳播媒體市場，導致經營業務日漸重疊，開啟跨媒體競爭與新一波媒體產權集中的可能性。雖然現行的廣電法規對於廣電事業的所有權移轉有所管制，但管制密度在民營化下逐漸寬鬆，一旦單一媒體集團藉由不同的媒體大量傳布特定資訊，將會對言論自由造成負面影響，甚至破壞民主社會的多元價值形成機制。

(2) Q&A

- 媒體是否有傳遞正確資訊的責任？又如果未善盡責任該如何監管？

人民有接受資訊的自由，政府若要保證人民接收資訊的正確性，過程中會進行資訊過濾，形成所謂的審查。但這並不表示不要管制假新聞，假新聞一直都存在，審查機制會不會有外溢效果，政策上必須評估正反面。

- 政府從控管到開放媒體，過程中是否可能有他國政府的介入？是否要增加某部分的限制？

全球化下很難避免這個情形，重點應是在於如何建立自我認同，境外人士灌輸的想法不見得要全盤收受，必須找到自我中心思想。

4. 網路治理的挑戰：網路人權

(1) 演講摘要

講者：邱文聰／中央研究院法律學研究所副研究員

當前網路人權的兩大挑戰為言論自由與資訊隱私。古典自由主義主張言論是自由競爭的市場，只要市場上有充足的言論，閱聽人就會自行判斷真假，因此，言論自由的保障範圍是越多越好，任何會引發寒蟬效應的行為，都屬侵害言論自由。而此主張是建立在社會中有中介團體擔任資訊守門員角色（如傳統的傳播媒體和政黨）的假設之上。

然而，今非昔比。網路時代言論的生產和傳遞成本都大幅降低，以致資訊充斥；而傳統中介團體的角色又式微，尤其臺灣媒體自我墮落，政黨功能亦不彰；加上注意力產業（attention industry）興起，業者會依使用者喜好而投放資訊，產生同溫層現象，並衍生洗版帶風向、轉移焦點、批判審查等問題。所以，社群媒體時代的言論市場已經失靈，言論本身竟然弔詭地變成緊縮言論的工具。

面對這項挑戰可以採用的法律工具應是類似《公平交易法》，雖然言論市場要仿效商品市場進行管制的難度很高，但至少要先打破「言論自由至高無上」想法，切記保障言論自由的前提是公平的言論市場。

而在資訊隱私方面，網路時代我們有大量的資訊被蒐集處理和利用，政府和產業界主張資料去識別化，即保障「機密性」，但其實沒有真正去識別化的方法，零散資訊仍然可以被重組成完整的個人檔案。另一方面，我們需要的隱私也不僅只是「機密性」，還需要有「自主權」，這也是為什麼公廁偷拍即使沒有拍到臉部仍被視為侵犯隱私的原因。然而，「自主權」也不是至高無上，當資料的利用有重大正當公益性時，如發生新型嚴重傳染疾病需要做資料分析以控制疫情，政府就可以直接使用；但一般研究則是要事前取得當事人的同意；只是每次都要事前取得同意可能導致研究無法進行，因此，有些國家正評估採用「預設同意但提供退出機制」的作法，以兼顧「自主權」和使用需求。

不過，也有很多人自願在社群媒體公布生活點滴，他們在「自主權」下自願放棄「機密性」看似沒問題。同樣地，一個全民同意被政府監控的國家似乎也符合「自主權」的要求，但這涉及「資訊隱私的價值」或稱為「隱私的品味」，會導致喪失獨立人格並破壞社會團結，而這兩者正是民主社會得以存在的要素。

(2) Q&A

- 如何培養辨別資訊真假的能力？能否推薦可信的媒體？

不要倚賴社群媒體而活，要有尋求更多資訊來源（如轉往中介媒體）的自我意識。不過，不敢推薦值得社會信賴的中介媒體。

- 對於 AI 的資料分享權，目前無相關立法，是否有建議措施？

我國個資法有很多需要改進的地方。資料的控制者不宜主張只要加密或去識別化後，資料不須經當事人同意即可分享利用。

5. 網路治理的挑戰：網路安全

(1) 演講摘要

講者：林克容／台灣網路資訊中心 (TWNIC) 網安組資深工程師

根據世界經濟論壇 (WEF) 2018 年全球風險認知調查，在科技方面，受訪者最擔憂的是資料詐欺及網路攻擊。2018 年發生的幾起大宗資安事件，一方面激發大眾對個資保護的重視，一方面也讓國家政府徹底體認關鍵基礎建設受網路攻擊的巨大風險，進而著手加強國家的安全防護體系。

而面對物聯網、關鍵資訊基礎建設、供應鏈、APT (Advanced Persistent Threat, 進階持續性滲透威脅)、DDoS (Distributed Denial of Service, 分散式服務阻斷攻擊) 等各種資安攻擊，最重要的就是做好資安防護。當中「人為因素」是資安防護的重要關鍵，因為資安漏洞的原因通常是使用者疏失；反之，使用者健全的資安素養，也是防堵資安漏洞、加強資安防護的關鍵因素。

資安防護也有若干多方利害關係人合作案例，如臺灣電腦網路危機處理暨協調中心 (Taiwan Computer Emergency Response Team & Coordination Center, TWCERT/CC) 參與的資安跨域聯防及情資分享。TWCERT 與國內各業界的 CERT 以及國際資安組織密切合作，透過多方情資互享與即時通報，建立跨國的資安聯防情報網路。

另一個案例是手機應用程式的資安防護。臺灣每年超過 4 千臺手機遭

駭，都是駭客透過應用程式入侵使用者的行動裝置。為了保護民眾，政府在諮詢多方利害關係人專家後，訂定應用程式的檢測標準，並設置實驗室進行檢測。不過，由於檢測成本遠高於開發成本，加上應用程式更新的速度太快，目前國內在行動裝置的資安防護上，尚未見到顯著成效。

(2) Q&A

- 目前臺灣需要提升的資安有哪些？

資安是全面向，只提升單一向恐不足以解決問題，因此，增加資安專業人才、導入資安標準和後續管理、加強資安技術等，都需要同步進行。

- 為什麼臺灣是惡意軟體很好的試驗場所？

因為臺灣的網路普及率很高，可從很多面向進行攻擊，測試不同的攻擊手法。

6. 網路治理的挑戰：經濟與新興科技

(1) 演講摘要

講者：熊全迪／理律法律事務所初級合夥人

(簡報資料詳「附件二」)

當新興科技運用到社會上，變成人類活動的一部分，即會產生治理或法律問題。目前新興科技與網路經濟的主要治理議題有下列幾項：

① 共享經濟

Uber所引起的爭議是行業執照取得的問題，交通部認為Uber是汽車運輸業而非資訊服務業，需申請執照才能營業，於是Uber暫時退出臺灣，改為和汽車租賃業者合作後才重回市場，但是交通部又透過修法封殺Uber現有制度。同樣的，Airbnb平臺下的民宿業者，也因未獲得營業執照即經營觀光旅館業務，而違反《發展觀光條例》；此外，Airbnb也未能查證房源是否合法。

② 人工智慧 (AI)

目前 AI 仍被視為一種工具，但也不排除隨著技術發展，未來 AI 可能像人類一樣會思考。近來 AI 的治理議題例如：肇事的責任歸屬、發明物品是否擁有著作權與專利權、所做的決定是否有歧視、如何解決道德和隱私問題等。

③ 區塊鏈

區塊鏈有分散式帳本技術 (distributed ledger technology)、去中心化，以及不可竄改的特徵。當前最主要的運用為虛擬貨幣，相關的治理議題集中在個資隱私保護方面，如跨境資料傳輸如何規範、在資料不可竄改的特徵下如何要求個資的請求刪除權與被遺忘權等。

④ 虛擬貨幣

根據瑞士金融市場監管機構 (FINMA) 分類，虛擬貨幣有支付型、使用型和資產型代幣，資產型代幣又稱為證券型代幣 (STO)，金管會擬開放 STO，但因涉及投資人保護，將採分級管理。

⑤ 物聯網 (Internet of Thing, IoT)

物聯網裝置無所不在，因此，必須考量個資和資安問題，以及當發生事故時的責任歸屬問題。

(2) Q&A

- 六都已試行無人車，但尚未通過相關法規或配套措施。在臺灣發展無人車，首要改善之處為何？

討論釐清 AI 的倫理規範以及道德內容。

- AI 的究責是否可比照經濟學，由法律、政府去判定所有權人以區隔責任歸屬？

經濟分析是否可以適用在法律或個案判決上，已有很多討論，目前還是有爭議點。

- 長期照護如需蒐集老人的生理數據，能否由照顧者代為處理同意書？

依民法規定，如果當事人年紀很小或年老無行為能力時，要有法定代理人。所以，須由法定代理人代為處理同意書。

7. 網路治理的挑戰：網路基礎建設

(1) 演講摘要

講者：吳國維／NII 產業發展協進會顧問

(錄影檔請至研習營活動網站「學習資源」igcamp.tw/resources/)

手機或電腦連網時，是以 IP 位址進行溝通，但因 IP 位址是由長串的數字組成，人類無法記憶，因此，網路先驅 Jon Postel 發明 DNS (Domain Name System，網域名稱系統或域名系統)，將 IP 位址和域名做相互對應。

以查詢 yahoo 財經網站 finance.yahoo.com 為例，手機或電腦會先查詢本機的快取 (cache)，如果有紀錄則直接顯示結果，沒有就往 ISP 的 DNS 尋找，然後再往更上一層的 Root Server (根伺服器) 尋找。若從域名的結構來看，則是從右到左進行解析。ISP 的 DNS 會先至 Root Server 查詢並得到 .com 的 IP 位址，接者至 .com 伺服器找到 yahoo.com 的 IP 位址，然後再至 yahoo.com 伺服器找到 finance.yahoo.com 的 IP 位址，最後將此結果回傳給使用者。

而網路治理的第一個問題正是源自此處。全球有 13 個 Root Server，10 個在美國，2 個在歐洲，1 個在日本；IP 位址則是透過五大洲的 RIRs (Regional Internet Registries，區域網際網路註冊機構) 發放。中、俄、印等國從 1996 年至今，仍在為了本國沒有 Root Server、為什麼 IP 位址須向 RIR 申請並繳費等問題，而爭論不休。

第二個問題為頂級域名，分成國碼頂級域名 (Country code top-level domain, ccTLD) 和通用頂級域名 (Generic Top-level Domain, gTLD) 兩種。全球共有 256 個 ccTLD，高達 7 成由企業營運，臺灣.tw 由 TWNIC 營

運；gTLD 過去全球只有 6 個而被視為壟斷，後來開放申請，目前約 1,500 個。相關的治理問題如：政府可以委託商業公司維運 ccTLD 嗎？.tw 由誰維運最符合公共利益？又.tw 註冊年費 NT\$800 元相較於其他頂級域名是否偏高？gTLD 壟斷問題經開放申請後是否已經解決？

另外，全球市值前 20 名的網路公司皆來自中、美兩國，顯示它們是全球網路發展的最大獲利者。因此，歐盟推出 GDPR 和新著作權法，以規範美國的科技龍頭。但 GDPR 實施結果卻是中小企業受害，有雄厚資本可以遵循法律的科技龍頭反而廣告收益持續成長。

上述問題有很多可以做為分組演練的題目。不過，網路治理沒有完美或單一的答案，而是要找出最大公共利益；共識也不是獲得每個人的同意，而是多數人接受、沒有強烈反對意見，即是共識。

(2) Q&A

- 為什麼域名可以被高價投資買賣？小公司怎麼辦？

如果某個域名已經被註冊，我們仍有許多其他域名可以使用，因此，域名買賣是市場自由機制，最貴的域名高達 2,500 萬美元。而如果涉及商標問題，可以透過 UDRP (Uniform Domain Name Dispute Resolution Policy，統一域名爭議解決政策) 處理，在臺灣的處理機構為資策會科技法律研究所及臺北律師公會，所需費用約為新臺幣 5 千元。

8. 網路治理的挑戰：媒體與內容

(1) 演講摘要

講者：胡元輝／中正大學傳播系教授

(簡報資料詳「附件二」；錄影檔請至研習營活動網站「學習資源」
igcamp.tw/resources/)

最近專家皆提倡停止使用假新聞(fake news)一詞，而改用不實資訊，

即 misinformation 或 disinformation，兩者差異在於前者是無心導致的錯誤訊息傳遞，後者則為刻意、具特定目的地散播假訊息。目前大眾最關切的，大多為” disinformation”。

如何判定一個訊息是否為「假訊息」，有幾個要素：是否為故意、是否具特定目的，以及是否造成實質的公共損害。假新聞這個舊產物之所以引起廣泛討論，主因為社群媒體的普及，提供更方便、便宜、快速的訊息傳播管道，加上缺乏管制、傳播對象為認識的人等特性，不僅大幅提升訊息散播的速度及範圍，使用者也因為缺乏防備而更容易輕信謠言。

防制假訊息應搭配長短程作法且多管齊下。短程方面，首重社群平臺的自律、事實查核，以及「打假」的新興科技，如謠言查證機器人等。長程而言，則應致力推動國內媒體結構的健全化，並培養民眾的媒體素養。

各國管制社群平臺散播假訊息的案例，例如德國已透過立法，懲處未能即時刪除假訊息的平臺業者；法國由司法機關負責裁決選舉相關的假訊息；歐盟目前仍未訂定任何具強制效力的法律，僅以行政要求業界共同訂定行為守則；美國國會目前也試圖立法規範政治廣告。學員們也可以思考臺灣應朝哪個方向前進。

(2) Q&A

- 請問政府打擊或管制假訊息是否不夠積極？

雖然政府應有所作為，如成立專責單位或制定相關法規，但是公民社會亦應負起責任，不應完全仰賴或信任政府。在提升自我媒體素養的同時，也要監督政府的作為是否跨越維護公共利益的界線，而變成言論管制。

- 大選將至，相關單位是否有境外網軍影響國內選舉的因應措施？

我們必須正視網路製造風向已朝產業化發展的問題，政府單位面對假訊息責無旁貸，但是公民社會也需有警覺心。如果政府要成立打擊假訊息的單位，必須在可問責的框架下，以免權力濫用。

- 是否有較明確的方式協助使用者判斷臉書粉絲專頁的真假？

政府應支持利用科技力量來抑制假訊息。台灣事實查核中心也有舉辦工作坊，分別教導民眾和專業媒體辨識假訊息的方式。

- 建立一個協助民眾自行判斷訊息真假的工具，會不會更有效益？

所有事實查核組織的類型和做法都不一樣，能夠互相補足缺失，沒有任何一種方法是萬靈丹，但每種方法都需要去嘗試。假訊息不可能完全消滅，只能做到某種程度的抑制或控制。

二、分組演練

分組演練課程旨在讓學員練習如何規劃並討論網路治理議題，同時藉由角色扮演，體會同一個政策議題對不同利害關係人而言，會因為立場不同而產生各種觀點，以及接續在討論過程中，能否做出價值的取捨，以凝聚政策共識。

進行方式首先將學員分成「網路人權」、「網路安全」、「經濟與新興科技」、「媒體與內容」4個主題組別，每組安排1名導師（即講習課程的各主題講者）全程指導，分組方式由學員依個人興趣自行選擇，每組皆有10位學員。課程進行則分成以下3個階段：

(1) 訂定議題

每組訂出研討主題與子題，並識別該主題涉及的利害關係人有哪些（參考資料：「學員手冊」國內外IGF）。

(2) 角色扮演

各組分配誰扮演什麼利害關係人，並依角色進行演練。

(3) 成果報告

各組指派代表上臺報告討論結果，包括達成什麼共識、哪些是無法化

解的歧見、哪些僅是個別建議等。各組報告內容可彙整如下表 6。

表6. 研習營學員成果報告彙整表

組別	1. 網路人權
題目	假新聞和人工智慧 (AI) 的挑戰與希望
共識	<ul style="list-style-type: none"> ● 所有利害關係人應各司其職以對抗假新聞，包括：政府提供透明公正的查核系統；非政府組織要推廣多元意見的價值觀；學術機構應提供技術支援；使用者則應具備媒體識讀能力。 ● 當人類享受 AI 所帶來的便利，同時也在濫用這些方便，如人臉辨識的濫用。
歧見	<ul style="list-style-type: none"> ● 對於 AI 未來發展方向，政府代表認為應以人民需求為優先；非政府組織代表強調要包容各方意見；民間企業代表表示，使用者要決定是否使用該服務；學術機構代表則認為應善用 AI 的辨識能力。
個別建議	<ul style="list-style-type: none"> ● 須有一貫的標準作業程序來辨識假新聞，幫助民眾了解哪些是好的新聞、哪些是不好的新聞。 ● 必須嘗試修正 AI 技術，讓 AI 做的決定不會造成歧視。
組別	2. 網路安全
題目	資料去識別化與應用範圍責任界定
共識	<ul style="list-style-type: none"> ● 去識別化相當重要，但同時也要讓資料能夠做創新發展。
歧見	<ul style="list-style-type: none"> ● 有些人認為去識別化技術無法完全保證不會被反向重組。 ● 公民團體主張業者要提供去識別化的演算法，但業者堅持演算法是無法公開的商業機密。
個別建議	<ul style="list-style-type: none"> ● 基於經濟發展與社會進步，政府應同意開放去識別化的資料。 ● 請技術社群研議如何確認 100% 去識別化。
組別	3. 經濟與新興科技組

題目	數位支付的隱私問題
共識	<ul style="list-style-type: none"> • 所有的多方利害關係人都應努力保護消費者的隱私。
歧見	<ul style="list-style-type: none"> • 針對業者若想使用超過既有同意書範圍的個資資料，是否需進行數位支付的二次認證，大家意見不同。
個別建議	--
組別	4. 媒體與內容
題目	如何防治假訊息擴散？以社群媒體自律為例
共識	<p>不同利害關係人的責任如下：</p> <ul style="list-style-type: none"> • 政府部門：短期要澄清事實並訂定罰則；長期則邀請多方利害關係人建立因應機制與政策，並培養民眾媒體識讀能力。 • 新聞媒體：應落實報導前的事實查核工作。 • 社群平臺：修正演算法與分潤政策。
歧見	<ul style="list-style-type: none"> • 對於政府管制程度與言論自由尺度意見不同。
個別建議	<ul style="list-style-type: none"> • 如果政府判定為明顯的假訊息，可要求平臺業者下架；而平臺業者如果不認為是假訊息，可以透過司法途徑請求國家賠償。

三、其它課程

1. 自我預習課程重點提示

本課程為開幕式後的第一堂課，由本計畫吳國維顧問以講解及問答方式，為自我預習課程作重點提示與複習，強化學員的網路治理基本概念，包括網路治理的發展與定義、多方利害關係人的意義與 ICANN 模式、ICANN 政策制定流程等重點。本堂課全程以英文進行。

2. 參與分享

(簡報資料詳「附件二」)

參與分享邀請上屆研習營優秀學員--薛福仁主講。他表示，參與網路治理的入門檻為大量的專有名詞，但只要願意投入時間就會收穫良多。以他參加 2018 APrIGF 為例，透過交流對話不但可以知道各國不同的想法，同時也了解臺灣亦有良好政策。而回國後，他也帶領臺東大學數位志工團參訪 TWNIC、自組團體關切最新網路技術發展，以及拜會越南網路協會並交流網路安全法等議題。至於他平時最關注的議題則是普及上網，也期望能為縮短臺東偏鄉地區的數位落差貢獻一份心力。

3. 未來參與機會介紹

(簡報資料詳「附件二」)

研習營最後由本會 (NII 產業發展協進會) 同仁介紹 2019 年下半年的國內外網路治理會議活動及獎學金申請訊息，包括：

- 7 月 5-6 日 2019 TWIGF 臺灣網路治理論壇
- 7 月 16-19 日 2019 APrIGF 亞太網路治理論壇
- 8 月 12-16 日 2019 APIGA 亞太網路治理學院 (獎學金申請期限 6/7)
- 9 月 5-12 日 APNIC 48 亞太網路資訊中心會議 (獎學金申請期限 6/9)
- 11 月 2-7 日 ICANN 66 (獎學金申請期限 4/11)
- 11 月 25-29 日 2019 IGF

第六節 印刷與影音紀錄

一、 布置與印刷品

本次課程的布置與印刷品包括：議程版、海報 (2 款)、學員手冊 (詳「附件三」、識別證 (3 款)，以及結業證書，成品如下圖 20 所示。

2019 網路治理研習營
2019 Internet Governance Training Camp

◎ 2019.5.31(五) ~ 6.1(六) ◎ 台北市IEAT會議中心

入門課程		5月31日 (五)
13:30 - 14:00	報到	
14:00 - 14:30	開幕致詞 & 學員自我介紹	
14:30 - 15:30	自我學習課程討論	
15:30 - 15:50	休息	
15:50 - 17:20	演講 (1): 認識網路治理	
	— 網路治理與政策模式	
	— 當前網路治理重要法規	
	— 數位匯流下的言論管制	

進階課程		6月1日 (六)
09:00 - 09:10	報到	
09:10 - 10:40	演講 (2): 網路治理的挑戰	
	— 網路人權	
	— 網路安全	
	— 經濟與新興科技	
10:40 - 11:00	休息	
11:00 - 12:00	演講 (3): 網路治理的挑戰	
	— 網路基礎建設	
	— 媒體與內容	
12:00 - 13:00	午餐	
13:00 - 13:40	分組演講 (上): 訂定討論主題、議題、多方利害關係人	
13:40 - 15:10	分組演講 (中): 扮演多方利害關係人討論治理議題	
15:10 - 15:30	休息	
15:30 - 16:00	分組演講 (下): 成果報告 (共講、意見與建議)	
16:00 - 16:30	參與分享及未來機會	
16:30 - 17:00	結業 & 交流	

指導單位：國家通訊傳播委員會
主辦單位：財團法人中華民國國家資訊基本建設產業發展協會
協辦單位：財團法人台灣網路資訊中心 TWIGF

指導單位：國家通訊傳播委員會
主辦單位：財團法人中華民國國家資訊基本建設產業發展協會
協辦單位：財團法人台灣網路資訊中心 TWIGF

研習證明書
TRAINING CERTIFICATE

王小明
Hsiao-Ming Wang

於2019年5月31日至6月1日
參加本研習活動共計16小時，特此證明
has completed the 16 hours training program
from 31 May to 1 June 2019

指導單位：國家通訊傳播委員會
主辦單位：財團法人中華民國國家資訊基本建設產業發展協會
協辦單位：財團法人台灣網路資訊中心 TWIGF

2019 網路治理研習營

◎ 2019.5.31(五) ~ 6.1(六)
◎ 台北市IEAT會議中心

指導單位：國家通訊傳播委員會
主辦單位：財團法人中華民國國家資訊基本建設產業發展協會
協辦單位：財團法人台灣網路資訊中心 TWIGF

學員手冊

2019 網路治理研習營

王小明
· NII產業發展協進會 ·

學員

2019 網路治理研習營

王小明
· NII產業發展協進會 ·

講師

2019 網路治理研習營

王小明
· NII產業發展協進會 ·

工作人員

2019 網路治理研習營

圖20. 研習營布置與印刷品

二、活動剪影



圖21. 研習營照片

三、課程簡報與錄影檔

本次課程專題講習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/>) 供開放使用。

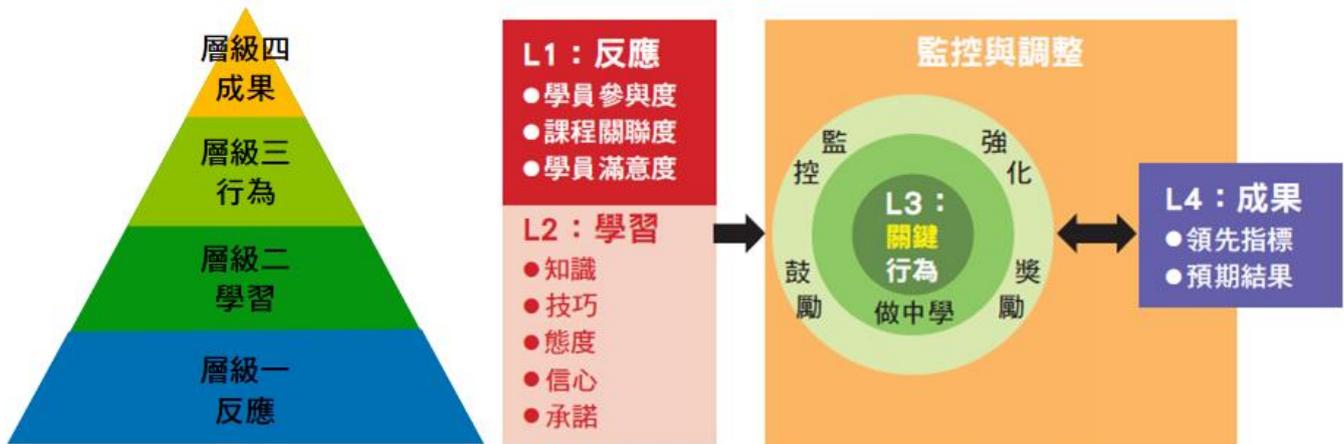
二、2019 研習營簡報	三、2019 研習營錄影檔
1. 網路治理與政策模式	1. 網路治理與政策模式
2. 當前網路治理重要法規	2. 當前網路治理重要法規
3. 經濟與新興科技	3. 數位匯流下的言論管制
4. 媒體與內容	4. 網路基礎建設
5. 網路治理參與分享	5. 媒體與內容

圖22. 研習營課程簡報資料與錄影檔

第七節 學習成效評估

一、評估範圍與方法

國內外常用的柯氏 (Kirkpatrick) 學習評估模式將學習成效的評估分成反應、學習、行為、成果四個層級 (圖 23)。由於第三層級的產生行為改變，屬於學習行為遞延階段，通常需要 3~6 個月後才會產生 (李沐恩，2016)，而且驅動因素除了支持面的獎勵外，還有責任歸屬面的監控 (如工作職責)，顯然與本研習營的屬性不同 (雖然本活動提供獎勵誘因，然而公共事務參與屬於自主性質，無法規定責任歸屬)；加上本活動僅為 2 天的短期課程，因此，當下學習成效評估的合理範圍應是層級一的反應，以及層級二的學習 (鍾佩君，2017)。



資料來源：鍾佩君

圖23. 柯氏學習評估模式

而相對應層級一與二的學習成效評估方法或工具，常用的有課後滿意度問卷調查、測驗、交付報告並評分等方式，惟每種方式如表 7 所列皆有其限制條件 (鍾佩君，2017；林亞蔚，2016)。因此，經綜合考量，本次研習營以「滿意度加上自我評估」之問卷調查，作為學習成效的評估方式。

另外，本計畫後續也持續觀察學員參與網路治理相關活動的狀況，作

為評估層級三的粗略參考。然而，如前所述，在缺乏責任歸屬面的驅動因素下，無法斷然將此參與概況和學員的學習成效直接畫上等號。

表7. 學習成效層級一與二之評估方式與限制

評估層級	評估方式 / 工具	限制條件	是否適用本研習營
層級一 反應	滿意度問卷調查	回收率難以控制	O 本研習營規定結業前繳回問卷，故回收率 100%
層級二 學習	測驗	須有前測與後測做比較，且對受測者形成壓力	X 影響報名和參與研習營意願
	交付報告並評分	耗時較長、成本高	X 2 天課程無充足時間給予學員撰寫報告

資料來源：本計畫彙整

二、問卷統計結果

本次研習營於第二天結業式前，進行問卷調查，共計回收 40 份問卷，回收率為 100%。問卷分為「課程內容滿意度」、「行政會務滿意度」、「學員自我評估」、「其他建議」等 4 個部分，統計結果說明如下。

1. 課程內容滿意度

本年度學員對於課程內容給予高度評價，尤其對課程的整體設計、教學方式、分組演練的滿意度（滿意及非常滿意）都超過 95% 以上；對於專題講習的滿意度亦高達 93%，預習教材的滿意度則為 85%。

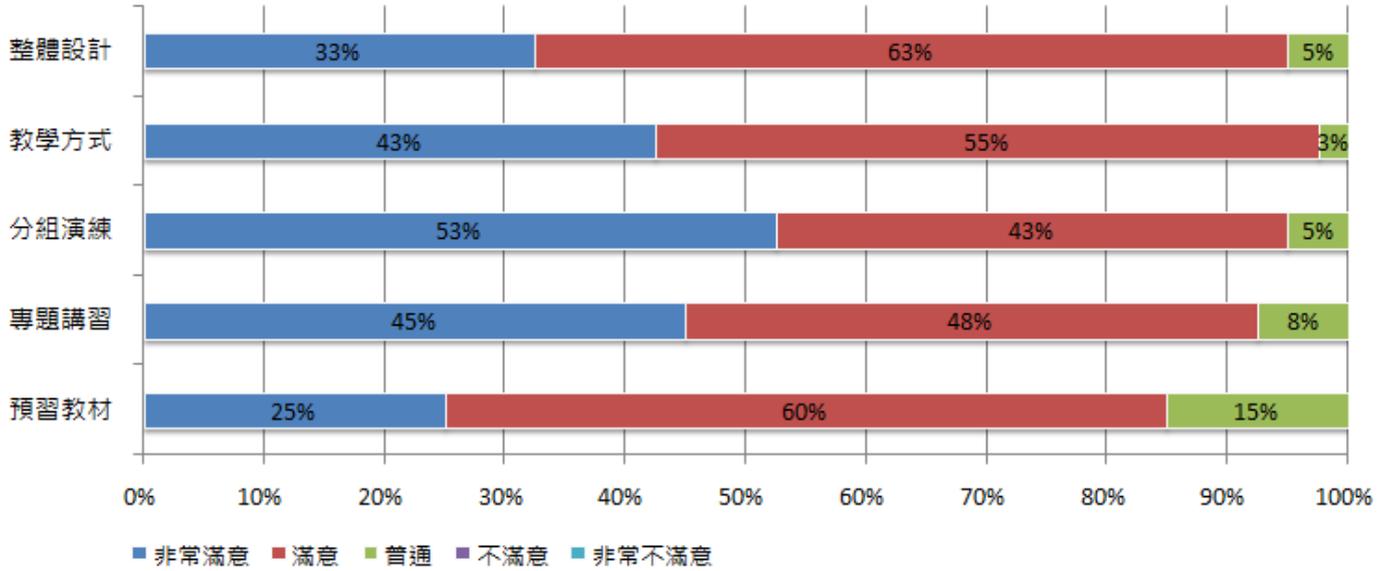


圖24. 研習營「課程內容」滿意度

2. 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，尤其對行政服務、餐飲、教室、活動地點的滿意度（滿意及非常滿意）都超過95%以上；對住宿補助的滿意度則為88%。

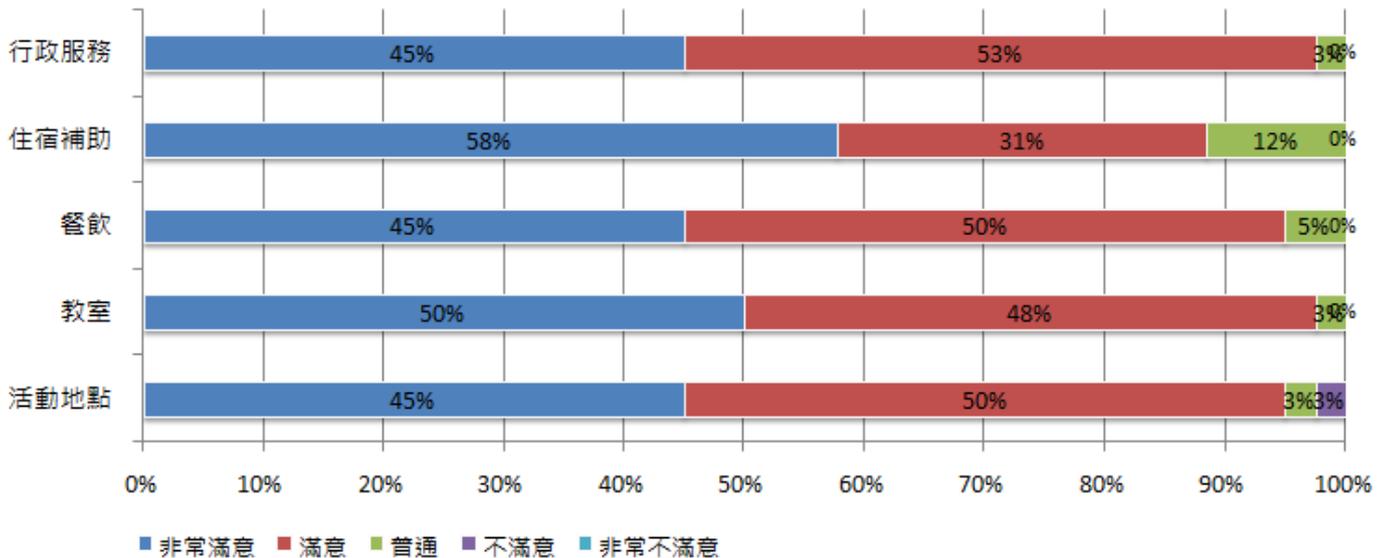


圖25. 研習營「行政會務」滿意度

3. 學員自我評估

高達 93% 學員表示他們對於網路治理的興趣增加(增加與大幅增加)；且多數學員認為本次課程學習到網路治理的基本概念、議題與挑戰、如何參與討論；更有 85% 學員表示未來願意參加 TWIGF，而願意參加國外論壇(線上參與)的比例則顯著下滑，分別是聯合國 IGF 43%，與 APrIGF 35%。

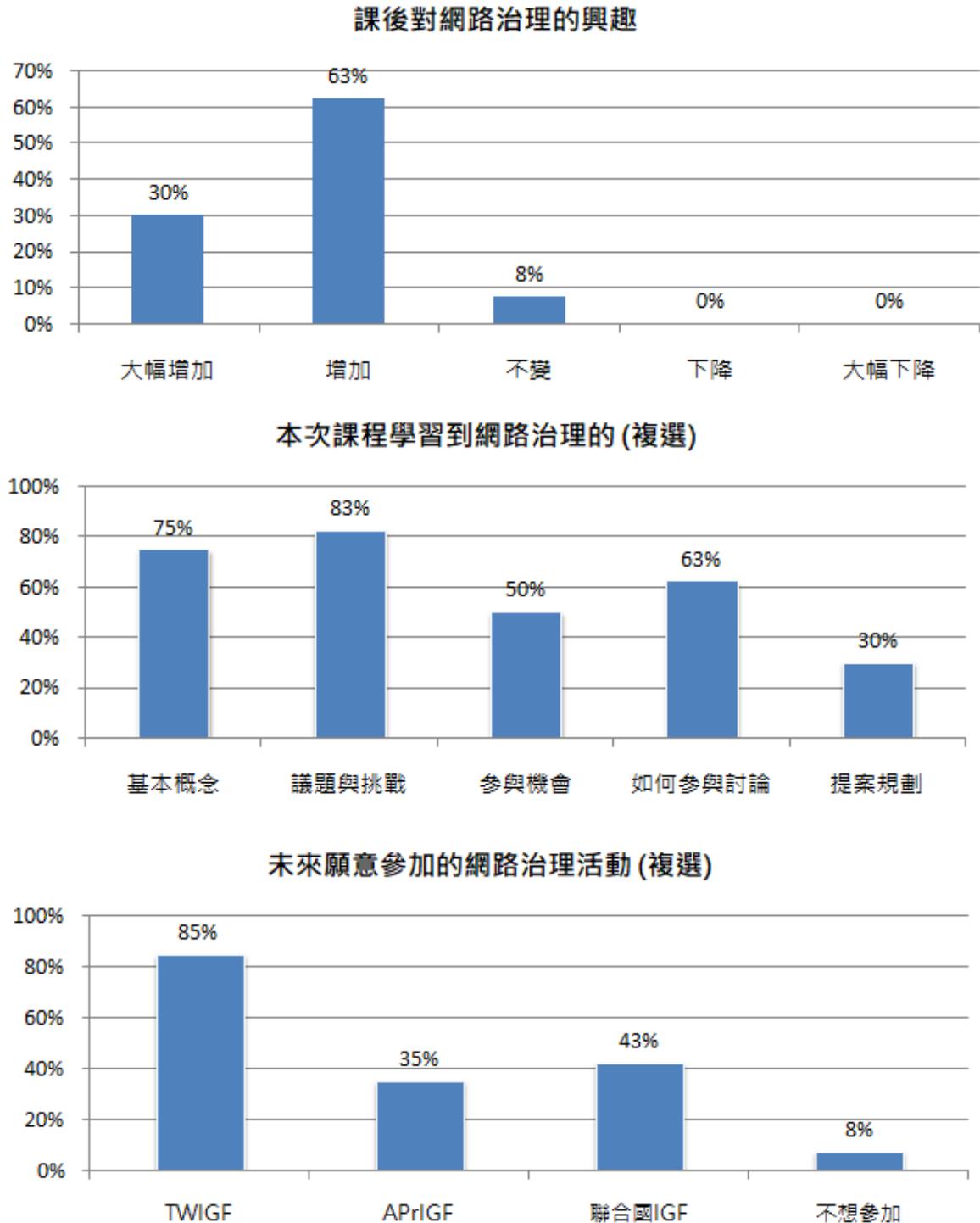


圖26. 研習營學員課後自我評估

4. 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」。學員的參與感想大多是表達謝意或表示收穫良多，而建議則可歸納如下：

- 增加時間
有些學員建議增加「專題講習」時間，有些則建議延長「分組演練」時間，還有人希望增加「休息」時間，或「整個活動」時間。
- 改善提問方式或次數
有些學員認為應該限制每位學員的提問次數，讓別人也有機會發問，或是改用線上提問系統 slido 進行。
- 語言與專有名詞問題
有些學員建議課程如以英文進行，應該事前告知。還有學員表示，希望講師提到英文專有名詞縮寫時，能先說明全稱以利了解。
- 其他
學員的其他建議包括：分組討論每組人數 4~5 人為佳、提供更多預習教材、小組成果報告方式一致化（本次課程有些小組製作投影片，有些則是手寫海報）。

三、後續參與情況觀察

本計畫持續追蹤學員於研習營後，參加本計畫或本會主辦的網路治理相關活動概況。

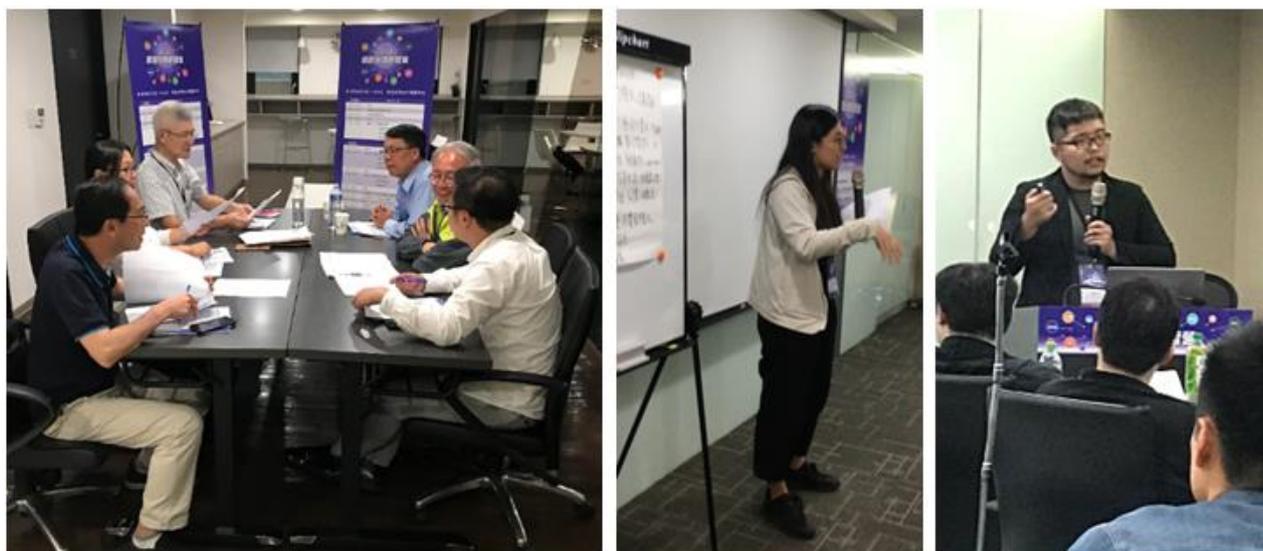
- 7月5日與6日 TWIGF：本屆學員共計 14 位參加，參加率為 35%；當中有 8 位學員同時參加本計畫 TWIGF 特派員活動，請詳本章第九節說明。
- 7月10日「掌握參與全球網路政策制定的機會」會議活動：有 4 位學員主動報名並出席。

第八節 選拔優秀學員參與國際會議

本屆 40 位學員有 21 位學員表達參加優秀學員甄選意願。本次評選小組由帶領分組演練的 5 位講師組成，從 21 位參加角逐的學員中，遴選 1 位優秀學員參加 7 月 16 日至 19 日於海參崴舉辦的 2019 APrIGF，全程差旅費由本計畫支應（另 1 個名額保留予持續參與國內外網路治理活動的上屆優秀學員）。

本次評選會議於研習營第二天（6 月 1 日）活動結束之際，於教室外的講師休息區舉行，先由每位評審委員推薦 1~2 位優秀學員，大家再共同討論這些學員於課堂上所表現出的學習熱忱、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。

本屆優秀學員經連繫後，確認為彰化師範大學英語學系應屆畢業生陳之亭小姐（正取），評選結果於 6 月 4 日公布於活動網站上。而上屆優秀學員薛福仁先生自臺東大學資訊工程學系畢業後，已自創電腦資訊科技公司。他們 2 位除了履行參與 APrIGF 義務外，同時也會參加本計畫 9 月份辦理的國際參與分享會議，於會中報告 APrIGF 參與經驗與心得感想。



左圖：評選會議；中間：本屆優秀學員做成果報告；右圖：上屆優秀學員分享參與經驗

圖27. 研習營優秀學員報告與評選會議照片

第九節 TWIGF 特派員活動

為鼓勵學員持續參與網路治理相關活動，尤其是國內網路治理的年度盛會 TWIGF，本計畫邀請所有學員申請擔任 TWIGF 特派員，凡是於期限內交付 2 場次 TWIGF 座談摘要報告，即可獲頒新臺幣\$2,000 元獎學金（公務員學員除外），摘要報告並具名刊載於研習營網站的「學習資源」。

TWIGF 2019 特派員活動

TWIGF 2019 (臺灣網路治理論壇)將於7/5(五)-7/6(六)於中華電信總公司大樓(臺北市中正區信義路一段21-3號)盛大登場，歡迎今年的網路治理研習營學員參加「TWIGF特派員活動」，只要是結業學員就可以申請擔任特派員，活動辦法請詳以下說明，名額只有20名，額滿為止！

申請方式

請於6/25 (二) 前完成以下3步驟，前20名即可擔任TWIGF特派員。

1. 請回覆本郵件，表明要申請擔任TWIGF特派員。
2. 請至[Google線上文件](#)登記即將記錄的場次（於特派員後填寫姓名），每人須登記2場次，每場次限2名（只有大會專題座談為3名），請勿刪除他人的登記。
3. 請至TWIGF網站完成 [線上報名](#)

遵守事項

1. 兩天活動皆須於上午9:00前報到簽名。
2. 完成應記錄的2場次摘要報告，格式如附檔。
3. 請於7/6 (六) 下午茶點時間至服務台領取獎學金領據，並於大會結束前填妥交回。
4. 請於7/14 (日) 23:59前將摘要報告E-mail給主辦單位，後續將會具名刊載於「2019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）。

結果公佈與通知

申請結果將於6/26 (三) 於本活動網站公布，並以E-mail個別通知。

獎勵方式

完成「遵守事項」的特派員，將獲頒新臺幣\$2,000元整獎學金。

圖28. 研習營「TWIGF 特派員活動」辦法與獎勵

結果本次共有 8 位學員申請擔任特派員，並如期提供摘要報告，報告刊載頁面如下圖 29 所示，各篇摘要報告請詳「附件四」。

四、2019 TWIGF 特派員報導

- | | |
|--------------------------|--------------------------|
| 1. 提高數位平臺業者信任度-1 | 9. 數位外交：如何用網路推展外交工作-1 |
| 2. 提高數位平臺業者信任度-2 | 10. 數位外交：如何用網路推展外交工作-2 |
| 3. 人工智慧：應用與治理-1 | 11. 數位匯流時代之隱私議題 |
| 4. 人工智慧：應用與治理-2 | 12. 女性在ICT領域的就業機會和未來-1 |
| 5. 軍方在資安治理的角色-1 | 13. 女性在ICT領域的就業機會和未來-2 |
| 6. 軍方在資安治理的角色-2 | 14. 假訊息：科技防制、事實查證與人權保護-1 |
| 7. 智慧物聯網（AIoT）時代的安全與隱私挑戰 | 15. 假訊息：科技防制、事實查證與人權保護-2 |
| 8. 晶片身分證：在隱私或資安上的風險 | 16. 數位支付、隱私與洗錢 |

圖29. 研習營「TWIGF 特派員活動」摘要報告刊登頁面

參考文獻

- 李沐恩 (2016)。學習 (訓練) 成效評估之應用實務。中國生產理中心，2016/1/6。 <https://mymkc.com/article/content/22262>
- 林亞蔚 (2016)。探索暨行動學習課程之發展與應用：國家文官學院 101 年至 104 年初任主管班研究成果。文官學院 T&D 飛訊第 223 期，105 年 10 月。 <http://www.nacs.gov.tw/NcsiWebFileDocuments/195e3ec6b91c84a03d3e7d423c6b2775.pdf>
- 鍾佩君 (2017)。初探新版柯氏學習評估模式。評鑑雙月刊第 68 期，2017 年 7 月。 <http://epaper.heeact.edu.tw/archive/2017/07/01/6789.aspx>
- 風伶紫 (2015)。課程與教學設計 ADDIE 與 4R 柯氏學習評估模式重要性。 <https://flipedu.parenting.com.tw/article/1296>

第四章 國際專家訪臺

第一節 專家簡介與行程安排

本計畫邀請來自日本的網路技術維運與相關國際事務協調專家 Mr. Maemura Akinori (前村昌紀) 於7月4日至6日訪臺，並安排拜會通傳會，以及至臺灣網路治理論壇 (TWIGF) 擔任開幕專題演說嘉賓，及參與 2 場座談會議「Internet Consolidation is Here」及「ISP DNS Block 架構跟問題」(擔任與談人) 等行程。

Mr. Maemura 擁有超過20年的網路技術維運與協調經驗，投入 APNIC (亞太網路資訊中心) 董事職務即長達十多年，且期間有 13 年擔任主席。他目前於推動日本網路發展的非營利單位 JPNIC (日本網路資訊中心) 擔任總經理，同時也是訂定全球網路資源政策的主要國際組織 ICANN (網際網路名稱與號碼分配機構)的董事。其主要職務經歷如下：

- 現任職務
 - 網際網路名稱與號碼分配機構 (Internet Corporation for Assigned Names and Numbers, ICANN) 董事 (2016 ~ 2019)
 - 日本網路資訊中心 (Japan Network Information Center, JPNIC) 網路發展部總經理 (2007 迄今)
 - 日本電腦網路危機處理暨協調中心 (Japan Computer Emergency Response Team Coordination Center, JPCERT/CC) 董事
 - 日本網路治理會議 (Internet Governance Conference Japan, IGCI) 秘書長
- 主要經歷
 - 亞太網路資訊中心 (Asia Pacific Network Information Centre,

APNIC) 董事、主席 (2000 ~ 2016)

- 法國電信集團負責亞洲的 IP 工程與產品管理等 (2000 ~ 2006)
- 推動建立日本網路維運社群 (Japan Network Operators' Group, JANOG)、JPNIC 的 IP 位址管理政策 (1997)
- 日本 NEC 公司網路工程師 (1994 ~ 2000)

第二節 拜會通傳會

一、會議資訊

- 時間：108 年 7 月 4 日 (四) 16:30~18:00
- 地點：國家通訊傳播委員會 805 會議室
- 與會者：陳耀祥代理主任委員、郭文忠委員、鄧惟中委員、通傳會處室首長及同仁、Mr. Maemura Akinori、吳國維顧問、本計畫同仁

二、演講摘要

(一) 主席致詞

- 陳耀祥代理主任委員

網路和數位科技帶動數位經濟的發展，通傳會作為通訊傳播的獨立主管機關，相信藉由推廣開放信任的網路環境，能促進數位經濟的發展潛能。然而，網路的快速發展也引起許多社會和法律問題，這也是網路治理的多方利害關係人模式被廣為採用的原因。近年來通傳會將推廣網路治理概念作為施政重點之一，感謝 NII 產業發展協進會邀請 Maemura 先生前來分享 IP 位址管理和網路內容封鎖等重要議題，相信 Maemura 先生在網路政策、技術層面和國際參與合作上的專業，能提供通傳會相關建議和幫助。

(二) 專家演講

1. 日本 IP 位址與.jp 管理方式

吳國維顧問首先說明臺日兩國管理網路資源的差異。日本是由 JPNIC (日本網路資訊中心) 負責 IP 位址的分配, JPRS (Japan Registry Services, 日本註冊管理機構) 負責管理.jp 域名。臺灣則是兩者 (IP 與.tw) 皆由 TWNIC (台灣網路資訊中心) 負責。

1990 年代日本政府不認為 TCP/IP (Transmission Control Protocol/Internet Protocol, 傳輸控制協定/網際網路協定) 會是下世紀的網路標準, 沒有熱衷投入, 以致當時日本的網路發展是由民間企業和學術單位主導, 慶應大學副校長 Jun Murai 因此被譽為日本網路之父, 同時他也擔任 ICANN 第一屆董事。

JPNIC 成立於 1991 年, 負責管理 IP 與域名。隨著網路商業化發展, JPNIC 於 1997 年獲得政府認可成為非營利法人機構, 財源主要來自會員費。在歷經網路泡沫化和使用率大幅增加, JPNIC 決定將域名業務商業化, 於 2000 年另成立 JPRS 股份有限公司, 提供.jp 國碼頂級域名的註冊和管理服務。依據 JPRS 與 JPNIC 合約, JPRS 是基於公共利益而經營域名事業。

JPNIC 除了管理 IP 位址、監管 JPRS 之外, 也促進日本國內網際網路教育的推動, 以及提供相關的教育訓練。此外, 也舉辦日本網路治理論壇 (IGF Japan), 但是日本民眾對網路治理議題的參與度不高, 期望未來能有所改善。

2. 日本網路政策案例：漫畫村事件與封鎖 DNS/IP

日本知名盜版漫畫網站「漫畫村」提供用戶數萬本的免費盜版漫畫, 造成漫畫商和出版界損失高達 3,200 億日圓(約 915 億臺幣), 堪稱日本史上最嚴重的侵權行為。因此, 日本政府於 2018 年 4 月要求 ISP (網路服務供應商) 封鎖該網站以做為「緊急因應措施」, 並於 2018 年 6 月成立工作小組進行討論, 小組成員包括 ISP、內容傳遞網路營運商(Content Delivery

Network, CDN)、律師、法官、廣告商、學者等 18 位多方利害關係人。

而在歷經 4 個月召開 10 次會議和研討會後，工作小組並沒有提出結論報告，因為小組成員對於該不該採取內容封鎖，仍呈現兩極化爭論。反對原因包括違反日本憲法所保障的通信秘密等。至於其他的因應措施如阻止搜尋結果、查禁廣告、從 CDN 移除內容、從使用端過濾等，工作小組成員也仍有不同意見 (表 8)，因此，在 2019 年持續進行討論。由此也凸顯研擬因應對策的困難，並建議臺灣觀察事件的後續發展與因應對策。

吳國維顧問補充說明指出，現在網路運作相當複雜，網站和 IP 並不是一對一的關係，一個網站可能有多個 IP (如存放於多個雲端伺服器)，一個 IP 也可能對應多個網站，所以，根本無法將所有 IP 羅列完整，也不可能為了 1 個違法網站而連帶關閉同一個 IP 上的更多合法網站。此外，為了能讓連網速度更快，CDN 已經無所不在，甚至個人手機都可以開放給 Google 做 CDN，也因此，無法做到內容封鎖。

表 8. 日本盜版漫畫網站討論中的因應措施

Measure	For-blocking argument	Anti-blocking argument
Reinforce DRM	Longer term solution	
Promote the distribution of legitimate content		
Moral education		
Outlaw downloading	Not yet	Now on the way (another problem)
Suppress search result	not enough to be effective	Getting more effective
Address Leech sites	Difficult to define the leech	On the way to define
Suppress ads	Not enough to be effective	action being taken
Removal request	CDN doesn't disclose the content origin	CDN does
Takedown at CDN	CDN doesn't take it down	Should be done at the origin
Identify and enforce	Difficult to enforce on those who are abroad	
Filtering at the client	Not enough to be effective	Already enforceable
Blocking at ISP	The only effective means	many other ways

資料來源：JPNIC

3. 臺日未來合作機會

JPNIC 和 TWNIC 長期維持良好的關係，今年 (2019) 4 月 ICANN 也與 TWNIC 共同舉辦 ICANN APAC-TWNIC Engagement Forum，針對域名、IP 位址及網路安全等主題，進行議題探討和知識分享，樂見未來臺日雙方有更多網路發展相關交流。

三、現場交流 (Q&A)

- 鄧惟中委員

是否可藉由其他商業模式解決侵權問題？以報紙為例，報紙以非常低廉價格提供消費者閱讀內容，但可從廣告獲利。

- Mr. Maemura

以網路產業來說，我們正目睹整個產業的重建，無論是軟體或硬體。不過，漫畫與 ICT 產業完全無關，它是一個勞力密集的產業，現在正面臨如何生存的轉捩點。漫畫家、出版商和消費者之間如何維持良好關係，以維護產業的健全發展，仍待大家共同努力。

四、會議剪影



圖30. 國際專家拜會通傳會照片

第三節 TWIGF 專題演講：網路的自治與正統性

一、會議資訊

- 時間：108 年 7 月 5 日 (五) 9:15~9:45
- 地點：中華電信總公司大樓 12 樓國際會議廳
- 演說主題：淺談網際網路的自治與正統性
- 出席人數：130 人

二、演講摘要

(簡報資料請詳「附件五」)

1. JPNIC 管理 IP 位址的原因

JPNIC 不是政府的外部單位，而是一個民間非營利組織，與 APNIC (Asia-Pacific Network Information Center, 亞太網路資訊中心) 訂有合約，APNIC 又與 ICANN 訂有合約，而 ICANN 與美國商務部也有合約。ICANN 為全球域名和 IP 資源的管理機構，過去約二十年來，美國商務部因為合約關係能夠監督 ICANN 運作，並因此引發兩種回應。其一是認為由美國商務部監管尚屬合理的，否則由民營企業管理更令人擔心；另一方面，則是中、俄等國質疑全球網路被單一國家（美國）控制，並堅持應改由聯合國管理。不過，ICANN 與美國商務部的合約已在 2016 年 10 月 1 日正式結束。

2. 全球網路資源管理的全面自治與正統性

全球網路的發展並不是由政府主導，而是網路社群自行訂出互連機制而逐漸茁壯，因此，在 90 年代中期發生域名和商標權爭議問題時，也是網路社群自行訂定 gTLD MoU (通用頂級域名備忘錄) 加以解決。

不過，由於網路是源自 60 年代美國國防部計畫，美國政府因此認定網路屬於美國。而後雖然美國商務部於 1998 年提出將網路單一識別碼移交民間機構管理，並推動成立 ICANN，且委託授權 IANA (Internet Assigned Numbers Authority，網路號碼指派機構) 業務，但商務部仍然擁有 IANA 監管權。直到 2014 年發生 Edward Snowden 監聽洩密事件，美國為了重拾國際聲譽，才同意將監管權移交給 ICANN，並於 2016 年 10 月 1 日完成移交手續，象徵全球網路資源管理邁向全面的獨立自治。

其實 ICANN 與網路維運社群已有超過 20 年的政策制定和管理經驗；且在 IANA 監管權移轉過程，也展現他們建立整合新機制的的能力；加上長期秉持開放、包容、由下而上的原則運作。另一方面，網際網路已經成為社會公共基礎建設 (public social infrastructures)。因此，國家主權沒有管理全球網路資源的正統性，這也是全球獨一無二的案例。

3. 治理網路需採多方利害關係人取向 (方式)

網路架構由下而上分為三層：基礎建設層、邏輯層、經濟與社會層。當前的網路問題大多屬於最上面的經濟與社會層，所以，網路治理不再只是治理網路 (governance of the Internet)，而是治理網路上所發生的問題 (governance on the Internet)，這些問題必須由公共政策和法規來管理。

不過，由於網路科技理解不易，快速的創新也衍生濫用問題，加上政府沒有跨越國界的管轄權，因此，治理問題需要透過多方利害關係人的取向(方式)，廣納各方意見，才能找到最佳解決方案。

三、會議剪影



圖31. 國際專家於 TWIGF 專題演講照片

第四節 TWIGF 座談：如何因應市場鞏固問題？

一、會議資訊

- 時間：108 年 7 月 5 日 (五) 13:30~15:00
- 地點：中華電信總公司大樓 1 樓 109 會議室
- 會議名稱：Internet consolidation is here: What are we going to do about it?
- 出席人數：18 人
- 主持人：Noelle de Guzman／網際網路協會 (ISOC) 亞太區域政策經理
- 與談人：Maemura Akinori／日本網路資訊中心 (JPNIC) 網路發展部總經理

吳國維／NII 產業發展協進會 顧問

簡維克／理律法律事務所 資深律師

二、座談摘要

(一) 主持人引言報告

1. Noelle de Guzman／網際網路協會(ISOC) 亞太區域政策經理

- 全球網路市場鞏固恐影響市場競爭機會

網路其中一項特性是去中心化的結構設計，無人能控制網路，也無須經由任何人同意便可連網，此特性將網路與其他大眾傳播模式作區隔，也是網路創新的重要因素。然而，近年來網路市場已出現鞏固(consolidation)現象，市場經水平與垂直整合，以致市場進入與競爭機會越來越少。

網路市場鞏固雖然具有加快採用網路標準的優點（因為大企業通常願意快速引進並推動使用網路標準），但是，也會帶來過度依賴的缺點。以 API (Application Programming Interface，應用程式介面) 為例，Uber 目前使用 Google 地圖來提供服務，假如 Google 決定不讓 Uber 使用這項功能，Uber 就得自行開發（事實上 Uber 已在進行）。然而，並不是每家企業都有能力開發系統，尤其是新創公司。又如果政府讓一家企業提供民生必須的公共服務，為了服務不中斷，政府是否不得不讓該企業持續運作？這些都是需要考量的問題。

(二) 與談人報告

1. Maemura Akinori／日本網路資訊中心 (JPNIC) 網路發展部總經理

- 如何處理全球市場壟斷需多方利害關係人討論

網路的初始設計可以帶來競爭和進步，不需要任何人的首肯便能進行網路創新。在日本，沒有一家企業能與 Facebook、Google 或 Amazon 競爭，但大家高度集中使用這些服務，令人感到不安。現今的網路環境也會產生網路效應 (network effect)，例如使用某一種社交媒體的用戶數越多，該媒

體所提供的好處也就越多，這很容易造成過度競爭、強者恆強弱者恆弱。這些問題如果是在國內尚有主管機構可以管理，但是如何處理全球性的競爭和壟斷則是一大問題，需在網路治理相關會議中，由多方利害關係人共同討論解決方案。

2. 吳國維／NII 產業發展協進會 顧問

- 傳統競爭法規不適用網路市場，重點為符合公共利益的管理機制

網路運作模式造成大者恆大的特殊現象，排名第一的企業人盡皆知，但之後的企業就默默無聞，因為落差實在太過懸殊。例如 Google Map 為第一大網路地圖服務供應商，但第二大是誰就無人知曉。

支配 (domination) 有兩種定義，其一是從使用角度來看，其二是從法律層面來看。一家企業可以支配市場，但不代表它有壟斷市場。如果將傳統競爭法套用在 Google Map 上是行不通的，因為 Google Map 並沒有利用其支配地位阻擋創新公司進入市場中，因此，必須修改競爭法規。

我們常將壟斷或支配市場視為負面，但在自由市場中，壟斷或支配的情形其實存在社會的不同層面，政府單位也可算是一種壟斷機構。因此，重點在於如何建立管理機制，並確認以公共利益為優先。

3. 簡維克／理律法律事務所 資深律師

- 數位產業大者恆大，是否濫用市場地位值得討論

數位市場提供許多免費服務，不像傳統市場可輕易透過價格比較來判斷市場，因此，目前公平交易委員會已經成立研究小組，試圖釐清科技巨擘是否有反托拉斯法的行為。數位產業有大者恆大現象，因為科技巨擘更容易取得用戶數據，也就能比其他競爭者取得先機。假若他們拒絕與其他競爭者分享資料，這樣是否造成濫用市場地位問題，值得大家討論。

- OTT 尚未規管造成市場不公平競爭

OTT 服務供應商在臺灣尚無法律規管，因此，有許多空間可以提供消費者更具彈性的服務。但是，傳統服務供應商如有線電視或衛星頻道業者卻受到現行法律的嚴格規管，造成市場不公平競爭，也許國內應該修法以減輕既有產業的負擔。

(三) 現場交流 (與會者分享觀點)

1. 黃勝雄／台灣網路資訊中心 執行長

- 科技巨擘擬操縱網路協定結構，應分散其權力以避免濫用市場力量

討論壟斷並非首要重點，關鍵在於企業是否濫用其市場力量。現今許多科技巨擘甚至試圖影響網路協定，例如 DNS over HTTPS (DoH) 就是由某科技巨擘發明用以影響網路流量的通訊協定，他們除了支配消費市場外，還想操縱滲透網路協定的結構。基本上，我們不該相信擁有超級權力的一方，應該要分散權力，將每個想在網路發聲者視為平等的個體。

2. 余若凡／國際通商法律事務所 合夥律師

- 壟斷亦有優點，應更著重建構產業健康發展環境

壟斷其實有好處與壞處，好處在於大型企業有較多資源可落實法律遵循及提供創新服務，小型企業則很難匹敵。在臺灣談到競爭法，總是圍繞在律師和經濟學家之間，但其實更應該思考競爭法會影響臺灣哪些層面，以及如何讓新創產業在這樣的生態中蓬勃發展，也就是說，我們應該要更有策略性，提供產業健康的發展環境。

三、小結

綜合本場座談的主持人、與談人，以及臺下專業與會者的觀點，雖然大家一致認為全球網路市場已出現高度集中化或鞏固(consolidation) 現象，不過，對此現象的影響性以及該如何因應，專家們則持不同看法，且大致

可歸納為兩種：其一是認為已影響市場公平競爭且需加以因應，另一方主張壟斷並非負面且不適用傳統競爭法規。相關論述彙整如下表 9。

表9. 「Internet Consolidation is here 座談」共識與歧見

項目	意見 / 觀點
共識	全球網路市場已出現高度集中化或鞏固 (consolidation) 現象，企業大者恆大，市場由少數科技巨擘主導支配
歧見	<p>對市場鞏固現象的影響性及該如何因應：</p> <ul style="list-style-type: none"> ● 類別 1：已影響市場公平競爭，且需討論因應 <ul style="list-style-type: none"> - 網路市場的進入與競爭機會越來越少，相關問題需要討論 - 本地企業完全無法競爭，全球市場壟斷問題有賴多方社群討論 - 是否濫用市場地位值得討論，但 OTT 未規管已造成不公平競爭 - 科技巨擘擬操縱網路協定結構，應分散其權力以避免濫用市場力量 ● 類別 2：壟斷並非負面，且不適用傳統競爭法規 <ul style="list-style-type: none"> - 支配市場不代表壟斷，壟斷也非負面，傳統競爭法規不適用，重點在於建立符合公共利益的管理機制 - 壟斷亦有優點，應更著重建構產業健康發展環境

四、會議剪影



圖32. 國際專家參與「Internet consolidation is here 座談」照片

第五節 TWIGF 座談：DNS 封鎖架構與問題

一、會議資訊

- 時間：108 年 7 月 5 日 (五) 15:15~16:45
- 地點：中華電信總公司大樓 1 樓 109 會議室
- 會議名稱：CP/TPP ISP DNS Block 架構跟問題
- 出席人數：31 人
- 主持人：黃立夫／雷亞遊戲 IT 部門主管
- 與談人：Maemura Akinori／日本網路資訊中心 (JPNIC) 網路發展部總經理
吳國維／NII 產業發展協進會 顧問
黃勝雄／台灣網路資訊中心 執行長
蔡志宏／智慧財產法院 法官

二、座談摘要

(一) 與談人報告 (簡報)

1. Maemura Akinori／日本網路資訊中心 (JPNIC) 網路發展部總經理

- 內容封鎖顯然違憲，且有其他因應措施

2017 年日本盜版網站「漫畫村」大肆崛起，嚴重侵害出版商的收益。2018 年 4 月日本內閣決定封鎖有害的盜版網站以做為緊急應變措施。接續於 6 月成立由 18 位多方利害關係人 (ISP、出版商、法官、廣告商等) 所組成的工作小組。然而，在歷經 4 個月召開 10 次會議後，工作小組最終沒有提出結論報告，因為內閣似乎想送出內容封鎖法案，而工作小組成員對於贊成或反對封鎖也仍嚴重分歧。

日本憲法明文保障通信秘密，內容封鎖顯然是違憲。其實打擊盜版侵

權行為還有許多措施，例如阻止搜尋結果、查禁廣告等短期措施，以及提升著作權認知教育、促進正版產品流通等中長期措施（同本章第二節之表 8）。因此，不宜貿然採行涉及違憲問題的內容封鎖。

2. 蔡志宏／智慧財產法院 法官

- 著作權人可向法院提告並要求停止侵權連線

依臺灣目前法律，若發生侵權行為，著作權人可向法院提告，憑勝訴判決要求 ISP 業者停止特定 IP 連線，或要求 DNS 業者不要提供域名解析。如果業者拒絕，對這個侵權內容就建立了故意或過失的基礎，業者可能要負起損害賠償的責任。

- 建議 OTT 業者對侵權以「直接提告」取代「定暫時狀態假處分」

一個侵權網站可能同時包含合法和非法的內容，若技術上可行，便可只針對侵權內容來封鎖，否則法院須衡量利弊得失，依比例原則作判決。封鎖侵權網站可考慮以網站實際經營者為被告，或以 WHOIS 登記的域名註冊者為被告，並依此登記地址作為公文書送達地址。如果沒有地址或送達不到，可用「公示送達」方式，將公文書用公告方式代替送達。

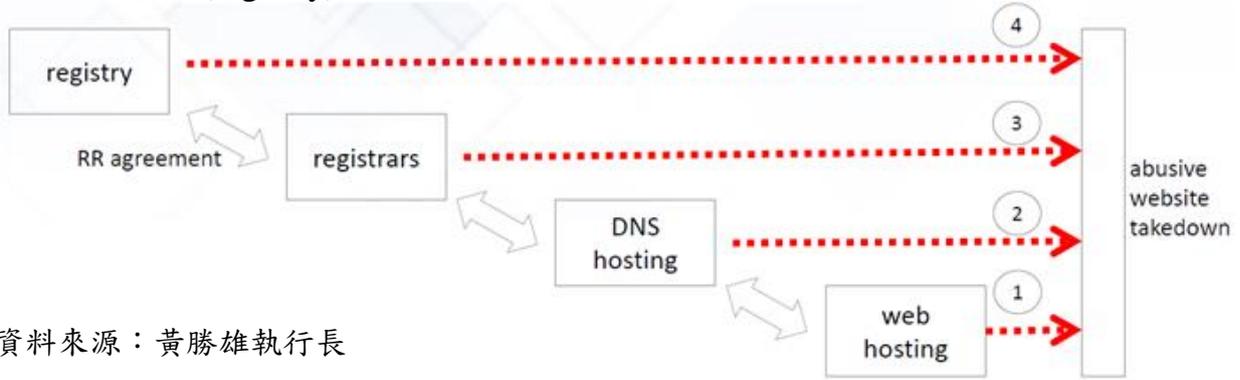
OTT 業者希望採用「定暫時狀態假處分」方式，以迅速處理侵權問題，但是擔保金昂貴，且根據法界經驗，法官此時態度較為謹慎和保守。因此，建議直接提起訴訟，讓法官更有時間思考，且此訴訟費用亦相對便宜，若訴訟成功便能開啟臺灣處理侵權訴訟的先例。

3. 黃勝雄／台灣網路資訊中心 執行長

- 下架常涉跨國處理曠日廢時，非法內容早已轉向他處

從域名層面來看網路犯罪的生態系統，其中一種代管服務供應商是防彈主機 (Bullet-Proof Hosting, BPH) 供應商，BPH 會保護其客戶身分並阻絕外部攻擊。若有執法單位要求，BPH 會拒絕交出客戶的個人資料。另一

種情況是公司立案於某個地區，而伺服器與營運商分別位於不同區域或國家，更容易發生多重反抗，讓執法更加困難。因此，若要阻止非法內容繼續傳輸，應該先找出最底層的網站主機代管業者、DNS 代管業者，要求其將內容下架；若不可行，再依序往上尋求域名註冊商 (registrars)、域名註冊管理機構 (registry)。

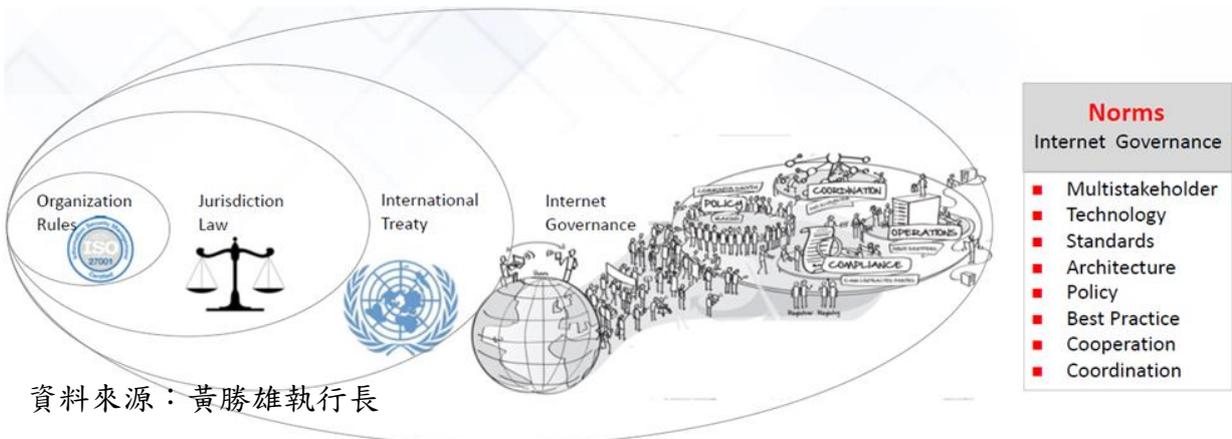


資料來源：黃勝雄執行長

圖33. 阻止非法內容傳輸之尋求服務供應商順序

不過，上述過程可能碰到國際業者拒絕配合，或須透過多個跨國司法互助協定 (Mutual Legal Assistance Treaty, MLAT) 處理，恐將曠日廢時，導致非法內容早已轉向其他伺服器。因此，據聞美國於處理網路空間問題上，已放棄使用 MLAT。

總之，當處理網路安全問題時，須同時考量速度、成本和品質，也許依序透過組織內部規範 (如導入國際標準組織的資安管理制度 ISO 27001)、國內司法、國際協議、網路治理常規，這樣的順序會較為可行。



資料來源：黃勝雄執行長

圖34. 處理網路安全問題的政策順序

4. 吳國維／NII 產業發展協進會 顧問

- 封鎖域名有技術和衍生成本問題，且恐無實質效益

封鎖域名或 IP 的流程非常複雜，因為一個域名可能有很多不同的 IP，一個 IP 也可能會對應很多不同的網站，所以，要判斷封鎖哪個 IP 十分困難。此外，對 ISP 業者來說，封鎖 IP 還有成本上的考量，萬一因此造成頻寬流量降低，其衍生的費用該由誰支付將成問題；若為跨境案件，情況又更加複雜。對國際大廠來說，他們寧可將時間用於擴大市場，因為封鎖 IP 的成本太高，且就算進行封鎖，也可能無法達到有效的目的。

(二) 現場交流 (Q&A)

1. 若技術層面不可行，還有甚麼方式可以保障權利人？

(1) 黃勝雄／台灣網路資訊中心 執行長

要將非法內容下架，除了法院命令外，還有其他方法。IETF (Internet Engineering Task Force，網際網路工程任務小組) 所訂定的協定標準可以過濾網頁原始碼或原始 IP 位址。

(2) 蔡志宏／智慧財產法院 法官

法律機制必須保護小型業者，他們沒有這麼多資源去創新，因此，更需要版權的保護。雖然網路空間不可能全面地執法，但不代表不要執法，而是要盡量讓侵權降到最低。

三、小結

本場座談的與談人從國家法規、國際協議、網路技術等層面，探討網站封鎖或下架問題。儘管基於違反 (日本) 國家憲法、跨國處理曠日廢時、網路技術限制及可能無實質效益等各種不同理由，但與談人一致認為「不」宜以網站封鎖或下架作為網路侵權問題的因應措施。另外，來自法

律界的與談人則是建議著作權人透過訴訟方式維護自身權益。相關重點如下表 10 所示。

表10. 「CP/TPP ISP DNS Block 架構跟問題座談」共識與建議

項目	意見 / 觀點
共識	「不」宜以網站封鎖或下架作為網路侵權問題的因應措施。至於各別原因則包括下列： <ul style="list-style-type: none">• 違反（日本）憲法保障的通信秘密，且有其他因應措施• 常涉及跨國處理且曠日廢時，非法內容早已轉向他處• 封鎖域名有技術和衍生成本問題，且恐無實質效益
個別建議	著作權人可透過訴訟方式維護自身權益，因為可憑勝訴判決，要求 ISP 業者停止特定 IP 連線，或要求 DNS 業者不要提供域名解析。

四、會議剪影



圖35. 國際專家參與「CP/TPP ISP DNS Block 架構跟問題座談」照片

第五章 舉辦座談會議

第一節 申辦通傳議題座談會議

一、提案規劃

本計畫依據「委託辦理工作項目」規定，從下表 11 指定題目中挑選 3 個，於國內具有一定規模的非營利性網路治理論壇，也就是臺灣網路治理論壇 (TWIGF)，申請辦理 2 場座談，包括「智慧物聯網(AIoT)時代的安全與隱私挑戰」與「搶眼球大戰下的 OTT 影音¹治理課題」，且皆獲得評選通過，並均於 TWIGF 的首日 (7 月 5 日) 召開，會議時間如下議程表 (表 12) 所示。後者並被大會指定為開幕後的共同會議，惟名稱改為「OTT 現狀、治理及未來展望」。

表 11. 通傳議題座談會之議題挑選與提案規劃

指定題目(挑選 3 個辦理 1 場座談)	本計畫規劃
1. 如何強化物聯網、人工智慧時代寬頻網路的治理	於 TWIGF 申辦「智慧物聯網 (AIoT) 時代的安全與隱私挑戰」座談
2. 如何促使民眾接取合法網站或網路內容	--
3. 如何導引視聽串流服務業者向主管機關登記及低度管理 (含誘因及業者義務)	於 TWIGF 申辦「搶眼球大戰下的 OTT 影音治理課題」座談 * 被指定為共同會議，並更名為「OTT 現狀、治理及未來展望」
4. 如何強化視聽串流服務衍生之消費者權益保護議題	
5. 如何利用 5G 行動寬頻服務解決數位落差議題	--

1 根據文化部「政府如何因應 OTT 產業新發展趨勢報告」，OTT (Over the Top) 泛指網路上所提供的應用服務，目前主要服務型態包括通訊服務、電子商務、雲端服務、遊戲、搜尋引擎、社群媒體、網路多媒體內容、APP 應用服務，及影音串流服務等。本報告將「視聽串流服務」簡稱為 OTT 影音。

表12. TWIGF 首日議程表與本計畫申辦場次

7月5日			
時段	議程		
	12樓國際會議廳		
08:30-09:00	報到		
09:00-09:15	開幕典禮 貴賓致詞： 吳國維 - 臺灣網路治理論壇 主席 林佳龍 - 交通部 部長 唐鳳 - 行政院 政務委員 陳耀祥 - 國家通訊傳播委員會 代理主任委員 鄺英傑 - 美國在台辦事處 處長 *依姓氏筆畫排列		
09:15-09:45	專題演講：Akinori Maemura- JPNIC 網路發展部 經理 / ICANN 董事 主題：淺談國際網路的自治與合法性 Small Talk on Autonomy and Legitimacy of the Internet		
09:45-11:00	大會專題座談(一)：OTT現狀、治理及未來展望		
11:00-11:15	茶點時間		
11:15-12:30	大會專題座談(二)：提高數位平臺業者信任度		
12:30-13:30	午餐時間		
	110會議室	109會議室	102會議室+101會議室
13:30-15:00	人工智慧：應用與治理 (理律法律事務所)	Internet consolidation is here: What are we going to do about it? (Internet Society)	軍方在資安治理的角色 (國防安全研究院)
15:00-15:15	茶點時間		
15:15-16:45	智慧物聯網 (AIoT) 時代的 安全與隱私挑戰 (NII產業發展協進會)	CP/TPP ISP DNS Block 架構跟問題 (黃立夫)	晶片身分證：在隱私或資安上的風險 (台灣人權促進會)

資料來源：TWIGF

2019 TWIGF 於 7 月 5 日至 6 日假中華電信總公司大樓 (臺北市信義路一段 21-3 號) 舉辦。大會主題為「建立開放、包容、信任、創新的數位社會」，所徵求的座談主題共有電信與網路政策、網路基礎建設與架構、網路人權、網路安全、數位經濟、新興科技、媒體與內容、其他等 8 項。本計畫申辦的 OTT 影音治理屬於「電信與網路政策」主題，AIoT 治理則屬於「新興科技」主題。

二、提案內容

(一) 「OTT 現狀、治理及未來展望」場次 (大會變更之會議名稱)

媒體調查結果顯示，2018年已有77%國人使用過OTT影音服務，平均每天觀賞時間超過80分鐘，且經常使用平臺的前三名皆來自國外，分別為YouTube的85%、愛奇藝的46%、LINE TV的23%。而通傳會去年的調查亦發現，雖然只有21%民眾有付費訂閱服務，但是付費平臺亦集中在國外業者，前兩名分別為愛奇藝的47%，以及Netflix的27%，第三名才是國內業者KKTV的8%。又愛奇藝臺灣站公布其每日活躍用戶數已高達200萬，且近來又傳出中國大陸的騰訊、優酷等主要業者將循愛奇藝模式於今年陸續登臺。由上凸顯，如何因應國外平臺大舉來臺、維護市場公平競爭、保護民眾消費權益等問題，已是刻不容緩。

愛奇藝於2016年申請來臺設立公司，遭經濟部投審會以「非陸資投資許可項目」駁回後，轉為透過臺灣代理商執行業務，包括提供收費服務。對此，陸委會日前已表示，主管機關經濟部正進行查處，一旦違反《兩岸人民關係條例》，最嚴重將把網站下架；而通傳會也曾回應指出，對於涉及國安疑慮的OTT影音，可以透過傳輸等技術方式使其不具收看品質。

不過，通傳會《數位通訊傳播法》(草案)第27條已明定政府應鼓勵境外業者「於我國設立分公司或代理商、依法於我國設立稅籍」，以完善數位通訊傳播發展環境，落實保障消費者權益。另一方面，國內相關產業組織如台灣線上影視產業協會(OTT協會)與新媒體暨影視音發展協會(NMEA)也都提出境外業者落地納管的訴求，包括要求繳稅、保護消費者個資、處理消費爭議、遵守版權規定，甚至播放一定比例的本國自製節目等措施，以維護市場的公平競爭。

綜合上述，本場座談將探討的問題如下：

(1) 國人OTT影音收視高度集中於國外平臺。對國外平臺實施落地管理或

拒絕其落地登記的優缺點分別為何？

- (2) OTT 影音平臺應具備哪些義務？又相關配套的誘因與懲處為何？
- (3) 消基會認為，目前收費 OTT 影音所提供的服務方式，如取消與退費等規定，對消費者不公平。究竟應如何提升消費者的權益保護？

(二)「智慧物聯網 (AIoT) 時代的安全與隱私挑戰」場次

結合人工智慧 (AI) 的消費性物聯網 (IoT) 產品，或稱為 AIoT 產品，正逐漸走入我們的日常生活中。以智慧音箱為例，美國家庭的普及率已經超過 4 成，國內則是近來電信商與製造商也開始紛紛推出自家品牌的智慧音箱。根據 IDC (國際數據資訊) 調查，2018 年全球智慧家庭裝置為 7 億臺，而就整個 IoT 市場來看，預估 2020 年全球 IoT 裝置將多達 500 億臺，等同平均每人擁有 6.6 臺。

然而，就在我們迎接更舒適便利的 AIoT 時代之際，我們也必須正視它所伴隨的安全與隱私風險，因為不論是 AIoT 或單純的 IoT 裝置，相關的災害事件已經層出不窮。例如：智慧玩具洩漏家長與孩童的對話資料；駭客利用連網的監視器、攝影機、印表機、路燈、自動販賣機等裝置做為殭屍網路大軍發動網路攻擊。而日前來臺演講的資安大師 Bruce Schneier 所舉的攻擊案例還包括汽車、魚缸、溫度控制器、醫療設備、無人機、智慧城市系統、發電廠等。這些事件造成的災害不但包括侵犯個資與隱私、癱瘓網站、勒索財物，甚至還會危害生命安全。

為此，各國政府或國際組織也提出各項因應措施。例如：美國加州將於 2020 年元旦實施《SB-327 資訊隱私：連網裝置》法案、荷蘭政府提出《數位軟硬體安全藍圖》、歐洲電信標準協會 (ETSI) 訂立全球物聯網安全標準等。而我國亦已開始實施物聯網資安標章制度，並持續針對各項連網裝置發布資安標準，以及資安檢測技術指引。

面對 AIoT 時代的安全與隱私挑戰，本場座談將探討以下問題 (經座談

主持人國家通訊傳播委員會基礎設施事務處羅金賢處長修正)：

(1) 消費者的資安意識

國內最普及的 AIoT 產品有哪些？消費者應該具備什麼風險意識？

(2) 廠商的資安防護

AIoT 產品的基礎資安防護基準為何？又該如何落實風險管理？

(3) 政府的資安策略

如何將資安由政府延伸至民間，重視產品裝置安全，透過政府和廠商共同建立民眾的信任感，以支持 AIoT 的持續應用？

(4) 數位隱私的落實

如何解決 AIoT 產品及服務符合 GDPR 隱私的難題？又臺灣個資隱私保護該如何落實，以打造消費者及產業雙贏局面？

(5) 資安標章的推動

我國多方利害關係人該如何共同促進 AIoT 的安全保護？又對資安標章的推動與落實有哪些期許與指教？

第二節 通傳議題座談：OTT 現狀、治理及未來展望

一、會議資訊

- 時間：108 年 7 月 5 日 (五) 09:45~11:00
- 地點：中華電信總公司大樓 12 樓國際會議廳
- 會議名稱：大會專題座談 (一)：OTT 現狀、治理及未來展望
- 出席人數：180 人
- 主持人：吳國維／NII 產業發展協進會 顧問
- 與談人：余若凡／國際通商法律事務所 合夥律師

黃勝雄／台灣網際網路協會 理事

錢大衛／台灣線上影視產業協會 (OTT 協會) 理事長

Darren Ong／Netflix 亞太區政府關係主管

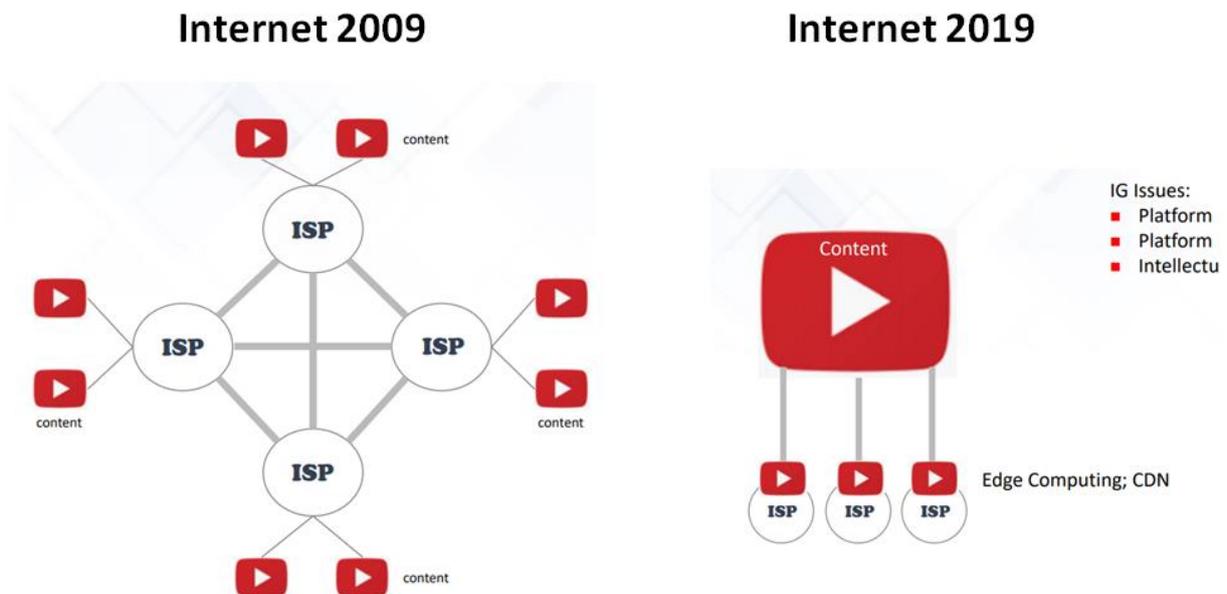
二、座談摘要

(一) 與談人報告 (簡報)

1. 黃勝雄／台灣網際網路協會 理事 (簡報資料請詳「附件六」)

- 網路治理主要議題從 ISP 移轉到平臺業者

10 年前的網路流量是許多不同內容業者，透過不同 ISP (網路接取服務提供者) 提供網路服務，因此，如果 ISP 偏好某家內容業者，為其優先遞送內容，即會產生網路中立問題。而今天的網路流量已經從過去的東西向變成南北向，內容業者成為市場的主導者，並且透過內容傳遞網路 (Content Delivery Network, CDN) 遞送訊息，所以，網路治理的主要議題也從過去的網路中立，變成平臺責任、平臺規範、侵權內容等。



資料來源：黃勝雄理事

圖36. 2009 年與 2019 年網路流量架構比較

- OTT 治理應注意 ISP 與 OTT 營運商的處境不同

OTT 治理議題除了版權與課稅之外，其他層面可看出 ISP 與 OTT 營運商的不同處境。例如：ISP 有義務遵守 QoS (Quality of Service，服務品質)，但 OTT 營運商不用遵守 QoS；ISP 的服務會受到地理限制，但 OTT 營運商不會受到地理限制；ISP 須負責投資網路基礎建設，但 OTT 營運商不用投資網路基礎建設。

2. 錢大衛／台灣線上影視產業協會 (OTT 協會) 理事長

- 機上盒與 APP 盜版問題執法成效良好

資策會的研究顯示，國內 OTT 影音盜版導致一年損失新臺幣 283 億元，所幸《著作權法》第 87 條第 1 項第 8 款經修法後，已將機上盒與 APP 納入規範，且實施成效良好，惟網路的侵權問題仍待未來研議規範。

- 從國家級戰略角度思考 OTT，建議納管境外業者

OTT 須從國家級的戰略角度思考，如中國大陸要求中國 OTT 平臺集體「出海²」即為一例。而我國因為尚無相關規範，以致許多海外平臺進軍臺灣，也影響消費者的權益，例如播放不順無人處理、沒有提供本地客服、不遵守消基會規定（無服務猶豫期、不能退租或手續不明確）、不遵守我國法規等；其他衍生的問題還有不繳稅、未達最低本土內容比例、版權糾紛等。因此，為了保護消費者、打擊盜版、維護市場公平競爭、保障稅收、振興本土影視產業，建議政府納管境外業者。

- 建議訂定專法並採低度管理，但一律強制登記

由於 OTT 影音產業仍在發展階段，因此，宜採取低度管理。但是，因為相關問題涉及通傳會、文化部、經濟部、財政部等多個部會，所以，需

2 根據國內多家媒體於 2019 年 3 月中旬報導，中國大陸廣電總局下令要求所有中國 OTT 業者都要「出海」，傳遞中華文化、宣揚國威。

要訂定專法。目前通傳會正在研擬《視聽串流服務法》，OTT 協會建議採取強制登記，且不論是本土或境外業者、收費或免費服務，皆須納管，項目則包括：在臺設立分公司或子公司（非透過代理商）並有本地客服、落實兒少法的內容分級制度、保護消費者個資且在地儲存、機房須在臺灣並接受管理、金流須在臺灣並繳稅、不可播放中國大陸直播的電視頻道、提供一定比例的本國自製內容等。而萬一有業者拒絕登記，OTT 協會也建議祭出不得使用本地機房與網路頻寬、不得使用本地金流、不得上架至本地的 APP 商店、不得在本地行銷宣傳、不得進行任何營業項目等懲處措施。

(二) 座談討論

1. 請問 Netflix 對全球 OTT 影音市場的看法？

(1) Darren Ong / Netflix 亞太區政府關係主管

- 臺灣有機會打入全球市場

現在全球市場都需要內容，可謂是內容創造的黃金時期，大家應該一起把餅做大而非急於瓜分市場。其實臺灣也有機會打入全球市場，目前 Netflix 已有超過 100 部臺灣戲劇在全球、亞洲或臺灣播出，且 Netflix 投資的 2 部原創中文戲劇都是來自臺灣。臺灣的發展已較其他東南亞國家良好，雖然業者很多且市場競爭激烈，但這對消費者和產業來說是好事，因為有競爭才有進步。

- 臺灣領先課稅可為全球學習範例

網路無國界，因此，有效的政策模式亦可跨越國界，供各國相互學習。經濟合作與發展組織 (Organisation for Economic Cooperation and Development, OECD) 尚在討論如何課徵數位稅，但臺灣早在 2017 年即開始課稅，Netflix 也繳交 2 年稅賦了，接下來印度、馬來西亞、新加坡、泰國等其他亞洲國家也將陸續推出類似的課稅措施，所以，臺灣可說是全球學習的範例。

- 東南亞國家的業者自律共管模式可供臺灣參考學習

由於信任對 Netflix 來說相當重要，所以，Netflix 在東南亞和 10 家當地及海外業者合作，並與政府討論後，於去年 6 月共同推出自律共管模式，內容包括落實分級制度、遵守版權規定、禁止仇恨內容、強化兒少保護等措施。此模式可供臺灣參考，也希望未來能朝此方向和大家一起努力。

2. 請問政府應從什麼角度來制定網路政策??

(1) 余若凡／國際通商法律事務所 合夥律師

- 網路政策需務實考量有效性與台灣現實處境

制定政策首要釐清政策目的為何，以及要解決什麼問題。有別於過去的傳統產業，網路商業模式的特性是全球化，消費者可以連到全球網站，而國外業者可以不用落地就經營當地市場。以處理盜版問題為例，無論法規多麼嚴苛，只要業者將伺服器置於國外，就會無法可管。再者，政策也是國家競爭力的一環，全球大型網路業者的區域辦公室都已經設在中國大陸、香港、新加坡等地，一旦臺灣再實施不好的政策，將導致外商更不願意來臺。因此，臺灣於制定網路政策時，要考量網路產業特性對法規實施的有效性，以及臺灣的現實處境。

- 贊成低度管理 OTT，提供市場公平競爭環境

現在世界各國都在談論如何管理網路，但真正能夠以法規來規範網路的國家，唯有築起防火牆的中國大陸，即使是印尼、泰國、印度等偏向嚴格管制的國家，也發現嚴管網路的困難。因此，先進國家如美、日、歐盟等都是採取低度管理，且個人也贊成我國《數位通訊傳播法》草案的低度管理精神。

而就 OTT 政策而言，隨著產業變化，不論是對於境內或境外業者、跨足 OTT 的傳統電信公司或原本就是 OTT 產業的網路公司，一個良好的政策應能提供所有人公平競爭的環境，而不好的政策只會帶給合法業者不必要

的負擔，導致非法業者擁有更多競爭利基。

3. 請問對於「歐盟期望未來網路法規應先請益技術專家」的看法？

(1) 黃勝雄／台灣網際網路協會 理事

- 網路政策應回歸政策目標、務實考量，並請益技術專家

網路樣貌變動快速，稍早提到的 10 年前後差異，只是從基礎建設的角度來看，尚未論及應用發展與安全問題。所以，如同余若凡律師所言，制定政策要回歸政策目標並務實考量。以今 (2019) 年 3 月「關注 31 條」網站域名下架事件為例，其實這些內容已經複製到各國不同的頂級域名下，凸顯訂定法規前要詢問技術專家，才能有效執行。

當年網路協定是由一群工程師自行決定，大家沒有預期到今日網路會發展成多樣性的運用，以致中間的網路 (network) 層和上方的應用層是各自獨立。所以，訂定網路法規要了解全球性的技術趨勢，有些事情管得到，有些則管不到或是成本高昂，加上也要符合全球的治理潮流，如此才能提高法規實施的成功機率。

4. 請問「低度管理」是指什麼程度和哪些項目？

(1) 錢大衛／台灣線上影視產業協會 (OTT 協會) 理事長

- 低度管理項目包括消費者權益、著作權、投資本地內容

雖然網路無國界，但由於 OTT 影音的特性是流量很大，如果機房不設在臺灣或不使用臺灣的內容傳遞網路 (CDN)，就會產生頻寬不足網速過慢的問題，由此來看 OTT 影音是可以被管理的。

至於低度管理的項目，包括保護消費者權益 (7 天猶豫期、允許退租、提供當地客服、資料儲存在臺灣)、保障著作權，以及投資本地影視內容。歐盟已透過課徵特別稅來補助當地影視內容發展，此舉可供臺灣參考學習。

(2) 余若凡／國際通商法律事務所 合夥律師

- 低度管理為國際潮流，項目有不當內容、廣告，以及版權

電信產業與有線電視因為歷史性因素而受到比較多的規範管理，因此，當論及 OTT 時，國際上的看法大致可分成 2 種。其一是基於同一市場應採相同法規，而主張加強管理 OTT，支持者如印度、印尼、泰國等。另一種是有鑑於電信產業環境已今非昔比，所以，認為應該重新檢視既有法規並改為低度管理，且改以業務行為而非行業別來做規管，這也是當前的國際潮流。至於比較有共識的管理項目則有不當內容、廣告，以及版權。

(3) 吳國維／NII 產業發展協進會 顧問

歐盟許多專家並不贊成資料在地化，此項政策如同效法中國大陸。

(4) Darren Ong／Netflix 亞太區政府關係主管

- 自製節目問題有待討論，以免導致節目品質下降

針對低度管理項目包含投資本地內容的建議，此問題需要更多討論。現在越來越多節目是跨國產製，例如 Netflix 投資的華語原創影集《彼岸之嫁》，即是橫跨馬來西亞與臺灣的導演、演員和製作團隊。所以，如何認定是本國自製很難定義；而雖然歐盟也有規定 30% 本國自製節目比例，但它是指泛歐盟，而非歐盟各別國家。再者，如果政策目標是要提升節目內容的品質，但是又規定自製比例，其結果就是品質下降，消費者不願意觀賞。因此，制定政策還是應回歸政策目標才能找到合適答案。

(三) 現場交流 (Q&A)

1. OTT 協會是否真的重視消費者權益？多方社群的對話機制是否充足？

(1) 錢大衛／台灣線上影視產業協會 (OTT 協會) 理事長

OTT 協會積極和政府溝通，每個月皆與通傳會、文化部、經濟部智慧局等單位開會，與會者包含產官學界人士。而在消費者保護方面，由於消費者才是企業永續經營的原動力，所以，OTT 協會重視消費者權益，並主

動找消基會討論，同時也鼓勵其會員（業者）修改並提供更佳服務條款³。另外，OTT 協會也歡迎外商 Netflix 入會。

(2) Darren Ong／Netflix 亞太區政府關係主管

Netflix 在臺灣經常和政府部門、OTT 協會、新媒體暨影視音發展協會 (New Media Entertainment Association, NMEA) 開會討論。大家的共識就是消費者是政策決策和服務決策的核心。

(3) 吳國維／NII 產業發展協進會 顧問

不只是 OTT 影音的問題，政府面對網路治理議題時，通常只是在處理發生糾紛的兩造雙方，往往忽略消費者。但其實消費者才是業者收入的來源，如果不重視消費者，他們便會移轉到其他業者的服務。

(4) 余若凡／國際通商法律事務所 合夥律師

保護消費者的定型化契約通常訂得很詳細，例如通知要達 2 次，但是境內業者需要守法，境外業者卻不用；而且將資源用於聘僱更多消保官以處理幾百元的消費糾紛，這樣成本也過高。信任是網路產業的要素，每當業者出現問題時，立即會引發許多負評。因此，政府的角色應是讓資訊更透明，公布惡質業者，後續則交由消費者自行判斷。

2. 身為 ISP 業者不便對本場議題評論，但能否請詹前主委發表看法？

詹婷怡／國家通訊傳播委員會 前主委

過去的電信法規是以核發當地市場執照或特許方式來規管電信產業，但是 OTT 不是一個產業而是一種提供服務的模式，所以，規管方式應該轉換成從資料或行為的角度來看，也可以透過登記制度處理課稅等問題。再

3 消基會於 2019 年 1 月 17 日召開記者會，指出目前收費 OTT 影音所提供的服務方式，如取消與退費等規定，對消費者造成不公，並呼籲業者比照有線電視的定型化契約精神，修正不公平的服務條款，以爭取消費者的信賴。另一方面，政府也要趕緊制定 OTT 影音的定型化契約。

者，網路業者和傳統電信業者的思維不同，他們很重視消費者，也希望能夠建立自律機制和準則。因此，希望大家共同努力，建構一個健康的生態系統，協力訂出不同層次的規範（基本法、準則、常規等），展現業者、消費者、政府等不同社群應有的行為或責任。

三、小結

本場座談討論顯示，與談人一致認為我國 OTT 影音的政策方向應採低度管理，政策內容要能務實考量，並維護市場所有參與者的公平競爭，同時也要重視消費者權益。然而，大家對於低度管理的程度與方式、管理項目，以及保護消費者的做法，則仍存在歧見。相關重點彙整如下表 13 所示。

表13. 「OTT 現狀、治理及未來展望座談」共識與歧見

項目	意見 / 觀點
共識	<ul style="list-style-type: none"> ● 低度管理（政策方向） 與談人皆支持低度管理，其原因包括產業尚在發展階段、順應國際趨勢等。 ● 政策務實 與談人皆認同政策訂定要回歸政策目的，並考量現實情況。部分與談人並指出政策應評估技術層面問題，才能有效執行。 ● 市場公平競爭 多數與談人認為市場應提供所有人公平的競爭環境，不論對象是本土或境外業者、電信商或網路業者。 ● 消費者權益 與談人普遍認同消費者是 OTT 產業的核心，因此，應重視消費者權益。
歧見	<ul style="list-style-type: none"> ● 低度管理的程度與方式 - 國內業者：訂定專法且採強制登記，並可藉由禁用本地機房與頻寬、禁用本地金流、不得上架至本地 APP 商店、不得進行任何行銷宣傳與營業項目等作為懲處。

- 國外業者：希望推動業者自律
- 低度管理的項目
 - 國內業者：在臺設立分公司與本地客服、落實內容分級制度、保護消費者個資且在地儲存、機房設在臺灣、金流在臺灣並繳稅、禁播中國大陸直播的電視頻道、提供一定比例的本國自製內容等。
 - 國外業者：投資本國自製節目的比例仍待討論，以免導致內容品質下降。
 - 法界人士：國際間較有共識的管理項目為不當內容、廣告、版權。
- 是否透過定型化契約保障消費者權益？
 - 國內業者：依據消基會建議，比照定型化契約精神，修改服務條款。
 - 法界人士：定型化契約通常規範過於詳細。政府角色應在於讓資訊透明化，公布惡質業者，後續則交由消費者自行判斷。
- 消費者資料是否應存放在本地？
 - 國內業者：應存放在本地，並要保護消費者個資
 - 技術社群：歐盟許多專家並不贊成資料在地化，否則如同效法中國大陸。

四、會議剪影



照片來源：TWIGF

圖37. 「OTT 現狀、治理及未來展望座談」照片

五、媒體報導



圖38. 「OTT 現狀、治理及未來展望座談」媒體報導

第三節 通傳議題座談：AIoT 時代的安全與隱私挑戰

一、會議資訊

- 時間：107 年 7 月 5 日 (五) 15:15~16:45
- 地點：中華電信總公司大樓 110 會議室
- 會議名稱：「智慧物聯網 (AIoT) 時代的安全與隱私挑戰」座談
- 出席人數：61 人
- 主持人：羅金賢／國家通訊傳播委員會基礎設施事務處 處長
- 與談人：林俊秀／經濟部工業局電子資訊組 組長

林宗男／國立臺灣大學電機工程學系 教授

張保忠／中華電信研究院資安所 所長

熊全迪／理律法律事務所 初級合夥人

二、座談摘要

(一) 主持人引言報告

1. 羅金賢／國家通訊傳播委員會基礎設施事務處 處長

(簡報資料請詳「附件七」)

- AIoT 淪為網路攻擊目標，意在奪取控制權、竊取隱私、中斷服務

根據 IDC (International Data Corporation, 國際數據資訊公司) 2019 年預測，亞洲近年破壞式創新產業第一名是人工智慧 (AI)，物聯網 (IoT) 排名第四；IDC 並推估 2019 年全球 IoT 衍生的商機逼近 1 兆美元，其中關鍵即是 AI 結合 IoT 所形成的 AIoT 新趨勢。然而 AIoT 也容易成為網路攻擊的目標，從 2013 年迄今的攻擊事件時有所聞，攻擊目標包括智慧系統、智慧電網、智慧建築、智慧城市、智慧醫療、智慧交通、智慧零售、智慧工廠、智慧移動，以及智慧家庭。隨著 AIoT 為消費者帶來更多便利性，為產業創造更多新商機的同時，許多實體與資訊安全的疑慮也開始升高，可能導致個資隱私外洩或駭客攻擊，並帶來奪取控制權、竊取隱私、中斷服務等三個面向的挑戰。

- 英、美、日、歐盟與我國皆有 AIoT 資安防護策略

許多國家因此推出 AIoT 資安防護策略，例如英國政府列出一系列 IoT 製造商在設計產品時所須遵循的安全流程；美國實施《IoT 網路安全促進法案》，針對政府採購 IoT 裝置進行規範，且商務部也推出《網路盾牌法案》，鼓勵廠商對其 IoT 商品進行資安分級標章認證；日本則是修改《電氣通信事業法》，要求 2020 年 4 月起連網終端設備須有防範非法登錄功能且獲得

認可才能上市；歐盟更是實施《通用資料保護規範》(General Data Protection Regulation, GDPR)、《消費者物聯網資安指引》、《網路安全法案》、《電子隱私條例(草案)》等相關法規。而我國亦有《國家資通安全發展方案》及《行政院資安產業發展行動計畫》，透過發展產業標準、落實產品認證、實驗場域淬煉、政府媒合助攻等四大策略，保障連網裝置的安全。

- AIoT 產品日漸普及，有賴多方社群對話以提升安全與隱私

AIoT 產品已逐漸打入消費者的生活，IDC 預估 2022 年全球智慧家庭裝置將有近 13 億台。以 2015 年 Amazon 推出的智慧音箱 Echo 為例，每年皆被資安相關單位提出遭到竊聽、個資外洩等安全問題，因此，如何提升 AIoT 產品的安全與隱私已是刻不容緩。OECD (經濟合作暨發展組織) 的資安策略指出，在政策循環中，與非政府機關的利害關係人對話，是制定良好資安政策的關鍵。所以，本場座談特別邀請來自學術界、服務提供商、公民社群、政府機關的代表，共同討論消費者的資安意識、廠商的資安防護、政府的資安策略、數位隱私的落實、資安標章的推廣等五個議題。

(二) 座談討論

1. 消費者的資安意識

- (1) 林宗男／國立臺灣大學電機工程學系 教授

AIoT 在臺灣大量使用的實例為網路攝影機，許多民眾購買後沒有改變預設的密碼，以致駭客不須技巧就可以入侵，所以，我們需要推廣消費者的資安意識。

- (2) 林俊秀／經濟部工業局電子資訊組 組長

消費者通常沒有資安意識，所以，工業局配合行政院資安處辦理提升資安意識活動，例如展示家用網路攝影機遭到入侵的情況。

(3) 張保忠／中華電信研究院資安所 所長

消費者應具備資安意識，了解使用任何軟硬體產品都會有風險，並購買通過安全標章的產品，密碼也要經常更新且使用強勢密碼，而設備移轉或報廢時也要清除資料。

(4) 熊全迪／理律法律事務所 初級合夥人

消費者擔心的是個資外洩，可以降低風險的具體作法包括選擇通過資安標章認證的商品或通過第三方資安制度認證的廠商，以及仔細閱讀廠商的個資使用聲明，萬一有無法認同之處（如將資料分享予關係企業），就不購買這項商品或服務。

2. 廠商的資安防護

(1) 林俊秀／經濟部工業局電子資訊組 組長

工業局推動資安產業發展，重視將安全導入設計 (secure by design)。例如網路攝影機於產品設計時，即要考量不能被輕易地啟動。另一方面，就個別廠商而言，如果不落實資安防護，可能帶來嚴重損失。例如台積電 2018 年 8 月遭到勒索軟體 WannaCry 入侵，損失新臺幣 52 億元。

(2) 張保忠／中華電信研究院資安所 所長

廠商對於資安防護是責無旁貸，中華電信做為產品和服務的提供者，除了落實基礎的資安防護準則，並通過經由公正第三方認證的資訊安全管理系統國際標準 ISO 27001 之外，也奉行 secure by design，在產品的開發流程中，不論是需求規格或設計規格都導入資安，於資料儲存或傳輸時採用加密等方式。而產品銷售前，也會通過政府的認證標章。

3. 政府的資安策略

(1) 林宗男／國立臺灣大學電機工程學系 教授

AIoT 產品的安全度越高，廠商的成本也會增加，而如果消費者選購產

品是以價格為優先考量，廠商就沒有動機提升產品安全。所以，政府的角色相當重要，可以透過立法規範產品須符合安全標準，就如同食品安全標準一樣。美國亦有針對沒有資安的產品祭出裁罰的案例。

(2) 林俊秀／經濟部工業局電子資訊組 組長

政府的資安策略包括人才培訓、產業輔導、拓展國際市場等不同層面。此外，政府單位採購具有資安標章的產品，有助於推廣資安標章，並擴大資安市場。

(3) 熊全迪／理律法律事務所 初級合夥人

政府的角色有兩種。從使用者角度，政府因為採購數量龐大，因此，可以帶頭購買安全的產品，廠商為了接單也會願意提升產品安全；而且政府持有國家重要與機密資料，本來就應使用更安全的產品。另一方面，身為政策的制定者，如同其他與談人所言，政府也可以比照食安，訂定資安的標準。

(4) 羅金賢／國家通訊傳播委員會基礎設施事務處 處長

政府已要求公務單位應採購經認證的產品，目前通傳會與工業局也期能針對常用產品訂出資安技術標準，以納入未來公務採購的規範中。

4. 數位隱私的落實

(1) 林宗男／國立臺灣大學電機工程學系 教授

AIoT 所蒐集的資料究竟屬誰，例如高速公路 ECT (電子收費系統) 所蒐集的行車紀錄是屬於民眾個人或遠通電收公司，此問題需要進一步討論。

(2) 熊全迪／理律法律事務所 初級合夥人

金管會近來正在討論修正銀行業委外雲端業者的相關規則，當中就涉及用戶交易資料的所有權歸屬問題，因為在資料經濟時代，釋出資料可以創造出新的價值。

5. 資安標章的推廣

(1) 林俊秀／經濟部工業局電子資訊組 組長

政府單位採購具有資安標章的產品，有助於推廣資安標章，並擴大資安市場。

(2) 羅金賢／國家通訊傳播委員會基礎設施事務處 處長

資通設備的主管機關包括通傳會（掌管電信終端設備）與工業局（掌管其他資通訊設備）。我國對於藍芽、wifi、手機型式，是採取強制認證，且違者祭有重罰。然而在資安方面，目前先進國家對於資安產品規範多屬於指引性質，沒有採取強制認證，因此，我國也是由廠商自行申請送檢，且迄今申請認證的款式不多。但未來 5G 時代將大量佈建 IoT，如要提升安全性則會增加成本，所以，在安全與成本之間需做取捨。此外，在國際資安認證體系中，還有一個 Common Criteria（安全評估共通準則，ISO/IEC 15408）認證，它是從整個產品的生命週期（研發、設計、製造、銷售）都要檢驗。我國曾申請加入這項國際標準，卻礙於非聯合國國家而未獲通過；另一方面，此項標準的認證費用非常高，是我國網通終端設備廠商難以負擔的金額。

(三) 現場交流 (Q&A)

1. 請問與談人對破壞資安的立法增加(如澳洲的反數據加密法)有何看法?

(1) 羅金賢／國家通訊傳播委員會基礎設施事務處 處長

電信業的主管機關為通傳會，如果是配合《通訊保障及監察法》及其施行細則，電信公司可以提供檢調單位經申請程序的調閱資料。另外，已通過立法的《電信管理法》則是規定業者不能干預與監控通訊內容。而《資安管理法》有規定要處理通報資安事件，涵蓋範圍有政府網路與學術網路，但是用戶端的商業網路就沒有相關法規。我國參考日本作法，成立惡意程式移除中心 (Cyber Clean Center, CCC)，當偵測到民眾的電腦中毒時，

請國內防毒軟體公司通知民眾下載解毒軟體，結果配合者只有 2 成多。儘管如此，未來如要民眾清除電腦病毒，避免淪為網路攻擊的跳板，仍需凝聚社會共識才能立法。

(2) 張保忠／中華電信研究院資安所 所長

針對檢調單位索取資料，中華電信一切依法處理。至於政府能否偵測個人裝備並通知中毒等問題，恐怕民眾會懷疑是駭客展開社交工程。而預留後門程式供政府使用，則是仍有爭議，美國政府曾要求解開重犯的手機內容，但是遭蘋果公司拒絕；中國大陸製造的產品也是因為被懷疑提供中共存取，而被一些國家或人士拒買。

(3) 熊全迪／理律法律事務所 初級合夥人

如前面與談人所提，現行法規已經允許基於犯罪偵查的通訊監察。至於是否應訂定商業網路的資安法規，則要在打擊犯罪、國家與公眾利益、人民基本隱私權等各種權益之間，做利害關係的權衡。

(4) 林宗男／國立臺灣大學電機工程學系 教授

針對國家政府基於反恐而要求預留後門程式，從技術觀點來看，由於恐怖威脅不可能停止，所以，是否立法涉及價值取捨與國家信任的問題。

(5) 林俊秀／經濟部工業局電子資訊組 組長

有關日本法規允許政府登入民眾連網設備以提醒保護該裝置⁴，由於日本的民族性是群體主義，民眾認為此事屬於公眾利益，因此，才訂定此項法規規範。

2. 請問與談人對服務提供者濫用資料、駭客蒐集數位足跡並發動攻擊看法？

4 根據本場座談主持人羅金賢處長的簡報資料，日本於 2019 年 2 月啟動 NOTICE 計畫，允許隸屬於日本總務省的 NICT (National Institute of Information and Communications Technology，國立研究開發法人情報通信研究機構) 於監督下，以產品原密碼和弱密碼登入民眾的 IoT 設備，並把可登入名單交給相關網路服務商，提醒消費者保護該裝置。

(1) 羅金賢／國家通訊傳播委員會基礎設施事務處 處長

通傳會對電信業監管嚴謹，業者不能違反個資法，且在資訊傳遞過程中，亦受到《電信管理法》有關業者不能監控內容等規範。而免費 APP 確實有過度要求資料權限的問題，民眾應具備使用免費軟體的風險意識，如果擔心個資隱私問題就不要點選「同意」並下載使用。

(2) 林宗男／國立臺灣大學電機工程學系 教授

AIoT 時代要保有隱私是越來越難，即使不是重要人物，數位足跡也會被 cookie 追蹤紀錄，因為成本相當低廉。而國家也難以制定隱私保護法規，美國甚至還有提供肉蒐的商業服務，加上技術面也無法給予民眾保護，因此，大家要提高警覺。

(3) 林俊秀／經濟部工業局電子資訊組 組長

我國個資法對於資料的蒐集、處理、利用，甚至是補償，都有相關規範。而數位足跡已被歐盟 GDPR 和日本法規視為個資，因此，屬於受到保護的項目。

(4) 張保忠／中華電信研究院資安所 所長

中華電信有強大的個資防禦系統與管理制度，產品於設計階段即考慮安全問題，完成後還做白帽駭客測試，可說是竭盡所能在保護個資。另外，中華電信也曾分析幾款市售常用手機，結果發現所有手機都有安全問題，差別只是嚴重程度不同，所以，消費者一定要有資安意識。

(5) 熊全迪／理律法律事務所 初級合夥人

有關服務提供商濫用個資問題，其實個資法對於使用目的與範圍，都有相關規定，且主管機關也可以指定各行業做安全維護計畫，例如通傳會指定電信業、金管會指定銀行業、教育部指定補習產業等。至於駭客的入侵，刑法也有妨害秘密罪等相關規範。

三、小結

綜合本場座談的討論與交流，可發現與談人一致認為消費者應該具備購買安全性產品等資安意識，而政府亦可透過訂定資安標準及帶頭示範採購安全性產品等方式，推動 AIoT 的安全與隱私，且多位與談人也提出廠商應從產品開發設計即將安全納入考量。不過，在政府能否基於資安或國安而偵測民眾的裝備，或要求產品預留後門程式方面，與談人則持有不同意見。另外，部分與談人也指出需討論 AIoT 所蒐集資料的歸屬權問題。相關重點如下表 14 所示。

表14. 「AIoT 時代的安全與隱私挑戰座談」共識與歧見

項目	意見 / 觀點
共識	<ul style="list-style-type: none"> 消費者的資安意識 資安風險無法完全消除，故消費者應具備資安意識，重點包括：購買安全性的產品（產品具有安全標章或業者通過第三方安全認證）、經常更新密碼、閱讀廠商的個資聲明(如不同意則不要使用該產品) 等。 政府的資安策略及資安標章的推廣 政府可以仿照食品安全，訂定資訊安全的標準；並發揮帶頭示範作用，採購安全性的產品。 廠商的資安防護 產品從開發設計之初，就應將安全問題納入考量。
歧見	<p>政府能否基於資安或國安而偵測民眾裝備，或要求產品預留後門程式？</p> <ul style="list-style-type: none"> 中立：需做利害關係的權衡取捨。 反對：日本案例實屬特例（民族性為群體主義）、可能引發社交工程及政府監控的疑慮。
個別建議	<ul style="list-style-type: none"> 數位隱私的落實 資料經濟時代，AIoT 所蒐集的資料歸屬權問題，有待進一步討論。

四、會議剪影



照片來源：TWIGF

圖39. 「AIoT 時代的安全與隱私挑戰座談」照片

第四節 國際參與分享會議：臺灣、亞太與全球的焦點議題

一、會議簡介

(一) 會議簡介

- 時間：108 年 9 月 17 日 (二) 15:00~17:00
- 地點：IEAT 會議中心 1 樓咖啡廳 (臺北市松江路 350 號)
- 講者：本計畫人員、研習營優秀學員、本計畫及其他 APrIGF 與會者
- 主題簡介與議程 (表 15)

盛夏時節之際，美、德、法、南韓等國家陸續舉辦了網路治理論壇 (Internet Governance Forum, IGF)，各國網路相關的各界人士齊聚一堂，共同討論自己國家當前所面臨的網路公共政策挑戰。根據聯合國統計，去年

全球已有 80 個國家召開「國家型 IGF」，凸顯在網路引領我們邁向智慧化生活的數位時代，如何把握網路與新興科技發展所帶來的創新契機，同時因應所衍生的安全、隱私、人權、民主、壟斷等各種衝擊，已經成為世界各國高度關切的問題。

當然，臺灣也有「國家型 IGF」，也就是臺灣網路治理論壇(TWIGF)，而且已經舉辦 5 個年度了。今年大會主題為「建立開放、包容、信任、創新的數位社會」，活動已於 7 月上旬圓滿落幕，現場可說是冠蓋雲集，且吸引近 300 人實地與會。

「國家型 IGF」之所以蔚為風潮，其實是源自聯合國 IGF。聯合國早從 2006 年起，就每年舉辦 IGF，推動全球的所有多方利害關係人(multi-stakeholder)，也就是政府、民間企業、技術社群、公民團體，共同針對影響網路發展與使用所涉及的法規、經濟、社會文化、關鍵網路基礎建設等層面問題，進行交流對話，期望藉此能強化全球網路安全穩定地持續運作。

儘管 IGF 會後不會形成國際規範或公約，但是這種多方社群以開放透明且平等方式共同商討網路政策的做法，意外地帶動「國家型 IGF」與「區域型 IGF」的興起。「區域型 IGF」同樣根據聯合國統計，目前全球共有 17 個，而在亞太地區即為亞太網路治理論壇(APrIGF)。今年 APrIGF 為第 10 屆會議，已於 7 月中旬在海蔘威召開，大會主題為「為亞太地區所有人提供安全與普及的網路」。

至於開山始祖的聯合國 IGF，今年即將邁入第 14 屆，訂於 11 月底在柏林舉辦，大會主題為「一個世界，一個網路，一個願景」，德國總理梅克爾也透過宣傳影片，邀請全球的多方社群報名參與。

本場分享會將掌握 2019 年網路治理年度盛會的精彩重點，除了回顧 TWIGF 的討論成果，以及分享 APrIGF 的亞太各國觀點之外，還將展望聯合國 IGF 的焦點議題。

表15. 「臺灣、亞太與全球的焦點議題」分享會議程

時間	主題	講者
14:40-15:00	報到&茶點	--
15:00-15:20	2019 臺灣 TWIGF 精彩回顧	梁理旋／NII 協進會 副執行長、TWIGF 秘書處 彭正文／中華電信法律事務處 工程師
15:20-16:20	2019 亞太區 APrIGF 參與分享	吳國維／NII 協進會 顧問、TWIGF MSG 主席 呂忠津／清華大學電機工程系 教授 鄭嘉逸／資策會科法所 專案經理 陳之亭／彰化師範大學英語系 學生 薛福仁／橙迅科技公司 工程師
16:20-16:40	2019 聯合國 IGF 展望：從巴黎到柏林	吳國維／NII 協進會 董事、TWIGF MSG 林郁敏／NII 協進會 資深經理
16:40-17:00	QA 與交流	--

(二) 活動宣傳

本次座談建置活動網站 (<https://www.nii.org.tw/events/igf19/>)，提供會議簡介、議程、會場與交通等資訊，以及線上報名功能。



圖40. 「臺灣、亞太與全球的焦點議題」分享會網站頁面

宣傳方式包括透過臺灣網路治理論壇 (Taiwan IGF) 臉書社團 (約有 2,750 位成員) 發佈活動訊息、發文至通傳會與致電邀請相關部會人員，以及寄發 email 給網路治理活動的訂閱者。

(三) 出席概況

本次會議共計包括通傳會、交通部、外交部、學者、研究人員、產業界人士、大專學生等共 44 人報名，最後雖然僅有 23 人到場，但與會者在問答時間踴躍提問與發言，互動交流熱絡。

二、會議摘要

(一) 2019 TWIGF 精彩回顧

1. 梁理旋 / NII 產業發展協進會副執行長

今年 (2019) TWIGF 擴大舉辦規模，兩日的活動中，同一時段有三場座談平行進行，而開幕典禮後的共同會議則是邀請日本專家進行網路歷史趨勢的專題演講，以及舉辦兩場專題會議，邀請國內外多方利害關係人分別討論數位平臺信任度和 OTT 的治理。今年共有 16 場座談，88 位講者，兩日的參與人數共約 450 人。所有座談皆由社群自行提案，經多方利害關係人指導小組 (MSG) 評選後產生大會議程，重點主題包括數位內容產業侵權、市場競爭、新興科技的隱私和資安等議題，其中人工智慧和假訊息也是今年 APrIGF 的熱門議題。另外，還有來自國際組織 ICANN (網際網路名稱與號碼指配組織) 和 ISOC (網際網路協會) 的提案。

TWIGF 強調每個場次的與談人來自不同的利害關係人族群，包括政府、學術機構、技術社群、公民團體和民間企業，透過特定議題的討論，不論是達成共識或產生歧見，皆可做為日後更深入探討的基礎。

2. 彭正文 / 中華電信法律事務處工程師

- 域名「下架」與網站「封鎖」面面觀

ISP 業者收到政府公文須執行域名下架或網站封鎖，從技術層面來看，困難度很高，也會造成許多副作用，而內容過濾牽涉到言論自由，更須審慎執行。處理盜版問題上，英國採用網站封鎖的方式，美國則是禁止廣告商於盜版網站安插與播放廣告以阻斷金流，國內目前尚在討論引進網路中介者治理模式。

- 數位匯流時代之隱私議題

數位匯流時代要保護個人隱私，又要促進資料自由流通，有時候會形成拉鋸戰。各國的個資法規不盡相同，例如，臺灣有《個人資料保護法》，美國則沒有專法來保護個資，但其《電信法》針對電信業者使用消費者個資有其限制，除非符合法律規定或取得客戶同意，否則僅能在提供電信服務的範圍內使用客戶資訊，但若移除客戶識別資訊，則可在電信服務目的之外做使用。另外，歐盟的 GDPR 對個資使用有嚴格的規定。

(二) 2019 亞太區 APrIGF 參與分享

1. 吳國維／NII 協進會顧問、TWIGF MSG 主席

- APrIGF 之「分享亞太國家 IPv6 布署經驗」座談

此座談由本人提案並擔任主持人。由於 IPv4 位址已幾乎用罄，而 IPv4 和 IPv6 的網路系統又是獨立互不相容，因此，從 IPv4 轉移到 IPv6 的速度越快越好，對電信業者和網路內容提供者都有益處，可省下維護 IPv4 的成本。臺灣 IPv6 的生態系統可分為使用者裝置、行動網路供應商和 ISP 業者，以及內容供應商等三大類別。十年前使用者裝置已完成 IPv6 的布署，前五大內容供應商也幾乎布署完成，最後只剩下 ISP 的問題要解決，因為在臺灣只要將手機的 IPv6 打開後，IPv6 的布建率即躍升為全球第 9 名。此經驗可與其他國家分享。

2. 呂忠津／清華大學電機工程系教授

- APrIGF 之「IoT 安全—消費者的差異」座談

本次出席 APrIGF 主要擔任 IoT 座談的與談人，並分享臺灣相關經驗。我國的「民生公共物聯網」為一整合空氣品質、地震、防救災、水資源等民生四大領域的資料服務平臺，將環境監測所收集的資料，提供政府、民間企業、NGO 組織和所有民眾使用。這些設備和工具（如監測器、感應器等）依靠網路相互連結，因此，必須考量資通安全，而我國也有 IoT 設備相關的資安標準與標章。

雖然 IoT 為人類生活帶來便利，但是由於 IoT 裝置數量過多又缺乏安全控制措施，易遭駭客作為攻擊目標，因此，如何保護消費者的隱私權和個資安全，成為討論重點。消費者在 IoT 的市場中看似弱者，但是集結起來的力量可以很大，透過抵制可迫使業者對產品的安全性做改善。

3. 鄭嘉逸／資策會科法所專案經理

- APrIGF 之「在資訊洪流時代因應錯誤訊息：誰該負責？」座談

今天主要分享 APrIGF 有關不實訊息/錯誤訊息/假新聞的座談討論。社群媒體是傳播假新聞的主要來源，因為免費、容易取得，以及與生活息息相關。假新聞可以蓄意製造出來，如北馬其頓的一個小鎮專門製造假新聞影響美國大選，另一種是藉由無意間的分享而傳播錯誤訊息。雖然政府可以因為政治或國安需求封鎖網路、關閉網站或規範假新聞，但是長久之計仍須培養閱聽人的素養，讓他們有判斷新聞可信度高低的能力。此外，未來也許可以利用 AI (人工智慧) 檢測假新聞，但目前 AI 的準確性仍受到質疑。

4. 陳之亭／彰化師範大學英語系學生

今天分享 APrIGF 的 2 場座談討論重點。

- APrIGF 之「科技巨頭無所不在：這是網路的未來？」座談

科技巨頭是否壟斷市場造成危害？這些企業是否大到不能倒？透過立法規範阻擾其營利行為，是否會影響其員工生計和旗下產業，進而影響科技發展？又規模龐大是否為邪惡的代表？市占率高是否就是壟斷？與談人們對上述問題沒有共識，但普遍認同消費者必須積極提高意識，讓業者了解所提供的服務是有限度的，不可過度蒐集使用者的個資並做服務以外的用途。另外，整體網路市場應該更多元化，政府需要對科技巨頭做適當的規範，讓中小企業能同時蓬勃發展。

- APrIGF 之「為 ICT 法規研究和資料庫建立擘劃亞洲藍圖」座談

本場座談邀請來自中國、韓國、俄羅斯和印度的講者分享各國的 ICT 法律和資料庫。中國有 3 個網路法庭，但缺乏資料保護法；韓國網路定罪必須要有明確的證據；俄羅斯在 2015 年網路使用人口達到 7 成後才開始有網路相關規範，並展開網路審查制度；印度代表則介紹南亞 ICT 法律的歷史和一個名為 Cyrilla 的資料庫。

5. 薛福仁／橙迅科技公司工程師

今天主要分享 APrIGF 的參與觀察，以及有關語言多樣性的座談討論。

- 參與觀察

就個人觀察，青年參與網路治理論壇遠比技術性論壇的熱度低，可能的因素為缺乏背景知識，以及沒有立即可回收的效益。另外，本次 APrIGF 柬埔寨的講者分享提升數位能力、減少數位落差的經驗，臺灣其實也有執行類似的計畫，但卻沒有人能在 APrIGF 發表，這是相對可惜。

- APrIGF 之「亞太地區語言多樣性：數位落差的挑戰」座談

亞太區有多樣性的語言，但網路使用的語言仍以英語為優先。該場次論及因搜尋引擎和技術困難的關係，很多語言是無法放在網路上，使得母

語為非英語族群的文化較難對外傳播。此外，在地內容不夠充足也是另一大因素。

(三) 2019 聯合國 IGF 展望：從巴黎到柏林

1. 林郁敏 / NII 產業發展協進會資深經理

第 14 屆聯合國 IGF 訂於 2019 年 11 月 25 日至 29 日於德國柏林舉辦，主辦單位為德國聯邦經濟暨能源部。大會主題為「一個世界，一個網路，一個願景 (One World. One Net. One Vision)」，會議場次超過 150 場。

就會議類型來看，則可分成主要會議 (Main Sessions)、座談 (Workshops)、動態聯盟 (Dynamic Coalitions)、開放論壇 (Open Forums)、最佳典範論壇 (Best Practice Forums)、國家區域 IGF (National and Regional IGFs, NRIs) 等類別。當中的座談是開放給全球申請，今年共有 431 件申請案，最後有 65 件獲得通過，討論議題依會議三大主題可歸納簡述如下：

- 資料治理：討論 AI、人權、個資、跨境資料流通等議題
- 數位包容：討論低度開發國家、偏鄉地區、弱勢族群的上網等議題
- 安全，保全，穩定及強韌：討論假訊息、違法內容、兒少保護等議題

主要會議由 IGF 的多方利害關係人諮詢小組 (MAG) 主辦，本次將討論治理與數位合作、AI 責任、極端內容等議題；動態聯盟由 IGF 的網路中立、平臺責任等 18 個動態聯盟申辦；而最佳典範論壇是 MAG 通過的年度計畫，如 IoT 與大數據及 AI、網路安全等，且最後會提供建議供大家參考；國家區域 IGF 由多個 NRIs 合辦，本次討論網路人權、資料保護等議題；開放論壇只有政府單位和國際組織可以申辦，如這次德、英、中等國政府與歐盟執委會，以及 OECD (經濟合作暨發展組織)、ISOC (網際網路協會) 等組織都有申辦，議題則包含網路自由、AI 責任、個資保護等。

法國總統馬克宏於 2018 年 IGF 致詞時表示，我們需要「歐洲式」的網

路治理模式，並提出《巴黎籲請信任與安全的網路空間》(Paris Call for Trust and Security in Cyberspace) 倡議，吸引全球超過 520 個政府、企業與國際組織簽署。而今年主辦國的德國總理梅克爾將發表什麼談話，又聯合國「數位合作高階工作小組」提出的「2020 年全球數位合作承諾」是否會獲得全球多方利害關係人的普遍認同，這些也是 2019 年 IGF 可以關注的焦點。雖然臺灣不是聯合國的會員國以致我們無法親臨現場與會，但是仍可透過線上系統同步參與會議。

(四) 現場交流 (Q&A)

1. 若想實際參與 APrIGF 卻缺乏資金，除了網路治理研習營之外，還有別的補助或獎學金可以申請嗎？
 - 吳國維顧問：許多網路治理相關組織，如 APIGA (亞太網路治理學院)、APrIGF、APNIC (亞太網路資訊中心)、ICANN、IGF，皆有提供獎學金，只要符合相關規定即可申請。非常鼓勵大家參加會議，因為除了 IGF 之外，這些組織都開放臺灣的參與，可和其他國家的與會者平起平坐，但是要了解參加的目的究竟為何。
2. 請問優秀學員持續參加網路治理活動的動力是什麼？
 - 陳之亭：由於網路治理是以多方利害關係人模式，由下而上的方式進行討論，開放所有人的參與，因此，可了解各國觀點，並與其他國家交流臺灣的經驗和技術。
 - 薛福仁：參與網路治理活動可以學習別國經驗，也將臺灣解決問題的方法推展到國外，技術的推廣是不受國界的限制。
3. 其他線上提問問題



資料來源：Slido 網站

圖41. 「臺灣、亞太與全球的焦點議題」分享會線上提問

三、小結

本次會議主要分享 2019 APrIGF 的討論重點，並簡介 TWIGF 與 IGF 的討論議題。整體來看，臺灣、亞太、聯合國的三個論壇皆討論新興科技衍生的隱私與安全、AI 倫理、假新聞等治理議題，凸顯網路無國界，各國也面臨許多共同的治理挑戰，有賴透過國內外多方利害關係人的共同討論，才能找出最佳解決方案。另外，與會者也問及參與的動力與補助等問題，顯示本次會議有助於提升部分與會者對網路治理的參與興趣。

四、會議剪影



圖42. 「臺灣、亞太與全球的焦點議題」分享會照片

參考文獻

- Ministry of Economic Affairs and Climate Policy (2018)。Roadmap for Digital Hard- and Software Security。
<https://www.government.nl/documents/reports/2018/04/02/roadmap-for-digi>

tal-hard--and-software-security

- ETtoday 新聞雲 (2018)。ET 民調／時代的眼淚 台灣 OTT 取代電視了嗎？ 2018/3/2。 <https://www.ettoday.net/news/20180302/1122503.htm>
- Unwire Pro (2019)。歐洲電信標準協會訂立全球物聯網安全標準。科技新報，2019/2/26。
<https://technews.tw/2019/02/26/etsi-global-standard-for-consumer-iot-security/>
- 文化部 (2016)。「政府如何因應 OTT 產業新發展趨勢報告」。立法院第 9 屆第 2 會期，教育及文化委員會第 6 次全體委員會議。
<https://mocfile.moc.gov.tw/files/201611/2ca24aad-12cc-4618-a1d7-c077a25b8bb9.pdf>
- 王宏仁 (2019)。「【資安大師觀點】 Bruce Schneier：萬物都是電腦，所有事也都變成了資安事」。iThome，2019/4/7。
<https://www.ithome.com.tw/news/129804>
- 林妍臻 (2018) 加州通過第一個 IoT 裝置安全法。iThome，2018/10/1。
<https://www.ithome.com.tw/news/126165>
- 消基會 (2019)。你追劇嗎？OTT 正夯，主管機關在哪裡？2019/1/18。
https://www.consumers.org.tw/contents/events_ct?id=1443
- 通傳會 (2017)。「《數位通訊傳播法》(草案) 說明」。
https://www.ncc.gov.tw/chinese/files/17012/3864_36859_170124_1.pdf
- 通傳會 (2018)。「107 年匯流發展調查結果報告」。
https://www.ncc.gov.tw/chinese/files/19012/4007_40972_190129_6.pdf
- 陳炳宏 (2019)。「〈財經週報-封面故事-隱私篇〉暗藏後門？用戶資料恐被看光光」。自由時報，2019/3/18。
<https://ec.ltn.com.tw/article/paper/1274888>
- 陳計策、賴宛靖 (2018)。「迎接 AIoT 智慧時代」。工業技術與資訊月刊，頁 18~21。
https://www.itri.org.tw/chi/Content/Publications/Book_abstract.aspx?&SiteI

D=1&MmmID=2000&CatID=620610314656502404&SYear=2018&MSID=777744404135653461

- 資策會 (2019)。AIoT (人工智慧 + 物聯網) 平台應用程式開發養成班。
<http://taipei.iiiedu.org.tw/training/aiot.html>
- 劉麗榮 (2019)。OTT 若涉國安疑慮 NCC：用技術讓它沒有收看品質。
中央社，2019/3/18。
<https://www.cna.com.tw/news/firstnews/201903180181.aspx>

第六章 參與國際會議

第一節 2019 亞太區網路治理論壇 (APrIGF)

一、會議簡介

(一) 會議背景

亞太區網路治理論壇 (Asia Pacific Regional Internet Governance Forum, APrIGF) 為亞太地區網路治理政策討論、意見交換、促進合作的平臺，以推動亞太地區網路治理的發展為目標，自 2010 年起已分別於香港、新加坡、東京、首爾、德里、澳門以及臺北舉辦，每年皆吸引亞太地區二十多國的 2~3 百位產官學研界、公民團體及民間非營利機構人士的參與。

多方利害關係人模式是 APrIGF 的核心原則，並著重於參與者的多樣性與討論議題的開放性；每年 APrIGF 的大會主題與各個座談場次，皆為公開徵求並由多方社群代表共同決定，會議結束後並彙整成綜合報告 (Synthesis Document)。

(二) 會議資訊

2019 APrIGF (第 10 屆) 於 7 月 16 至 19 日在俄羅斯海參崴舉辦，主辦單位為 .RU 頂級域名協調中心 (the Coordination Center for TLDs .RU/.PФ)，共吸引來自 30 個國家地區的約 180 人與會。

本次大會主題為「為亞太地區所有人提供安全與普及的網路」(Enabling a Safe, Secure and Universal Internet for All in Asia Pacific)，座談主題涵蓋下列六大類別：

- 網路安全與法規
- 連網與普及通用

- 新興科技與社會
- 網路人權
- 網路治理角色演進與多方利害關係人參與
- 數位經濟

APrIGF 的會議型式包括會前入門課程、正式會議、週邊會議等，本年度的正式會議共計 28 場，議程請詳 <https://2019.aprigrf.asia/prog/?p=prog>，本計畫人員吳國維顧問所參與之場次如下表 16 所示。

表16. 2019 APrIGF 參與場次

主題	場次名稱
開幕	Opening Ceremony 開幕典禮
	Plenary Session- Internet Governance in Asia Pacific: The State of Play and Outlook 大會專題座談-亞太區網路治理之現況與展望
網路安全 與法規	WS. 20 Cyber Norms in Asia-Pacific 亞太區的網路規範
	WS. 48 A Roadmap for Studying ICT Laws and Building a Database for Asia 為 ICT 法規研究和資料庫建立擘劃亞洲藍圖
	WS. 12 Coping with Misinformation in an Era of Information Deluge: Who is Responsible? 在資訊洪流時代因應錯誤訊息：誰該負責？
連網與普及通用	WS42. Sharing IPv6 Deployment Experiences among Asia Pacific Countries 分享亞太國家 IPv6 布署經驗
新興科技 與社會	WS. 30 The Ethics behind Computing Machines: Raising Awareness of Digital Talents 電腦設施背後的道德：提升數位人才的認知
	WS. 22 IoT Security – a Differentiator for Consumers IoT 安全—消費者的差異

主題	場次名稱
網路人權	Merger 3 Online Resistance Movements and Political Organising against and Countering Hate Speech in Asia 亞洲對抗仇恨言論的網路運動與政治動員
數位經濟	WS. 23 Big Tech Everywhere: Is this the future of the Internet? 科技巨頭無所不在：這是網路的未來？
閉幕	Closing Plenary 閉幕典禮

(三) 與會人員與目的

本計畫共計 3 人飛抵海參崴參加 2019 APrIGF，包括吳國維顧問，以及 2019 與 2018 網路治理研習營優秀學員各 1 名。吳國維顧問並主持「分享亞太國家 IPv6 布署經驗」會議，及擔任「提升科技人對道德設計的認知」會議與談人，而 2 位優秀學員從各場座談中也學習更多網路治理相關知識及議題觀點，並與亞太區的多方社群交流互動，深化未來持續參與國內外網路治理的知識技能及興趣熱忱。

本節主要摘要吳國維顧問所參與的會議場次重點內容。至於 2 位優秀學員的參與情況與心得，請詳「附件八：研習營優秀學員 2019 APrIGF 出國報告」。

二、重要討論

(一) 開幕典禮暨大會專題座談

1. 聯合國 IGF 秘書處代表 Mr. Chengetai Masango

Mr. Masango 表示，雖然亞太各國的網路普及率差異很大，但大家的共同目標都是希望利用 ICT 產業以實現永續發展。不過，網路的濫用行為也帶來許多負面的社會影響。面對這些挑戰，並無一體適用的解決方案，除了使用多方利害關係人模式外，還必須有跨領域（跨學科）的討論。

2. APrIGF MSG 主席 Mr. Rajnesh Singh

Mr. Singh 表示，現今處在網路治理的十字路口。一方面是網路基礎建設、服務或應用層面，都面臨網路分裂的情況；另一方面則是網路市場出現集中化的現象，少數大企業掌控許多網路基礎建設和服務。此外，數位落差的討論再度成為重點，世界有一半的人口尚未能連網，5G 技術的出現可能加深經濟、社會和數位素養的不平等，因為有些發展中國家無法獲得或負擔得起這樣的基礎建設。

3. 大會專題座談：Internet Governance in Asia Pacific: The State of Play and Outlook

「亞太區網路治理的現況與展望」專題座談是由亞太頂級域名協會 (APTLD) 總經理 Mr. Leonid Todorov 主持，與談人包括 ICANN 代表、印度和亞美尼亞的公民社群代表、薩摩亞政府代表，以及南韓和菲律賓的學術界代表。

與談人們針對網路治理領域中，目前各社群最關切的議題與趨勢發表意見。ICANN 代表表示，如何保護網路的核心並使其安全穩定，以及如何維護網路衛生 (cyber hygiene) 是重點項目，還有網路治理須結合多方利害關係人模式和多邊模式。亞美尼亞公民社群代表指出，他們重視的是網路的普及性、多語化、數位素養，尤其是確保老年人皆有能力獲得網路所提供的服務和資訊。印度公民社群代表表示，至 2021 年印度的網路使用人口將超過 6 億，但印度過時的網路安全法案無法處理現今的網路治理議題；她並認為應該釐清網路治理的定義，讓大眾了解其所牽涉的廣泛領域。

薩摩亞政府代表說明該國正進行政府數位化和數位改造，也將成立電腦網路危機應變小組，希望建立一個安全的網路環境，以促進企業和觀光發展。南韓學術界代表則提及南韓為全球網路普及率最高的國家之一，而亞洲又是全球經濟的中心，使用多方利害關係人模式來處理網路治理問題是非常重要的。菲律賓學術界代表認為，必須提升民眾對網路治理的意

識，促進網路普及，並透過教育鼓勵創新。而 yIGF (青年網路治理論壇) 即是一項很有意義的計畫，鼓勵學生參與網路治理的討論，進而改變世界。

(二) 網路安全與法規

1. WS48. A Roadmap for Studying ICT Laws and Building a Database for Asia

「為 ICT 法規研究和資料庫建立擘劃亞洲藍圖」座談由印度進步通訊協會 (APC) 申辦並由其代表主持，與談人包括印度和南韓公民社群代表、俄羅斯技術社群代表，以及中國大陸學者。

中國大陸學者表示，中國政府已經制定一些重要的資通訊法律，如電子商務法和網路安全法，目前缺乏的是全面性的資料保護法。南韓公民社群代表認為，韓國的法律混淆網路基礎設施和內容的管理，以致造成寒蟬效應。主持人也表示，目前許多網路法律不僅更嚴格限制言論自由和其他權益，而且也祭出更嚴厲的懲罰，甚至使用多重條款來定罪，而且國家之間還會相互學習和複製立法。

印度公民團體代表則介紹一個開發中的免費線上資料庫 Cyrilla，記錄亞洲各國有關數位權益的立法和判例資料，並分析重大法律條款，讓人權倡議者、研究人員和律師可相互學習。

2. WS20. Cyber Norms in Asia-Pacific

「亞太區的網路規範」座談由澳洲戰略政策研究所 (ASPI) 申辦並主持，與談人包括我國台灣經濟研究院助理研究員陳映竹、APNIC (亞太網路資訊中心) 代表、印尼學術界代表、澳洲政府代表等。由於有多位與談人是透過遠端參與，因此，會議也同時開放現場的臺下與會者參與討論。

主持人表示，聯合國政府專家小組 (GGE) 於 2015 年即提出《網路空間負責任的國家行為規範》(Norms of Responsible State Behavior in Cyberspace)，要求各國政府不得故意破壞資通訊基礎建設及其所提供的公

共服務，以及於確保資安的同時，必須兼顧保護網路人權、數位隱私、言論自由等。不過，南韓學者認為，這項在聯合國框架下所制定的國際規範不夠透明，但要套用多方利害關係人模式也有困難，因為網路安全常被視為政府的權責。而其他與會者亦回應表示，應透過多方利害關係人參與討論，才能成功建立並實施網路規範。台經院助理研究員陳映竹則表達臺灣因為不是聯合國成員而無法共同參與制定網路規範的遺憾，並指出亞太國家通常藉由法令管控科技，因此，不容易發展出所謂的規範。

而吳國維顧問認為，必須先釐清網路規範的定義，不可混淆 norm (常規) 和 regulation (法規)。他表示，norm 通常不具約束力，它代表的是一個群體的共識和理解，但現在許多國家已經朝向訂定更嚴格的規範來限制網路空間的行為，若再賦予 norm 制裁的能力，將對網路世界和全球社會帶來負面的影響。但 APNIC 代表提出不同看法，他認為網路的生態系統十分複雜，網路規範和國際法的意義可能有部分重疊，有時候規範會變成法律，而有些法律也是始於規範，因此，重點在於兩者該如何運作。

3. WS12. Coping with Misinformation in an Era of Information Deluge: Who is Responsible?

「在資訊洪流時代因應錯誤訊息：誰該負責？」座談由印度公民社群 CCAOI (印度網路咖啡協會) 申辦並主持，與談人包括南韓學術界代表、Diplo 基金會印尼代表，以及尼泊爾、巴勒斯坦和澳洲的公民代表。

主持人分享印度在 2019 年普選後，社群媒體、平臺業者和政府，透過能力建構和事實查核，來改善假訊息的傳播；另外，修訂中介機構的責任法規也是另一種因應措施。但巴勒斯坦代表表示，自阿拉伯之春後，許多中東國家政府更嚴格控制資訊流通，如埃及政府可以輕易封鎖發布假新聞或仇恨言論的社群媒體帳號。尼泊爾代表也指出政府加強對媒體控制的問題，並建議透過業者自律和學習最佳典範來因應。澳洲代表亦對內容封鎖、斷網等問題表示擔憂，並強調政府採用任何法規之前，都應與所有利

害關係人討論。印尼代表則認為，網路內容的分類應有更詳細的討論，如假新聞、錯誤訊息、異議和仇恨言論，皆需明確定義。

而臺下與會者也紛紛提出看法，包括本計畫研習營優秀學員陳之亭分享臺灣 LINE 推出自動機器人「美玉姨」打擊網路謠言，以及其他與會者提出只靠 AI 等科技無法抑制假新聞的傳播、演算法存有歧見、監控訊息會破壞言論自由等。最後，與會者皆同意，所有利害關係人都有責任遏止假新聞的散佈，且決策者、執法者和社會大眾都需加強相關的能力建構。

(三) 連網與普及通用

1. WS42. Sharing IPv6 Deployment Experiences among Asia Pacific Countries

「分享亞太國家 IPv6 布署經驗」座談由本計畫吳國維顧問申辦並擔任主持人，與談人包括亞太網路資訊中心 (APNIC) 總裁 Paul Wilson、日本網路供應商協會 (JIPA) 代表，和尼泊爾技術社群代表。

吳顧問分享臺灣 IPv6 布建率如何從 2017 年 12 月的 0.03% 躍升到 2019 年 7 月的 36.77% (世界排名從第 64 名攀升到第 9 名)。他表示，行動網路供應商是關鍵因素，只要手機開啟 IPv6 預設連網後，便可大幅提升布建率。目前臺灣使用者裝置和前五大內容供應商的 IPv6 布署幾乎都已完成。

Mr. Wilson 則指出，提升 IPv6 布建率的因素可能還包括同業競爭帶動發展，以及 IPv6 性能比 IPv4 良好，且不需使用昂貴的 CGNAT (電信級網路位址轉換器) 等。他並表示，APNIC 測量結果顯示全球 IPv6 使用率已達到 25%，而 APNIC 也會致力於技術能力建構，協助其會員布建 IPv6。

日本 JIPA 代表說明日本一開始是因為政府施壓而推動 ISP 業者布建 IPv6，接著再推廣到網路業者。他也指出，為了讓 IPv6 轉換順暢，電信業者不會告知消費者相關訊息，以免造成消費者的疑慮或擔憂。

(四) 新興科技與社會

1. WS30. The Ethics behind Computing Machines: Raising Awareness of Digital Talents

「電腦設施背後的道德：提升數位人才的認知」座談由印尼大學申辦，與談人包括印尼和新加坡學術界代表、南韓技術社群代表，以及本計畫吳國維顧問。

吳國維顧問表示，道德標準並非固定不變，社會規範會隨著時代的創新而改變，道德標準也會受到質疑和挑戰。他也認為，軟體工程師並非全無道德設計的概念，有些企業在招募工程師時會訂下特定的道德守則。

印尼學術界代表指出，IEEE (電機電子工程師學會)等技術組織皆發布AI設計的道德準則，然而要讓它成為日常實踐卻相當不易，或許置於技職和大專院校的課程中會較有成效，且訓練時採用跨領域方式，讓學生從法律、傳播、心理和企業的角度學習道德設計，更能達到全面性的理解。

南韓技術社群代表則認為，要求機器承擔責任的可行性不高，因為雖然數據和學習過程是由人類提供與設計，但是機器的流程與細節都在無法公開 (涉及商業機密) 的黑盒子中。

臺下的日本學者也分享個人看法，他認為隨著道德不斷更新變動，我們需要學習的特定議題也越來越多，例如如何在程式中定義性別等，甚至從學程的基礎課程就得開始接觸這些議題。

2. WS22. IoT Security - a Differentiator for Consumers

「IoT 安全—消費者的差異」座談由網際網路協會 (ISOC) 申辦，主持人和與談人包括巴基斯坦和澳洲技術社群代表、yIGF 代表，以及我國清華大學電機系呂忠津教授。

呂忠津教授表示，IoT 的安全風險從最底部的感應器層、中間的網路層，到最上方的應用層都有，例如設備遭病毒入侵、網路被 DDoS (分散式

阻斷服務) 攻擊、應用程式介面 (API) 遭攻擊。因此，各國也紛紛推出加強 IoT 的安全措施或計畫，如英國的消費者 IoT 安全實踐準則 (Code of Practice for Consumer IoT Security)、我國的民生公共物聯網計畫等。

澳洲技術社群代表則指出，任何違法監視竊聽他人通訊及蒐集個資，都違反《聯合國人權宣言》的隱私權和言論自由權，也與民主社會的原則相抵觸。但是，目前許多消費性 IoT 產品，不論是有意或無意，經常洩漏使用者的行蹤或個資、竊聽記錄他們的對話，或有安全漏洞危及人身安全，這些都違反人權宣言。可惜技術社群的成員大多不在乎隱私權問題。

而 yIGF 代表認為，科技創新發展，以及安全、隱私和道德標準，兩邊存在不平衡的關係，儘管有法律框架保護消費者，但消費者本身也應負起責任，閱讀產品說明書並了解其安全性和弱點，不能只期望科技帶來方便，卻不負起保護自身安全的責任。

(五) 網路人權

1. Merger 3 Online Resistance Movements and Political Organising against and Countering Hate Speech in Asia

「亞洲對抗仇恨言論的網路運動與政治動員」座談由數位權益基金會 (DRF) 申辦，進步通訊協會 (APC) 的代表主持。本場會議是由主持人帶領臺下與會者分組討論的方式進行，討論問題如什麼是仇恨言論、又如何判斷、如何成功煽動仇恨活動等。討論結果與主持人總結可歸納如下：

- 由於「仇恨」一詞具有強烈的情感意涵，在不同的情境、文化或脈絡下，要能理解和辨識仇恨言論有其難度，因此，目前國際間對其定義仍無共識，在亞洲也沒有任何國家將仇恨言論視為犯罪行為。
- 散佈不實訊息可能引起民眾恐懼或分化族群，進而煽動仇恨活動，但如能集結群眾力量並透過各式媒體傳播正確資訊，將可以反制或反轉仇恨言論。

- 亞洲為世界上種族、宗教、經濟發展程度最多元化的地區，仇恨言論也更加普遍，且可能導致暴力行為，但網路科技卻允許少數族群被邊緣化。因此，在制定網路政策時，除了討論仇恨言論的定義、審查制度和言論自由的規範之外，同時也要研議對民間企業究責。

(六) 數位經濟

1. WS. 23 Big Tech Everywhere: Is this the Future of the Internet?

「科技巨頭無所不在：這是網路的未來？」座談由網際網路協會(ISOC)申辦並主持，與談人包括印度和日本技術社群代表、南韓學術界代表等。

印度技術社群代表指出，網路在應用或傳輸層面都因為科技巨頭掌握市場，而讓消費者的選擇變得有限，且產生隱私和安全疑慮，但其部份原因來自消費者只追求便宜和便利，導致市場更趨於集中化。南韓學術界代表認為，企業因行銷等商業需求而蒐集消費者資訊是可以接受的，但服務條款必須以淺顯易懂的文字，讓消費者知道哪些資訊被蒐集與如何使用。日本技術社群代表則表示，科技巨頭可以提供良好且穩固的服務，但他們也希望這些大企業的運作模式能更加透明和多元化。

本計畫吳國維顧問亦主動發言分享看法。他表示，網路市場由少數企業支配的情形並不同於壟斷，且壟斷也不全然是有害的，重點在於如何訂定管理機制，讓科技巨頭除了追求獲利之外，也為公共利益服務。與談人之一的日本技術社群代表也回應指出，須有公正的衡量標準來判斷科技巨頭是否造成網路集中化，測量方法有直接量測（如市場占有率）和間接量測（如生態系統中的多元性）等。

三、小結

(一) 東南亞國家熱衷參與 APrIGF，我國也應展現積極參與

近年來，東南亞國家非常熱衷參與 APrIGF，尤其今年 (2019) 座談場

次至少有 6 成是由這些國家主辦，其中印度主辦的場次即高達 6 場（共 25 場）；另外，菲律賓每年也派送十多名大學生參與 yIGF。因此，我國也應該展現積極參與，促進網路治理政策的對話與交流。

（二）掌握國際趨勢方向，為政策研擬鑑往知來

APrIGF 為亞太區網路治理政策相互交流與學習的平台，因此，本屆論壇各場次對治理議題所提出的主張或建議，也有諸多值得我國參考之處。例如：網路空間國際規範的制定應有多方利害關係人參與；改善 AI 道德設計準則難以實施的問題可從大學教育著手；應檢討當前許多消費性 IoT 產品侵犯隱私與人權問題；網路市場集中化的優劣尚無定論但需討論如何管理市場；亞洲亦有仇恨言論氾濫問題，需從定義開始討論並訂定治理政策。

四、會議剪影

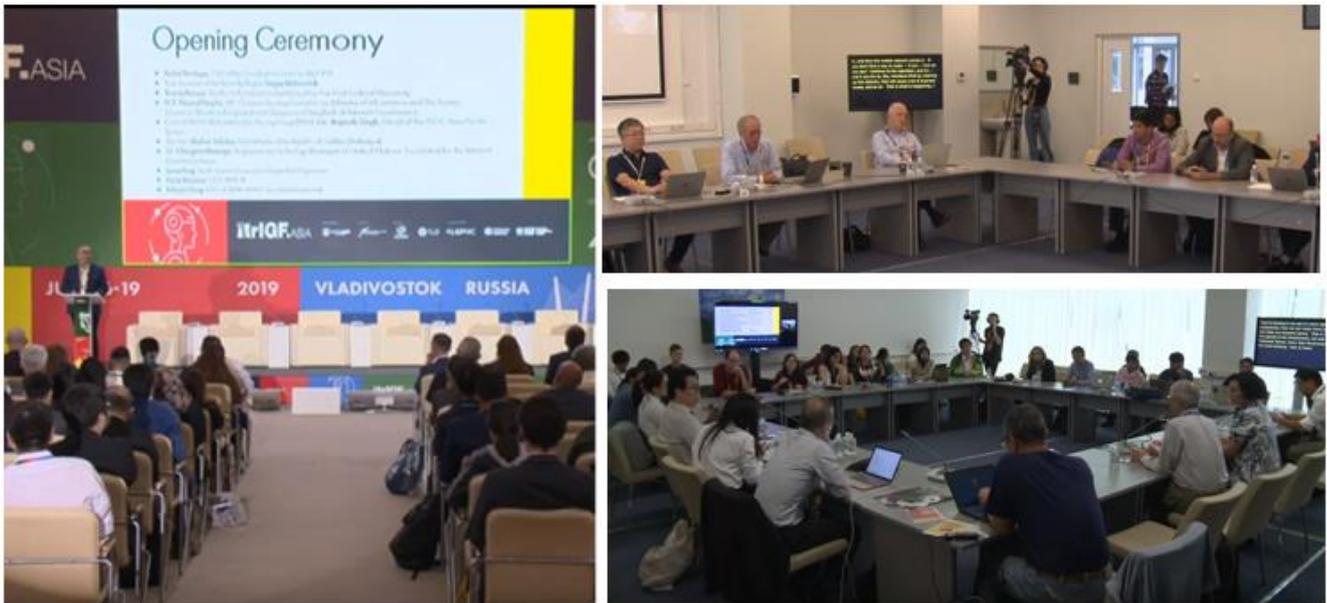


圖43. 2019 APrIGF 會議剪影

第二節 2019 聯合國網路治理論壇 (IGF)

一、會議簡介

(一) 會議背景

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或發表談判結果，但是卻能促進多方社群的討論互動，以及典範實務的分享交流。因此，除了各大洲與各個國家紛紛見賢思齊地舉辦多方論壇，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 作為全球多方社群平等參與網路政策討論的平臺地位。

(二) 會議資訊

第 14 屆 IGF 於 2019 年 11 月 25 日至 29 日於德國柏林召開，主辦單位為德國聯邦經濟暨能源部，會場設於 Estrel 會議中心，共計有來自全球 161 國、超過 3,600 人與會，遠端參與人數也約 3,000 人。

本次大會主題為「一個世界，一個網路，一個願景」(One World. One Net. One Vision)，討論主題涵蓋「資料治理」、「數位包容」、「安全、保全、穩定與強韌」三大類別。

IGF 的會議型式包括主要會議(Main Sessions)、分場座談(Workshops)、開放論壇(Open Forums)、最佳典範論壇(Best Practice Forum, BPF)、動態聯盟(Dynamic Coalition, DC)等。本年度共約 200 場會議，議程請詳 <https://igf2019.sched.com/>。本計畫人員遠端參與場次如下表 17 所示。

表17. 2019 IGF 遠端參與場次

主題	場次名稱
開幕	Opening Ceremony 開幕典禮
主要會議	Internet Governance and Digital Cooperation 網路治理與數位合作
	Applying Human Rights and Ethics in Responsible Data Governance and Artificial Intelligence 在負責任的資料治理和 AI 中納入人權與道德
	Governance Challenges in the Digital Age: Finding New Tools for Policy-Making 數位時代的治理挑戰 - 找尋政策制定的新工具
	Legislative Main Session 立法會議
資料治理	OF. 25 Technological Innovation and Challenges to Data Governance 科技創新和資料治理的挑戰
	OF. 18 Personal Information Protection 個人資料保護
安全、保 全、穩定 與強韌	OF. 6 ICANN - DNS, Threats and Opportunities 網域名稱系統的威脅與機會
	WS. 41 Tech Nationalism: 5G, Cybersecurity and Trade 科技國家主義：5G、網路安全和貿易
	WS. 59 Digital Sovereignty and Internet Fragmentation 數位主權和網路分裂

(三) 參與方式

本次會議由計畫團隊透過網路遠端參與，以了解當前全球最關切的網路治理議題及其討論重點，進而提供我國現階段與未來網路治理相關政策的參考建議。

二、重要討論

(一) 開幕典禮

1. 聯合國秘書長 Antonio Guterres

現今網路世界冒著地緣政治破裂、貿易安全和網路系統嚴重毀壞的風險，以及圍繞 5G 技術的政治角力，有些國家一方面建立日益嚴格的網路國界，另一方面也不斷增加跨境網路攻擊的次數。IGF 應提升為全球首要平臺，讓各方利害關係人共享政策專業、辯論新興技術議題，最終就基本原則達成共識。聯合國數位合作高階小組 (UN High Level Panel on Digital Cooperation, UN HLPDC) 將指派科技特使與各政府、企業和公民團體合作，幫助促進國際框架的建立。

2. 德國總理 Angela Merkel

全球網路變得脆弱不穩，一旦分裂，中伊等國將築起高牆，其他國家也會在選舉或社會動盪時關閉網路，或強化對公民的監控及網路審查，剝奪人們獲得資訊和通訊的基本權利。因此，我們必須捍衛網路的自由與人權，反對獨裁政權對網路施加政治與思想箝制。

多邊主義 (multilateralism) 是政府間合作的傳統方式，面對網路分裂的情況日益嚴重，必須擴大多邊方式，重新思考全球網路的治理結構，修改網路治理的監管框架，才能保護網路這項公共財。但網路的未來不能僅由國家政府來決定，網路議題影響每個人的生活，因此，需要採取多方利害關係人的方式。

(二) 主要會議

1. Internet Governance and Digital Cooperation

「網路治理與數位合作」場次是由 IGF 多方利害關係人諮詢小組 (MAG) 主席 Lynn St. Amour，和巴西大使暨前聯合國加強合作工作小組 (WGEC) 主席 Benedicto Fonseca 共同主持，與談人包括德國聯邦經濟事務與能源部副局長 Daniella Brönstrup，以及聯合國秘書長執行辦公室策略協調助

理秘書長 Fabrizio Hochschild。

本場會議主要聽取與會者對 UN HLPDC (聯合國數位合作高階小組) 於今年 (2019) 6 月發布成果報告的評論與意見。報告內容包括如何利用數位科技實現聯合國永續發展目標 (SDGs) 等議題，並為推動全球數位合作提出三個方案：IGF Plus、分散式共同治理架構、數位評論員，且建議採用當中的 IGF Plus 模式，並於 2020 年聯合國建立 75 周年簽署「全球數位合作承諾」。

Hochschild 表示，目前以國家或區域法規因應個資隱私、言論自由、網路安全的巨大挑戰，導致法規衝突和網路分裂 (成為美、中主導兩種網路)，進而可能破壞網路自由開放的本質。Fonseca 指出，當前需要發展國際法律框架，但過程中會受到國際政治力量，及擔心破壞市場自由和人權的干擾。

多位臺下與會者則是表達支持 IGF Plus 模式。德國學者暨全球網路空間穩定委員會 (Global Commission on the Stability of Cyberspace, GCSC) 委員 Wolfgang Kleinwächter 進一步表示，國際網路事務已有十多個國際政府間組織作為決策單位，如安全方面有 UN GGE (聯合國政府專家小組)、經濟議題有 WTO (世界貿易組織)，因此，IGF Plus 模式應加強討論平臺和這些決策平臺之間的互動連結。

2. Applying Human Rights and Ethics in Responsible Data Governance and Artificial Intelligence

「在負責任資料治理和人工智慧中納入人權和道德」場次是由南方網路治理學院 (South School of Internet Governance) 學術總監 Olga Cavalli 和 Diplo 基金會 (DiploFoundation) 資安總監 Vladimir Radunovic 共同主持，與談人包括日本政府官員、聯合國人權辦公室代表、IEEE (電機電子工程師學會) 代表、梵諦岡神學家、微軟公司代表等人。

Cavalli 說明許多組織和團體已針對 AI 發展如何兼顧道德和人權，建立

道德指南和原則框架，這些框架大致包含開發 AI 演算法時應以人為中心，保障人類的尊嚴、安全和公正性；在開發過程要更當責、負責任和透明化；找出解決當前鴻溝，以及賦權給使用者和提供勞工適當技能的機制，並強調多方利害關係人合作的重要性。

日本政府官員表示，負責任和可信賴的 AI 除了要以人為本、穩定、易於理解，也要具有包容力。IEEE 代表指出，如果決策者自己無法掌控會對某人造成傷害的決策，此即為不負責任。梵諦岡神學家認為，開發者使用資料庫時，即會被過去的偏見所影響。微軟公司代表表示，AI 應該是讓大眾受益的工具以及成為解決方案的一部分，而不是問題的來源。而 Diplo 基金會代表則建議企業，實施人權影響評估和專業審查，如此可在 AI 發展中獲得競爭優勢。

但聯合國代表強調，當務之急是有效協調現有框架，找出尚未充分解決的問題和未來可行的方向。另外，也有與會者認為，應該重視資料的治理與共享，因為資料是 AI 的推動力。最後，與談人普遍認同，AI 的責任主要在於企業與技術社群，但媒體、學術界、使用者也需要承擔責任。

3. Governance Challenges in the Digital Age: Finding New Tools for Policy-Making

「數位時代的治理挑戰－找尋政策制定的新工具」場次是由聯合國秘書長辦公室政策顧問 David Kelly 主持，與談人包括剛果政府暨 OECD 代表、公民社群--全球數位夥伴 (GPD) 代表、國際組織－國際商會 (ICC) 代表等人。

OECD 代表表示，數位科技可用於促進政策的討論和相關利害關係人的參與，且我們需要在網路普及化上做更大努力，以提升參與的包容性。公民社群 GPD 代表認為，利害關係人團體應由對該議題有充分理解的專家來帶領，雖然政策制定應打破各部門獨立進行的穀倉式(silo)運作方式，但仍須在各部門間建立以專家為導向的網絡，且越是複雜的問題越是需要多

方利害關係人的參與。而國際商會 (ICC) 代表則強調，管理利害關係人的期望和互動性的重要，才能進行成功且具有成效的政策討論。

4. Legislative Main Session

「立法程序」場次是本屆 IGF 首創，期望能將 IGF 討論成果帶給各國立法機構，讓其採取後續具體的行動。

各國議員首先分享他們在這次會議聽到的討論重點，如德國議員分享有關 AI 議題的討論，並指出各國的目標不應只在成為 AI 科技的領導者，而是要針對 AI 的共同標準、道德價值和技術原則建立國際協議；而埃及議員則建議，應制定有助於量化網路空間和平與衝突的指標。

整體而言，各國議員關注以人為本且民主的 AI 發展、維護網路自由開放的國際合作、保護關鍵基礎建設安全、維護數位時代的國際和平、網路是民主的工具或陷阱等議題，也深刻了解各國政府的決策會影響全球網路能否維持自由開放且不分裂，以及網路政策需從整體生態系統角度來研議。

最後，與會的 56 國議員共同發表一份參與訊息/公報 (Message)，文中並對各國議員提出以下建議：

- 針對網路相關的政策議題加強國際合作與交流。
- 確保提升國安與促進數位經濟的新立法將會充分保護人權與自由。
- 以因應數位時代挑戰的精神重新思考現有的國家法律。
- 訂定新法案時，會充分包含各社群 (透過公聽會與公開質詢程序) 並推動多方利害關係人方法。
- 推動成立非正式的「議會 IGF 小組」，以強化議員於 IGF 對話。

(三) 資料治理

1. OF. 25 Technological Innovation and Challenges to Data Governance

「科技創新和資料治理的挑戰」開放論壇是由中國大陸國家互聯網信息辦公室（簡稱網信辦）以及中國大陸網路空間研究院主辦，與談人來自法國、中國大陸、新加坡、巴西的技術社群、政府、學術界和企業等多方利害關係人代表。

中國大陸網信辦代表表示，以數據為導向的新技術（如 AI、5G 和大數據）對全球網路治理體系和規範產生深遠的影響，政府單位也須更新其資料治理框架，特別是在網路安全和資料保護方面，以面對隨之而來的挑戰。巴西學者則是提到金磚五國的加強數位合作，並認為這些國家所採用的新資料保護框架，不僅對一般用戶有利，而且也為企業提供更多信任和可預測的環境。

但新加坡學者指出，目前出現的「三大數位王國」（中國大陸、美國和歐盟）各有不同的政策利益，且對如何處理網路監管也形成明顯的對比。法國技術社群代表也認為，未來幾年內網路可能將更加分裂，因此，應加強數位合作，解決因新科技發展和數位創新所帶來的挑戰。

2. OF. 18 Personal Information Protection

「個人資料保護」開放論壇是由中國大陸國家互聯網信息辦公室主辦，與談人包括中國大陸學者與新浪網等企業代表，以及德國微軟公司代表等人。

本場次主要交流國際上保護使用者隱私權的經驗和方式，並將討論重點放在中國大陸立法框架，以及該國為促進使用者權利的措施。中國大陸學者解釋，中國民法中有關人格權的草案已進入三讀和公共諮詢階段，隨著社會經濟不斷數位化，法律必須和科技發展與時俱進，該法律為確保人格尊嚴和合理的生活品質提出重要措施，也將隱私和可識別的個人資料作出區隔。

中國大陸新浪網代表指出，企業蒐集個資時須遵守同意原則，而使用

時須優先考量國家安全、主權和穩定。德國微軟代表則說明 GDPR 於保護個資與隱私所扮演的重要角色，並指出微軟亦有隱私原則，讓全球用戶能掌控其個資。

(四) 安全、保全、穩定與強韌

1. OF. 6 ICANN - DNS, Threats and Opportunities

「網域名稱系統的威脅與機會」開放論壇由 ICANN 董事 Chris Disspain 主持，與談人包括 ICANN 主席暨執行長 Göran Marby、董事長 Maarten Botterman、董事 Becky Burr 與 Ron da Silva，以及技術長 David Conrad。

與談人皆同意 DNS 安全威脅是 ICANN 目前面對的關鍵議題之一。ICANN 持續密切關注可能影響 DNS 應用的新興科技，如 IoT、5G 等科技應用及商業模式。許多與會者關心 DNS over HTTPS (DoH)、DNS over TLS (DoT) 等新 DNS 安全技術協定的問題，表示這是除了國家主導的網路分裂外，另一種由企業主導的網路分裂型態，但 ICANN 會議中卻缺乏相關討論。ICANN 技術長 Conrad 回應，ICANN 社群中確實有 DoH、DoT 的討論，但這些技術協定依使用情境、各國法律規範不同，產生的後續效應也不同，深入討論容易牽涉無關 DNS 的議題，超出 ICANN 的權責範圍。

不少人也關注最近網際網路協會 (ISOC) 計畫將.ORG 頂級域名註冊管理機構 Public Interest Registry (PIR) 售予私人企業的事件。由於此事發生於 ICANN 與 PIR 更新合約及取消.ORG 註冊價格調漲限制不久，眾人質疑兩起事件的關聯性，並認為 ICANN 有責任介入。ICANN 執行長 Marby 回應，董事會及 ORG 在 ISOC 公告前，都對這筆交易一無所知。他雖承諾 ICANN 董事會與 ORG 都會由自身權責角度介入調查此事，但也建議與會者，ISOC 有眾多員工也出席本次 IGF，大家可以直接向 ISOC 了解內情。

若干與會者提出，ICANN 社群中各利害關係團體的權力分配不均，某些團體說的話比其他團體更有分量。主持人也同意這是 ICANN 必須改善

的問題，但 ICANN 董事長 Botterman 認為 ICANN 的多方利害關係治理模式已是目前能達到的最佳制衡體系；執行長則強調，有動機、長久持續參與的團體聲量較大是無可避免，所以應鼓勵更多人參與 ICANN，透過實際投入議題討論，改變不平衡的現況。

2. WS. 41 Tech Nationalism: 5G, Cybersecurity and Trade

「科技國家主義：5G、網路安全和貿易」座談是由美國喬治亞理工學院網路治理計畫(IGP)創辦人 Milton Mueller，和瑞士蘇黎世大學教授 William Drake 共同主持，與談人包括澳洲政府官員、德國和印度學者，以及華為美國公司代表等。

主持人 Mueller 和 Drake 首先提及當前把網路安全和政府問題混為一談的現象，並指出這種發展可視為一種推翻電信業自由化的趨勢。德國學者認為，科技民族主義可視為政府面對新技術不確定性的一種方式，其根本考量在於不同司法管轄權的問題，而非資料儲存在哪裡的問題。

澳洲政府官員則指出，政府處理網路空間相關議題的方式有了轉變，科技現今已成為地緣政治的中心，因此，澳洲禁用華為 5G 設備是出於國安考量，避免日後須替換基礎建設而對國家產業造成毀滅性的影響。但是華為美國公司代表駁斥表示，政府機構可以對華為的產品進行驗證，並強調必須平衡國家安全、網路安全和貿易創新。

德國學者進一步表示，5G 供應商的主要問題之一，是信任以及伴隨原產國的定義。他並以美國為例，指出史諾登 (Snowden) 事件後，美國情報業務更加透明，反而幫助美國科技公司重獲國際市場的信任。

3. WS. 59 Digital Sovereignty and Internet Fragmentation

「數位主權和網路分裂」座談是由美國喬治亞理工學院網路治理計畫(IGP)創辦人 Milton Mueller 和瑞士蘇黎世大學教授 William Drake 共同主持，與談人包括 Google 代表 Vint Cerf、中俄和埃及學者、巴西政府官員、

歐洲電信網路營運商協會 (ETNO) 代表等人。

Drake 表示，全球網路的概念和國家在網路空間行使主權的趨勢，造成不斷升高的緊張局勢，且如同國安議題，許多國家認為行使主權比其他政治問題更為重要，一些西方民主國家甚至也開始援引數位主權。對此，中國大陸學者指出，儘管許多國家捍衛資訊自由流通，但仍有例外的情況，如中國大陸是為了社會穩定，歐盟和美國則分別基於隱私保護和國家安全的理由。

Cerf 認為，網路原本應是一個不受政府規管的自由主義者的空間，而即使政府要行使主權，也應明訂是在哪一層網路架構，並要考量如電纜等基礎設施已明確分派予相對應的管轄範圍。巴西政府官員則指出，網路源自主權工具和美軍的通訊工具，而今權力和利益都集中在少數美中兩國企業，要停止網路分裂和網路主權的發展趨勢，必須瓦解這些科技巨頭。

埃及學者表示，資料在地化是網路分裂的來源之一，並認為 GDPR 造成有條件的資料流通。但 ETNO 代表並不認同 GDPR 會導致網路分裂，只是她也強調，在經貿協議中納入資料自由流通條款的重要性。另外，俄羅斯公民團體代表也說明俄羅斯網路主權法案 (Sovereign Runet) 的影響，它讓俄羅斯聯邦政府可對該國的網路訊務行使主權並控制網路空間。

總結來說，與談人們普遍認為國際法可避免國家法規產生相互矛盾，進而嚴重影響網路的本質。不過，對於哪種法規應被視為行使主權，以及在不影響網路本質下可允許行使主權到何種程度，與談人則是沒有共識。

三、柏林 IGF 公報 (Berlin IGF Messages)

為了呈現本年度 IGF 的討論結果，大會針對 3 大主題類別，根據各場會議主辦單位的會後報告與現場討論，彙整成重點結論——柏林 IGF 公報 (Berlin IGF Messages)。以下為摘要簡介，詳細內容可至 <https://www.intgovforum.org/multilingual/content/berlin-igf-messages> 下載。

(一) 資料治理

1. 跨境資料流通與發展

將多種法律和監管框架套用在跨境資料，可能會動搖全球以資料為導向的供應鏈，對社會經濟和創新發展產生不利的影響，且限制言論和集會自由，並帶來安全風險。發展普遍認可的價值觀和原則有助於建立大眾對跨境資料流通的信心，帶來社會經濟效益，幫助中小企業在其他國家市場拓展事業。

2. 資料是社會經濟的重要資源

公共服務要以人為本和以資料為導向，服務的設計要確保多元參與和透明度。永續發展和保護基本權益應為決策的整體目標。必須發展全球和國家型的資料治理，不能只讓科技巨頭受益於資料的使用，且中小企業也要能共享資料，同時免於受到資料外洩和隱私權迫害的風險。

3. 資料治理、道德與基本權益

在匿名的大數據集使用 AI，會去除匿名性並識別出特定的個人，因此開發演算法時，須在用於善途的資訊和用於侵犯基本人權的資訊上，取得平衡。此外，具有資料互通性的協定必須是資料治理模式的一部分。

(二) 數位包容

1. 具包容力的網路普及

發展數位基礎建設不應犧牲其他的實體基礎建設。由當地建立和管理的社區網路不僅有助於網路普及，加強社會聯繫和當地經濟，更可實現永續發展目標。為改善失能者的連網經驗，必須就通用設計原則達成共識，使用 ICT 技術幫助失能者突破通訊和連網障礙，加強其移動力並促進獨立生活和社會融合。

2. 發展數位包容和創新所需的技能

數位技能和素養是達成數位包容不可或缺的要素。學校教育、培訓課程和網路治理學院是網路發展、政策和法規等多元領域中，建立知識以及培養領導能力的有效平臺，因此，多方利害關係人的能力建構需要更多資源。AI 引起許多新的社會挑戰並影響勞動力市場，需要制定更具包容力的政策和法規，確保未來的工作市場能讓婦女和弱勢族群維持生計。

3. 社會和經濟包容、性別平等與人權

向社群媒體課稅會限制人們的日常通訊，並非國家獲得收入的有效方式。善用科技創新才能降低數位、社會和經濟分歧，包容弱勢族群的討論必須是網路治理和公共政策對話的中心，解決方案必須切實可行，並從性別角度考慮基礎建設和連網問題。

4. 當地內容和語言多樣性

推廣全球通用 (Universal Acceptance) 和國際化域名 (Internationalized Domain Names, IDNs) 需要多方利害關係人的參與，以及政府以身作則使用 IDNs。保護文化遺產和當地內容需要當地社群的積極參與，以及永續的基礎建設，讓人民可以藉由創造內容為生。

(三) 安全、保全、穩定和強韌

1. 保全和網路安全

解決仇恨言論是所有利害關係人共同的責任，使用不同的機制或工具不應妨礙人們對仇恨內容的理解。網路安全、人民基本權益和自由可以共存，但是當需要權衡優先考量安全問題時，必須是合法並符合比例原則。國際多方利害關係人社群必須準確定義有關不實訊息和干擾選舉過程議題的範圍和術語，並對可接受和負責任的行為達成共識。實現網路安全需要多方利害關係人的參與，產業行為者必須探究蒐集和共享資訊實際可行的方式，以預防網路濫用。

2. 基礎建設的安全

目前解決非法或濫用內容的趨勢是取消、轉移、刪除或暫停域名，雖然快速簡便，但並非移除惡意內容的長期有效方式。網路平臺業者和內容供應商應與執法機構合作，提供預防措施的資訊。決策者和相關行為者應透過多方利害關係人合作關係，了解解決措施在技術上的可能性和局限。

3. 政策與合作

多方利害關係人和跨領域方式有助於建立社群支援的網路安全規範，必須加強協作以發展和執行政策解決方案，也必須發展具包容力和尊重人權的規範。

4. 能力建構

當網路使用者了解危機和風險的存在、自身的權益，以及學習如何採取行動時，才會成為負責任的使用者。網路安全培訓和能力建構可讓包含弱勢和邊緣族群在內的使用者，有能力捍衛其人權和確保其網路活動的安全。透過採取有意義的行動，和不同的多邊、雙邊或區域型倡議和論壇，各國和多方利害關係人之間可建立關係、交流經驗並學習創新方法，來改善全球生態系統的安全。

四、小結

(一) 關注 IGF Plus 模式發展，為全球數位合作貢獻心力

今年 (2019) IGF 大會主題為「一個世界，一個網路，一個願景」，凸顯當前全球網路因為許多國家主張網路主權、各國網路法規衝突等因素，而面臨網路分裂的危機，這也是今年許多場次不斷討論的問題。因此，如何透過國際合作以維護全球網路的自由開放，已成為當務之急。而在全球專家所提出的國際合作模式中，又以在現有基礎上強化具體產出的 IGF Plus 模式獲得廣泛支持，因此，我國應密切關注其後續進展，適時為推動

全球數位合作貢獻一份心力。

(二) IGF 首度強調議員參與，56 國議員建議值得我國學習參考

由於各國法規衝突也是導致全球網路分裂的主要風險，因此，為了能讓 IGF 討論成果在各國立法機關發揮作用，本屆論壇首度為立法人員舉辦專屬場次，且共有 56 國議員參與，他們除了深刻了解各國的立法決策會影響全球網路能否維持自由開放外，也共同發表對各國議員的建議，包括針對網路相關的政策議題加強國際合作與交流、確保提升國安與促進數位經濟發展的新立法將會充分保護人權與自由、以因應數位時代挑戰的精神重新思考現有的國家法律、訂定新法案時會充分納入各社群並推動多方利害關係人方法等。這些建議充分反映當前網路政策與立法所需的基本精神，值得我國政府部門與立法單位參考並學習。

五、會議剪影





照片來源：ECO Association; GIP Digital Watch

圖44. 2019 IGF 會議剪影

* 本計畫於 2019 年 12 月 12 日下午 2 點至通傳會報告 APrIGF 與 IGF 參與心得及重要討論議題，並由吳國維顧問擔任講者。

第七章 治理議題分析

第一節 全球主要討論議題

聯合國 IGF 堪稱全球規模最大的網路治理議題交流平臺，不但每年的年度論壇皆有超過上百場由全球多方利害關係人申辦的各式會議，而且還吸引超過 2 千位來自全球各界人士的現場與會。因此，IGF 的會議議題可以充分反應當時全球主要討論議題或全球的議題趨勢。

2019 年 IGF 的各式會議共計超過 150 場，本節將從中彙整歸納出目前全球主要討論議題。

一、專家精選議題：AI 治理、內容治理、網路分裂、合作與發展...

IGF 年度論壇的大會主題、討論議題的主題類別，以及主要會議 (Main Sessions) 是由其多方利害關係人諮詢小組 (Multistakeholder Advisory Group, MAG) 訂定與主辦。MAG 成員由來自全球約 50 位多方利害關係人的專業人士組成⁵，因此，這些主題與會議可代表全球專家選出的當前重要議題。

2019 年 IGF 大會主題為「一個世界，一個網路，一個願景 (One World. One Net. One Vision)」，凸顯專家們認為當前全球網路面臨分裂的重大挑戰，並期許能透過大家共同努力，維護全球單一網路的持續運作。而討論議題的主題類別包含資料治理、數位包容、安全和保全與穩定及強韌 (Security, Safety, Stability & Resilience，以下簡稱安全穩定) 3 大類。主要會議則有下表 18 所列的 AI 治理、內容治理(極端內容)、合作與發展等 10 場。

5 MAG 成員由來自全球五大洲的 50~55 位多方利害關係人代表，包括政府部門、公民團體、民間企業、技術及學術社群的代表共同組成。候選人須先由機關團體或個人提名，經遴選後，最後由聯合國秘書長任命。MAG 成員的任期為一年，但可延長任期，也可重複參選。

表18. IGF 2019 專家精選的討論議題

2019 大會主題「一個世界，一個網路，一個願景」凸顯網路分裂的重大挑戰		
主題類別	主要會議名稱	討論議題
資料治理	<ul style="list-style-type: none"> • 將人權與道德套用於負責任的資料治理與 AI • 數位連網世界的資料自由流通、ICT 產品與服務議題 	<ul style="list-style-type: none"> • AI 治理 (人權、道德、責任) • 跨境資料(流通)
數位包容	<ul style="list-style-type: none"> • 新興科技及其與包容、安全、人權的介接 	<ul style="list-style-type: none"> • 普及上網等
安全穩定	<ul style="list-style-type: none"> • 因應線上暴力極端內容：權力、責任、回應與風險 • 保護連網的萬物 • 網路治理與數位合作 • 在數位時代達成永續發展目標 • 動態聯盟：共同努力達成永續發展目標 • 數位時代政策制定的跨領域框架 • 立法會議 (Legislative Main Session) 	<ul style="list-style-type: none"> • 內容治理(極端內容) • 網路安全(IoT 安全) • 合作與發展 • 合作與發展 • 合作與發展 • 政策制定 • 政策制定

* 以上會議由本計畫依據 IGF 2019 Themes 進行分類，大會並未就此做主題分類。

二、政府關切議題：AI 治理、內容治理、個資保護、網路人權...

各國政府關切的議題可從 IGF 的開放論壇 (Open Forums) 加以觀察，因為開放論壇只供全球政府單位和國際組織申辦。

2019 年 IGF 開放論壇共有 34 場，當中有 15 場是由政府單位及政府間國際組織主辦 (下表 19)，討論議題集中在 AI 治理 (4 場)、個資隱私保護 (3 場)、網路人權 (2 場)、內容治理 (2 場)。此外，國家政府關切的議題還包括資料經濟與競爭法、普及上網、網路安全，以及政策制定等議題。

表19. IGF 2019 政府關切的討論議題

主題 類別	開放論壇名稱	討論議題	主辦單位
資料 治理	• 資料治理與競爭	• 資料經濟與競爭法	• 德國經濟暨能源部
	• 為大數據與 AI 發展提供政策選擇	• AI 治理 (影響及人權)	• 聯合國教科文組織 (UNESCO)
	• 資料治理的技術創新與挑戰	• 個資隱私保護	• 中國網信辦
	• 人權與 AI 錯誤：誰該負責？	• AI 治理(責任及人權)	• 歐洲理事會
	• 個人資料保護	• 個資隱私保護	• 中國網信辦
	• 為 AI 與兒童權利訂定政策指南	• AI 治理(安全及權益)	• 聯合國兒童基金會 (UNICEF)
	• AI-從原則到落實	• AI 治理(國際政策)	• 經濟合作暨發展組織(OECD)
數位 包容	• 打破孤立- 低度開發國家與世界	• 普及上網(低開發國)	• 巴拉圭外交部
安全 穩定	• 網路空間的信賴，常規與自由	• 網路人權(自由)	• 愛沙尼亞外交部
	• 人權與數位平臺是矛盾的嗎	• 網路人權(平臺責任)	• 歐洲理事會
	• 未成年使用者的線上保護	• 網路安全(兒少保護)	• 中國網信辦
	• 透過數位安全強化數位轉型	• 內容治理(不實訊息)	• 印尼資通科技部
	• 資訊分享 2.0：隱私與網路安全	• 個資隱私保護	• 以色列國家網路局
	• 線上不實訊息：降低傷害與保護權力	• 內容治理(不實訊息)	• 英國文化、傳媒與體育部
	• 歐盟的未來網路治理策略	• 政策制定(治理策略)	• 歐盟執委會

* 以上各場會議的主題分類係依據 IGF 2019 議程表標示，惟當中有 2 場次本計畫基於合適性考量進行類別調整。

三、各界關切議題：AI 治理、內容治理、個資保護、普及上網...

全球各界的關切議題概況可從 IGF 座談會議 (Workshops) 觀察，因為

此會議是開放給全球多方利害關係人在 3 大主題類別下，提案申辦的會議。

2019 年座談會議共有 431 件申請案，最後有 64 件獲得通過 (2019 年 10 月資料，如下表 20)，主要討論議題包括：個資隱私保護 (8 場)、AI 治理 (6 場)、跨境資料 (4 場)、普及上網 (7 場)、促進參與 (5 場)、本地資料／內容 (3 場)、能力建構 (2 場)、內容治理 (6 場)、網路安全 (4 場)、網路主權／分裂 (3 場)、網路衝突 (3 場)、IPv6 移轉 (2 場)。

表 20. IGF 2019 各界關切的討論議題

主題類別	座談名稱	討論議題
資料治理	<ul style="list-style-type: none"> • 資料導向的民主：確保數位時代的價值 • 各界於個資保護的角色：亞太的實施狀況 • 評估演算法對選舉過程的影響 • 法治是數位生態系統中的關鍵概念 • 數位環境下的兒童隱私和資料保護 • 超越道德委員會：如何真正進行 AI 治理 • 以人為本的數位身份 • 以人為本的設計和開放資料：如何改善 AI • 智慧城市交通服務的資料治理 • 跨境資料：讓中小企業連結全球供應鏈 • 公益資料：我們在哪裡？ 做什麼？ • 金磚四國的個資價值與法規 • 全球通用的資料保護框架？如何使其運作？ • 賦予公眾公平治理資料的權利 • 資料治理的公共政策要點教學 • 讓全球資料治理也能落實於開發中國家 • 為永續發展目標強化大數據的合作 	<ul style="list-style-type: none"> • AI 治理 (決策、人權及民主) • 個資隱私保護(亞太地區) • AI 治理(演算法與選舉) • 司法制度與治理問題 • 個資隱私保護(兒少) • AI 治理(道德、人權) • 個資隱私保護(數位身份) • AI 治理(道德、人權) • 個資隱私保護(智慧交通) • 跨境資料(流通) • 個資隱私保護(開放公益使用) • 個資隱私保護(金磚四國法規) • 個資隱私保護(法規全球框架) • 個資隱私保護(個人控制權) • 跨境資料(流通與集中化) • 資料治理(開發中國家) • 跨境資料(流通與集中化)

	<ul style="list-style-type: none">• 讓 AI 治理資料：將人權置於風險之中？• 執法部門取得跨境資料的解決方案• 揭示數位貿易影響：呼籲所有利害關係人• 讓 AI 為永續發展目標而準備	<ul style="list-style-type: none">• AI 治理(人權、責任)• 跨境資料(司法管轄權)• 國際貿易政策與網路課稅等• AI 治理(永續發展、包容)
數位 包容	<ul style="list-style-type: none">• 讓資料存在 - 將資料視為公共利益• 賦予殘疾人上網能力• ICANN 多方主義的包容性和合法性• 數位包容的運營模式是什麼？• 實現數位包容的綜合政策框架關鍵• 商業創新促進數位包容，縮小差距• 在多語言域名空間顯示線上身份• 包容與代表性：促進本地內容成長• 網路服務是否值得課徵罪惡稅？• 建立公平且永續的社區主導網路• 釋放開發中及低開發國家的數位潛力• NRIs 的永續性：IGF 的未來戰略• 青年於改善網路道德與數位包容的參與• 縮小邊緣化地區的數位鴻溝• 性工作，吸毒，減少傷害與網路• 社區自建網絡：機會，挑戰和解決方案• 線上包容的知識多樣性：新規則？• 殘疾人士的無障礙網路：新的參與性方法• 重新思考弱勢族群的未來工作• 讓青年擁有數位化技能：多種全球方法• 如何以及為什麼要有效地涵蓋兒童的觀點	<ul style="list-style-type: none">• 本地資料/內容(使用與 AI)• 普及上網(殘疾人士)• 促進參與 (ICANN)• 普及上網(弱勢族群)• OECD 之 Going Digital 可行性• 本地資料/內容(殘疾人士參與)• 域名系統與 email 的全球通用• 本地資料/內容(開發中國家)• 網路課稅對數位包容影響• 普及上網 (社區網路、女性)• 普及上網(非洲國家)• NRIs 永續發展模式• 促進參與(青年)• 普及上網(偏鄉地區)• 促進參與(弱勢族群)• 普及上網(社區網路)• 促進參與(弱勢族群)• 普及上網(無障礙環境)• 能力建構(南半球弱勢族群)• 能力建構(南半球青年)• 促進參與(兒少)
安全 穩定	<ul style="list-style-type: none">• 科技民族主義：5G，網路安全與貿易	<ul style="list-style-type: none">• 網路主權/分裂 (5G 基建與民族主義)

- 網路分裂：如果網路主權盛行將會如何
- 數位主權與網路分裂
- 常見的疑問：制定網路常規的範圍探究
- 線上國民健康：影子法規-藥品獲取
- 以數位識讀因應兒童網路霸凌
- 量化網路空間的和平與衝突
- 兒童上網：如何確保他們的安全
- 邁向以人權為中心的網路安全訓練
- 對抗線上非法內容：捍衛數位權利
- 全球供應鏈中的 IT 安全
- 不實訊息治理方法的探討
- 網路排毒：終結線上性別歧視的成功方案
- 公眾外交與不實訊息：中間有紅線嗎？
- IoTs 的透明與控制
- 我們應該藉由 DNS 處理非法內容嗎？
- 建立網路空間信任措施 (CBM) 路線圖
- 跨境網路中斷：新式網路回擊
- IPv6：我為什麼應該關心？
- IPv6 獨立日：安息 IPv4
- 對抗線上仇恨言論：多方利害關係人方法
- 不實訊息，責任與信任
- 網路主權/分裂(盛行原因、影響)
- 網路主權/分裂(模式、影響)
- 國際網路常規的制定流程
- 網路藥局監管政策的訂定
- 網路安全(兒少保護)
- 網路衝突(威脅影響量化研究)
- 網路安全(兒少保護)
- 國家侵犯網路人權因應方式
- 內容治理(違法內容)
- 網路安全(企業強化資安標準)
- 內容治理(不實訊息)
- 內容治理(仇恨言論)
- 內容治理(不實訊息、民主)
- 網路安全(IoTs 產品安全)
- DNS 封鎖的效益與廠商責任
- 網路衝突(緊張情勢緩解)
- 網路衝突(攻擊與中斷的規範)
- IPv6 移轉(認知宣導)
- IPv6 移轉(準備措施)
- 內容治理(仇恨言論)
- 內容治理(不實訊息)

* 以上各場會議的主題分類係依據 IGF 2019 Workshop Selection Results 標示，惟當中有 3 場次本計畫基於合適性考量進行類別調整。

四、共同研討議題：AI 治理、普及上網、促進參與、網路安全...

除了年度論壇的討論議題外，IGF 還有全球多方利害關係人長期共同

研討的議題，主要是透過動態聯盟 (Dynamic Coalition, DC)⁶及最佳典範論壇 (Best Practice Forum, BPF)⁷進行研究討論，且過程皆開放所有人參與。

目前 IGF 共有網路中立、平臺責任、IoT 等 18 個從 2008 年起至近期成立的動態聯盟，以及網路安全、IoT 與大數據與 AI 等 4 個於 2019 年通過的延續性的最佳典範論壇。每個動態聯盟及最佳典範論壇都於 2019 年 IGF 申辦其主題相關會議，討論議題如下表 21 所示，主要包含普及上網 (4 場)、促進參與(3 場)、網路安全(3 場)、能力建構 (2 場)、AI 治理(2 場)等。

表21. IGF 共同研討議題

主題類別	會議名稱	討論議題	主辦之 DC 或 BPF
資料治理	• 網路空間的資料治理	• 資料的安全與治理模式	• 網路核心價值 DC
數位包容	• 殘疾人士的 ICT 使用	• 普及上網(殘疾人士)	• 普及上網與殘疾人士 DC
	• 更佳區塊鏈治理的能力建構	• 能力建構(區塊鏈)	• 區塊鏈科技 DC
	• 社區網絡：政策與法規	• 普及上網(社區網路)	• 社區連網 DC
	• 性別與網路治理	• 促進參與(性別平等)	• 性別與網路治理 DC
	• 從資料到政策的普及上網	• 普及上網(新技術等)	• 連接未連線的創新做法
	• 網路權益與原則的永續發展	• 網路人權(智慧城市)	• 網路權益與原則 DC
	• 公用上網對成功公共政策的貢獻	• 普及上網(圖書館)	• 圖書館公用上網 DC
	• 網路治理學院的分類	• 網路治理課程彙整	• 網路治理學院 DC
	• 強化開發中島國的未來	• 促進參與(加勒比海地區)	• 網路經濟下的開發中島國 DC

6 動態聯盟是以特定議題為主的自發性常態組織，由多方利害關係人社群自主發起，並經 IGF 秘書處審核通過，之後的研討過程皆開放所有人參與。

7 最佳典範論壇是 IGF 多方利害關係人諮詢小組 (MAG) 通過的年度計畫，針對計畫主題進行研究討論，且過程中皆開放所有人參與，最後並產出方向性的建議報告以供全球做政策參考。而 2019 年通過的 4 個最佳典範論壇皆為延續 2015 年至 2018 年的計畫。

	• 青年參與網路治理論壇	• 促進參與(青年)	• 網路治理青年聯盟
	• 性別與普及上網	• 能力建構(女性)	• 性別與普及上網BPF
	• 在地內容	• 在地內容(有利發展條件)	• 在地內容 BPF
安全 穩定	• 如何兼顧兒童遊戲權與被保護	• 網路安全(兒少保護)	• 兒少網路安全 DC
	• 全球通用對政府的重要性	• 全球通用的重要性	• DNS 議題 DC
	• 5G、IoT 與零費率對網路中立挑戰	• 網路中立與 5G 等	• 網路中立 DC
	• 平臺責任：利益衝突、AI 與避稅	• 平臺責任(AI 決策、避稅)	• 平臺責任 DC
	• IoT 的購買使用與課責發展	• 網路安全(IoT 課責)	• IoTs DC
	• 不太自由的市場	• 網路市場公平競爭	• 新聞業與媒體永續發展DC
	• IoT 與大數據與 AI	• AI 治理 (及 IoT 政策、挑戰)	• IoT 與大數據與 AI BPF
	• 網路安全	• 網路安全(國際協議)	• 網路安全 BPF

* 以上各場會議的主題分類係依據 IGF 2019 議程表標示，惟當中有 8 場次本計畫基於合適性考量進行類別調整。

五、小結

綜觀以上的專家精選議題、政府關切議題、各界關切議題，以及共同研討議題，可發現當中尤其以 AI 治理治理、普及上網、內容治理、網路安全等 4 項最為備受關切 (表 22)，討論層面包括：

- AI 治理：AI 涉及的人權、道德、責任、安全、演算法、社會影響 (包含民主與選舉)、國際政策等問題。
- 普及上網：殘疾人士、弱勢團體、女性、非洲地區、低度開發國家、偏鄉地區的上網問題；及透過社區自建網路促進連網等。
- 內容治理：極端內容、不實訊息、仇恨言論、違法內容的因應方式。
- 網路安全：提升兒少保護、企業資安、IoT 安全；推動國際協議等。

表22. 全球關切議題 (IGF 2019) 彙整

主題類別	專家精選議題 (Main Sessions)	政府關切議題 (Open Forums)	各界關切議題 (Workshops)	共同研討議題 (DC 與 BPF)	前4項統計
資料治理	<ul style="list-style-type: none"> AI 治理 跨境資料 	<ul style="list-style-type: none"> AI 治理*4 場 個資隱私*3 場 資料經濟與競爭法 	<ul style="list-style-type: none"> AI 治理*6 場 跨境資料*4 場 個資隱私*8 場 	<ul style="list-style-type: none"> AI 治理*2 場 	<ul style="list-style-type: none"> 4 2 2 1
數位包容	<ul style="list-style-type: none"> 普及上網等 	<ul style="list-style-type: none"> 普及上網 	<ul style="list-style-type: none"> 普及上網*7 場 促進參與*5 場 本地資料/內容*3 場 能力建構*2 場 	<ul style="list-style-type: none"> 普及上網*4 場 促進參與*3 場 能力建構*2 場 	<ul style="list-style-type: none"> 4 2 1 2
安全穩定	<ul style="list-style-type: none"> 內容治理 網路安全(IoT) 合作與發展*3 場 政策制定*2 場 	<ul style="list-style-type: none"> 內容治理*2 場 網路安全 政策制定 網路人權*2 場 	<ul style="list-style-type: none"> 內容治理*6 場 網路安全*4 場 網路主權/分裂*3 場 網路衝突*3 場 IPv6*2 場 	<ul style="list-style-type: none"> 網路安全*3 場 	<ul style="list-style-type: none"> 3 4 1 2 1 1 1 1

*「各界關切議題」及「共同研討議題」因場次眾多，僅列出 2 場以上 (包含 2 場) 場次。

在數位匯流發展趨勢下，上述 4 個議題皆與通傳會業務直接或間接相關，即使是新興議題如 AI 治理，已被網路治理暨數位政策專業網站 GIP Digital Watch observatory (<http://dig.watch/>) 歸類於基礎建設項目下。有鑑於普及上網議題的討論情境多以低度開發國家為主，而網路安全議題中討論最多的兒少保護，在國內已有通傳會等部會共同籌設的 iWIN 網路內容防護機構專責推動，因此，本計畫挑選 AI 治理、內容治理，加上委辦項目指定的 5G 治理，共 3 項議題，做進一步探討。

六、參考文獻

- IGF 2019. <https://www.intgovforum.org/multilingual/content/igf-2019>
- IGF 2019 Themes. <https://www.intgovforum.org/multilingual/content/igf-2019-themes>
- Dynamic Coalitions. <https://www.intgovforum.org/multilingual/content/dynamic-coalitions>
- Best Practice Forums. <https://www.intgovforum.org/multilingual/content/best-practice-forums-BPF>
- GIP Digital Watch observatory. <http://dig.watch/>

第二節 AI 治理：歐盟與 OECD 政策建議

一、前言

AI (Artificial Intelligence, 人工智慧) 是當前全球正快速發展與使用的策略性科技之一，亦被形容是驅動第四次工業革命的核心科技，並可望帶來提高製造業生產力與經濟成長、協助疾病診斷及醫療保健、促進資源有效使用及環境永續、降低交通與工殤意外事故、協助偵測資安威脅與打擊犯罪等正面效益。因此，近年來各國政府紛紛推出 AI 國家策略，積極佈署 AI 發展，以在全球 AI 競賽中搶得先機。根據外交基金會 (Diplo Foundation, 2019) 統計，目前全球已有超過 50 個國家提出 AI 發展策略或相關政策措施，當中也包括我國的《臺灣 AI 行動計畫》。

儘管 AI 帶來促進經濟繁榮、激勵產業創新，以及造福人類社會的美好願景，但同時也伴隨社會面與倫理面的挑戰。例如：對勞動市場的衝擊、對個資隱私的風險、發生意外事故的責任歸屬、自動化決策的公正性等。因此，部分國家政府、企業、學研單位、技術社群，以及國際間組織，陸續對 AI 的潛在風險提出應對機制或建議，例如日本政府提出《以人為本的 AI 社會原則》(2019 年 3 月)、Google 宣布實施開發 AI 的道德原則

(Google' s AI Principles, 2018 年 6 月)、電機電子工程師學會 (IEEE) 發布第 2 版 AI 道德設計準則(Ethically Aligned Design, 2017 年 12 月)等。而當中特別針對國家政府提出政策建議的有歐盟及經濟合作暨發展組織 (Organization for Economic Co-operation and Development, OECD)，因此，本節將就此進行探討。

二、歐盟 AI 策略

歐盟執委會 (The European Commission, EC) 於 2018 年 4 月 25 日發布《歐洲人工智慧通告》(Communication...on Artificial Intelligence for European)，也就是《歐盟 AI 策略》，闡述歐盟發展 AI 的方式將會與眾不同，除了要確保歐盟於 AI 領域的競爭力外，還要讓所有人與整體社會都能從數位轉型中受益，且 AI 發展必須符合歐盟價值與基本人權。

根據《歐盟 AI 策略》，AI 係指「展現出智能行為的系統，它們具有一定程度的自主性去分析環境並採取行動，以達成特定目標。而 AI 的應用可以是單純的軟體系統，或是植入硬體裝置中，且許多 AI 高度倚賴資料或學習方法 (機器學習) 來達成結果」。

《歐盟 AI 策略》並訂定從以下 3 個方向推動 AI 發展：

(一) 提振公私部門投資 AI

鼓勵公部門與民間企業投資 AI 的研究與創新，以提升歐盟的 AI 技術與產業能量，在技術發展取得領先地位，並促進整體經濟善用 AI。

(二) 因應 AI 帶來的社經變化

因應措施包括鼓勵教育和培訓系統的現代化、培養優秀人才、預測勞動力市場變化、支持勞動力市場轉型，以及實施社會保護機制。

(三) 確保合適的倫理與法規框架

此框架係基於歐盟的價值觀（尊重人類尊嚴、自由、民主、平等、法治、人權），且符合《歐盟基本權利憲章》，內容包括：訂定現有產品責任規範指南、對新興挑戰做詳細分析，以及由利害關係人合作訂定 **AI 倫理準則**。

三、歐盟 AI 倫理準則

依據前述《歐盟 AI 策略》的工作方向，歐盟執委會於 2019 年 4 月 8 日發布《可信賴 AI 的倫理準則》(Ethics Guidelines for Trustworthy AI)，強調歐盟要發展以人為本的 AI，並透過 G7、G20 等場合建立國際共識，讓歐盟成為可信賴 AI 的國際領導者。

此倫理準則是由歐盟高階專家小組 (The High-Level Expert Group on AI, AI HLEG) 所制定，並獲得歐盟執委會的支持推動，且建議歐盟國家視為政策決策的重要參考。該小組由 52 位來自產業界、公民團體、學術界的專家組成，且準則也納入超過 500 份利害關係人的意見。

至於內容則包含組成要素、基本倫理原則、關鍵要求（實施準則）、實施方法、實施評估等，主要是為達到組成要素當中的「倫理的 AI」及「穩健的 AI」提供指引。至於「合法的 AI」則將另外提供建議（請詳本節之「三、歐盟 AI 政策建議」）。以下逐一簡介準則的重點。

（一）可信賴 AI 的組成要素

可信賴 AI 由下列 3 項要素組成，這些要素須同時兼備。

1. **合法的**：系統應遵守所有適用的法律及規範。
2. **倫理的**：系統應與倫理原則和價值觀一致。
3. **穩健的**：系統於技術面與社會面都應是穩健的。

（二）基本倫理原則

可信賴 AI 的基本倫理原則反映《歐盟基本權利憲章》所保障的下列 4

項基本權利，期能讓 AI 改善個人和全體人類的福祉。

1. 尊重人類的自主性

AI 系統設計應遵循以人為本的原則，並確保人類可以監督 AI 系統的作業過程。

2. 預防傷害

AI 系統應保護人類尊嚴及身心健康，因此，系統及運作環境應是安全穩健，以確保不被惡意使用。

3. 公平性

AI 系統的開發、布署和使用須具備實質與程序的公平性，讓人們免於偏見歧視，且負責決策的實體（人或物）與過程也應明確。

4. 可解釋性

AI 系統的功能、目的和決策，應可被公開透明地說明，才能建立和維護用戶對 AI 的信任。

(三) 關鍵要求（實施準則）

可信賴 AI 的系統於設計、開發和使用的所有階段（整個生命週期）都應持續實施下列 7 條「關鍵要求」（實施準則）：

1. 人類自主性及監督

AI 系統不應侵犯人類的自主性和基本權利，而是應該予以支援，以促進社會公平；同時也要建立人類監督機制。

2. 穩健性及安全性

AI 演算法必須安全可靠且穩健，以便系統隨時可以處理錯誤或不一致；且整個系統要能抵禦攻擊、有備用計畫、高準確度。

3. 隱私及資料治理

人民應能完全控制自己的資料，資料不應被用於加諸傷害或歧視；而是

應該被充分保護，確保隱私性、準確性、公平性、完整性。

4. 透明度

確保 AI 系統決策過程所使用資料的可追溯性，以及技術程序的可解釋性；同時系統也要能讓人類辨別，與他們互動的究竟是人類或是 AI 系統。

5. 多元性、無歧視及公正性

AI 系統應考慮人類整體的能力、技能及需求，允許所有人平等使用 AI 產品與服務，並要避免 AI 系統本身和所使用的資料導致不公平的歧視。

6. 社會及環境福祉

AI 系統應用於推動正向社會發展，應評估系統對人類的社會關係和民主進程的影響，且系統的開發與使用也應強化對環境永續性和生態責任。

7. 問責機制

應建立稽核機制，包括對演算法、資料、系統開發過程做評估，以確保 AI 系統及其結果的權責及責任歸屬問題，尤其是重要應用（如涉及人身安全）應進行獨立稽核，但不意味要公開相關的商業模式和智慧財產權。

(四) 實施方法

可信賴 AI 的實施方法涵蓋系統的設計、開發和使用的所有階段（整個生命週期），並可分成技術、非技術兩大面向，各項方法可為互補或取代。由於 AI 系統是在變動環境中持續發展，因此，必須針對所採用的方法及改進的流程，不斷地進行評估與檢驗。

1. 技術面方法

(1) 建立可信賴 AI 架構

應將「關鍵要求」轉換為應操作程序和限制性程序，如建立「應遵守行為」和「禁止行為」清單。另外，具有自主學習能力的 AI 系統可能出現意外行為，故應確保系統於開發設計時，已將「關鍵要求」融入系統的“sense-plan-act”週期模式中。

(2) 將倫理和法治融入設計

AI 系統於設計時，即應有法規遵循的理念；公司有責任確認 AI 系統的影響及應遵循的規範。而要獲得信賴，AI 的流程、資料和結果都須維持安全和穩健；且應實施故障安全關閉機制，並在強制關閉（如攻擊）後重新恢復操作。

(3) 可解釋的方法

人類應該了解 AI 系統為何有特定的行為，及為何提供特定的闡釋，而研究領域中的可解釋 AI (Explainable AI, XAI) 即是嘗試從系統的底層機制來回應此問題。惟對於以神經網路為基礎 AI 系統而言，相關的演算法設計和資料正確解讀仍是個挑戰。

(4) 測試和驗證

應儘早進行系統的測試和驗證，以確保系統在整個生命週期都能穩定運行。測試須包括系統的資料、訓練前的模型、環境以及整個系統的行為。測試過程應由不同族群的人員來設計和執行，並回報系統錯誤和弱點。最後需確保整體結果和前述的測試過程結果是一致的。

(5) 服務品質指標

為 AI 系統定義適當的服務品質指標，確保對安全和防護方面的測試和開發有基礎了解，這些指標包括評估演算法和訓練措施的指標，以及功能、性能、可用性、可靠性、安全性和可維護性等傳統軟體指標。

2. 非技術面方法

(1) 法規

目前已有支援可信賴 AI 的法規，如產品安全法規和責任框架。這些法規可能需要修訂、調整或採用，以作為一種保護和推動力。

(2) 行為準則

組織和利害關係人可簽署本指導方針，並調整企業責任章程、關鍵績效指標、行為準則或內部政策文件。而開發或使用 AI 系統的組織可記錄

其用意，並加諸基本權益、透明度等普世價值標準，以確保符合初衷。

(3) 標準

設計、製造和商業行為的標準，可做為 AI 消費者和政府的品質管理方式。此外，還有認證系統 (如 ISO 標準)、職業道德準則等方式。而未來可能使用「可信賴 AI」標籤，以確認系統的安全性、健全性和透明性。

(4) 認證

認證將採用針對不同應用領域和 AI 技術而開發的標準，並與其他的工業和社會標準做適當結合。但認證無法取代責任，因此要輔以課責框架 (包含免責聲明、審查和補救機制)。

(5) 透過管理框架進行問責

組織應建立內外部的管理框架，以為 AI 系統相關的倫理議題提供監督和建議，其方式可為任命個人、內外部道德委員會，或委託認證機構。但此機制無法取代法律規定的事項 (如個資法規定任命資料保護官等)。

(6) 透過教育培養倫理觀

溝通、教育和培訓對發展可信賴 AI 至關重要，要讓 AI 潛在影響的知識廣為傳播，並讓大眾知道可以參與形塑社會的發展。整個社會都應培養基礎 AI 素養，更要確保倫理學家擁有適當的技能和訓練。

(7) 利害關係人參與及社會對話

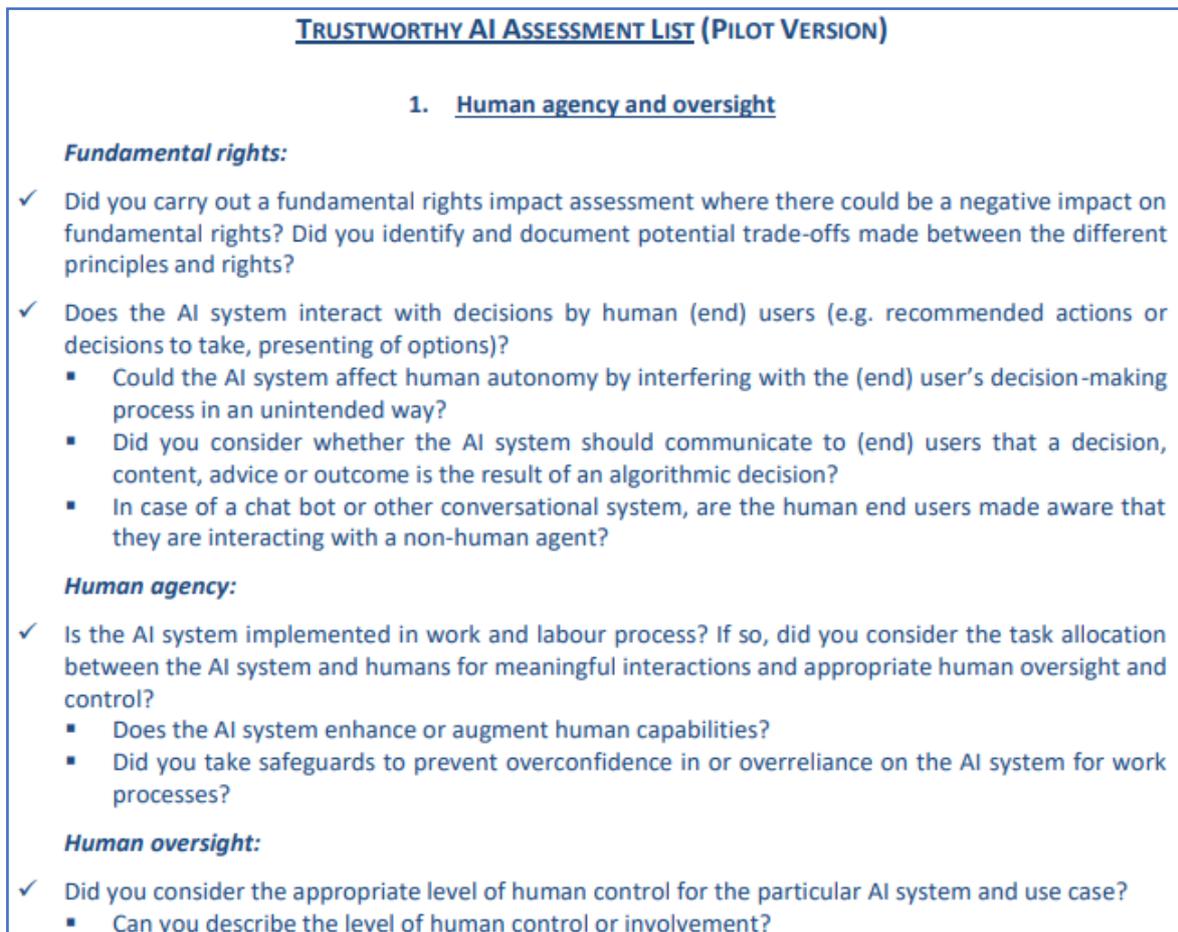
AI 系統有諸多優點，進行公開討論和鼓勵各利害關係人參與，才能確保所有人從中受益。許多組織已仰賴利害關係小組討論 AI 系統和資料分析的使用，成員包括法律、技術、倫理學的專家，及消費者、勞工代表。

(8) 多元和包容的設計團隊

隨著 AI 系統自動執行更多任務，設計團隊須能反映使用者和整體社會的多元化，以增進系統的客觀性與包容性。團隊成員最好能來自不同的性別、文化、年齡、專業、技能背景。

(五) 實施評估

此份倫理準則一併提供評估清單（目前為測試版，預計 2020 年初提出修正版本），以利組織自我檢視實施狀況。評估清單內容如下圖 45 所示的「第 1 項人類自主性及監督」（亦是「關鍵要求」的第 1 條）截圖，評估子項分成基本人權、人類自主、人類監督共 3 類，細項問題如：此 AI 系統是否在無意間干擾使用者的決策過程，進而影響人類的自主性？該系統如用於勞工的作業過程，是否有提升人類的能力？特定 AI 系統的人類控制者是誰，又什麼情況下人類可以介入干涉？



資料來源：歐盟執委會

圖45. 歐盟《可信賴 AI 的倫理準則》實施評估清單

不過，使用評估清單也有注意事項，包括：清單不可能詳盡無遺，所以，應不斷檢視「關鍵要求」的實施情況，並評估解決方案，以確保系統

的持續改善；整份準則沒有進一步探討「合法的 AI」問題，因此，即使完全符合評估項目也不代表達成法規遵循；AI 系統的應用軟體有其特殊性，所以，使用評估清單前，需針對系統運作的個別情況進行調整；進行評估時，建議邀請所有關係人(管理高層，及法務、產品與服務、品管、人資、採購、日常維運等部門人員) 共同參與。

四、歐盟專家 AI 政策建議

歐盟 AI 高階專家小組 (AI HLEG) 於 2019 年 6 月 26 日發布《可信賴 AI 的政策與投資建議》(Policy and investment recommendations for trustworthy AI)，從利益最大化、風險最小化及預防的角度，為歐盟建立永續、有競爭力、包容、可信賴的 AI 提供政策建言，當中也包含回應前述的 AI 倫理準則中，未能涵蓋的「合法的 AI」問題。歐盟執委會表示，此份建議有助於歐盟會員國後續討論 AI 合作計畫。

《可信賴 AI 的政策與投資建議》內容分成 2 大部分——建立 AI 的正面影響，以及實現可信賴的 AI；並針對人類社會、民間部門、政府部門、學研單位、資料與基礎建設、技能教育、法規架構、資金投資等 8 個面向，提出 33 項建議，其架構與建議標題如下表 23 所示。

表23. 歐盟《可信賴 AI 的政策與投資建議》列表

類別		建議 (標題)
一 運 用 可 信 賴 的	(一)賦權和保護 人類與社會	1.透過增加對 AI 的知識和認知，賦權人類
		2.保護人類、社會和環境的完整性
		3.在工作場合中推廣以人為本的 AI 方法
		4.絕不拋下任何人
		5.衡量和監測 AI 對社會的影響
	(二)改變歐洲的	6.促進歐洲各行業採用 AI 技術和服務

AI 在 歐 洲 建 立 正 面 影 響	民營企業	7.透過推動創新和技術移轉，促進和擴展 AI 解決方案	
		8.建立公私合作夥伴關係，以培育各部門的 AI 生態系統	
	(三)歐洲政府部門為永續發展和創新的催化劑	9.為民眾提供以人為本的 AI 服務	
		10.將政府做為促進歐洲 AI 發展的平臺	
		11.利用政府採購以資助創新，並確保可信賴的 AI	
		12.維護 AI 公共服務中的基本權利，並保護社會基礎設施	
	(四)確保世界級的研究能力	13.發展和維護歐洲 AI 研究之策略藍圖	
		14.增加和簡化基礎研究和目的導向研究的資金提供	
		15.透過發展和招募 AI 研究人員，擴展歐洲的 AI 研究能力	
		16.建立世界級的歐洲研究能力	
	二 利 用 歐 洲 的 推 動 力 實 現 可 信 賴 的 AI	(五)為 AI 建立資料和基礎建設	17.支援會員國的 AI 基礎設施
			18.發展符合法規和道德的資料管理，並在歐洲分享倡議計畫
			19.支持歐洲在開發 AI 基礎建設上的領導地位
			20.發展和支持 AI 專用的網路安全基礎建設
		(六)為 AI 開設適當的技能和教育	21.重新設計學齡前至高等教育的教育系統
			22.培養和留住歐洲高等教育人才
23.增加科學和技術領域中的女性工作者比例			
24.提升現有勞動力的技能，並教導其新技能			
25.建立利害關係人的認知，並為技能政策提供決策支持			
(七)建立合適的治理和法規架構		26.確保政策決策是基於風險考量和多方利害關係人方法	
		27.從最相關的法律領域開始評估，必要時修訂歐盟法律	
		28.考量建立新法規的需求，確保得到充分保護免受不良影響	
		29.考量是否需要修改既有體制架構以確保相稱和有效的保護	
		30.建立「歐洲可信賴 AI 單一市場」的治理機制	
(八)募集資金和		31.確保本文件提出的建議獲得足夠資金	

投資	32.因應市場的投資挑戰
	33.推動開放且可獲利的投資風氣，以獎勵可信賴的 AI

資料來源：歐盟執委會；本計畫彙整

上述建議中，除了類別「(二) 改變歐洲的民營企業」、「(四) 確保世界級的研究能力」與「(八) 募集資金和投資」屬於產業發展、技術研發及市場投資的建議外，其他類別中皆有與網路治理相關的政策建議，重點簡介如下：

(一) 賦權和保護人類與社會

確保人們了解 AI 的功能、侷限與影響，提供他們使用 AI 的必要技能，為 AI 普及化的工作環境做好準備，並保護他們免於受到 AI 可能帶來的任何傷害。例如：政府不宜以「社會安全」為由進行大規模監控、商業行為的監控也應受到限制、「免費服務」須符合隱私等基本權利、應強制 AI 系統揭露與使用者互動的是人類或系統等。

(三) 歐洲政府部門為永續發展和創新的催化劑

政府部門應成為促進 AI 發展的平臺與推動者，並應以身作則，提供以人為本的 AI 系統公共服務，嚴加保護民眾的基本權利。尤其要禁止使用 AI 建立大規模的個人評分系統，並訂定明確且嚴格的法規，規範基於國安和公共利益所實施的監控。即使合法、必要、符合比例原則，且確保不會用於打壓政治對手或破壞民主程序的監控，也要以可信賴的方法來實施。

(五) 為 AI 建立資料和基礎建設

除了備妥發展 AI 必要的實體面和技术面的基礎建設（如高速網路、分散式叢集運算、邊緣計算等）外，還需制定完整的資料治理方案，包括資料的存取、分享、使用、再利用、相容性等規範，甚至是自願捐贈資料等規則，以確保在符合法規（如歐盟 GDPR）和道德（如公平、合理、無歧視）的前提下，建立歐盟的跨國資料共享基礎架構。

(六) 為 AI 開設適當的技能和教育

重新規劃學齡前至高等教育的整個教育系統，讓所有人都學習數位素養、程式編碼、STEM (科學、科技、工程、數學)，及以人為本的技能 (如解決問題、創新、批判性思考、同情體諒、溝通說服等)。而在勞工的部分，則是要透過法規賦予民眾持續學習的權利、獎勵企業提供因應 AI 的職能升級訓練、將歐盟的電腦技能證照(ECDL) 升級為 AI 技能證照等。

(七) 建立合適的治理和法規架構

AI 政策決策應基於風險考量，並依不同的風險程度，實施不同強度的監管；如為有科學佐證的無法接受風險，或是會造成實質傷害的風險，例如對民主造成威脅、危害人類健康、破壞環境等，則應改採預防性方法。而政策方向則應採取原則性方法及結果導向，如歐盟的 AI 政策措施是以歐盟的價值觀為基礎，並將理想目標轉化成一套可評估實施成效的具體指標。至於進一步發展 AI 監管框架，建議宜針對特定領域量身訂製，因為保護個人的必要措施及 AI 系統的開發部署在 B2C (企業對消費者)、B2B (企業對企業)、P2C (產品對消費者) 的情境都不同。

再就法規面來看，應全面性、系統性地盤點現有相關法規，包括民事、刑事犯罪、消保、資料保護、禁止歧視、資安、競爭等，並評估現有的法規是否仍然適用於 AI 驅動的世界 (如對於落實倫理準則的助益程度為何)、是否需要訂定新的法規 (如禁止追蹤/識別個人的 DNA 或情緒等生物和身心特徵、限制發展自動化致命武器、監管開發個性化的兒童 AI 系統)、是否需要修改既有的體制架構 (如要求 AI 系統於設計時即規劃人類的監督與補救機制、不得賦予 AI 系統或機器人在法律上的人格權) 等。

上述問題都應該透過多方利害關係人的對話討論，以建立合適的治理規範，避免阻礙有益的 AI 創新，同時也確保人類與社會免於負面衝擊。

五、OECD AI 原則

經濟合作暨發展組織 (OECD) 於 2019 年 5 月 22 日通過《OECD AI 原則》(OECD Council Recommendation on Artificial Intelligence, 簡稱為 OECD Principles on AI), 提倡推動創新、可信賴、尊重人權與民主價值的 AI。OECD 表示, 這是第一個獲得政府承諾將盡責管理 AI 的國際標準, 並開放給非成員國加入。

OECD 並預計於 2020 年初發布「AI 政策觀測平臺」(OECD AI Policy Observatory), 進一步提供跨領域、以證據為基礎的 AI 政策分析, 以及政策監督評估工具, 同時還將透過平臺促進全球多方利害關係人的合作與對話。

此份《OECD AI 原則》是由來自政府部門、企業、勞工、公民團體、學術界、技術社群等 50 多位專家共同研擬, 內容分成「可信賴 AI 的盡責監管原則」、「可信賴 AI 的國家政策與國際合作」2 大部分, 以及基於人權與民主價值的各 5 條原則。

(一) 可信賴 AI 的盡責監管原則

1. 包容性成長、永續發展與福祉

利害關係人應積極地盡責監管 AI, 以追求對人類和地球有益的成果, 如增強人類的能力與創造力、促進代表性不足族群的融入、降低社會經濟和性別等不平等現象、保護自然環境等。

2. 以人為本的價值與公平性

AI 系統的設計應尊重法治、人權和民主價值觀 (包括自由、尊嚴、自治, 隱私和資料保護、非歧視與平等、多樣性, 公平、社會正義、國際公認的勞工權益), 並應有適當的保護機制, 例如於必要時允許人類介入。

3. 透明度與可解釋性

AI 系統應是透明並有責任揭露相關資訊, 包括讓人類意識到是和機器互動, 以及讓人類了解 AI 作用的結果, 並能於受到負面影響時提出質疑,

且了解決策的邏輯基礎。

4. 穩健、安全及保全

AI 系統須在整個生命週期中，穩健、安全和可靠地運作，且潛在風險（包括隱私、資安、保全與偏見）也應被持續地評估和管理。為此，AI 系統的所有資料都應保有可追溯性，以能夠對系統結果進行分析。

5. 問責機制

開發、部署和維運 AI 系統的組織與個人，應根據上述原則，對 AI 系統的正常運作負責。

(二) 可信賴 AI 的國家政策與國際合作

1. 投資 AI 的研究與發展

政府應促進公部門與民間企業投資於 (1) AI 的研究與發展，以激勵可信賴 AI 的創新；(2) 開放資料，其前提為尊重隱私與資料保護，以支持良好的 AI 研究發展環境（沒有不當偏見、改善互通性，且採用標準）。

2. 為 AI 強化數位生態系統

政府應強化可信賴 AI 的數位生態系統發展，包括特定的數位科技與基礎建設，以及 AI 知識分享機制。為此，政府應推動資料信賴機制，以支持安全、公平、合法、有倫理地分享資料。

3. 為 AI 塑造有利的政策環境

政府應推動有利於從研發階段過渡至部署與維運可信賴 AI 系統階段的政策環境，並應酌情審查和調整其適用於 AI 系統的政策、監管框架及評估機制，以鼓勵可信賴 AI 的創新與競爭。

4. 培養人類能力並為勞動市場轉型做準備

政府應與利害關係人緊密合作，為勞動世界和社會的變革做準備。

他們應使人們具備必要的技能，並能有效地使用 AI 系統，確保部署 AI 時勞工能公平地轉型，以及 AI 的正面效益能被廣泛且公平地分享。

5. 值得信賴 AI 的國際合作

政府應與利害關係人積極合作，提倡上述原則及可信賴 AI 的盡責監管。又政府也應於 OECD 及其他國際場合，共同努力促進 AI 知識共享，並推動多方利害關係人發展以共識為導向的可信賴 AI 之全球技術標準。

六、歐盟、OECD、G20、美、日之 AI 政策關聯性

(一) 歐盟與 OECD 之 AI 政策建議比較

下表 24 彙整前述的歐盟與 OECD 之 AI 政策建議，並可發現兩者有許多共同點。例如：兩份建議皆是由 50 多位多方利害關係人組成的專家小組所制定、皆是基於自由民主與人權等基本價值而勾勒出發展以人為本及可信賴 AI 的政策目標、皆是要求落實人類自主和安全穩定及透明問責等原則、皆是建議在促進產業與技術發展的同時須兼顧公正公平並因應勞動市場衝擊等挑戰，以及皆有（將）提供相對應的實施方法與評估工具。

表24. 歐盟與 OECD 之 AI 政策建議比較

政策名稱	歐盟《可信賴 AI 的倫理準則》，及《可信賴 AI 的政策與投資建議》	《OECD AI 原則》(建議)，及 AI 政策觀測平臺
制定者	多方利害關係人專家小組	多方利害關係人專家小組
價值基礎	歐盟價值觀 (自由、民主、平等、法治、人權...)	人權和民主價值觀 (自由、自治，隱私、非歧視、多樣性，公平、正義.....)
政策目標	發展以人為本、可信賴的 AI；成為可信賴 AI 的國際領導者	發展創新、可信賴、以人為本的 AI；成為政府盡責管理 AI 的國際標準
實施準則/要求/原則	1.人類自主性及監督 2.穩健性及安全性	1.以人為本的價值與公平性 2.穩健、安全及保全

	3.隱私及資料治理	3.透明度與可解釋性
	4.透明度	4.包容性成長、永續發展與福祉
	5.多元性、無歧視及公正性	5.問責機制
	6.社會及環境福祉	
	7.問責機制	
政策建議	1.賦權和保護人類與社會	1.投資 AI 的研究與發展
	2.改變歐洲的民營企業	2.為 AI 強化數位生態系統
	3.歐洲政府部門為永續發展和創新的催化劑	3.培養人類能力並為勞動市場轉型做準備
	4.確保世界級的研究能力	4.為 AI 塑造有利的政策環境
	5.為 AI 建立資料和基礎建設	5.值得信賴 AI 的國際合作
	6.為 AI 開設適當的技能和教育	
	7.建立合適的治理和法規架構	
	8.募集資金和投資	
實施方法	1.技術面：建立架構、融入設計、可解釋的方法等 5 項	於 2020 年年初發布
	2.非技術面：法規、行為準則、標準、認證等 8 項	
評估工具	評估清單(對照 7 條實施準則)	於 2020 年年初發布

(二) G20 採用《OECD AI 原則》

《OECD AI 原則》除了獲得 36 個成員國通過外，也開放給非成員國採認，且獲巴西、阿根廷等 6 國共襄盛舉。此外，G20 (20 國集團)也於 2019 年 6 月 8 日通過《G20 AI 原則》，其條文內容與《OECD AI 原則》完全相同。G20 於其貿易與數位經濟部長聲明 (G20 Ministerial Statement on Trade and Digital Economy) 中指出，負責任地發展和使用 AI 可以實現永續和包容的社會，為所有人提供機會，因此，G20 致力支持以人為本的 AI 發展及源自 OECD 的 AI 原則。

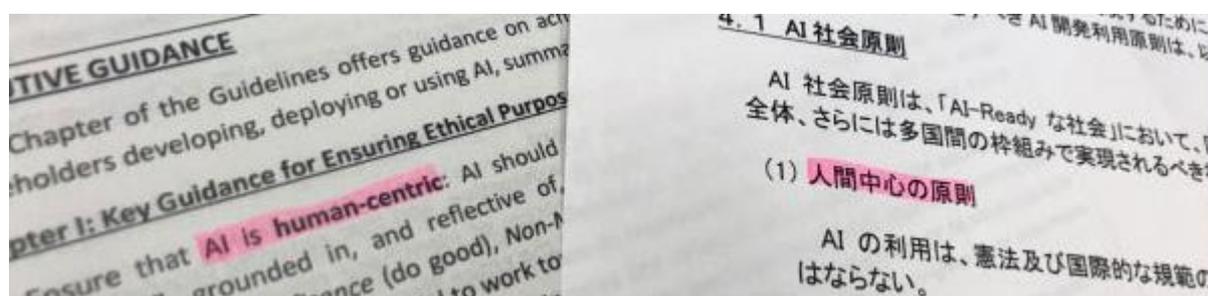
總計 OECD 成員國、非成員國、G20 及歐盟國家 (歐盟亦是 G20 一

員)，並扣除重複，全球直接或間接採認《OECD AI 原則》者已約 60 國。

(三) 歐盟與日本於 G20 共推 AI 倫理原則

歐盟於發布《可信賴 AI 的倫理準則》時即表示，由於技術、資料和演算法不分國界，因此，將加強與日、加、星等國合作，並持續透過 G7、G20 等國際場合，將 AI 治理倫理概念推向全球。

不過，日本政府內部指稱，歐盟的準則是參考日本的 7 項社會原則，但也表示，雙方擁有相同的基本價值觀和個資保護思維，且同樣擔憂 AI 技術發展失控，因此，可於推動 AI 倫理的國際規則上合作(日經中文網,2019)。



資料來源：日經中文網

圖46. 歐盟 AI 倫理原則與日本 AI 社會原則

日本內閣府（由日本首相直接統領的中樞機構。鄭力軒，2019）於 2019 年 3 月 29 日公佈《以人為本的 AI 社會原則》，基於「尊重人類尊嚴、所有人受惠(多元與包容)、永續」3 個基本理念，透過「以人為本、教育與素養、確保隱私、確保安全、確保公平競爭、公平性、責任說明及透明性、創新」7 項 AI 社會原則，及討論中的國際 AI 開發使用原則，期能實現 AI-Ready 的日本「超智能社會」(Society 5.0)。

日經中文網 (2019) 並分析指出，相較於 AI 發展領先全球的中、美兩國，日本和歐盟立場皆強調 AI 的風險及倫理保護，加上 2019 年 G20 峰會由日本擔任主席國，因此，日歐雙方攜手努力爭取制定 AI 國際規則。

(四) 美國 AI 國家策略呼應《OECD AI 原則》

對於《OECD AI 原則》，身為 OECD 和 G20 要員且為 AI 強國的美國，也有相關回應。美國白宮於「美國人的 AI」(Artificial Intelligence for the American People) 網站上指出，美國引領多個提倡信賴 AI 科技的國際活動，如與 OECD 成員國一起推動《OECD AI 原則》且 G20 也採用，這是美國首次和志同道合的民主國家承諾遵守的 AI 共同原則，且這些原則也和《美國 AI 倡議》(American AI Initiative) 相互呼應。

《美國 AI 倡議》是川普總統於 2019 年 2 月 11 日啟動的美國 AI 國家策略，透過「投資 AI 研發、釋放 AI 資源、訂定 AI 治理標準、打造 AI 勞動力、國際參與並保護 AI 優勢」等 5 大方向，因應 AI 時代的衝擊。美國白宮並強調，美國的 AI 發展必須符合美國的基本價值，包括自由、人權、法治、社會穩定、隱私權、智財權等，必須考量 AI 對社會的廣泛影響，以確保 AI 以負責任、可信賴的方式發展。

不過，部分美國學者認為，此份倡議偏重工商界且學術界和公民團體的意見不足，而且對於維護自由和隱私也著墨不多 (BBC News 中文, 2019)。

七、小結

推動 AI 發展亦是我國的重大政策之一，我國於 2018 年啟動為期 4 年的《臺灣 AI 行動計畫》(2018~2021)，以打造臺灣成為產業創新的數位沃土，加速邁向智慧國家。而有鑑於 AI 可能伴隨負面衝擊，科技部也於 2019 年 9 月 23 日發布《人工智慧科學發展指引》，以完善我國的 AI 科學研發環境。綜觀本節的歐盟 AI 策略、歐盟與 OECD 對「國家政府」的 AI 政策建議和準則，以及從中延伸簡述的美、日兩國 AI 政策，本計畫提出下列建議：

(一) 發展可信賴 AI 已成國際趨勢，關注 AI 規範是否成為下個 GDPR

歐盟《可信賴 AI 的倫理準則》與《可信賴 AI 的政策與投資建議》，以及《OECD AI 原則》的政策目標，皆為發展以人為本、可信賴的 AI，且對

應的實施準則及政策建議也高度相似，並在歐、美、日等國的合作推動下，讓 G20 也採用《OECD AI 原則》。本計畫統計發現，目前全球已有約 60 個國家直接或間接採認 OECD 原則。因此，發展以人為本、可信賴的 AI，可說已成國際趨勢，甚至如 OECD 所稱的成為「國際標準」。

另一方面，曾任德國國防部長的新任歐盟執委會主席范德賴恩 (Ursula von der Leyen) 已承諾，將在就任 100 天內，針對 AI 對人類與倫理的衝擊，提出立法。美國《政治》(Politico)等媒體報導認為，AI 法規可能成為下一個 GDPR，除了因為歐盟已在研究限制人臉辨識技術、標示與人類互動者為機器人/演算法、訂定 AI 決策的法律責任等規範外；德國總理梅克爾也表示「擁有確保 AI 為人類服務、類似 GDPR 的法規，是下任歐盟執委會主席的工作」。不過，報導也指出，歐盟專家和美國網路業者並不贊同立法措施，他們擔心此舉可能阻礙創新發展。(Pop, 2019；Kayali, 2019)。

歐盟 2018 年起實施的 GDPR 對全球的影響仍持續發酵中，包括我國政府也正和歐盟協商取得符合 GDPR 的適足性認定，並很可能須修改我國現行的《個人資料保護法》。而一旦歐盟推出類似 GDPR 的 AI 法規，勢必將為全球帶來新一波的法規衝擊。因此，相關後續發展值得我國高度關注。

(二) 歐美日以國家總體策略迎接 AI 時代，我國 AI 產業計畫應進行升級

從《歐盟 AI 策略》、《OECD AI 原則》、《美國 AI 倡議》、日本《以人為本的 AI 社會原則》可發現，先進國家是以各自的基本價值觀為基礎，從整體社會的角度，並透過國家層級的總體策略，來因應 AI 時代的機會與挑戰。尤其歐盟依據總體策略推出的《可信賴 AI 的倫理準則》及 OECD 的《OECD AI 原則》，更是由多方利害關係人組成的專家小組所制定，且兩者皆於 2019 IGF 舉辦座談，和全球各界分享與交流。

相較之下，我國雖訂有《臺灣 AI 行動計畫》及《人工智慧科研發展指引》，且科技部也推出「AI 之人文社會研究計畫」，以及國發會亦進行「數位經濟及 AI 對社會影響與因應策略」研究。然而，在缺乏基本價值的支

撐、偏重產業思維而非整體社會權益、未能從國家層級應對倫理挑戰，以及欠缺多方利害關係人充分對話⁸等情況下，恐怕難以全面且有效地迎接 AI 發展及因應衝擊。連台積電創辦人張忠謀也提醒政府不能太過樂觀，要注意 AI 可能帶來的失業、貧富差距等社會問題（鄭鴻達，2019）。



圖47. 美國、歐盟、臺灣之 AI 策略重點

其實國內許毓仁等立法委員已針對我國缺乏國家層級且兼顧社會倫理面的 AI 政策問題，展開具體行動--提出《人工智慧發展基本法》，該法案並已獲得一讀通過（潘維庭，2019）。不過，目前國際趨勢仍以透過國家策略推動 AI 發展為主，即使是前述的歐盟情況也仍待後續觀察。因此，面對攸關每個人權益的 AI 發展與治理問題，我國的當務之急應是採取網路治理方法，邀請多方利害關係人透過界定議題範圍、啟動多方模式、運行工作小組等多方模式的實施步驟，充分討論基於臺灣基本價值的 AI 願景、準則、推動方式（是訂定國家策略或立法措施），以及實施方法等問題，最後並產出解決方案或建議事項，以迎接 AI 時代的機會與挑戰（有關多方模式的實施細節可參考 <https://www.twnic.net.tw/mps/page28.html>）。

8 根據科技部新聞稿（2019.9.23），《人工智慧科研發展指引》是科技部邀請各領域「學者專家」討論後完成。而歐盟《可信賴 AI 的倫理準則》是由來自產業界、公民團體、學術界的 52 位專家組成的高階專家小組訂定，過程中並納入超過 500 份利害關係人的意見，且後續還展開大規模測試與修正；《OECD AI 原則》亦是由來自政府部門、企業、勞工、公民團體、學術界、技術社群等 50 多位專家共同研擬。

八、參考文獻

- BBC News 中文 (2019)。特朗普的科技夢：AI 也要“美國第一”。2019/2/13。 <https://www.bbc.com/zhongwen/simp/science-47218301>
- 日經中文網 (2019)。沒有 IT 大企業的日本如何推進 AI 戰略？2019/4/23。
<https://zh.cn.nikkei.com/industry/scienceatechnology/35257-2019-04-23-05-00-00.html?start=1>
- 台日科技合作推動辦公室 (2019)。(日本) 以人為本的 AI 社會原則。
<https://tjsto.nccu.edu.tw/以人為本的ai社會原則/#top>
- 李世暉 (2019)。日本 AI 原則的經濟思維。能力雜誌 764 期 (聯合新聞網 2019/10/7 轉載)。 <https://udn.com/news/story/6868/4087525>
- 沈婉玉、林于蘅 (2019)。台歐 3 度協商 GDPR 國發會：我個資法勢將調整。聯合新聞網，2019/11/27。 <https://udn.com/news/story/7238/4189338>
- 科技部 (2019)。科技部訂定「人工智慧科研發展指引」 完善我國 AI 科研發展環境。新聞資料，2019/9/23。
https://www.most.gov.tw/folksonomy/detail?subSite=main&article_uid=dbf8da09-22be-4ef1-8294-8832fc6e8a26&menu_id=9aa56881-8df0-4eb6-a5a7-32a2f72826ff&l=CH&utm_source=rss
- 國發會 (2019)。數位經濟及 AI 對社會影響與因應策略。2019/11/4。
https://www.ndc.gov.tw/Content_List.aspx?n=153BD64D42FBAD4D
- 潘維庭 (2019)。「解開政府對人工智慧的最後一道枷鎖」 許毓仁籲速審《人工智慧發展基本法》。風傳媒，2019/10/1。
<https://www.storm.mg/article/1775906>
- 鄭力軒 (2019)。官僚之國的崩解：日本內閣如何從文官手中奪回政策主導權？關鍵評論，2019/7/24。 <https://www.thenewslens.com/article/122437>

- 鄭鴻達 (2019)。張忠謀疾呼：留心 AI 衝擊帶來失業、貧富差距問題。聯合新聞網，2019/11/5。 <https://udn.com/news/story/11316/4144644>
- EC (2018). Communication Artificial Intelligence for Europe (Eruopean AI Strategy). 25 April 2018.
<https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>
- EC (2019a). Artificial intelligence: Commission takes forward its work on ethics guidelines. Press release.
https://europa.eu/rapid/press-release_IP-19-1893_en.htm
- EC (2019b). Ethics Guidelines for Trustworthy Artificial Intelligence. 8 April 2019.
<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
- EC (2019c). Trustworthy AI: Joining efforts for strategic leadership and societal prosperity. Brochure. 18 September 2019.
<https://ec.europa.eu/digital-single-market/en/news/trustworthy-ai-brochure>
- G20 (2019). G20 AI Principles. attached in Annex of G20 Ministerial Statement on Trade and Digital Economy.
<https://www.mofa.go.jp/files/000486596.pdf>
- GIP Digital Watch (2019). Artificial intelligence.
<https://dig.watch/issues/artificial-intelligence>
- Kayali, L. (2019). Next European Commission takes aim at AI. POLITICO, July 18, 2019.
<https://www.politico.eu/article/ai-data-regulator-rules-next-european-commission-takes-aim/>
- OECD (2019a). Artificial intelligence.

<https://www.oecd.org/going-digital/ai/>

- OECD (2019b). OECD AI Policy Observatory.
<https://www.oecd.org/going-digital/ai/about-the-oecd-ai-policy-observatory.pdf>
- OECD (2019c). Recommendation of the Council on Artificial Intelligence.
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- OSTP (2019). Accelerating America's Leadership in Artificial Intelligence. February 11, 2019.
<https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/>
- PoP, V. (2019). No Relief for Big Tech Under New EU Leadership. The Wall Street Journal, Sept. 2, 2019.
<https://www.wsj.com/articles/no-relief-for-big-tech-under-new-eu-leadership-p-11567428651>
- The White House (2019). Artificial Intelligence for the American People.
<https://www.whitehouse.gov/ai/>

第三節 內容治理：發展中的全球政策標準

一、前言

隨著網路成為攸關國家社會運作的關鍵基礎建設，但同時也衍生日益嚴重的網路濫用問題，因此，近年來，各國政府祭出越來越多的網路規範。例如：歐盟為保護個資隱私的 GDPR (2018)、德國為打擊仇恨暴力等違法內容的網路執行法 (NetzDG, 2018)、澳洲為控管暴力內容的社群媒體新法⁹

⁹ 該法案全名為 Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act，規定社群媒體必須「迅速移除」令人反感內容，否則可處數十億美元或全球年營收 10% 罰鍰，且公司高層也可能面臨 3

(2019)、英國正在推動中的有害內容立法¹⁰，以及中國大陸打造網路審查的防火長城高牆、土耳其與俄羅斯對民眾使用社群網路進行監控等。

研究報告和媒體報導紛紛指出，網路環境正發生顛覆性的巨變，國家政府從過去對網路空間的不加干涉，轉變成過度監管，逐漸築起網路空間的國家疆界，也讓全球步入「法規軍備競賽」；在此同時，人民的網路使用範圍也變成由各國（或地區）法規決定。例如：在歐洲無法連上 4 成以上的美國新聞媒體網站¹¹、在中國大陸無法使用 Google、YouTube、FB 等服務。而如果我們放任這些問題持續發展，將會導致全球網路分裂、增加國際緊張局勢，並破壞過去網路所帶來的創新與繁榮 (Condliffe, 2019；Lomas, 2019；Meeker, 2019；Scott, 2018；I&J Policy Network)。

為此，全球網路治理專家也開始討論因應之道，並提出政策實施規範等階段性成果，期能降低跨境網路法規的衝突與緊張，並發展成為全球性的政策標準，進而維護全球單一互連的網路。本節將針對當中與「內容治理」相關的國際政策環境、趨勢，以及實施建議進行探討。

二、美、歐、印、中的網路內容監管強度

《2019 網路趨勢報告》(Internet Trends Report 2019)¹² 亦指出，網路世界已經變成由各國法規所取決，並從「網路連線」、「內容規範」及「使用者規範」等三個面向，觀察全球網路人口大國——美、歐、印、中的網路法規概況，且將美國列為低度監管，歐盟（主要 7 國）為低度與中度監管，印度為中度監管，而中國大陸則為中度與高度監管（圖 48）。

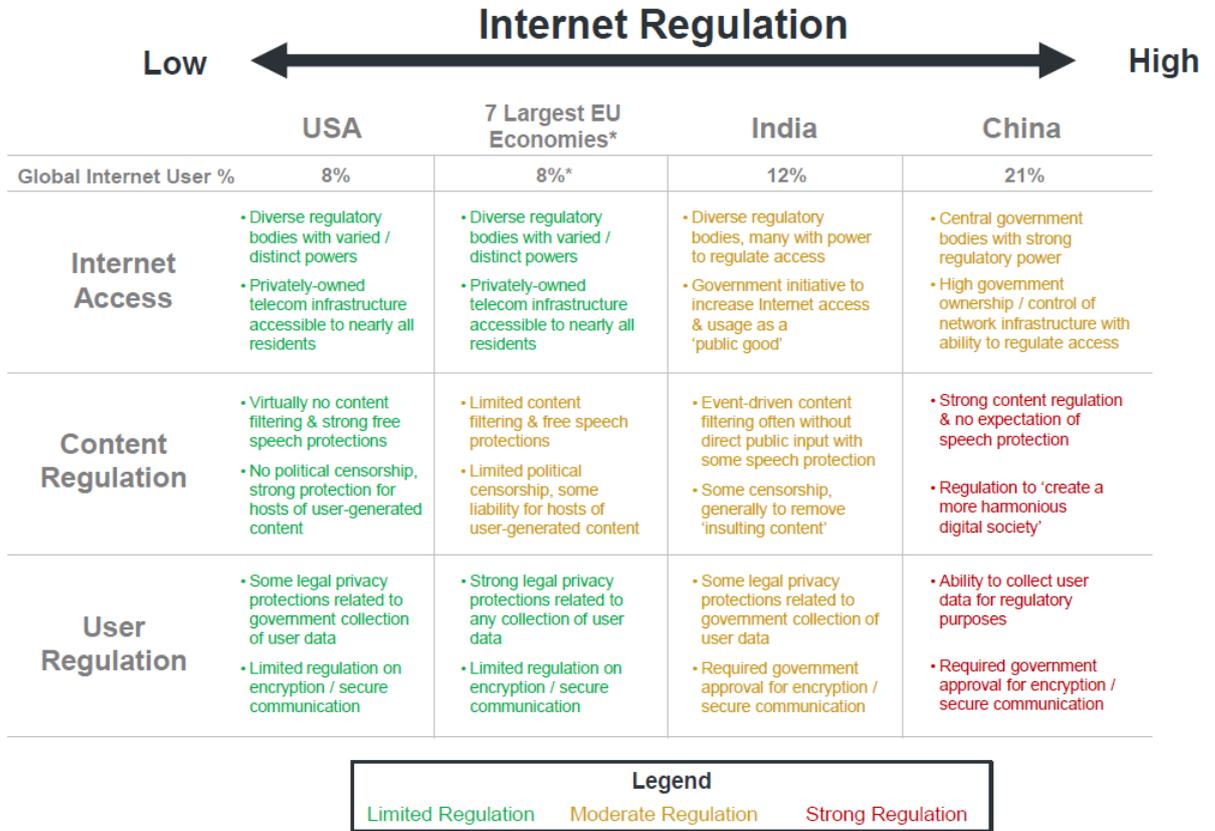
年有期徒刑。此為全球第一個要求社群媒體為其內容負責的法律。

10 英國政府於 2019 年 7 月完成 Online Harms White Paper 公開徵詢，但尚無具體立法時程表。

11 根據 Top10VPN.com 調查，GDPR 實施一年後，42% 美國新聞網站限制來自歐洲的連線 (Stewart, 2019)。

12 此報告由知名創投人士、素有「網路女王」之稱的 Mary Meeker 自 1995 年起每年發布。

World Wide Web = Webs of Worlds Driven by Local Regulation...



資料來源：Internet Trends 2019

圖48. 美、歐、印、中之網路法規強度

進一步就「內容規範」來看，《2019 網路趨勢報告》認為，由於美國幾乎沒有內容過濾和政治審查，也沒有特別立法保護言論自由與使用者內容，故為低度監管。但歐盟因為實施部分程度的內容過濾、政治審查、言論自由保護、平臺課責（使用者產出內容的平臺），所以，被列為中度監管。而印度因為針對某些事件實施內容過濾，且有部分的言論保護與審查措施，因此，亦為中度監管。至於中國大陸，由於實施嚴格的內容規範與社會信用制度，且完全沒有言論自由可言，因此，屬於強度監管。

三、網路內容與跨境法規挑戰

根據全球第一份闡述網路空間跨境法規挑戰的報告--《網路與管轄權全球現況報告》(Internet & Jurisdiction Global Status Report)，全球網路治理專家對於當前網路情勢與法規發展表示相當擔憂。此報告調查訪問超過 150 位來自各國多方利害關係人的網路治理專家，並呈現以下調查結果(Svantesson, 2019)：

- 69% 受訪專家認為，網路濫用的情況（如仇恨言論、騷擾、駭客攻擊、侵犯隱私、詐騙）正持續增加中。
- 95% 受訪專家表示，未來 3 年跨境網路法規挑戰將更加嚴峻。
- 79% 受訪專家指出，目前全球缺乏充足的國際協調與合作，以處理跨境網路法規的挑戰。
- 只有 15% 受訪專家相信，目前已經有合適的組織或機構來因應跨境網路法規的挑戰。

報告並指出，我們的世界從未像現在如此地緊密相連，這也是網路跨越國界的本質。但是網路濫用行為的增加，使得網路的內容、安全與經濟成為當前跨境網路法規挑戰的主要議題，各議題包含的子題如下所列：

- 內容：極端主義與恐怖主義及仇恨言論、毀謗、網路詐騙、色情、假新聞與錯誤訊息（對民主的破壞、平臺的管理責任）、資料隱私等。
- 安全：網路犯罪（執法困境、暗網）、數位證據取得、監控（加密與後門程式…）、網路安全（資料外洩、駭客…）等。
- 經濟：智慧財產權、電子商務與競爭法及消費者保護、網路課稅、物聯網（智慧家庭、智慧城市、穿戴健康裝置）、區塊鏈（加密貨幣…）、國際與區域經貿協議（數位保護主義…）。

此份報告是由德國政府、丹麥政府、愛沙尼亞政府，及歐盟執委會共同贊助，由「網路與管轄權政策網絡」(Internet & Jurisdiction Policy Network) 委託澳洲法律學者 Svantesson 教授執行研究調查，並於 2019 年 6 月發布出

版報告，期能藉此協助網路政策的創新、促進政策研擬的能力建構、提升政策的一致性，進而維護全球單一且開放互連網路所帶來的利益。

報告並發現，當前網路法規的討論重點已不再是該不該管，而是該如何管，但是網路技術的快速發展和網路跨越國界的本質，使得透過傳統的國家法律工具來處理網路濫用問題，變得更加困難。另一方面，在缺乏國際共識和信任下，各國又以最強大的法規取代合作，將本國網路法規延伸到域外。因此，報告也強調「沒有單一政府、企業或組織，可以獨自解決問題」的觀念，並呼籲國際間推動更多的協調與合作，且堅守多方利害關係人主義，如此才能有效因應網路濫用問題，避免發生網路分裂、法規不確定性升高、使用者不信任網路、阻礙網路創新與經濟成長等不良後果。

四、網路內容政策的實施方案

有鑑於仇恨言論、安全威脅、煽動暴力、歧視等網路濫用行為增加，但是各國因應處理時，卻面臨同一內容在不同國家有合法與非法的兩極判別，加上各界對於網路平臺的課責仍持不同立場等問題，因此，全球網路治理專家自 2016 年起即透過「網路與管轄權政策網絡全球會議」(The Global Conference of the Internet & Jurisdiction Policy Network) 討論解決之道。

此會議迄今已經舉辦 3 屆 (2016 年、2018 年、2019 年)，歷屆主辦單位分別為法國政府、加拿大政府，以及德國政府；合作單位包括歐盟執委會、歐洲理事會、ICANN、OECD、UNESCO (聯合國教科文組織) 等組織；參與會務與政策發展的專家包括網路之父 Dr. Vint Cerf、ICANN 董事長 Maarten Botterman、瑞典前首相 Carl Bildt 等人；至於與會者則每次僅開放給全球多方利害關係人的資深代表約 200 人參加。

而在歷經近 3 年的政策討論與方案研擬後，專家們於 2019 年會議提出《內容與管轄權計畫：實施方案》(Content & Jurisdiction Program: Operational Approaches) 文件，以為網路內容治理提供具體可行的解決措

施，並發展成為全球的政策標準 (I&J Policy Network, 2019)。

此實施方案的內容包括發展現況、規範 (常規)、標準 (準則)，以及「機制」。由於「機制」並非整個方案的實施機制，而是僅針對標準 (準則) 當中的「第 10 條申訴」提供更多的背景描述與建議，且全球專家後續將就各標準提出更詳盡的建議措施，因此，本節暫不介紹「機制」。

(一) 發展現況

1. 網路內容的挑戰

提供使用者創造內容的線上平臺，是行使言論自由和公開辯論的關鍵工具，但是這些線上服務也可能被濫用，成為大家日漸意識到的網路非法或有害內容。利害關係人所面臨的共同挑戰包括如何即時有效地解決濫用問題，並同時兼顧國際人權保障、數位經濟發展，且讓跨國法規可以共存於同一個網路空間。

2. 規範的演進

各國政府日益強化線上內容的立法和執行。雖然某些內容 (如兒童性虐待) 已獲全球共識被視為無法接受的內容，但是對於更多其他內容 (如煽動暴力、仇恨言論、騷擾、誹謗或假消息) 的合理限制標準，則仍存有巨大差異，並可能導致國際緊張局勢。另一方面，全球主要業者也時常檢視更新其服務條款和社群守則，這些規範也會直接影響全球網路內容的合法性判定，因此，未來法規協調亦須將服務條款與社群守則納入考量。

3. 中介者角色的演進

過去網路中介者受到歐美相關法規的免責保護，但隨著內容濫用行為增加，新的立法轉為要求中介者承擔更多責任，包括縮短發現濫用內容的回應時間，中介者也因此開發演算法等工具，以檢測濫用內容並防止重新上傳，進而成為網路內容的裁決者。而這種公私部門的責任移轉將會產生什麼結果，目前尚無答案。

4. 合作框架

面對因應網路濫用行為極為複雜的挑戰，此計畫的全球利害關係人專家基於共同的原則，合作制定實施標準。這些原則包括：將必要保護措施與傷害補救最大化、將限制言論自由最小化並促進數位經濟持續發展、妥善處理濫用內容須有明確的指引與機制（以領土做為管轄權基礎的現有機制可能需要檢討，並進行制度創新）。

(二) 實施規範（常規）

當網路業者依據國家相關法規要求，或基於社群守則的規定，而必須採取內容限制措施時，可依據下列的實施規範／常規（Norms）。

1. 明確的架構

- 訂出定義：對於非法內容、有害內容，及限制性措施的種類，應有共同定義，以反應法規的實施及公司的做法。
- 基本事項：國家法律和民間社群守則的用字如能清楚明確，可確保人人都理解規範。
- 確立權責：明訂公私利害關係人各自的權利和責任，並視情況考量服務的性質和規模。

2. 符合比例原則

- 決策考量：限制性措施的決策，要考量其目的在於達成調解，或至少是平衡所有相關者的權益。
- 程度範圍：限制性措施的實施範圍應儘量最小化，並保留最大化的合法內容。
- 選擇行動：有多種技術解決方案可作為內容刪除的替代方案，以確保合乎比例原則。

3. 程序保證

- 設計格式：設計明確的提交格式，讓內容限制的檢舉資訊成為決策的參考。
- 標記功能：用戶可透過易於使用的管道，標記出他們認為違反社群守則的內容。
- 雙重檢測：結合自動檢測和人工查核有助於降低過度限制的風險。
- 用戶通知：在執行內容限制措施之前，用戶會先收到通知。此外，也應讓用戶知道遭到限制的原因。
- 緊急條款：訂定適用於正當緊急情況的特定條款。
- 申訴／補救：要有快速、有效、明確、公開的申訴機制，並在申訴期間盡可能保留內容。

4. 問責機制

- 決策記錄：內容限制須完整記錄業者的標準、程序和回報層級路徑，並可供大眾查閱。
- 一致的標準：業者於實施其社群守則和法律要求時，應採取一致的標準，並為此目的分配適當的資源。
- 透明度：公私部門可藉由可匯出格式產出的詳細定期報告，做為內容限制機制和決策合法性的佐證。
- 監督：持續監測可對內容限制措施進行適當的監督，以增強對正當程序和問責的信任。

(三) 實施標準 (準則)

所有決策者在發展、評估、實施內容問題的解決方案時，都可以使用此標準／準則 (Criteria)，其內文分成框架明確性、偵測、符合比例原則的

行動、通知/申訴、延伸擴展等 5 大部分共 11 條標準。下表 25 列出各條標準並摘要其重點。

表25. 內容治理實施標準(準則)之條文摘要

大類	標準	條文摘要
明確的架構	1. 內容的種類	<p>內容的種類眾多，合法與否也因國家地區而異，且目前仍缺乏國際定義。以下嘗試彙整內容的種類，以協助關係人針對每種內容挑戰，發展更細緻的因應方法。</p> <ul style="list-style-type: none"> • 兒少權益相關內容：虐待兒童或令未成年反感、網路誘拐或性侵 • 隱私權相關內容：洩漏個資、誹謗、造假(包含 deep fakes)、性具象化、私密圖片 • 言論自由相關內容：不實訊息、醫療錯誤訊息、色情、褻瀆宗教、誹謗、霸凌、騷擾、暴力、宣傳犯罪、教唆自殘或自殺、洩漏機密訊息、冒犯君主或批評歷史人物 • 宣傳戰爭與煽動仇恨相關內容：仇恨言論、暴力極端主義 • 智慧財產權相關內容：版權、商標 • 受管制商品和服務相關內容：受管制的商品和服務、性交易 • 欺騙相關內容：誤導性的元素、勒索敲詐、詐騙(為經濟利益)、垃圾資訊(包含 AI 刺激點閱率)、虛假帳號
	2. 規範的基礎	<p>研擬國家法規和企業社群守則的主要挑戰，在於協調取捨各種有衝突的權益，如言論自由和預防傷害。以下要點有助於因應此挑戰：</p> <ul style="list-style-type: none"> • 調和日益複雜的規範來源：包括國際人權原則、國家/區域相關法規、業者的服務條款與社群守則 • 符合國際規範的一致性：目前國際對內容是否合法有 4 種看法 <ul style="list-style-type: none"> - 普遍認為非法 (如兒童性虐待) - 普遍認為非法，但各國判斷標準差異很大 (如誹謗) - 非普遍認為非法，但接受國家特殊法律 (如將否認大屠殺定罪) - 非普遍反對，但有些國家認為不該視為違法(如歧視、性別取向) • 可選擇的平臺管理方式：由群組管理員監管、根據社群守則監

		管、根據國家/區域法規或國際協議監管
偵測	3. 第三方通知 (檢舉)	對於依據法規而執行的內容限制，政府宜研擬有適當保護措施的程序，以加快評估速度，避免業者在情況不明下(如尚未取得法院批准但又必須即時下架)過度限制內容。此外，民間相關組織也會對內容提出檢舉，如著作權保護組織、兒少保護組織、事實查核單位等。
	4. 平臺業者的偵測	越來越多平臺業者使用 AI 對內容進行主動偵測，但是自動化工具仍有偏見、誤判等諸多問題，因此，需要進一步做適當的評估與監督，且決策過程也須進行人工審查。
符合比例原則的行動	5. 即時性	近來立法強調縮短刪除特定內容(如恐怖主義、極端主義、暴力)的處理時間，但快速決策可能產生錯誤研判、傷害言論自由、影響用戶權益等風險。
	6. 評估	內容檢舉應提供哪些內容可能違反哪項條款的資訊。而平臺業者須做綜合評估(如內容來源者的語言文化背景、發布內容的動機、對閱聽者的影響、是否影響其他的司法管轄權、禁止此類內容是否符合國際共識...)，以確保所採取措施的適當性，並了解其潛在影響(如言論自由、隱私、經濟、成為決策先例...)。
	7. 符合地理性比例原則的行動	非法內容的法律規定因國家而異，有些國家甚至連國際人權標準所保護的言論自由都禁止。基於數位內容不受地理限制的特性，但同時也尊重其他主權國家的法律，如果確定該內容違反其國家法律，則限制措施應儘限於在該國的管轄權範圍內。此類限制措施可參照第 2 條標準，以確保符合地理性比例原則。至於業者的服務條款/社群守則，基本上其內容限制規範是全球適用，但仍要確保符合地理性比例原則。
	8. 可選擇的行動措施	處理違法/有害內容，或違反服務條款/社群守則的內容，有下列方式，應選擇適當措施以做最少的限制： <ul style="list-style-type: none"> • 內容供應商、平臺、搜尋引擎 提供背景或解釋資料、標識警告內容、年齡確認/管制、賦予用戶回應權、暫停/停用帳號、封鎖搜尋索引、封鎖關鍵字、暫時

		<p>或永久移除有害內容、封鎖或保留特定地區的內容/使用者或 IP...</p> <ul style="list-style-type: none"> •網路/託管中介商 <p>深度封包檢測型封鎖 (如關鍵字封鎖清單、URL 或 HTTP 表頭封鎖)、IP 和協定型封鎖、降低性能、丟棄封包、封鎖 DNS/封鎖頂級域名、重新分配/沒收域名、斷網、下架伺服器...</p> <ul style="list-style-type: none"> •法律管轄之外的封鎖 <p>封鎖/干擾/投放重啟 (Reset, RST) 封包</p>
通知/申訴	9. 用戶通知	<p>如果評估結果是限制內容，則應在實施之前通知用戶；萬一有特殊情況，也要在實施的同時或之後通知用戶；只有少數例外情況 (如無法識別用戶、當地法律對機密性的要求) 可不用通知。而通知內容則應包含法規/規範的依據、遭到限制的原因、申訴管道和時程等。</p>
	10. 申訴	<p>目前針對內容限制的申訴機制，有下列 2 種做法：</p> <ul style="list-style-type: none"> •業者設立(外部)審查機構 <p>業者可考慮設立(外部)審查機構，處理用戶內容因違反社群守則而遭限制的個別申訴。此作法為第三階段的內容評估決策(第一為 AI 偵測暨人工審查，第二為內部申訴機制)，且被視為具有效力的企業特定工具。而在籌設前應討論機構的權限、正當程序 (須尊重人權)、組織的組成運作等問題。</p> <ul style="list-style-type: none"> •設立全國型的自律委員會 <p>另一種建議做法為設立全國型的獨立自律機構——社群媒體委員會，以做為因應社群媒體平臺限制內容的申訴機制。籌設前同樣應討論機構的權限、正當程序 (須尊重人權)、組織的組成運作等問題。</p>
延伸擴展	11. 小型業者/國家的能力 (挑戰)	<p>面對內容審查與限制的快速發展，以及國際常規通常是針對大型市場而建立，小型業者因為資源有限，以致無法負擔日益沉重的內容評估工作、開發自動化偵測工具、建立自己的申訴機制。而小型國家也面臨全球性的社群守則不適用於當地情境、國際平臺業者的審核小組不了解當地語言文化等問題。</p>

資料來源：Internet & Jurisdiction Policy Network；本計畫彙整

(四) 後續工作重點

此計畫的全球專家後續將針對上述各項標準，提出更詳盡的建議措施，以促進不同規範之間、不同利害關係人之間的互通協調性，並預計於 2021 年的第 4 屆「網路與管轄權政策網絡全球會議」發布文件並進行討論與確認。

- 促進不同規範之間的互通協調性

研議國際人權規範、相關的國家法規與國際協議、業者的服務條款與社群守則，之間的相互作用及其對使用者的影響。例如「標準第 2 條--規範基礎」有關各種人權規範的一致性、「標準第 3 條--第三方通知 (檢舉)」有關政府依據社群守則提出檢舉的影響。

- 促進不同利害關係人之間的互通協調性

研議利害關係人 (政府、通知者、業者、使用者) 在內容限制上的程序關係。例如「標準第 4 條--業者偵測」有關 AI 決策的評估與監督機制、「標準第 9 條--用戶通知」有關通知格式與內容要項。

五、全球資訊網合約

同樣有感於網路濫用問題的日益嚴重，如利用網路進行政治操控、侵犯隱私、散播不實訊息等，全球資訊網 (World Wide Web) 發明人 Tim Berners-Lee 於聯合國 IGF 柏林會議前夕 (2019 年 11 月 24 日) 發布《全球資訊網合約》(Contract for the Web)，呼籲全球政府、企業、民眾共同承諾捍衛網路不被濫用、不會損害人權與民主，並確保網路用於造福人類。

此份合約是以既有的國際人權規範為基礎，並由來自各國政府部門、企業與民間組織的 80 多位專家耗時 1 年多完成。雖然不具約束力，但目前已獲得超過 150 個單位／組織表示支持，如 Google、Microsoft、Facebook、電子前線基金會 (EFF)，以及德法等國政府部門(Krill, 2019)。

Tim Berners-Lee 表示，將網路引領至錯誤方向的力量向來非常強大，不論對企業或政府來說，控制網路都有巨大的利益或權力。而當中最大的挑戰即是網路日漸朝向分裂敵對的「巴爾幹化」發展，且中、俄等國政府對網路的審查與監控更是日益嚴峻。因此，我們必須立即採取行動（明報，2019）。

《全球資訊網合約》共有下列 9 大原則，包括政府、企業、民眾各有 3 條應遵守的原則，這也是全球首個明列網路使用者應共同承擔責任的倡議 (World Wide Web Foundation, 2019)。

- 政府
 - 原則 1：確保人人都可連網
 - 原則 2：讓所有網路在任何時候都能連線使用
 - 原則 3：尊重並保護人們的線上隱私與資料權利
- 企業
 - 原則 4：讓網路是可負擔且可連接的
 - 原則 5：尊重並保護人們的隱私與個資以建立網路信任
 - 原則 6：開發可支持最佳人性與挑戰最壞人性的技術
- 民眾
 - 原則 7：成為網路上的創造者與合作者
 - 原則 8：打造尊重公民話語權和人類尊嚴的強大社群
 - 原則 9：捍衛全球網路

上述 9 大原則中，與內容政策相關的，主要集中在「原則 2：讓所有網路在任何時候都能連線使用」第二項的 a ~ d，也就是政府要確保刪除非法內容的要求，是以符合人權法規的方式進行：

- a. 透過合適的立法或規範，確保既有國際人權規範所保障的言論、集會結社、獲取資訊等自由，同樣確實落實於網路上的言論、行為與資訊。

- b. 贊助研究並舉辦多方利害關係人論壇，以訂定符合人權標準的爭端解決機制及內容下架（包含錯誤訊息與不實訊息）等規範。
- c. 建立機制以確保所有來自政府單位的刪除內容請求，皆是於法有據、留下文件記錄，且符合人權標準的合法性、必要性、依比例原則，包括通知發文者和潛在受眾，並受制於申訴機制和司法審查。
- d. 發展機制以確保政治廣告有效的透明度。

另外，企業應遵守的「原則 6：開發可支持最佳人性與挑戰最壞人性的技術」，當中也有部分涉及網路內容，其第一項之 c 即要求企業，應藉由定期報告展現對工作的負責，報告內容包括如何判斷與因應自家科技所衍生的網路內容（如錯誤訊息與不實訊息等）等風險。

而除了號召更多的政府、企業、公民團體與個人，連署此份合約外，研擬合約的專家們還準備發展相關的量測方法與問責機制，並推動將此合約納入聯合國的規範，進而成為全球的網路政策標準及各國的法令依據 (Krill, 2019；陳曉莉，2019)。

六、小結

正如《網路與管轄權全球現況報告》所指，網路因為跨越國界的本質以致網路治理的問題是「沒有單一政府、企業或組織，可以獨自解決」。而要藉由傳統的國家法律工具來處理包括有害與違法內容在內的網路濫用問題更是困難，並造成當前各國法規衝突、推升全球網路「巴爾幹化」現象。因此，全球網路治理專家正試圖建立一致性的政策標準，並已完成相關準則或原則。本計畫因此建議：

(一) 參考相關國際政策準則／原則，檢討我國內容治理措施

《內容與管轄權計畫：實施方案》已彙整出有害或違法內容的種類，並提供決策者於因應有害或違法內容時，可採用的實施標準（準則），如研

擬國家法規要調和不同的規範來源（國際人權原則、國家／區域相關法規、平臺服務條款與社群守則）並符合國際規範的一致性（如普遍認為兒童性虐待、誹謗為非法）、政府對於依法執行的內容限制要有適當的保護措施以免業者過度限制內容等。

而《全球資訊網合約》亦列出政府於內容治理上，應確保刪除非法內容是符合人權法規（包括透過多方利害關係人論壇訂定爭端解決機制和內容下架等規範）、建立政府單位要求刪除內容的合法機制、建立確保政治廣告透明度的機制等。

儘管這兩項國際計畫的實施標準（準則）或原則的執行細節等項目，尚在持續研擬中，且能否各自達成其預期目標——成為全球政策標準，也仍有待觀察，但現階段我國仍可就上述準則或原則，盤點檢視國內相關政策或措施，並就結果進行研議與改善，以確保我國的內容治理符合國際主流趨勢。

（二）支持全球政策標準發展，共同維護全球單一互連網路

目前部分全球網路治理專家正針對《內容與管轄權計畫：實施方案》中的各項標準（準則），提出更詳盡的建議措施，以促進不同規範（國際公約、各國法規、社群守則等）之間、不同利害關係人（政府、通知者、業者、使用者）之間的互通協調性。未來需密切關注計畫進展，如有公開徵詢意見時，則提出建議，以支持全球政策標準發展。

另外，對於 Tim Berners-Lee 所倡導的《全球資訊網合約》，雖然部分評論從過去類似倡議未能奏效而不看好此計畫，但他們也認同現在大家必須有所行動，共同推動網路改革 (Benjamin, 2019)。因此，對於此份以國際人權規範為基礎，且德、法政府皆已簽署的合約，強調以人權立國的我國亦應共襄盛舉，以共同為維護全球單一互連的網路盡一份心力。

七、參考文獻

- 明報新聞網 (2019)。萬維網之父籲「救網」 巨企響應「網絡契約」。2019/11/26。 <https://news.mingpao.com/pns/國際/article/20191126/s00014/1574707721967/萬維網之父籲「救網」-巨企響應「網絡契約」>
- 陳曉莉 (2019)。WWW 之父 Tim Berners-Lee 發起「網路合約」以捍衛全球網路。iThome, 2019/11/27。 <https://www.ithome.com.tw/news/134430>
- Bershidsky, L. (2019). Tim Berners-Lee Invented the Web. Can He Save It?. Bloomberg Opinion, 2019/11/26. <https://www.bloomberg.com/opinion/articles/2019-11-26/big-tech-and-tim-berners-lee-can-save-the-web>
- Condliffe, J. (2019). The Week in Tech: We Might Be Regulating the Web Too Fast. The New York Times, 2019/4/12. <https://www.nytimes.com/2019/04/12/technology/tech-regulation-too-fast.html>
- I&J Policy Network (2019). Content & Jurisdiction Program : Operational Approaches. 2019/4/24. <https://www.internetjurisdiction.net/publications/paper/content-jurisdiction-program-operational-approaches>
- Krill, P. (2019). Contract for the Web wants your endorsement. InfoWorld, 2019/11/26. <https://www.infoworld.com/article/3481678/contract-for-the-web-wants-your-endorsement.html>
- Lomas, N. (2019). UK quietly ditches porn age checks in favor of wider online harms rules. TechCrunch, 2019/10/16. <https://techcrunch.com/2019/10/16/uk-quietly-ditches-porn-age-checks-in-favor-of-wider-online-harms-rules/>

- Meeker, M (2019). Internet Trends 2019.
<https://www.bondcap.com/report/itr19/>
- Scott, M. (2018). The internet is broken. Can this group fix it? Politico, 2018/2/25.
<https://www.politico.eu/article/internet-governance-ottawa-regulation-balkanization-splinternet-global-jurisdiction-policy-network/>
- Stewart, T. (2019). Over 40 per cent of US news sites are still blocked in Europe a year after GDPR. 2019/5/29.
<https://mobilemarketingmagazine.com/us-news-sites-blocked-european-union-top10vpn>.
- Svantesson, D. J. B (2019). Internet & Jurisdiction Global Status Report. The Internet & Jurisdiction Policy Network, 2019/06/03.
<https://www.internetjurisdiction.net/publications/paper/internet-jurisdiction-global-status-report-key-findings>
- World Wide Web Foundation (2019). Contract for the Web.
<https://contractfortheweb.org/>

第四節 5G 治理：公眾健康、資安與國安

*本節特別邀請黃勝雄博士撰文分析

一、前言

5G (5th generation mobile networks, 第五代行動通訊系統) 建立在 4G LTE (長程演進技術) 網路架構基礎之上，以提升網路傳輸量、可靠性、及因應大量終端網路設備如 IoT 等連網需求。5G 主要技術規範包含大量物聯網設備(Massive Machine Type Communications, mMTC)、超低延遲通訊技術(Ultra Reliable Low Latency Communications, uRLLC) 及高速行動網路

(Enhanced Mobile Broadband, eMBB)。

目前 5G 尚在前期的佈建發展階段，國際網路治理領域對 5G 議題的討論大多集中於 AI、IoT、智慧城市等關鍵應用情境上，其他層面的討論則相對有限¹³。因此，考量通傳會的業務職掌，並排除已累積相當研究的 5G 頻譜議題，本節擬探討 5G 衍生的公眾健康及資安與國安議題。

自行動通訊服務發展以來，無線電波對人體的影響一直受到公眾關注，從社區到國家都曾提出不同管制行動基地臺的限制措施或建議方案。5G 網路標榜大量連網設備、高速低延遲網路等特性，更讓公眾憂慮 5G 網路無線電波是否對人體健康產生影響，無線電波對公眾健康影響自然成為 5G 網路的重要議題。

另一方面，今日世界數位經濟和社會快速發展，5G 網路被視為未來數位經濟與社會的網路骨幹。它涉及數十億個互連的人和系統，包括能源，交通，銀行和衛生等關鍵領域，並且涵蓋敏感資訊及涉及系統安全的工業控制系統。因此，5G 網路的安全性和韌性，也是至關重大議題。

二、5G 與公眾健康

(一) 科學家的研究報告

5G 網路包括多種頻率組合，工業界對 5G 技術工程細節仍在開發中。例如新的 5G 天線將很快安裝在當前 4G 天線的基地台，新的手機和設備將具有多個天線，可以在這些技術之間來回切換。然而，來自 41 個國家地區的 240 多位科學家和醫生發表研究報告，呼籲聯合國採取緊急行動，減少

13 2018 年 IGF 有座談場次討論 5G 等新興科技對網路中立與數位落差帶來的挑戰，惟討論內容多在談論其它的科技，對 5G 著墨甚少。而 2019 年 EuroDIG (歐洲網路治理論壇) 亦有座談探討 5G 法規與網路經濟的挑戰，但討論結果僅有法規須在商業創新與社會衝擊之間取得平衡，因此有賴相關利害關係人參與討論。另外，2019 年 IGF 亦有“Tech Nationalism: 5G, Cybersecurity and Trade”座談，討論摘要請詳本報告第五章第二節「2019 聯合國網路治理論壇 (IGF)」。

日益增加的無線輻射暴露。他們認為，5G 網路對人類健康和環境具有嚴重風險，因此也連署要求美國聯邦通訊委員會 (FCC) 暫停 5G 網路的推廣。

另外，2019 年瑞士保險報告亦將 5G 行動網路列為影響財產和傷亡索賠的高影響力新風險。報告並指出，由於人們對於電磁場 (EMF) 對健康影響仍有許多爭論，因此，相關潛在的健康損害賠償預期將會拖延很久。

其實目前 2G，3G 和 4G 的無線網路技術，包含我們所使用的手機、電腦和可穿戴技術，皆會產生無線電頻率暴露，且對人類、動物和環境構成一定程度的健康風險。科學家警告說，在推出 5G 網路之前，必須首先完成對人類健康影響的研究，以保護公眾健康和環境安全。

(二) 美國情況

美國政府積極推動 5G 網路建設，並於各州和聯邦政府頒布法規，以簡化 5G 網路擴充部署申請。美國疾病管制局 (CDC) 和環境保護局 (EPA) 的官方網站亦顯示行動通訊產生的輻射是安全的，且政府也沒有推出更審慎的公共衛生措施來確保公眾的安全。

美國 5G 網路訂於 2020 年才正式提供商業服務，現在已有部分城市成為 5G 測試區域。根據電信服務公司 Verizon 公司和 Sprint 公司所發布的訊息，這些 5G 測試區包括華盛頓特區、亞特蘭大、達拉斯、邁阿密和紐約等。

不過，基於微波可能影響健康考量，美國舊金山北邊 Mill Valley 市議會於 2018 年 9 月即已通過投票，規定住宅區禁止安裝 5G 小型基地台。這項限制將使未來 5G 於全美國推動所面臨的變數，更加複雜。

(三) 歐洲與其他國家情況

行動網路公司的文件清楚說明 5G 網路增加天線附近的無線頻率輻射量。中、俄、意大利和瑞士等國訂定嚴格的輻射限制規定，5G 網路增加的輻射如果超出輻射限制，將不允許部署無線網路。行動網路輻射規定限縮

行動網路業者的網路建設，行動網路業者一方面希望政府放寬輻射限制，另一方面必須投入更多資源改善網路設施環境，以符合法規要求。

歐洲調查發現，至少有三項行動通訊對健康風險的研究，其資金來源與產業之間存在連結關係。由產業資助的研究產出健康風險的可能性低於由中立研究機構資助的研究。考量產業資助的研究可能會產生偏見，歐洲調查組織於 2019 年由 14 名科學家組成小組，協助總部位於德國的非政府組織——國際非游離輻射防護委員會 (ICNIRP) 研究電磁場暴露準則。

同樣基於不確定 5G 新技術對健康潛在影響的考量，瑞士伯爾尼聯邦政府認為臨時凍結 5G 網路建設，是各州政府阻止 5G 網路技術所能採取的最合理措施。日內瓦和沃州政府則進一步通過凍結架設 5G 天線的許可證，以控制管轄區域內的 5G 網路建設。而即便業者安裝的新 5G 天線符合瑞士聯邦政府發布的法規，瑞士綠黨仍然認為需要更廣泛的公開討論，不僅只評估 5G 網路電波對健康的影響，更應該廣泛探討所有移動天線發出無線電波對健康的影響。



照片來源：AFP; The Guardian

圖49. 瑞士、澳洲民眾上街抗議 5G 建設

(四) 設備過熱問題

5G 網路的發展帶給資訊社會很多創新想像，如行動物聯網、AR/VR (虛擬實境/擴增實境)、低延遲網路等，但設備發熱卻是業界一直無法解決

的問題。毫米波在高頻率（接近微波）運行，晶片需要極高時鐘速率，產生的熱量集中在手機極小部分的元件中，並沒有簡單的方法移除這些熱量。只要網速達到4Gbps以上，手機短短幾秒內就會升溫到45度高溫。雖然設備製造商終究應可以解決散熱問題，但截至目前仍無太大進展。

三、5G 與資安、國安

(一) 關鍵安全議題

5G網路包含許多重要的關鍵安全議題，與現有網路的情況相比，這些關鍵安全議題在5G網路設計概念顯得更加突出。關鍵安全議題包含關鍵創新技術、網路攻擊風險增加、對技術供應商依賴程度等。

1. 關鍵創新技術

現有的通訊網路設計概念主要以通訊硬體元件組合為主，5G網路支持廣泛的應用服務與應用程序，以軟體設計及軟體架構為主軸的5G網路對於資訊安全的重要性遠高於現有行動網路。5G網路在資通安全方面具有獨特挑戰。5G網路的主要功能是基于軟體而非硬體來實現。相對於傳統行動網路，這是5G網路的優勢，但它同時也是資安漏洞的來源，因為軟體容易受到利用其資安漏洞的潛在惡意攻擊。此外，當今的資訊科技系統極為複雜，智慧手機系統擁有超過80億個電晶體，作業系統擁有超過5000萬行程式碼。由於軟體更新需求系統提供遠端接取的隱藏後門程式，這可能為惡意攻擊者提供更多的資安漏洞。攻擊者利用系統漏洞取得重要資料或系統控制權。如果無法檢測和監控後門程式，勢必損害5G網路的安全性。

2. 網路攻擊風險增加

5G網路架構使得無線接取網路（基地台和天線）與核心網路之間區別更加模糊。智慧運算功能逐漸朝網路邊緣而不是網路核心發展，這可能對網路安全產生重大影響。分佈在邊緣網路的智慧運算越多，連接的設備數

量將迅速增加，受到網路攻擊接觸範圍就越大。巨量成長的網路流量將使檢測惡意網路流量變得更加困難。

5G 網路技術提供者內部軟體開發流程不當而產生系統安全漏洞，將使 5G 網路面臨的風險更加嚴峻。網路攻擊者可利用系統安全漏洞插入惡意軟體，這類產品內嵌型風險難以事先被發現，營運者也不易規劃風險防範措施。雖有很多方法可以解決這些問題，安全評估、程式碼審查和滲透測試都有助於提高整體軟體品質，但是幾乎沒有一項有效的技術方法能證明系統沒有惡意程式或後門。

3. 對技術供應商依賴程度

在此背景下，政府對 5G 設備供應商的特質和品質的擔憂是可以理解的。事實上，從技術角度根本不應該信任任何資通設備，這使得對設備製造商的信任度更加重要。但這點取決於設備製造商運營所在地的司法管轄權、法律體系和法治。對 5G 網路產品的風險評估應考慮所有相關因素，包括適用的法律環境和供應商生態系統等因素。政府面臨的問題是如何確保部署高度彈性且信賴的 5G 網路基礎設施，由此基礎推動國家未來的經濟和社會發展。

(二) 資安與國安

1. 美國對華為 5G 採限制措施

以美國為例，美國認為中國大陸華為公司可能涉嫌違反美國出口管制向伊朗出售敏感科技。美國訂定若干措施抵制華為公司網路通訊產品，尤其是 5G 網路產品。美國政府認為華為公司 5G 設備具嚴重網路安全威脅，華為公司產品除了有系統後門資安漏洞，且是個殺戮開關 (Kill Switch)，即是系統平時可能維持正常運作狀態，但是到了某時間點系統資安漏洞開關被開啟，可以癱瘓網路造成重大災難。英國「華為安全評估中心」研究報告亦指出「華為產品在軟體工程與網路安全能力方面有嚴重缺陷」。

雖然華為公司宣稱沒有任何公司的網通產品能夠達到 100% 的系統安全，但此說法不足以說服美國政府或營運商，願意導入已知重大安全缺陷的華為產品。多數網路營運商採安全網路架構設計限制攻擊者的攻擊能力，並結合其他安全控制措施，增加攻擊者利用系統漏洞的攻擊難度。這樣的機制下，如果導入相對安全可靠通訊產品，仍能將網路安全控制在一個可接受範圍。

但美國政府以國家安全為由，將華為技術列入黑名單，並且禁止美國公司未經政府事先批准出售技術和軟體給華為公司。美國同時敦促其他國家共同禁止華為技術。中國大陸於 2017 年公布《國家情報法》是一個重要因素，該法規允許政府強迫華為等公司關閉客戶的電話，或使用其基礎設施為政府提供情報優勢。雖然華為最高管理層一再表示，他們寧願倒閉而不願成為中國大陸政府的間諜，並提出與美國、德國和英國的無間諜協議，但由於華為無法證明其網通系統無惡意程式碼，除非網路完全實體隔離，否則系統如果被入侵破壞將無法實現政府期望的高韌性網路。

市場部分分析師認為，美國限制華為等中國大陸公司技術出口可能最終適得其反，因為如果以安全為由對華為的禁令是合理的，那麼停滯出口可能會使情況變得更糟。例如，阻止 Google 與華為交易將推動中國華為公司創建自己的 Android 版本，該版本可能比原有 Google 版本具有更多的錯誤。尤其是在中國大陸這反而會增加華為手機被入侵的風險。此外，儘管出口禁令將削弱華為公司的實力，但不會令華為公司倒閉，最終可能為中國大陸提供更強大的動力，使其在技術上獨立於美國。限制美國技術出口也將減少美國的產出和就業機會。

美國與中國大陸的科技戰未必是美國的最佳選項。與 4G 網路情況不同的是，目前中國大陸顯然是 5G 網路的領先者。美國國防部國防創新委員會最近的一份報告明確指出「隨著 5G 相關頻段部署全球，中國大陸的手機和其網路服務即使被排除在美國之外，也會佔有一定程度的主導地位。中國大陸可望在 5G 網路重現美國於 4G 網路所經歷的一切」。

2. 歐盟進行 5G 網路安全評估

美國政府和歐洲國家在 5G 安全管制措施不盡相同。歐洲選擇的是較為謹慎的作法。2019 年 3 月 22 日的歐盟理事會上，各國領導人表示需要對 5G 網路的安全採取協調一致的方法，歐盟委員會建議採取一系列步驟和措施來確保歐洲 5G 網路的安全，包括導入現有工具（如認證方案）或發展新工具來進行風險評估。每個成員國都被要求實施風險評估，以完成整個歐洲 5G 網路威脅樣態的風險評估。

歐盟理事會於 2019 年 10 月 9 日公布 5G 網路安全評估報告，彙整各國依據現況評估 5G 導入對網路安全的影響，這些影響包含邊緣網路架構改變、供應鏈改變、供應商依賴度、對 IT 應用衝擊等主要構面。5G 網路將集中式網路架構移轉至邊緣運算架構，使得邊緣設施對資訊安全敏感度大為提高，例如基地臺或接取網路等。5G 網路供應鏈將有更多第三方供應商提供服務並因此提高資安風險。基於 5G 高技術障礙，使網路服務提供者對技術供應商依賴程度提升，此依賴度集中現象形成技術提供商高依賴風險。5G 服務場域包含企業應用服務垂直整合，此架構不僅衝擊企業資訊的機密性與隱私，也影響其完整性與可用度，對於網路安全將是一大挑戰。

英國國家網路安全中心在減緩資通安全政策研究提出多種建議措施以降低 5G 網路風險，包括要求網路每個區塊必須具備多家供應商之規定；核心網路機敏設施必須規避高風險供應商；網路設計必須兼容非特定品牌設備避免供應商風險；建立持續的監控風險機制。歐洲成員國將建構 5G 網路作為建立資通訊技術供應鏈審查流程機會，以評估 5G 網路對國家安全產生的風險。

四、小結

(一) 行動通訊技術的健康疑慮未曾間斷，著手準備 5G 公眾回應方案

無線通訊網路涉及的公眾健康議題，從過去的行動通訊技術，到即將大量部署的 5G 網路，一直未曾間斷，今年 (2019) 瑞士與澳洲都發生民眾上街抗議 5G 建設的案例。這些問題也造成網路服務提供者的不確定因素。但無論如何，在行動通訊技術與服務推陳出新發展下，這個議題將會繼續存在，並持續受到公眾檢視。因此，即使截至目前尚無有效措施可以降低公眾對於無線輻射的疑慮，但主管機關仍應著手準備如何與公眾溝通或回應公眾的相關方案，以因應我國即將於 2020 年啟動 5G 商轉。

(二) 了解 5G 網路特性，透過多管齊下降低國安風險

5G 網路本質以軟體為主軸，軟體系統對於資訊安全的影響甚巨，甚至衝擊關鍵基礎設施發展。網路營運商應採安全網路架構設計，限制攻擊者的攻擊能力，並結合其他安全控制措施以減緩網路攻擊。而政府主管機關則應了解 5G 網路以軟體導向的技術特性、軟體系統優缺點、各項技術可行的量測工具、5G 核心設備製造商運營所在地的司法管轄權、法律體系和法治，同時參考國際降低 5G 風險的可能政策措施，包含多家供應商原則、持續監控風險機制、技術供應鏈審查流程等措施。透過多管齊下方式，將 5G 網路對國家安全的可能衝擊降到最低。

五、參考文獻

- Environmental Health Trust (2019). 5G and the IoT: Scientific Overview of Human Health Risks.
- European Union External Action. (2019) . EU-coordinated risk assessment of 5G network security.
https://eeas.europa.eu/headquarters/headquarters-homepage/68637/eu-coordinated-risk-assessment-5g-network-security_my
- Le News. (2019). Geneva blocks the erection of 5G mobile antennas.
<https://lenews.ch/2019/05/02/geneva-blocks-the-erection-of-5g-mobile-ante>

nna/?fbclid=IwAR2h7cRZlof7qxZAEy0sTgfC_efkJWp4d7vapGwxs228fug8r8I0cbpV2jE

- National Instruments (n.d.). 5G New Radio 的五大要點.
<https://www.ni.com/zh-tw/innovations/wireless/5g/new-radio.html>
- Newman, J. (2019) Thousands take to the streets of Switzerland protesting against 5G mobile phones signals amid fears the electromagnetic technology could damage people's health. MailOnline, 2019/9/22.
<https://www.dailymail.co.uk/news/article-7492349/Thousands-streets-Switzerland-protesting-against-5G-mobile-phones-signals.html>
- Taylor, J. (2019). 5G in Australia: getting up to speed with the future of mobile. The Guardian, 2019/7/27.
<https://www.theguardian.com/technology/2019/jul/28/5g-in-australia-getting-up-to-speed-with-the-future-of-mobile>
- Wagstaff, J. (2019). 5G's Achilles Heel: Heat.
<http://www.loosewireblog.com/2019/10/5gs-achilles-heel-heat.html?fbclid=IwAR2YMOtMfGHQvcn30blzIKeuJpaLn4pQnVFKMqu1tpAQdC6yQf2WkF5h23M>

第八章 結論與建議

本計畫透過舉辦 6 場大專院校宣講活動，及開辦兩天一夜的研習課程，提升大專青年對網路治理議題的認知，並培養我國網路治理的多元專業人才。另一方面，也邀請國際專家訪臺，分享國際網路治理政策，並與國內相關各界交流。同時亦規劃舉辦 OTT 影音與 AIoT 治理議題的座談會議，增加國內多方社群對話機會，促進凝聚政策共識。此外，還參與 APriIGF 與 IGF，與各國交流治理政策議題，並將參與心得與國內各界分享。最後，本計畫也彙整分析 AI、網路內容、5G 等治理議題，以協助我國掌握通傳政策議題動向，促使我國網路治理發展符合國際趨勢。

本計畫並針對上述各項工作，提出結論與建議：

一、大專院校宣講

- 不同宣講場合各有其深廣度宣傳效果，值得持續辦理

本計畫辦理 6 場次大專院校宣講活動，其場合有特定課程或全系所的固定集會活動，科系則橫跨文科與理科，出席者涵蓋大學生與研究生，出席人數每場最少為 31 人，最多高達 210 人。整體而言，特定課程的學生人數雖然較少，但卻提供講師和學生深度交流的機會；而全系所活動則因人數動輒上百人，有助於擴大網路治理的宣導廣度。至於科系與系所，大致上是研究生對網路治理較有興趣，但科系則未能有明顯定論（如成大電機所、政大行政管理所的學生都積極提問）。無論如何，大專院校宣講活動都值得未來持續辦理。惟許多研究所的班級學生人數較少，又北部大專院校的數量也相對較多，因此，未來計畫規格設計宜保留執行彈性，以利能從宣講效果角度尋求較為合適的宣講學校與系所（本年度有每場 30 人以上、北中南各 2 所學校等規定）。

二、人才培訓課程

- **學員出席率與結業率皆達 100%，時程與課程規劃可為未來參考**

本年度 40 位學員皆全程出席並完成 2 天的研習課程，出席率與結業率皆為 100%，遠高於去 (2018) 年的 77% 與 70%。推估原因可能和活動期程從 4 天縮短為 2 天，以及活動時間從 7 月暑假提前至 5 月底 6 月初有關¹。另外，學員對於演練課程的滿意度也從去年的 85% 增加為今年的 95%，且講師陣容也廣獲學員好評，因此，本年度的時程與課程規劃可作為未來參考。惟亦有學員反應 30 分鐘的專題講習時間太短，且休息時間也不足，所以，未來可改為 1 小時 1 堂課 (包含講習、Q&A、休息) 的安排規劃。

- **學員國內參與興趣大於國際，未來課程可增加國內議題的比重**

根據課後問卷調查，85% 學員表示願意參加 TWIGF，但願意參加 (線上參與) 聯合國 IGF 與 APriGF 者，分別只有 43% 與 35%，凸顯大約 6 成學員對於網路治理的國際參與興趣缺缺，因此，未來課程內容可增加國內議題與國內參與機會的比重。

- **興趣及知識未能充分轉為行動力，促進參與有賴各界共襄盛舉**

本年度高達 93% 學員表示上完課程後對網路治理的興趣增加、85% 表示願意參加 TWIGF，且多數學員 (63%~83%) 認為學習到如何參與討論、治理議題挑戰、基本概念等，顯示達到柯氏 (Kirkpatrick) 學習成效的學習層級 (第二層級)。不過，經本計畫追蹤，實際出席 TWIGF 者只有 35% (14 位)，且當中有 8 位是參加本計畫提供獎學金 (新臺幣 2 千元) 的 TWIGF 特派員活動，凸顯只憑短期誘因，且缺乏責任歸屬的驅動要素下，難以將學員的興趣及知識技能轉化成具體行為力。此問題有賴社會各界共同創造長期穩定的誘因 (如工作機會、持續參與國際會議的機會) 才能改善。

- **整體計畫時程宜提前啟動，以保留充足的宣傳與報名時間**

本年度計畫自 4 月 24 日開始執行，並於 5 月 31 日即開辦研習營活動，以避免和大專院校的期末考試時間衝突，並趕上安排優秀學員參與 APriGF

的出國事宜。雖然本計畫已提前展開前置規劃，並於4月26日正式對外公開活動暨受理報名，且在高度壓縮評選作業、通知回覆作業、會務行政等工作時程下，已儘可能將報名截止日期延後至5月12日。不過，仍有大專院校反應收到活動公文已逾報名期限；另一方面，也無法搭配本計畫的大專院校宣講活動，讓兩者發揮宣傳綜效。因此，建議未來計畫時程宜提前展開，以保留充足的宣傳、報名，甚至是整個計畫的規劃與作業時間。

三、國際專家訪臺

- 國際專家訪臺開拓治理議題視野，促進臺日網路治理交流

本年度邀請網路技術維運與相關國際事務協調專家、現任 ICANN 董事的 Mr. Maemura Akinori 訪臺。透過拜會通傳會，以及至 TWIGF 發表專題演說並參與座談討論等行程，Mr. Maemura 除了分享日本當前最主要的治理議題案例--封鎖盜版漫畫網站，並分析其政策發展尚未成功的原因外，也促使我們認識全球正關切的網路市場高度集中化或鞏固 (consolidation) 現象，讓我國得以借鏡並開拓治理議題視野。此外，他還說明「國家主權沒有管理全球網路資源的正統性...但網路治理的經濟與社會問題必須由公共政策和法規管理，且透過多方利害關係人取向 (方式)」的觀念，強化我國推動多方利害關係人參與的信念。Mr. Maemura 並提到日本民眾不太關心網路治理議題，日本 IGF 也只是數十人參與。而在親臨 TWIGF 後，相信他也會將臺灣的參與盛況帶回日本分享。

四、通傳議題座談會議

- 低度管理 OTT 影音及共促 AIoT 安全為共識，歧見亦可為後續討論基礎

本計畫於 TWIGF 申辦 OTT 影音治理，及 AIoT 安全與隱私，共 2 場座談。前者的與談人一致認為我國 OTT 影音的政策方向應採低度管理，政策內容要能務實考量，並維護市場所有參與者的公平競爭，同時也要重視消

費者權益；後者的與談人也都認同 AIoT 的安全隱私有賴各方共同推動，包括消費者應具備購買安全性產品等資安意識、政府要訂定資安標準及帶頭示範採購安全性產品、業者要將安全納入產品開發設計等。這些共識可作為相關政策的參考。

而儘管大家對 OTT 影音治理的低度管理程度與方式、管理項目，以及保護消費者的做法等層面，仍有許多不同意見；另外，AIoT 安全隱私場次對於政府能否基於安全而偵測民眾的裝備或要求產品預留後門程式，也未形成共識。不過，這些歧見仍有助於促進彼此的理解與溝通，可作為後續政策討論的基礎。

五、國際會議參與

● 東南亞國家熱衷參與 APrIGF，我國也應展現積極參與

近年來，東南亞國家非常熱衷參與 APrIGF，尤其今年 (2019) 座談場次至少有 6 成是由這些國家主辦，其中印度主辦的場次即高達 6 場 (共 25 場)；另外，菲律賓每年也派送十多名大學生參與 yIGF。因此，我國也應該展現積極參與，促進網路治理政策的對話與交流。

● 關注 IGF Plus 模式發展，為全球數位合作貢獻心力

今年 (2019) IGF 大會主題為「一個世界，一個網路，一個願景」，凸顯當前全球網路因為許多國家主張網路主權、各國網路法規衝突等因素，而面臨網路分裂的危機，這也是今年許多場次不斷討論的問題。因此，如何透過國際合作以維護全球網路的自由開放，已成為當務之急。而在全球專家所提出的國際合作模式中，又以在現有基礎上強化具體產出的 IGF Plus 模式獲得廣泛支持，因此，我國應密切關注其後續進展，適時為推動全球數位合作貢獻一份心力。

● IGF 首度強調議員參與，56 國議員建議值得我國學習參考

由於各國法規衝突也是導致全球網路分裂的主要風險，因此，為了能讓 IGF 討論成果在各國立法機關發揮作用，本屆論壇首度為立法人員舉辦專屬場次，且共有 56 國議員參與，他們除了深刻了解各國的立法決策會影響全球網路能否維持自由開放外，也共同發表對各國議員的建議，包括針對網路相關的政策議題加強國際合作與交流、確保提升國安與促進數位經濟發展的新立法將會充分保護人權與自由、以因應數位時代挑戰的精神重新思考現有的國家法律、訂定新法案時會充分納入各社群並推動多方利害關係人方法等。這些建議充分反映當前網路政策與立法所需的基本精神，值得我國政府部門與立法單位參考並學習。

六、治理議題分析

• 發展可信賴 AI 已成國際趨勢，關注 AI 規範是否成為下個 GDPR

歐盟《可信賴 AI 的倫理準則》與《可信賴 AI 的政策與投資建議》，以及《OECD AI 原則》的政策目標，皆為發展以人為本、可信賴的 AI，且對應的實施準則及政策建議也高度相似，並在歐、美、日等國的合作推動下，讓 G20 也採用《OECD AI 原則》。本計畫統計發現，目前全球已有約 60 個國家直接或間接採認 OECD 原則。因此，發展以人為本、可信賴的 AI，可說已成國際趨勢，甚至如 OECD 所稱的成為「國際標準」。

另一方面，新任歐盟執委會主席范德賴恩 (Ursula von der Leyen) 已承諾，將在就任 100 天內，針對 AI 對人類與倫理的衝擊，提出立法。美國《政治》(Politico)等媒體報導認為，AI 法規可能成為下一個 GDPR。歐盟 2018 年起實施的 GDPR 對全球的影響仍持續發酵中，包括我國政府也正和歐盟協商取得符合 GDPR 的適足性認定，並很可能須修改我國現行的《個人資料保護法》。而一旦歐盟推出類似 GDPR 的 AI 法規，勢必將為全球帶來新一波的法規衝擊。因此，相關後續發展值得我國高度關注。

• 歐美日以國家總體策略迎接 AI 時代，我國 AI 產業計畫應進行升級

綜觀《歐盟 AI 策略》、《OECD AI 原則》、《美國 AI 倡議》、日本《以人為本的 AI 社會原則》可發現，先進國家是以各自的基本價值觀為基礎，從整體社會的角度，採取多方利害關係人的方式，並透過國家層級的總體策略，來迎接 AI 時代的機會與挑戰。相較之下，我國雖訂有《臺灣 AI 行動計畫》及《人工智慧科研發展指引》，且科技部也推出「AI 之人文社會研究計畫」，以及國發會亦進行「數位經濟及 AI 對社會影響與因應策略」研究。然而，在缺乏基本價值的支撐、偏重產業思維而非整體社會權益、未能從國家層級應對倫理挑戰，以及欠缺多方利害關係人充分對話等情況下，恐怕難以全面且有效地迎接 AI 發展及因應衝擊。

其實許毓仁等立委已針對我國缺乏國家層級的 AI 政策問題，提出《人工智慧發展基本法》並獲得立法院一讀通過。不過，目前國際仍未有透過立法推動或因應的案例。我國的當務之急應是採取網路治理方法，邀請多方利害關係人充分討論基於臺灣基本價值的 AI 願景、準則、推動方式（訂定國家策略或立法措施），以及實施方法等問題，以迎接讓整體社會受益的 AI 發展，同時將衍生的負面衝擊降到最低。

● 參考相關國際政策準則／原則，檢討我國內容治理措施

《內容與管轄權計畫：實施方案》已彙整出有害或違法內容的種類，並提供決策者於因應有害或違法內容時，可採用的實施標準（準則），如研擬國家法規要調和不同的規範來源（國際人權原則、國家／區域相關法規、平臺服務條款與社群守則）並符合國際規範的一致性（如普遍認為兒童性虐待、誹謗為非法）、政府對於依法執行的內容限制要有適當的保護措施以免業者過度限制內容等。而《全球資訊網合約》亦列出政府於內容治理上，應確保刪除非法內容是符合人權法規（包括透過多方利害關係人論壇訂定爭端解決機制和內容下架等規範）、建立政府單位要求刪除內容的合法機制、建立確保政治廣告透明度的機制等。

儘管這兩項國際計畫的實施標準（準則）或原則的執行細節等項目，

尚在持續研擬中，且能否各自達成其預期目標——成為全球政策標準，也仍有待觀察，但現階段我國仍可就上述準則或原則，盤點檢視國內相關政策或措施，並就結果進行研議與改善，以確保我國的內容治理符合國際主流趨勢。

- **支持全球政策標準發展，共同維護全球單一互連網路**

目前部分全球網路治理專家正針對《內容與管轄權計畫：實施方案》中的各項標準（準則），提出更詳盡的建議措施，以促進不同規範（國際公約、各國法規、社群守則等）之間、不同利害關係人（政府、通知者、業者、使用者）之間的互通協調性。未來需密切關注計畫進展，如有公開徵詢意見時，則提出建議，以支持全球政策標準發展。

另外，對於 Tim Berners-Lee 所倡導的《全球資訊網合約》，雖然部分評論從過去類似倡議未能奏效而不看好此計畫，但他們也認同現在大家必須有所行動，共同推動網路改革 (Benjamin, 2019)。因此，對於此份以國際人權規範為基礎，且德、法政府皆已簽署的合約，強調以人權立國的我國亦應共襄盛舉，以共同為維護全球單一互連的網路盡一份心力。

- **行動通訊技術的健康疑慮未曾間斷，著手準備 5G 公眾回應方案**

無線通訊網路涉及的公眾健康議題，從過去的行動通訊技術，到即將大量部署的 5G 網路，一直未曾間斷，今年 (2019) 瑞士與澳洲都發生民眾上街抗議 5G 建設的案例。這些問題也造成網路服務提供者的不確定因素。但無論如何，在行動通訊技術與服務推陳出新發展下，這個議題將會繼續存在，並持續受到公眾檢視。因此，即使截至目前尚無有效措施可以降低公眾對於無線輻射的疑慮，但主管機關仍應著手準備如何與公眾溝通或回應公眾的相關方案，以因應我國即將於 2020 年啟動 5G 商轉。

- **了解 5G 網路特性，透過多管齊下降低國安風險**

5G 網路本質以軟體為主軸，軟體系統對於資訊安全的影響甚巨，甚至

衝擊關鍵基礎設施發展。網路營運商應採安全網路架構設計，限制攻擊者的攻擊能力，並結合其他安全控制措施以減緩網路攻擊。而政府主管機關則應了解 5G 網路以軟體導向的技術特性、軟體系統優缺點、各項技術可行的量測工具、5G 核心設備製造商運營所在地的司法管轄權、法律體系和法治，同時參考國際降低 5G 風險的可能政策措施，包含多家供應商原則、持續監控風險機制、技術供應鏈審查流程等措施。透過多管齊下方式，將 5G 網路對國家安全的可能衝擊降到最低。

附件

附件一：「大專院校宣講活動」簡報資料

附件二：「網路治理研習營」課程簡報資料

附件三：「網路治理研習營」學員手冊

附件四：「網路治理研習營」TWIGF 特派員座談摘要報告

附件五：國際專家訪臺專題演講簡報資料

附件六：「OTT 現狀、治理及未來展望座談」簡報資料

附件七：「AIoT 時代的安全與隱私挑戰座談」簡報資料

附件八：研習營優秀學員 2019 APrIGF 出國報告