

# 國家通訊傳播委員會補助計畫

## 「網路治理交流與人才培育」計畫

### 期末報告

報告日期：107 年 12 月 19 日

計畫期程：107 年 3 月 23 日至 107 年 12 月 31 日止

執行單位：財團法人中華民國國家資訊基本建設產業發展協進會



## 目 錄

摘 要 .....	vii
壹、 計畫簡介.....	1
一、 緣起與目標 .....	1
二、 計畫架構與內容 .....	1
三、 執行時程及進度 .....	2
四、 預期成果與績效指標 .....	3
貳、 人才培育.....	5
一、 研習營活動簡介 .....	5
二、 宣傳與評選 .....	15
三、 課程內容重點 .....	22
四、 印刷與影音記錄 .....	34
五、 滿意度調查結果 .....	36
六、 選拔優秀學員參與國際會議 .....	37
參、 議題分析與多方參與.....	40
一、 資料在地化座談 .....	40
二、 國際參與分享座談 .....	54

---

三、	歐盟《防止散播線上恐怖主義內容法案》 .....	65
四、	歐盟《處理線上不實訊息之歐洲作法通告》 .....	78
五、	歐盟《著作權指令》法案 .....	91
六、	法國與歐盟爭取全球網路治理領導角色 .....	98
七、	美國商務部公開徵詢國際網路政策優先議題 .....	107
八、	俄羅斯號召金磚國家另建網路系統 .....	125
<b>肆、</b>	<b>國際參與及交流 .....</b>	<b>132</b>
一、	邀請國際專家訪臺 .....	132
二、	2018 亞太區網路治理論壇 (APrIGF) .....	143
三、	ICANN 第 63 次會議 .....	159
四、	2018 聯合國網路治理論壇 (IGF) .....	170
<b>伍、</b>	<b>結論與建議 .....</b>	<b>183</b>
一、	人才培育 .....	183
二、	議題分析與多方參與 .....	184
三、	國際參與及交流 .....	188

## 圖目錄

圖 1. 計畫架構圖.....	2
圖 2. 研習營活動網站.....	16
圖 3. 活動宣傳：TWIGF 與 NetMission 臉書社團.....	17
圖 4. 活動宣傳：TWNIC 網站與 5 月份電子報.....	18
圖 5. 活動宣傳：大專院校訊息發布.....	18
圖 6. 活動宣傳：發文邀請.....	19
圖 7. 合格報名者的得分分佈.....	20
圖 8. 研習營學員組成概況.....	21
圖 9. 網路運作流程圖.....	26
圖 10. ICANN 多方利害關係人模式.....	27
圖 11. 研習營布置與印刷品.....	34
圖 12. 研習營照片.....	35
圖 13. 研習營授課課程錄影檔之頁面截圖.....	36
圖 14. 研習營活動滿意度問卷調查結果.....	37
圖 15. 研習營網站公布優秀學員名單.....	38
圖 16. 全球實施「資料在地化」措施概況 (2015 年).....	41
圖 17. 世界各國限制資料流通概況 (2017 年).....	42
圖 18. 「資料跨境流通與資料在地化對我國的挑戰」座談照片.....	53

圖 19. 「從臺灣、區域與全球看當前網路治理發展」座談會網站頁面 .....	57
圖 20. 「從臺灣、區域與全球看當前網路治理發展」座談會臉書社團宣傳	57
圖 21. 2018 聯合國 IGF 會議類型與討論議題 .....	60
圖 22. 「從臺灣、區域與全球看當前網路治理發展」座談會線上提問 .....	63
圖 23. 「從臺灣、區域與全球看當前網路治理發展」座談會照片 .....	64
圖 24. 歐盟執委會因應線上「違法內容」措施發展 (截至 2018 年 3 月)...	69
圖 25. 歐盟處理假新聞與不實訊息的政策發展(至 2018 年 4 月).....	81
圖 26. 《歐盟不實訊息實踐準則》簽署範例-- Google .....	86
圖 27. Internet DNS Root System 註冊與解析 .....	126
圖 28. 國際專家 Mr. Fred Baker 訪臺照片 .....	142
圖 29. 2018 APrIGF 會議剪影 .....	158
圖 30. ICANN 63 會議照片 .....	169
圖 31. 聯合國 IGF 會議剪影 .....	182

## 表 目 錄

表 1. 計畫執行時程及進度.....	2
表 2. 計畫績效指標.....	4
表 3. 原訂中文課程表.....	7
表 4. 原訂英文課程表.....	8
表 5. 新版中文課程表.....	9
表 6. 新版英文課程表.....	10
表 7. 「從臺灣、區域與全球看當前網路治理發展」座談會議程.....	55
表 8. 2018 TWIGF 座談題目.....	59
表 9. 歐盟線上「違法內容」類別與因應措施.....	66
表 10. 歐盟《防止散播線上恐怖主義內容法案》的爭論與說明.....	74
表 11. 《歐盟不實訊息實踐準則》業者承諾事項.....	84
表 12. 歐盟因應線上內容問題的類別與政策措施.....	87
表 13. 美國 NTIA 徵詢國際網路政策優先議題之題目.....	110
表 14. 多方社群回覆 NTIA 徵詢國際網路政策優先議題.....	113
表 15. 2018 APrIGF 參與場次.....	144
表 16. 亞太各國 IGF 辦理概況.....	151
表 17. ICANN63 參與場次.....	160
表 18. 2018 IGF 參與場次.....	171



## 摘要

本計畫透過人才培育、議題分析與多方參與，以及國際參與及交流等工作，培養我國參與國內外網路治理之人才，促進國內網路政策對話與未來國際參與，並掌握當前全球重要網路政策議題與未來前瞻發展，強化國際雙向且實質交流，促進我國網路治理發展符合國際趨勢。

本計畫執行時程自 107 年 3 月 23 日起至 107 年 12 月 31 日止。本報告依據計畫書與補助契約書，如期完成下列所有工作項目。

	契約書規定項目	本計畫完成情況概述
期中報告	1.完成至少 20 人的人才培訓課程，並選拔優秀人才參與國際會議	共計 31 位學員完成人才培訓課程，並評選出 2 名優秀學員參與 2018 APrIGF
	2.舉辦至少 1 場次國內研討會、座談會或論壇，並提供重要議題報告	完成舉辦「資料跨境流通與資料在地化對我國的挑戰」座談及重要議題報告
	3.邀請國際專家至少 1 人訪臺交流	完成國際網路技術標準與政策專家 Mr. Fred Baker 訪臺行程
期末報告	1.舉辦至少 1 場次國內研討會、座談會或論壇，並提供重要議題報告	完成舉辦「從臺灣、區域與全球看當前網路治理發展」座談及重要議題報告
	2.出席 2018 年亞太區網路治理論壇 (APrIGF)，並提供重要議題報告	完成出席 2018 APrIGF (包括人才培訓 2 名優秀學員) 並提供重要議題報告
	3.出席 ICANN (網際網路名稱與號碼指配組織) 63 公共會議，並提供重要議題報告	完成出席 ICANN 63 公共會議並提供重要議題報告
	4.提供至少 6 篇國際議題分析	完成 6 篇國際議題分析，包括：

契約書規定項目	本計畫完成情況概述
	<ul style="list-style-type: none"> <li>• 歐盟《防止散播線上恐怖主義內容法案》</li> <li>• 歐盟《處理線上不實訊息之歐洲作法通告》</li> <li>• 歐盟《著作權指令》法案</li> <li>• 法國與歐盟爭取全球網路治理領導角色</li> <li>• 美國商務部公開徵詢國際網路政策優先議題</li> <li>• 俄羅斯號召金磚四國另建網路系統</li> </ul>
5. 出席 2018 年聯合國網路治理論壇 (IGF)，並提供重要議題報告	完成出席 2018 IGF 並提供重要議題報告

綜合各項執行成果，本計畫提出下列結論與建議。

### 1. 人才培育

- 四成錄取者放棄學員資格，如何鼓勵社會參與仍待努力
- 大專學員背景知識較為不足，未來課程可採分級並做延續性規劃
- 追隨人才培育國際趨勢，於大專院校開設學分課程

### 2. 議題分析與多方參與

- 借鏡歐盟以多方程序循序漸進治理內容，法規介入僅為最後手段
- 歐盟會員國不易落實《著作權指令》，政策規劃須兼顧各方權益
- 從動態發展中尋求我國最佳多方治理模式，把握公開公平原則
- 參考美國資訊自由流通等網路政策，惟我國立場應由多方討論
- 俄羅斯另建網路系統可行性低，維持現有系統符合我國最大利益

### 3. 國際參與及交流

- 積極參與 WHOIS 新政策討論，確保兼顧我國權益
- 追隨國際議題趨勢，正視 AI 治理挑戰以因應數位衝擊

# 壹、計畫簡介

## 一、緣起與目標

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，提升通傳會主管數位匯流發展與網路治理之權責，強化通傳與網路治理相關機關與國際之合作與交流，通傳會爰辦理公告「網路治理交流與人才培育」補助計畫。

本計畫期藉由受補助團隊在網路治理方面之豐富經驗，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 (multi-stakeholder, 以下或簡稱多方社群) 參與模式，舉辦至少 2 場次與通傳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，並提供國際議題分析及建議等事項，俾利通傳會研擬提升我國網路治理環境之施政參考。

本補助計畫將培養我國參與國內外網路治理之人才，以利朝向多方模式發展，並進行與國際網路治理組織交流合作，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。

## 二、計畫架構與內容

本計畫內容依據國家通訊傳播委員會(以下簡稱通傳會)公告之辦理工作項目，可歸納為「人才培育」、「議題分析與多方參與」，以及「國際參與及交流」三大項目，並可進一步分成規劃與開辦課程、選拔人才參與國際會議、分析國際議題、舉辦研討會/座談會/論壇、參與國際會議、邀請國際專家訪臺等六個子項目，計畫架構如下圖 1 所示。



圖1. 計畫架構圖

### 三、執行時程及進度

本計畫執行時程為自 107 年 3 月 23 日起至 107 年 12 月 31 日止。各項工作進度的規劃，以及計畫契約書規定的查核項目彙整如下表 1 所示。

表1. 計畫執行時程及進度

工作項目	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
1 人才培育	課程 規劃	學員 招募	評選 公布		課程 辦理	優秀學 員參與 APrIGF	會後分 享於 座談 2			
2 議題分析 與多方參 與	座談 1 規劃	座談 1 提案			座談 1 舉辦		座談 2 舉辦	議題分 析 1~3	議題分 析 4~6	

工作項目	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
3 國際參與及交流				國際專家訪臺		參加 APrIGF		參加 ICANN 63	參加 IGF	
查核項目	查核點									日期
a 期中報告	1.完成至少 20 人的人才培訓課程，並選拔優秀人才參與國際會議。 2.舉辦至少 1 場次國內研討會、座談會或論壇，並提供重要議題報告。 3.邀請國際專家至少 1 人訪臺交流。									7/31
b 期末報告(初稿)	1.舉辦至少 1 場次國內研討會、座談會或論壇，並提供重要議題報告。 2.出席 2018 年亞太區網路治理論壇(Asia Pacific Regional Internet Governance Forum, APrIGF)，並提供重要議題報告。 3.出席 ICANN (Internet Corporation for Assigned Names and Numbers，網際網路名稱與號碼指配組織) 63 公共會議，並提供重要議題報告。 4.提供至少 6 篇國際議題分析。									11/30
c 期末報告(定稿)	依審查意見修訂完成之期末報告，包含出席 2018 年聯合國網路治理論壇(IGF)之重要議題報告。									12/28

#### 四、預期成果與績效指標

本計畫執行「人才培育」、「議題分析與多方參與」，以及「國際參與及交流」等工作項目，預期可達到下列成果或效益：

- 提升我國網路治理知識能量，培育參與國內外網路治理之人才。
- 掌握全球網路規則脈絡變動與政策議題方向潮流，提供決策參考，協助我國網路治理發展符合國際趨勢。

- 推動多方模式合作並凝聚政策共識，共同促進我國國家型 IGF 發展。
- 蒐集並引進國際網路治理第一手資訊，拓展國際人脈，於國際分享宣傳我國網路治理經驗，達到實質雙向國際交流。

此外，依據政府研究資訊系統 (GRB) 績效指標項目，本計畫的績效指標包括「D 研究報告」、「E 辦理學術活動」與「F 形成教材」，相關的質化與量化指標之說明如下表 2 所示。

表2. 計畫績效指標

選填	績效指標	量化指標	質化指標
✓	D 研究報告	<ul style="list-style-type: none"> <li>• 國際議題分析≥6</li> <li>• 出席國際會議重要議題報告≥3</li> </ul>	掌握全球網路規則脈絡變動與政策議題方向潮流，提供決策參考，協助我國網路治理發展符合國際趨勢
✓	E 辦理學術活動	<ul style="list-style-type: none"> <li>• 網路治理研討會/座談會/論壇≥2</li> </ul>	推動多方模式合作與對話，凝聚政策共識，共促我國國家型 IGF 發展
✓	F 形成教材	<ul style="list-style-type: none"> <li>• 人才培訓課程教材≥1 (培訓人數≥20)</li> </ul>	提升我國網路治理知識能量，培育參與國內外網路治理之人才
✓	其他 (國際交流) *非 GRB 項目	<ul style="list-style-type: none"> <li>• 出席國際會議重要議題報告≥3</li> <li>• 邀請國際專家訪台≥1</li> </ul>	蒐集並引進國際網路治理第一手資訊，拓展國際人脈，於國際分享宣傳我國網路治理經驗，達到實質雙向國際交流

## 貳、人才培育

目前國際上的網路治理人才培訓課程大致可分為 1 天內快速入門課程、3~5 天短期課程、長期學分／學位專業課程，以及中長期的線上課程等不同類型。本計畫綜合考量下列要素，規劃本次的人才培訓研習營活動：

- 本計畫之人才培育目標為培養我國參與國內外網路治理之人才，因此，學員應具有持續參與網路政策討論的熱忱；而英文能力較佳的學員，還可以成為未來參與國際會議的人選。
- 目前國內相關各界或多方社群對於網路治理的基本定義與內涵，仍然相當陌生，因此，本次課程從基礎入門知識開始授課。
- 國人對於非職能／技能、非學位的課程，願意投入時間相對有限，因此，本次課程參考教育部「青年國際事務人才培訓營」、外交部「NGO 國際事務人才培訓班」辦理天數皆為 2 天，將時程定位為短天數活動。
- 為提供良好的課程品質，協助學員獲得更佳的學習成效，並拓展網路治理的國際觀點，本次課程特別邀請具豐富人才培訓經驗的香港專業團隊來臺，和國內專家共同傳授網路治理的知識與技能。
- 為能讓學員立即發揮課堂所學，同時也為我國網路政策邁向正面發展貢獻一份心力，本次課程結合臺灣網路治理論壇 (Taiwan Internet Governance Forum, TWIGF)<sup>1</sup>活動，期能發揮相輔相成效果。

### 一、研習營活動簡介

---

<sup>1</sup> TWIGF 自 2015 年起每年舉辦一次會議，並於 2017 年籌組包含公民團體、政府、民間企業，以及技術社群代表的多方利害關係人指導小組 (Multi-Stakeholder Steering Group, MSG) 後，正式轉型為完全由民間自籌經費的自發性組織，成為我國的國家型 IGF；其運作完全符合聯合國訂定的國家型與區域型 IGF 推動 (National and Regional IGF Initiatives, NRIs) 組織原則。

本次培訓活動原訂於107年7月11日(三)至7月14日(六)舉辦，前兩日為課堂教學(表3與表4)，後兩日為參加TWIGF實地演練。由於11日遇颱風瑪莉亞侵臺，活動地點所在地(板橋)之主管機關新北市政府宣布當日停班停課，因此，本計畫臨時取消11日的課程，並調整12日的課程內容，且延長上課時間至晚上19:30(表5與表6)。

## (一) 活動資訊

- 名稱：網路治理研習營暨青年網路治理論壇 (yIGF)
- 時間：107年7月11日(三)至7月14日(六)
- 地點：中華電信學院板橋所綜合大樓(新北市板橋區民族路168號)
- 住宿：中華電信學院板橋會館
- 簡介

在國家社會運作、產業經濟發展，以及民眾就業生活都以網路為基礎的數位時代，包括臺灣在內的世界各國，都積極探討該如何治理這個虛實融合世界才能因應數位變革所帶來的契機與挑戰。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，才能找到網路治理的最佳方案。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，數位世界的當前轉換與未來發展都需要您的積極參與。

本研習營為四天三夜的免費人才培訓活動，包括兩天的課堂學習與兩天的會議活動。首先將由國內外網路治理領域的重要專家帶您認識網路治理的發展、國際網路規則的訂定方式，以及網路安全、人權、數位經濟、新興科技、網路基礎建設等重要議題；然後再透過參與2018臺灣網路治理論壇(TWIGF)，立即發揮課堂所學，同時也為我國網路政策邁向正面發展貢獻一份心力。此外，優秀學員還有機會參加國際網路治理相關會議。

## (二) 課程表

表3. 原訂中文課程表

7月11日(三)網路治理概論		
	一般學員	大專學員
09:00 - 09:30	報到 & 茶點	
09:30 - 10:00	開幕致詞	
10:00 - 10:45	學員自我介紹 & 關切議題	
10:45 - 12:00	網路治理模式發展史	
12:00 - 13:00	午餐	
13:00 - 13:45	全球網路生態系統 & 治理模式	
13:45 - 15:00	網路治理議題討論 I 資安 & 線上保護；網路人權；數位經濟 & 新興科技；連網 & 賦權 & 多元化	
15:00 - 15:15	休息 & 茶點	
15:15 - 16:30	網路治理議題討論 II	
16:30 - 17:30	角色演練準備	角色演練準備
17:30 - 18:30	角色演練：圓桌會議	角色演練：圓桌會議
7月12日(四)政策制訂與未來趨勢		
	一般學員	大專學員
08:30 - 09:00	早餐	
09:00 - 09:30	前日課程之主題摘要報告	
09:30 - 11:00	名稱與號碼：網路如何運作 & ICANN 政策	
11:00 - 12:00	ICANN 內部運作	
12:00 - 13:00	午餐	
13:00 - 15:15	ICANN 模擬會議	ICANN 模擬會議
15:15 - 15:30	休息 & 茶點	
15:30 - 16:30	亞太地區當前政策趨勢 & 對網路治理的影響 & TWIGF 介紹	
16:30 - 17:00	亞太地區合作 & 機會	
7月13~14日(五~六)臺灣網路治理論壇		

議程請詳 [www.igf.org.tw](http://www.igf.org.tw)

表4. 原訂英文課程表

<b>11 July : Overview on Internet Governance</b>		
	Main Track	Youth Track
<b>09:00 - 09:30</b>	Onsite Registration & Coffee Break	
<b>09:30 - 10:00</b>	Welcome Remarks	
<b>10:00 - 10:45</b>	Self-Introduction & Concerned Issues	
<b>10:45 - 12:00</b>	History of Internet Governance Models	
<b>12:00 - 13:00</b>	Lunch	
<b>13:00 - 13:45</b>	Global Internet Ecosystem & Governance Models	
<b>13:45 - 15:00</b>	Idea Wall + Discussion Session on Internet Governance Part I Cybersecurity & Online Protection; Human Rights Online; Digital Economy & Emerging Technology; Access & Empowerment & Diversity	
<b>15:00 - 15:15</b>	Coffee Break	
<b>15:15 - 16:30</b>	Discussion Session on Internet Governance Part II	
<b>16:30 - 17:30</b>	Role-Play Preparation	Role-Play Preparation
<b>17:30 - 18:30</b>	Stakeholders Roundtable	Stakeholders Roundtable
<b>12 July : Policies Making &amp; Future Trends</b>		
	Main Track	Youth Track
<b>08:30 - 09:00</b>	Breakfast	
<b>09:00 - 09:30</b>	Presentation on Thematic Summaries from Day 1	
<b>09:30 - 11:00</b>	Names & Numbers: How the Internet Works & ICANN Policies	
<b>11:00 - 12:00</b>	Inner Workings of ICANN	
<b>12:00 - 13:00</b>	Lunch	
<b>13:00 - 15:15</b>	Model ICANN Meeting	Model ICANN Meeting
<b>15:15 - 15:30</b>	Coffee Break	
<b>15:30 - 16:30</b>	Current Policy Trend in AP & Implications on Internet Governance & TWIGF	
<b>16:30 - 17:00</b>	Asia Pacific Regional Collaborations & Opportunities	
<b>13~14 July : TWIGF</b>		

[www.igf.org.tw](http://www.igf.org.tw)

表5. 新版中文課程表

7月12日(四) 議程			講者
時間	一般學員	大專學員	
09:00 – 09:30	開幕致詞 & 引言		<ul style="list-style-type: none"> <li>• 黃天陽，通傳會綜合規劃處科長</li> <li>• 陳文生，NII 協進會執行長</li> <li>• 吳國維，TWIGF MSG 主席／NII 協進會顧問／前 ICANN 董事</li> <li>• Edmon Chung，DotAsia 執行長</li> <li>• Joyce Chiu, NetMission 網路使命青年大使</li> </ul>
09:30 – 10:15	網路治理發展史		吳國維， TWIGF MSG 主席
10:15 – 12:15	網路治理議題討論		主持人： NetMission 與談人／講者： <ul style="list-style-type: none"> <li>• 梁理旋，NII 協進會副執行長</li> <li>• 邱伊翎，台灣人權促進會秘書長</li> <li>• 吳國維，TWIGF MSG 主席</li> <li>• 陳文生，NII 協進會執行長</li> </ul>
12:15 – 13:15	午餐		
13:15 – 14:00	名稱與號碼： 網路如何運作 (遊戲)		DotAsia
14:00 – 15:00	ICANN 政策 & 內部運作		主持人：Edmon Chung，DotAsia 執行長 與談人／講者： <ul style="list-style-type: none"> <li>• 吳國維，TWIGF MSG 主席</li> <li>• 黃勝雄，TWNIC 執行長／APNIC 董事</li> <li>• 喬敬，中域國際集團執行長</li> </ul>
15:00 – 15:45	角色演練準備	角色演練準備	DotAsia & NetMission
15:45 – 16:00	休息 & 茶點		
16:00 – 18:00	ICANN 模擬會議	ICANN 模擬會議	DotAsia & NetMission
18:00 – 18:15	休息		
18:15 – 19:00	從全球、區域與在地看當前政策趨勢		<ul style="list-style-type: none"> <li>• Joyce Chen，ICANN GSE 策略與發展資深經理</li> <li>• Yannis Li，DotAsia 合作發展主任</li> <li>• 吳國維，TWIGF MSG 主席</li> </ul>
19:00 – 19:30	未來參與機會 & 總結		• 主辦單位 & DotAsia

表6. 新版英文課程表

Contingency Agenda on 12 July (Thursday)			Speakers
Time	Main Track	Youth Track	
09:00 – 09:30	Welcome Remarks & Introduction		<ul style="list-style-type: none"> <li>• Tony Huang, Section Chief of Department of Planning, NCC</li> <li>• Vincent Chen, CEO of NIIIEPA</li> <li>• Kuowei Wu, MSG Chair of TWIGF/Advisor of NIIIEPA/ Former ICANN Board Member</li> <li>• Edmon Chung, CEO of DotAsia</li> <li>• Joyce Chiu, Ambassador of NetMission</li> </ul>
09:30 – 10:15	History of Internet Governance		Kuowei Wu, MSG Chair of TWIGF
10:15 – 12:15	Idea Wall on Internet Governance Issues <ul style="list-style-type: none"> <li>• Cybersecurity &amp; Online Protection</li> <li>• Human Rights Online</li> <li>• Digital Economy &amp; Emerging Technology</li> <li>• Access &amp; Empowerment &amp; Diversity</li> </ul>		Moderator: NetMission Panelists/Speakers: <ul style="list-style-type: none"> <li>• Sophie Liang, Deputy CEO of NIIIEPA</li> <li>• E-Ling Chiu, Secretary General of Taiwan Association for Human Rights</li> <li>• Kuowei Wu, MSG Chair of TWIGF</li> <li>• Vincent Chen, CEO of NIIIEPA</li> </ul>
12:15 – 13:15	Lunch		
13:15 – 14:00	Names & Numbers: How the Internet Works (Game)		DotAsia
14:00 – 15:00	ICANN Policies & Inner Workings		Moderator: Edmon Chung, CEO of Dot Asia Panelists/Speakers: <ul style="list-style-type: none"> <li>• Kuowei Wu, MSG Chair of TWIGF</li> <li>• Kenny Huang, CEO of TWNIC/EC Member of APNIC</li> <li>• ChingChiao, CEO of Brandma.co Limited</li> </ul>
15:00 – 15:45	Role Play Preparations	Role Play Preparations	DotAsia & NetMission
15:45 – 16:00	Break		
16:00 – 18:00	Model ICANN Meeting	Model ICANN Meeting	DotAsia & NetMission
18:00 – 18:15	Break		
18:15 – 19:00	Current Policy Trends from Global, Regional to Local		<ul style="list-style-type: none"> <li>• Joyce Chen, Senior Manager of ICANN GSE Strategy and Development</li> <li>• Yannis Li, Director of Corporate Development of DotAsia</li> <li>• Kuowei Wu, MSG Chair of TWIGF</li> </ul>
19:00 – 19:30	Future Engagement Opportunities & Wrap-Up		• Local Host & DotAsia

### (三) 講師簡介

依姓氏筆畫排列



Edmon Chung  
香港 DotAsia 行政總裁

#### 經歷

- ICANN 國際化域名(IDN)工作小組 共同主席
- 香港 ISOC 分會副主席
- 亞太區網路治理論壇(APrIGF) MSG 委員

#### 專長

- 網路技術標準
- 網路治理發展與生態系統
- 國際事務推動及參與



Joyce Chen  
ICANN 全球利害關係人參與策略&  
發展 資深經理

#### 經歷

- Manager, Strategy Planning & Coordination, Singapore Institute of Technology
- Manager, Corporate Communications, Singapore Institute of Technology
- Foreign Service Officer, Singapore Ministry of Foreign Affairs

#### 專長

- 行銷管理、策略規劃
- 外交事務



#### 經歷

- 亞太區青年網路治理論壇(yIGF) 主辦單位
- NextGen@ICANN 計畫創立者
- 青年網路治理訓練營(Youth Internet Governance Camp) 主辦單位
- 香港青年網路治理論壇 主辦單位

#### 專長

- 青年網路治理的推動及訓練課程
- 數位包容的推廣
- 多方利益關係人模式的討論與模擬



吳國維  
NII 產業發展協進會 顧問

#### 經歷

- 中華電信股份有限公司 董事
- 亞太區網路治理論壇(APrIGF) MSG 委員
- 臺灣網路治理論壇(TWIGF) MSG 主席
- NII 產業發展協進會 前執行長
- ICANN 前董事

#### 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



邱伊翎  
台灣人權促進會秘書長

#### 經歷

- 人權公約施行監督聯盟 執委 (現職)
- 法扶基金會發展 專門委員 (現職)
- 西藏台灣人權連線 執委 (現職)
- 亞太難民權利 網絡執委
- 東亞科技與社會國際期刊 編輯助理

#### 專長

- 人權概論、聯合國人權公約審查及特別機制、人權捍衛者、難民移民人權
- 公民社會與社會運動
- 隱私權



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) MSG 委員
- 教育部電算中心 前組長、副主任等
- 高雄第一科技大學 前計算機中心主任、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) 前執行長
- 中國科技大學資訊學院 前院長

#### 專長

- 網際網路應用與管理、軟體專案管理
- 資訊安全、資訊管理、網路治理



喬敬

Brandma.co Limited

創辦人和執行長

#### 經歷

- ICANN Generic Names Supporting Organization (GNSO) Council 顧問
- DotAsia Organisation Limited 董事
- 台灣網路協會 監事
- Asia Pacific Networking Group 主席

#### 專長

- 網路域名
- 網路政策
- 行銷



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
- 亞太網路治理論壇(APrIGF) MSG 委員
- 亞洲(.asia)頂級網域註冊管理局 諮詢委員
- ICANN Root Zone 中文標識生成委員會 副主席

#### 專長

- 網際網路通信技術
- 資訊治理、政策規劃
- 關鍵網路資源
- 國際事務推動及參與

## (四) 活動辦法

### 1. 報名資格

本研習營為四天三夜的免費課程，並提供住宿、茶點與午餐，以及大台北地區以外的長途大眾運輸交通補助（憑收據與票根核實報銷）。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）

## 2. 報名時間與方式

請於 107 年 5 月 31 日(四)前完成線上報名，並簡答報名表中以下問題：

- 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

## 3. 評選與錄取

- 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。

- 錄取名額

本研習營預計對外招收 35 名學員（另有 10 名內部學員共同上課）

- 結果公告與錄取通知

評選結果將於 **107 年 6 月 11 日（一）** 於本活動網站公布，並以 email 各別通知錄取學員。

- 繳交出席保證書

為避免浪費學習資源，錄取學員須於 **107 年 6 月 22 日(五)**前，繳交出席保證書，並報名 2018 TWIGF。出席保證書表單格式等資訊將

載於錄取公告上；2018 TWIGF 報名請至 [www.igf.org.tw/](http://www.igf.org.tw/)。

- 繳交監護人(家長)同意書(未滿 20 歲者)

參照民法相關規定辦理，未滿 20 歲之錄取學員請於 **107 年 6 月 22 日(五)**前，繳交監護人(家長)同意書，表單格式將載於錄取公告上。

#### 4. 學員獎勵

- 結業證書與獎學金

全程參與培訓課程的學員，將獲頒結業證書；外部學員另由 TWNIC 頒發新臺幣\$3,000 元整獎學金，以茲獎勵學員積極學習。

- 參與國際會議 (2 名)

主辦單位將組成評選小組，從結業的本國籍外部學員中，遴選 2 名優秀學員(正取 2 名，備取 2 名)參與國際網路治理相關會議，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、2018 TWIGF 參與狀況等。獲選學員除了應配合主辦單位的相關安排參與國際會議外，會後並應提供出國報告，且參加至少 1 場次的分享交流會議。

## 二、宣傳與評選

本次研習營活動於網站上線當日 (107 年 4 月 20 日) 開始對外進行宣傳招生，招募對象包括多方社群與大專青年，受理報名時間至 5 月 31 日止，名額共計 35 名，另保留 10 個名額給予公務單位，相關細節說明如下。

### (一) 活動網站

本次研習營活動網站共有首頁、活動內容、活動辦法、錄取名單、交通資訊、線上報名等 6 個單元，網站之部分頁面如下圖 2 所示。

首頁

活動內容

活動辦法

錄取名單

交通資訊

線上報名

# 網路治理研習營暨 青年網路治理論壇(yIGF)

2018.7.11 (三) ~ 14 (六)  
中華電信學院板橋所

指導單位：國家通訊傳播委員會

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

TWNIC 財團法人台灣網路資訊中心  
www.twinc.nsl.tw TAIWAN NETWORK INFORMATION CENTER

TWIGF  
臺灣網路治理論壇

協辦單位：NETMAGIC Lab

TOP

## 中華電信學院板橋所

地址:新北市板橋區民族路168號

- 搭乘火車：板橋火車站下車
- 搭乘高鐵：板橋站下車
- 搭乘捷運：捷運板南線（BL藍線）板橋站下車
- 搭乘公車：57、265、307、657、796、847、
- 抵達**板橋站**後您可選擇以下方式到達會場
  - 步行：路程約850公尺，約11分鐘即可抵達
  - 公車：於公車站第一月臺搭乘307（往臺
  - 計程車：車資約新臺幣100元



圖2. 研習營活動網站

## (二) 活動宣傳

本次研習營活動宣傳主要透過網路治理相關組織的官網與臉書社團，以及全國各大專院校的訊息發布，其中 TWIGF 的臉書社團已有超過 2 千位成員。而公務人員則是透過發文並致電邀請通傳會，及交通部郵電司、行政院資通安全處、經濟部、外交部等我國「ICANN 工作小組」相關人員。

- TWIGF 網站、臉書社團與香港 NetMission 臉書社團



圖3. 活動宣傳：TWIGF 與 NetMission 臉書社團

• TWNIC 網站與 5 月份電子報



圖4. 活動宣傳：TWNIC 網站與 5 月份電子報

• 大專院校訊息發布



圖5. 活動宣傳：大專院校訊息發布

• 發文 (並致電) 邀請

財團法人中華民國國家資訊基本建設產業發展協進會 函

地 址：10483台北市松江路317號7樓  
承辦人：黃安謙  
電 話：(02)2508-2353轉127  
傳 真：(02)2507-3507

**受文者：經濟部**

遠別：普通件  
密等及解密條件：一般  
發文日期：中華民國107年05月02日  
發文字號：(107)資協董字第107060號  
附件：

主旨：本會訂於本(107)年7月11日至14日舉辦「網路治理研習營暨青年網路治理論壇(yIGF)」人才培訓活動，敬請派員報名參加，請查照。

說明：

一、 旨揭人才培訓活動包括2天課堂學習與2天臺灣網路治理論壇(TWIGF)座談交流，前者(課堂學習)係本會辦理國家通訊傳播委員會「網路治理交流與人才培育」補助計畫之工作項目之一，後者(TWIGF)則為國內多方利害關係人(multi-stakeholder)共同舉辦之活動，可讓學員於課堂學習後立即發揮所學。

二、 本活動為期4天3夜，全程免費，請詳<https://igcamp.tw>，主要資訊如下：  
(一) 時間：7月11日(星期三)至14日(星期六)  
(二) 地點：中華電信學院板橋所綜合大樓(新北市板橋區民族路168號)  
(三) 住宿：中華電信學院板橋會館(2人一室)  
(四) 課程主題：網路治理的發展、國際網路規則的訂定方式與模擬會議，以及網路安全、人權、數位經濟、新興科技、網路基礎建設等重要議題

三、 本活動預計對外公開甄選35名學員，特為政府機關額外保留少數名額，敬請貴單位派員1人參加，並於5月25日前完成線上報名(<https://goo.gl/forms/s3bA9ZDbg1d1Jure2>)；全程參與者將核發學習時數32小時。

正本：交通部郵電司、行政院資通安全處、經濟部  
副本：

財團法人中華民國國家資訊基本建設產業發展協進會

圖6. 活動宣傳：發文邀請

### (三) 學員評選

#### 1. 報名與評選

本次研習營活動共計 98 人報名(不含公務人員保留名額)，扣除 12 位資料填寫不完整者，計有 86 人進入評選階段。本次評選作業由台灣網路資訊中心 (TWNIC) 國際事務委員會之 9 位委員擔任評審委員，針對報名者的申請動機、對網路議題的關切度、相關事務或活動參與經驗及熱忱、英文程度等項目，進行綜合評估。評選方式採線上審查及審查會議兩階段作業：

- 線上審查：每位評審委員對 86 位合格報名者給予評分，優先推薦者獲 2 分，推薦者獲 1 分，不推薦者為 0 分。評分結果之得分分佈如下圖 7 所示。
- 評審會議：評審委員針對線上審查結果進行討論與調整，並依最後得分排序選出 35 名正取學員與 10 名備取學員。

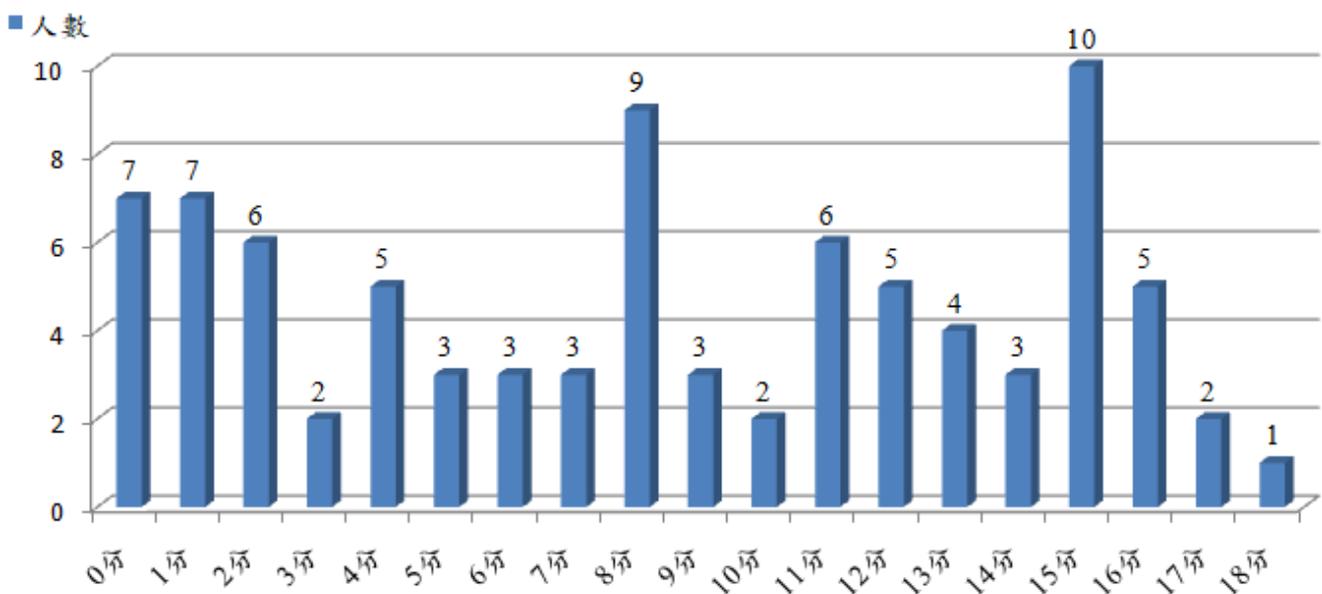


圖7. 合格報名者的得分分佈

## 2. 學員組成概況

經通知聯繫 35 名正取學員、10 名備取學員，以及 9 名公務人員學員後，共有 37 名學員表示會參與課程，學員的組成概況如下圖 8 所示。惟當日實際出席者為 34 名，最後可獲得結業證書之全勤學員共計 31 名。此外，在 34 名學員中，近 7 成學員(23 人)選擇住宿，並有 8 人申請交通補助。

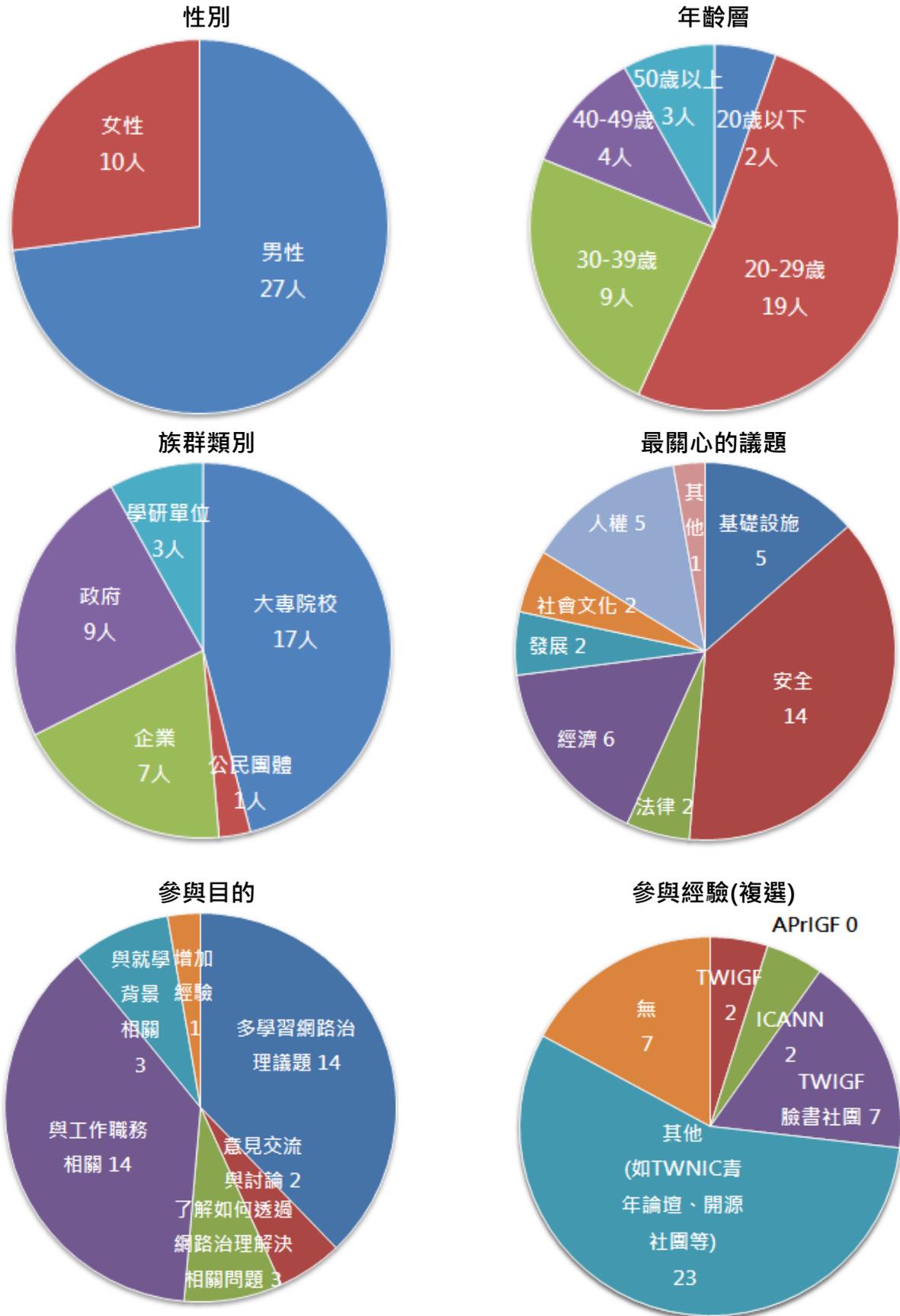


圖8. 研習營學員組成概況

### 三、課程內容重點

#### (一) 網路治理發展史

- 講者：吳國維，NII 協進會顧問／TWIGF MSG 主席

網路最初是以開放性的原則去設計，讓網路上的每個裝置可以和任何一個其他裝置做封包交換，也可以拒絕交換。網路之父 Vint Cerf 和 William Drake 等專家 2015 年提出網路分裂的說法，認為網路可能受到被切割、分裂的危險，進而影響到它對外的連線，但 Milton Mueller 持反對意見，認為既然可以拒絕接受訊息，就不會有分裂化。

網路自 1993 年發展至今，全球已有近 40% 人口可以上網。網路原本是 1969 年美國國防部 DARPA 的一個計畫；1974 年 TCP/IP (Transmission Control Protocol，傳輸控制協定) 開始運作；1986 年 IETF (Internet Engineering Task Force，網際網路工程任務小組) 成立，它是一個沒有正式註冊的單位，但是卻制定網路所有相關標準，它所提倡的精神是開放、透明、由下到上、共識決。

1994 年 Yahoo 成立，它是網路產業第一個商業化的公司，帶動了網路快速蓬勃發展；1998 年 ICANN 成立，在全球網路治理扮演非常重要的角色。1994、1995 年網路已成為許多人使用的工具，但它的關鍵資源，如根伺服器、IP 位址、域名等，該由誰發放，產生許多問題。

2004 年聯合國成立 WGIG (Working Group of Internet Governance，網路治理工作小組)，將要討論的議題結構和範圍訂出來；2005 年突尼西亞會議訂出網路治理的題目，但不做結論；2006 年至今，每年都會舉辦 IGF 討論網路治理的相關議題；2010 年 FB 等社群媒體興起，美國國務卿 Hilary Clinton 提出 free Internet，造成許多國家的恐慌，認為網路是顛覆政府的工具；2011 年 SOPA (Stop Online Privacy Act，禁止網路盜版法案) 為解決智

慧財產權問題，造成網路世界與人權團體的對立；2013 年發生 Edward Snowden 事件；2016 年歐盟通過 GDPR (General Data Protection Regulation, 通用資料保護規範)；2017 和 2018 年監控、臉孔辨識和人工智慧成為熱門話題，政府若以國家安全為理由要執行臉孔辨識，應有哪些規範與流程？又有哪些法律可保護人民？這些都是網路治理要討論的議題。

• Q&A：

問：AI 會對少數民族或女性族群做出偏見的判斷，那所謂的 free Internet，是有多自由？是由誰去定義的？

答：人權團體曾要求 ICANN 章程要把人權寫進去，ICANN 也一直試圖在董事會裡創造男女平等的環境；其實聯合國 IGF 或是 APriGF 會議中，女性議題並沒有被忽略。對於 AI 造成偏見的情況，全球資訊網 (World Wide Web, WWW) 的發明人 Tim Berners-Lee 提出將演算法公開透明化，讓大家去檢視是否有造成歧視的問題。

## (二) 網路治理議題討論

- 主持人：NetMission
- 帶領討論講者：資安&線上保護 / 梁理旋，NII 協進會副執行長  
網路人權 / 邱伊翎，台灣人權促進會秘書長  
數位經濟&新興科技 / 吳國維，TWIGF MSG 主席  
連網&賦權&多元化 / 陳文生，NII 協進會執行長

本堂課透過分組討論，增進學員對網路治理不同主題的認識與興趣，並學習從多元與廣泛的角度，探討網路治理議題。課程首先由 NetMission 團隊介紹 4 個分組討論主題的範圍、相關議題，以及其正面效益與爭論等。接著，讓學員自由選擇加入 4 個主題分組，每組都有專家帶領學員討論。然後，各組學員先自由提出各自關切的議題，大家再從中挑選數個議題進行討論。最後，再由各組學員派員上臺報告與分享討論結果。

## 1. 資安&線上保護

「資安&線上保護」分組學員以網路資訊的透明度作為討論重點，認為網路資料的儲存地點是重要問題，它涉及法規如何規範與業者如何遵循等不同層面。雖然有些業者會在「隱私權聲明」等相關文件，向使用者說明其資料儲存的位置(境內或境外)，但沒有人會去驗證其真實性，且實務上也曾有業者將應該儲存於 A 國的資料轉存於 B 國，因此，有些學員主張應該由政府相關部門進行檢驗，以保護消費者的資料安全。

不過，也有些學員表示，隨著數位經濟的興起，多數業者的資料都是放在網路平臺上，但政府人力有限，不可能做到全面的檢視，何況政府單位也不一定有權力可以要求業者公布所有資料，因此，最重要還是要靠業者自律與誠實履行，並與客戶達成協議，必要時可以委託第三方公正單位進行資安相關的驗證，如此會是比較務實的做法。

## 2. 網路人權

「網路人權」分組學員主要討論網路內容管理與假新聞議題。首先，在網路內容管理方面，學員們提出向社群平臺檢舉仇恨言論無效、女性運動照片遭網路平臺下架、教育部的「網路守護天使」系統會屏蔽廢死聯盟或同志網站等多個案例，並表示網路平臺該承擔什麼責任與擁有什麼權限、如何訂定內容下架的標準，以及何謂不適當的內容等問題，都沒有明確答案，需要進一步討論與訂定。

至於假新聞議題，有學員表示，如今網路上除了內容不實的假新聞外，更充斥著「假裝是新聞平臺」的內容農場，其中的文章又被稱為偽新聞。講者指出，許多人認為假新聞 (fake news) 一詞更精確的說法是錯誤資訊(misinformation)。但究竟該如何防範假新聞，又如何防治假新聞與保護言論自由之間取得平衡，小組則未討論出答案。

## 3. 數位經濟&新興科技

「數位經濟&新興科技」分組學員主要討論 AI、虛擬貨幣、行動支付與跨境電商課稅問題。學員們認為，面對 AI 蓬勃發展，AI 演算法如何融入道德設計是重大議題，例如自駕車如何做安全判斷（是保護車主或行人）、國安系統如何判斷恐怖分子等。而在虛擬貨幣方面，學員們指出，以比特幣為代表的虛擬貨幣，能否獲得真正貨幣的定位，仍有待觀察。

至於行動支付，學員們表示，雖然中國大陸的行動支付發達，讓當地民眾享有無現金支付的便利性，同時也令不少臺灣民眾稱羨，但是卻可能淪為中國大陸政府監控人民的利器。最後，在跨境電商課稅問題上，學員們認為，即使政府規定境外電商必須落地成立分公司，但是許多外商仍然不會遵守，此問題已於 WTO 討論十多年，但至今仍然沒有解決方案。

#### 4. 連網&賦權&多元化

「連網&賦權&多元化」分組學員首先針對連網議題指出，網路業者會考量建置成本，如果用戶數量不夠多，他們不會花錢建設，因此，建議採用指向性的 4G 來降低網路佈線成本；惟臺灣民眾不喜歡基地臺建在自家附近，此問題需要教育民眾正確的知識，才能推展網路建設與服務。

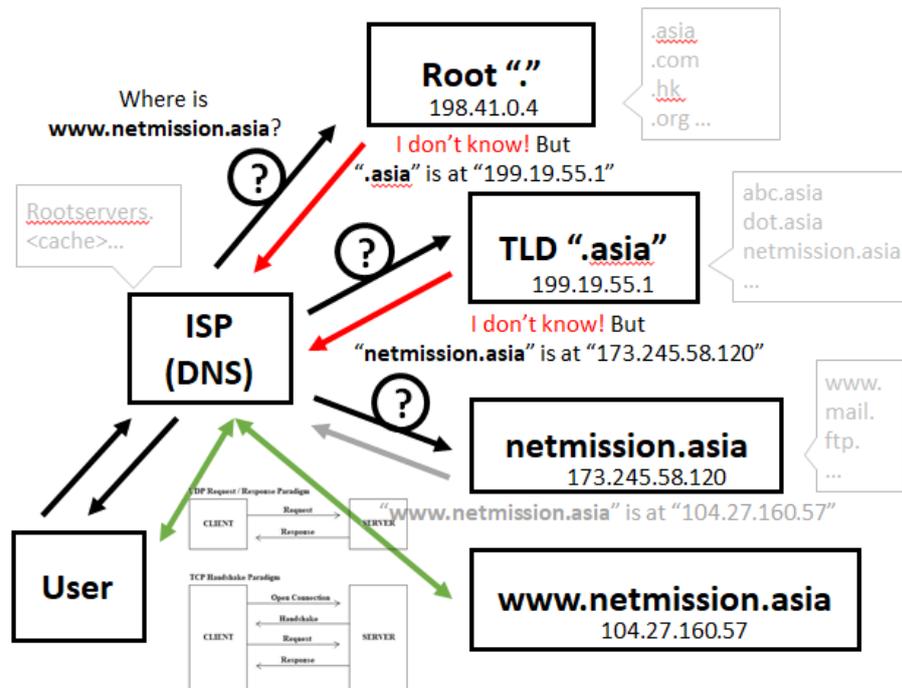
對此，講者吳國維表示，政府設有普及基金，開放所有電信業者申請去偏鄉進行網路建設，但最後只剩中華電信持續執行。臺灣天然災害很多，後續維護也是一大問題，目前技術尚未能解決偏鄉建設的特有問題。

而在多元化方面，學員提到維基媒體基金會努力促進女性和多元性別族群使用網路的話語權，並在臺灣成立「薇姬的房間」，且附帶育兒區，作為女性於維基寫作與討論活動的專屬空間，藉此鼓勵更多優秀女性透過寫作與聚會在維基百科上發聲。

### (三) 名稱與號碼：網路如何運作

- 講者：Edmon Chung，DotAsia 執行長

本堂課透過讓學員扮演 DNS (Domain Name System, 網域名稱系統)、Root Server (根伺服器)、頂級網域 Server 等角色, 以查詢 www.netmission.asia 為例, 讓機器設備做擬人化的移動與問答, 藉此說明網路如何透過域名與 IP 位址運作。其流程如圖 9 所示, 意即當使用者要連到 Netmission 網站, 輸入 www.netmission.asia 網址時, 手機或電腦會向 ISP 的 DNS 查詢上述的網址, DNS 會先檢查自身的快取, 如果有記錄, 會直接將結果傳給使用者; 如果查無記錄, 則會向 Root Server 查詢, 並得到 .asia 的 IP 位址。接著, DNS 會向 .asia 的 server 查詢, 並得到 netmission.asia 的 IP 位址。然後, DNS 再向 netmission 的 server 查詢, 並得到主機 www 的記錄, 將此記錄存入快取, 同時也將結果傳回給使用者。



資料來源：Edmon Chung

圖9. 網路運作流程圖

#### (四) ICANN 政策&內部運作

##### 1. 「多方利害關係人」治理模式介紹

- 講者：Edmon Chung，DotAsia 執行長

香港將「多方利害關係人」(multi-stakeholder)譯為「多持分者」，似乎更能展現此模式「所有人都可分一杯羹」的精隨。聯合國 IGF 的多方社群包括政府、產業界、公民社會中的技術與學術社群。而在 IETF 中，由於它負責開發並制定全球的網路標準，這些標準必須有全球通用性，因此，IETF 的決策並非透過投票表決，而是採取粗略共識決 (rough consensus)。

再看 ICANN 組織，下圖 10 顯示 ICANN 董事會係由多方社群組成，包括 4 個諮詢委員會(Advisory Committee, AC)、3 個支援組織(Supporting Organization, SO)、ICANN 主席兼執行長(代表 ICANN 組織)、2 個技術諮詢團體-- IETF 與 TLG，以及僅負責提名董事會成員的提名委員會(Nominating Committee)。

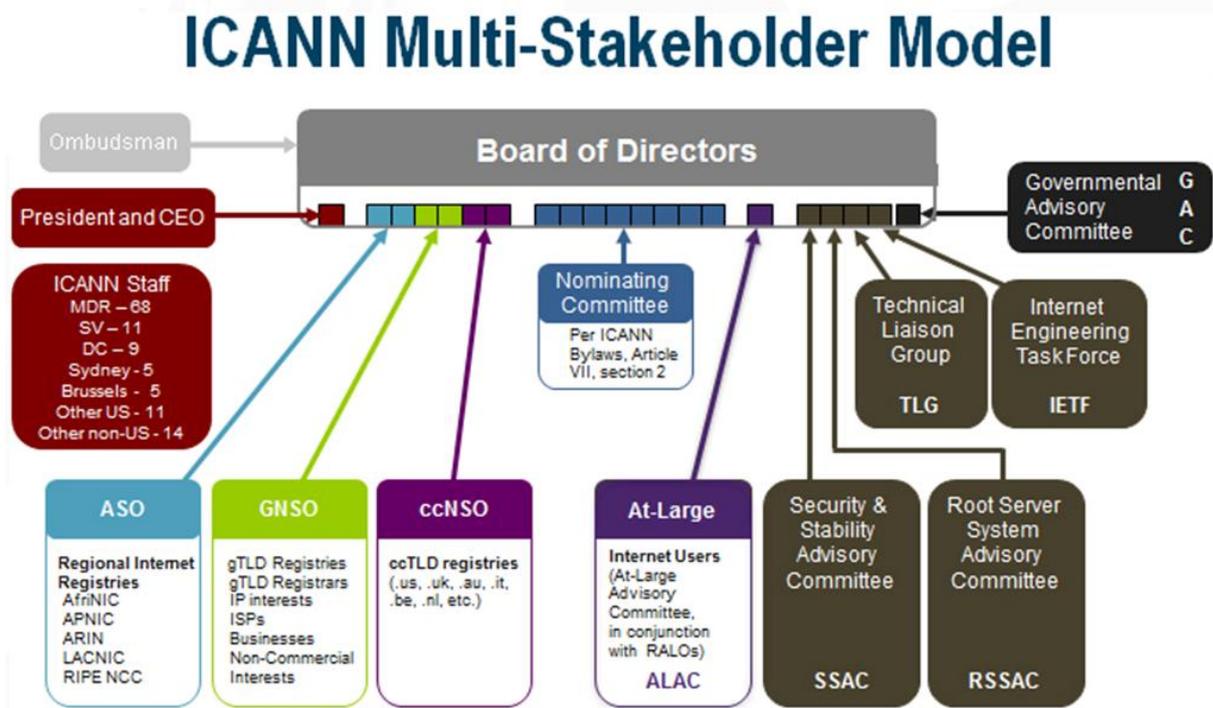


圖10. ICANN 多方利害關係人模式

## 2. 分享座談

- Edmon Chung，DotAsia 執行長
- 吳國維，NII 協進會顧問／TWIGF MSG 主席
- 黃勝雄，TWNIC 執行長／APNIC 董事
- 喬敬，中域國際集團執行長

講者們以對話方式，介紹 ICANN 多方社群當中的 GNSO (Generic Names Supporting Organization，通用域名支援組織) 與 ccNSO (Country Code Names Supporting Organization，國碼名稱支援組織)。重點包括：

- GNSO 的組成最為複雜，可從是否和 ICANN 簽約，分成「合約方」與「非合約方」兩大類。前者包括註冊管理局 (registry) 與註冊商 (registrar)；後者又可複分為商業團體 (商業企業用戶、智慧財產團體、ISPs) 與非商業團體 (非商業用戶、非營利單位)。ICANN 董事會並不參與政策制定，而是由 GNSO 討論後提到董事會，交由董事會審批，政策制定是由下而上，從提案到通過，短則一年，長則三至五年。
- ccNSO 與 ICANN 的關係也有幾個不同的類別，有些 ccNSO 和 ICANN 簽署交換信件 (Letter Exchange)，代表知道雙方的存在；有些簽署問責架構 (accountability framework)，表示雙方將治理方式透明化；還有些簽署備忘錄 (Memorandum of Understanding, MOU)，彼此間沒有法律關係。

最後，講者們也提到，我們不能用實體世界的運作方式看待網路世界，因為政策與法律往往落後於科技發展，也因此，我們要參與網路治理，可以先發現問題所在，提出看法並想出解決方法，而非等到問題擴大時才由政府介入。

## (五) ICANN 模擬會議

- 主持人：DotAsia 與 NetMission

本堂課藉由模擬 ICANN 開會，讓學員了解 ICANN 政策制定的過程，以及 ICANN 多方社群如何在不同的利害關係立場中，達成政策共識。模擬會議的主題是目前 ICANN 正進行的新一輪新通用頂級域名(new gTLD)政策研擬，並將學員分成一般組與大專組，於 2 個不同的教室同時進行。雖然 2 組學員所討論的子題不同，但同樣都是將各組學員再分成以下 3 個 ICANN 社群，讓他們扮演這些社群的代表，並提出各自立場。

- 政府諮詢委員會(Governmental Advisory Committee, GAC)：由各國政府代表組成。
- 通用域名支援組織 (Generic Names Supporting Organization, GNSO)：成員包括 gTLD 註冊管理局與註冊商、商業團體(商業企業用戶、智慧財產團體、ISPs)、非商業團體(非商業用戶、非營利單位)。
- 一般會員諮詢委員會 (At-Large Advisory Committee, ALAC)：由全球各網路社群人士組成，代表廣大的網路個人使用者。

## 1. 一般學員組

- 討論題目(1)：擬申請什麼 new gTLD 及註冊限制？

GAC 擬申請 .iot 、 .mtm 、 .china 、 .taiwan ； GNSO 擬申請 .roc 、 .green 、 .islam 、 .ily 、 .michelin ； ALAC 擬申請.drone、.help、.data、.islam。上述 new gTLD除了.michelin規定只有餐廳業者可以申請註冊外，其他域名皆採完全開放註冊。

不過，.help 遭 GAC 反對，他們認為此字涉及公眾利益，不應作為商業使用。此外，GAC 當中的中國代表也表示反對.roc，而 ALAC 中的 ISOC Taiwan 則出面維護；面對雙方立場不同，GAC 的歐盟代表指出，.roc 可由歐盟管理以維持中立性。

最後，本堂課講者 Edmon Chung 也說明，其實 ISO 3166 表中所列的國家地區名稱，不論是全稱或縮寫，都是保留字，因此，.china 與 .taiwan 都是不能申請的字串，而 .roc 則不屬於保留字。

- 討論題目(2)：GAC 對申請案件擁有反對權，是否應該修改此規定？

ALAC 主張 ALAC 為廣大網路使用者的代表，且政府往往有政治或外交考量而無法完全維護公眾利益，加上多方機制講究平等參與，因此，ALAC 也應該和 GAC 一樣，擁有反對權；GNSO 也認為，ICANN 應該維護多方機制的平等性，讓大家都享有反對權。不過，GAC 除了質疑由少數人組成的 ALAC 是否能真正代表廣大的網路使用者外，還強調社群中只有政府背負維護國家主權與長遠發展的義務，也因此，只有 GAC 需要擁有反對權。

- 討論題目(3)：是否需要訂定地理或敏感字的保留清單及如何訂定？

GAC 認為應該事前建立禁止申請的保留字清單，且所有社群皆可提出各自的保留字清單(但有限量且須具法律明確性)，並供大家討論與採認，以避免申請案步入曠日廢時的行使反對權階段。不過，ALAC 與 GNSO 都持反對意見。ALAC 指出，網域名稱應該回歸使用者需求，而非事前的空想設限，何況建立清單本身就是個大工程。GNSO 也表示，網域名稱應該回歸網路自由的精神，以及市場機制，讓商業行為可以快速得到結果，以免延誤商機。

## 2. 大專學員組

- 討論題目(1)：是否應該保留專屬域名 (closed generic gTLD)<sup>2</sup>？

討論結果為 GNSO 支持保留，因為既有利於企業保護其商標及市場，而且也可以讓非營利組織避免其網站遭冒用來詐欺；GAC 也同意企業應有

---

<sup>2</sup> 係指由單一註冊管理機構管理，且唯有該註冊管理機構或其子公司才可使用的 gTLD，如現有的 .app、.baby、.beauty 等都屬於專屬域名。

申請專屬域名的權利；不過，ALAC 認為專屬域名不利於個人使用者，因此提出反對意見。

- 討論題目(2)：是否須修正社群反對 (community objection)的條件？

由於學員們聚焦於討論「如何定義社群」，以致未能有足夠時間針對既有的反對條件是否合理進行討論。

## (六) 從全球、區域與在地看當前政策趨勢

### 1. ICANN 當前重要議題

- 講者：Joyce Chen，ICANN GSE 策略與發展資深經理

WHOIS<sup>3</sup>如何符合歐盟《通用資料保護規範》(General Data Protection Regulation, GDPR) 是目前 ICANN 最熱門也是最迫切的討論議題。GDPR 已經開始實施，而 WHOIS 又被判定違反 GDPR，因此，ICANN 社群啟動緊急政策發展程序(E Expedited Policy Development Process, EPDP)，以在一年內達成共識，完成頂級通用域名(Generic Top-level Domain, gTLD)註冊資料的暫時性規範。

其次，是新一輪的新通用頂級域名 (new gTLD) 政策討論，目前正進行上一輪的成效檢視與改善，同時也成立 5 個工作小組，包括：總程序及推廣、合約義務、字串異議和爭論、國際化域名(Internationalized Domain Name, IDN)與相關技術、地理名稱保留字。前 4 個工作小組已經發布初步報告並受理公開評論，期限至今年(2018)9 月 5 日止。

此外，還有網域名稱系統 (DNS) 的加密金鑰 (Key Signing Key, KSK) 更換。基於安全考量，ICANN 將更換已使用長達 10 年的金鑰，因此，網

---

<sup>3</sup> WHOIS 是查詢一個域名或 IP 位址的註冊者相關資訊的系統。根據 ICANN 政策規範與合約，每當註冊域名時，註冊者必須提供姓名、地址、email、電話等聯絡資訊；而域名管理局則必須提供 WHOIS 公開查詢服務，查詢結果並會顯示註冊者的聯絡資料。

域名稱安全擴充架構 (Domain Name System Security Extensions, DNSSEC) 相關的網路營運商，還有網路服務業者 (ISP) 都應備妥相關作業，以在今年(2018) 10 月 11 日正式啟用新的金鑰。

## 2. 聯合國 IGF 與亞太區 APrIGF 當前重要議題

- 講者：Yannis Li，DotAsia 合作發展主任

前幾年聯合國 IGF 較強調如何透過網路，協助達成聯合國 2030 年全球永續發展目標。但 2017 年 IGF 的焦點轉為人工智慧(Artificial Intelligence, AI)、假新聞、大數據、物聯網(Internet of Things, IoTs)、虛擬實境(Virtual Reality, VR)、區塊鏈 (Blockchain)等新興科技相關的政策議題，以及網路中立。而 2018 年的主要議題，若從申請提案的類別來看，將會聚焦於安全&信任&隱私、人權&性別&青年，以及發展&創新&經濟等主題。

此外，IGF 自 2014 年開始舉辦最佳典範論壇 (Best Practice Forum, BPF)，2018 年新增的主題有 AI、IoT 與大數據，而網路安全、性別與連網、在地內容，則是近年持續討論的議題。

在 APrIGF 方面，2018 年論壇邁入第 9 年，在 8 月 13 日至 16 日於萬那杜舉辦，大會主題為「讓亞太區社群建立一個可負擔、包容、開放與安全的網路」，從申請提案的類別來看，主要將討論連網&賦權、線上隱私&保護、網路安全等相關議題。

## 3. 臺灣 TWIGF 發展

- 講者：吳國維，NII 協進會顧問／TWIGF MSG 主席

TWIGF 自 2017 年正式轉型為完全由民間自籌經費的自發性組織，其決策由多方利害關係人指導小組(MSG) 決定，期望能推動臺灣的網路政策發展採取由下而上的方式，並與國際接軌，以 TWIGF 名義參加 APrIGF。目前 MSG 有 29 人，以民間企業代表居多，同時他們也是後續 2 天論壇活

動的贊助者。當然，政府也有參與 TWIGF，如通傳會詹婷怡主委不但於開幕典禮上致詞，而且還將擔任與談人，和大家一起討論議題。此外，TWIGF 還有臉書社團，成員已經超過 2 千人，而且每 2 個月也會舉辦演講會。這些網路與實體活動，都歡迎大家的參與。

## (七) 未來參與機會&總結

- 講者：Yannis Li，DotAsia 合作發展主任

研習營學員於課後有許多國際會議可以參加，包括 8 月在萬那杜舉辦的 2018 APrIGF、9 月在新喀里多尼亞舉辦的 APNIC (Asia-Pacific Network Information Centre，亞太網路資訊中心) 第 46 次會議、10 月在巴塞隆納舉行的 ICANN 第 63 次會議、11 月於曼谷舉辦的 IETF 第 103 次會議、11 月在巴黎舉辦聯合國 IGF 等。無法親臨現場者，可以透過遠端方式參與會議。另外，也可以向 ISOC (Internet Society，網際網路協會)、ICANN 等單位申請補助經費去參加會議。

- 講者：梁理旋，NII 協進會副執行長

本次研習營將挑選 2 位優秀學員參加 8 月份萬那杜 APrIGF，評分標準包括學習熱忱、論述與表達能力、英文程度、TWIGF 參與狀況等，請學員於後續 2 天的 TWIGF 踴躍參與討論。此外，學員們未來也還有其他參與國際會議的機會，例如 2019 年 3 月於日本舉辦的 ICANN 64 會議，NII 協進會將於 8 月底舉辦說明會，介紹國際相關獎學金計畫，並邀請 2 位於國際事務有卓越表現的青年做經驗分享，歡迎大家蒞臨與交流。

## 四、印刷與影音記錄

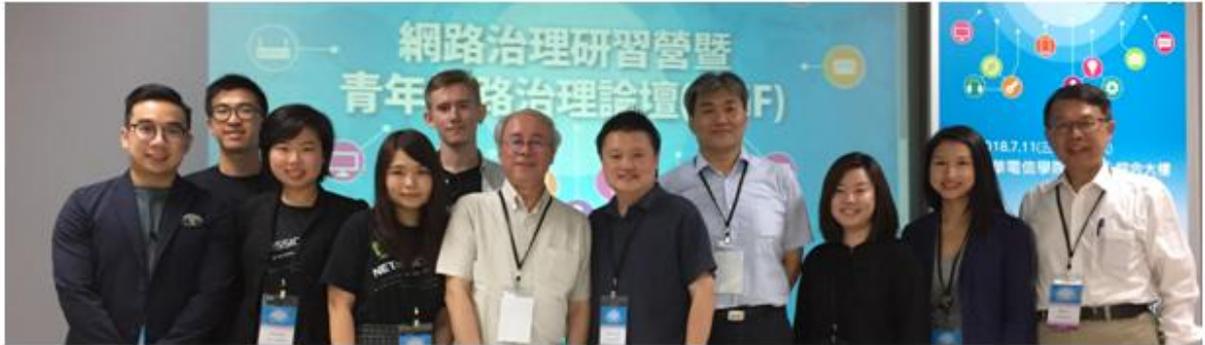
### (一) 布置與印刷品

本次課程的布置與印刷品包括：戶外直立旗、海報 (5 個不同尺寸)、議程板、識別證 (4 款)、學員手冊，以及結業證書，成品如下圖 11 所示。



圖 11. 研習營布置與印刷品

## (二) 活動剪影



致詞貴賓與講師合影



分組討論學員意見



模擬會議 (一般學員組)



模擬會議 (學生組)



講師與全體學員合照

圖12. 研習營照片

### (三) 課程錄影

本次研習營聘請專業攝影師全程拍攝，講師授課之內容（不含學員討論或報告）可於 YouTube 觀賞，網址為

<https://www.youtube.com/channel/UC9XuqZJU4H0ARFkU8h9wzxxw/videos>



資料來源：NII 直播(YouTube)

圖 13. 研習營授課課程錄影檔之頁面截圖

## 五、滿意度調查結果

本次研習營活動針對第一天的授課課程進行滿意度問卷調查，共計回收 20 份問卷（學員總人數為 34 人），統計結果如下圖 14 所示。整體而言，學員給予本次活動高度滿意的評價，尤其對於講習課程、整體課程設計、講師、教室、地點、工作人員等項目，「滿意度（滿意與非常滿意）」都超過 90% 以上；出現「不滿意」的項目則有宿舍、地點、餐飲等三項，但比例都低於 10%，且沒有任何項目是「非常不滿意」。

而在整個研習營天數方面，65%的學員表示願意投入 3~4 天參加活動

(3 天為 35%，4 天為 30%)，與本次研習營的天數吻合。不過，也有學員於 TWIGF 閉幕典禮上表示，對上班族而言，請假 4 天參加研習非常困難。此外，本計畫人員於電話聯繫學員時，也獲得相同回應。然而，由於本次授課課程因颱風來襲而從原訂 2 天縮短為 1 天，因此，也有學員反映課程太過緊湊來不及吸收，以及討論時間、QA 時間不足，甚至連休息時間都不夠。

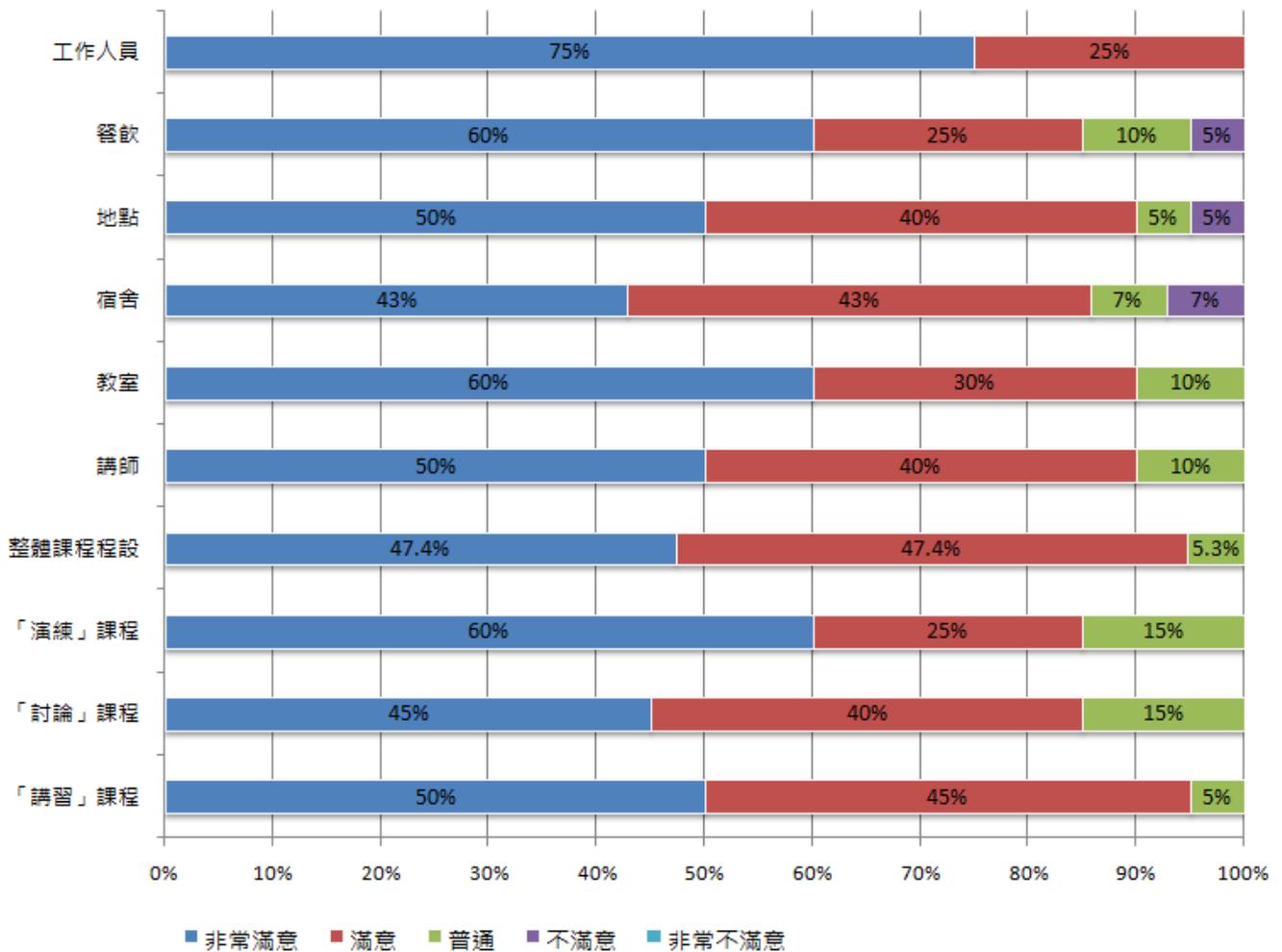


圖14. 研習營活動滿意度問卷調查結果

## 六、選拔優秀學員參與國際會議

### (一) 評選方式與結果

本次研習營由 7 位講師（包括來自香港與新加坡的 4 位講師，與國內 3 位講師）組成評選小組，從出席的 27 位非公務人員學員中，針對他們的學習熱忱、論述與表達能力、英文程度、2018 TWIGF 參與狀況等項目，進行綜合評估，以選出 2 位優秀學員，參加 8 月 13 日至 16 日於萬那杜舉辦的 2018 APrIGF，全程差旅費由本計畫之國際差旅費項目支應。

本次評選作業共召開 2 次討論會議，第一次會議於 7 月 13 日 TWIGF 會後假會場貴賓室舉行，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的特色與合適性，並決議將名額分配予學生組與一般組各 1 名，且最後推選出 2 組的正取學員各 1 名，以及備取學員各 2 名。

評選小組於 7 月 14 日 TWIGF 閉幕典禮後，召開第 2 次評選會議，針對正、備取學員於當日 TWIGF 的參與情況，進行二度評估，同時也考量是否有表現特別傑出的其他學員。經討論與調整後，確認學生組的正取學員為就讀大學資訊工程學系的薛先生，一般組的正取學員為就職於民間團體的周小姐，評選結果於 7 月 17 日上午於活動網站上公布。

## 錄取名單

恭喜以下 2 名學員錄取參與 2018 年亞太區域網路治理論壇(2018 APrIGF)

姓名	居住
周〇汝	新北市
薛〇仁	臺東縣

圖 15. 研習營網站公布優秀學員名單

本計畫並立即與正取學員聯繫，2 位優秀學員皆表示可以如期參加 2018 APrIGF，並簽署出席保證書，同時承諾履行以下義務：

- 於會後（9/7 前）繳交出國報告，包含討論議題摘要、心得建議。
- 於會後（預定 9 月底）參加一場分享交流會議。

## (二) 2018 APrIGF 簡介

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 年舉辦以來，每年皆吸引亞太地區二十多國的 2~3 百位多方社群代表參與。會議結束後並彙整成綜合報告(Synthesis Document)，且於聯合國 IGF 提出分享。

2018 APrIGF 將於 8 月 13 日至 16 日於萬那杜召開，大會主題為「讓亞太區社群建立一個可負擔、包容、開放與安全的網路」，主辦單位為萬那杜政府資訊總監辦公室(the Government Chief Information Officer, OGCIO)，以及電信與無線通訊監管機構 (Telecommunication and Radiocommunications Regulator, TRR)。開幕致詞貴賓除了萬那杜總理 Hon. Charlot Salwai 外，還包括網路之父 Dr. Vinton Cerf，以及當地與周邊國家的政府高層。

而在議程方面，8 月 13 日為會前日，提供與會者入門課程與 yIGF 課程等活動。接續 3 天則為正式會議，共有 30 個場次，討論議題涵蓋 GDPR、跨境資料、透明度報告、斷網、資訊安全，以及太平洋島國較有興趣的連網與天然災害管理等。

本次出國的兩位學員其中一位為學生，因此，報名參與 yIGF 活動，另一位則報名參加一般會議。

## 參、議題分析與多方參與

### 一、資料在地化座談

#### (一) 規劃說明

「政府」為網路治理的多方社群主要成員之一，並在許多先進國家的國家型 IGF 發展，扮演重要合作夥伴或共同支持者的角色。因此，本計畫透過在 TWIGF 申辦一場 90 分鐘主題座談(workshop)，邀請國內多方社群代表針對通傳會業務相關的議題，展開對話交流，以凝聚未來政策方向共識，同時也展現通傳會對我國國家型 IGF 的積極參與。

2018 年 TWIGF 的大會主題為「臺灣的數位蛻變與未來：危機與挑戰」，所徵求的工作坊主題有六大項目，包括：電信與網路政策、網路安全、數位經濟、數位包容(inclusive)、新興科技議題及其它議題等。

有鑑於資料已經成為數位經濟的關鍵資源，而世界各國又基於維護安全、保護個資等各種因素，紛紛實施限制資料跨境流通的相關規範，因此，本計畫提案申辦「電信與網路政策」主題中的「資料在地化 (Data Localization)」子題，題目則訂為「資料跨境流通與資料在地化對我國的挑戰」，在國內的相關規範包括《數位通訊傳播法》草案第 21 條、《個人資料保護法》第 21 條等。

本計畫並依據 TWIGF 公告辦法，於 107 年 4 月 10 日收件截止日前完成提案申請。經 TWIGF 多方利害關係人指導小組(MSG) 評選，本提案在 26 個提案書中，榮獲最高分數。

#### (二) 國際概況

目前國際間對於「資料在地化」一詞，並沒有統一的定義。根據美國

資訊科技與創新基金會 (the Information Technology and Innovation Foundation, ITIF) 的相關報告 (Cory, 2017)，凡是對跨境資料流通設立障礙，不論是明確的法規要求或是限制性的行政措施，都屬於「資料在地化」的概念。例如：要求企業必須在當地儲存副本或處理資料、必須獲得政府許可才可跨境傳輸資料等。而這些政策將對全球數位貿易產生新的障礙。

美國顧問公司 Albright Stonebridge Group (ASG) 於 2015 年的研究指出，全球有 23 個國家或地區實施強度不一的「資料在地化」政策，包括我國被歸類於相對低度、僅限制「特定行業」資料傳輸的國家 (圖 16)。而 ITIF 於 2017 年的研究則發現，全球實施「資料在地化」相關措施的國家已增加為 36 個，且當中包含許多已開發國家。我國也因為《個人資料保護法》第 21 條而出現在列表中 (圖 17)。

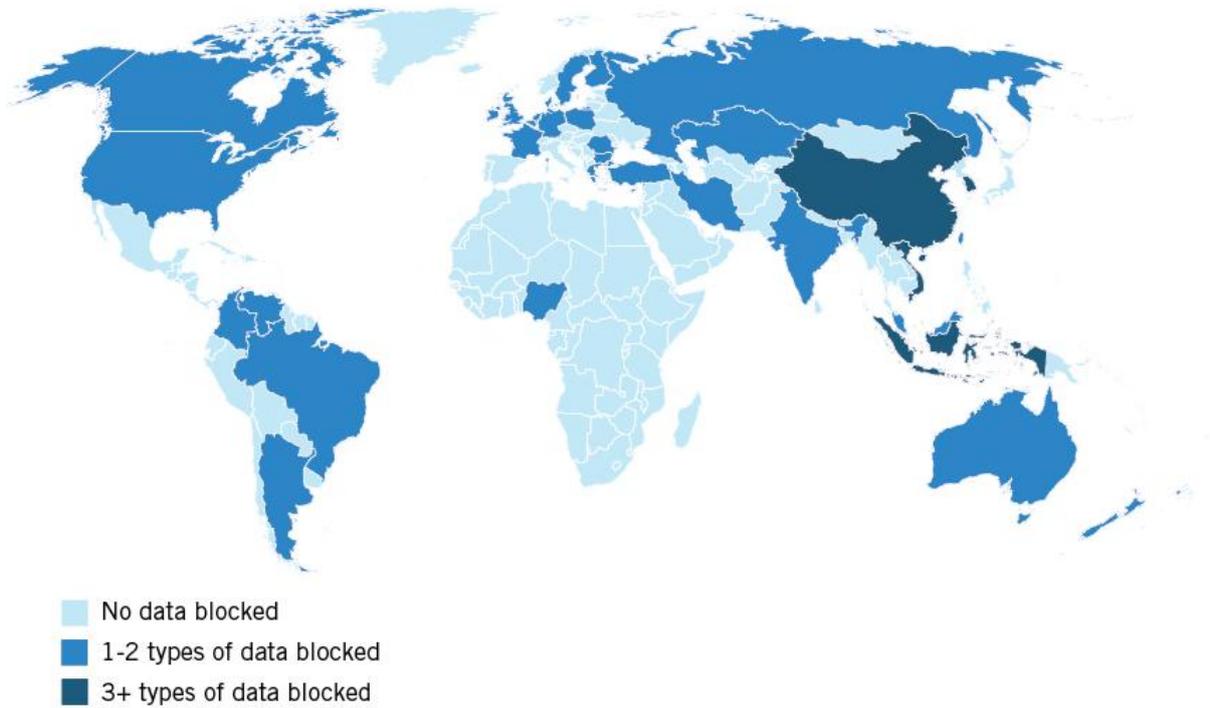
### GLOBAL SPREAD OF DATA LOCALIZATION\*

COLOR	STRENGTH OF MEASURES	COUNTRIES
	<b>Strong:</b> Explicit requirements that data must be stored on servers within the country.	Brunei, China, Indonesia, Nigeria, Russia, Vietnam
	<b>De Facto:</b> Laws that create such large barriers to the transfer of data across borders that they effectively act as data localization requirements.	European Union
	<b>Partial:</b> Wide range of measures, including regulations applying only to certain domain names and regulations requiring the consent of an individual before data about them is transferred internationally.	Belarus, India, Kazakhstan, Malaysia, South Korea
	<b>Mild:</b> Restrictions on international data transfers under certain conditions.	Argentina, Brazil, Colombia, Peru, Uruguay
	<b>Sector-specific:</b> Tailored to specific sectors, including healthcare, telecom, finance, and national security.	Australia, Canada, New Zealand, <u>Taiwan</u> , Turkey, Venezuela
	<b>None:</b> No known data localization laws.	Remaining Countries

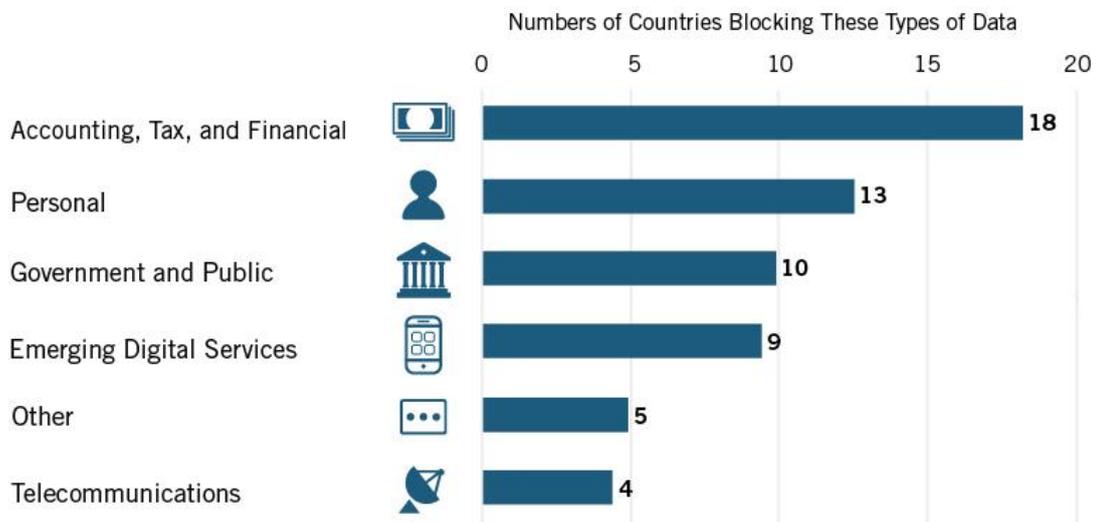
資料來源：ASG (2015)

圖 16. 全球實施「資料在地化」措施概況 (2015 年)

### Which Countries Block Data Flows?\*



### What Types of Data Are Blocked?\*



Taiwan		<p>Article 21 of Taiwan's Personal Data Protection Act permits government agencies the authority to restrict international transfers in the industries they regulate, under certain conditions, such as when the information involves major national interests, by treaty or agreement, inadequate protection, or when the foreign transfer is used to avoid Taiwanese laws.</p>
--------	--	--

資料來源：ITIF (2017)

圖17. 世界各國限制資料流通概況 (2017 年)

### (三) 國內外相關法規或規範

#### 1. 我國《數位通訊傳播法》草案

《數位通訊傳播法》草案之立法，以數位經濟發展為目標，促進數位通訊傳播的流通，並兼顧隱私資料及資訊安全政策。因此，對於涉及資料跨境流通及配套訂有相關的規範，例如：

- 第 11 條：數位通訊傳播服務提供者應依其服務性質，揭示服務使用條款，包含隱私權及資訊安全政策。
- 第 21 條：數位通訊傳播服務提供者對其位於我國境內之使用者，不得以不合營業常規之方式規避經由我國境內通訊傳播設施傳輸、接取、處理或儲存與使用者相關之數位訊息。前項之通訊傳播設施，包括利用其他數位通訊傳播服務提供者之通訊傳播設備與電腦運算、儲存及備援設備。
- 第 27 條：政府應採取若干措施鼓勵境外數位通訊傳播服務提供者於我國設立稅籍，以保障消費者權益。

#### 2. 我國《個人資料保護法》

- 第 21 條：非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：
  - (1) 涉及國家重大利益。
  - (2) 國際條約或協定有特別規定。
  - (3) 接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。
  - (4) 以迂迴方法向第三國(地區)傳輸個人資料規避本法。

#### 3. 歐盟 GDPR

歐盟《通用資料保護規範》(General Data Protection Regulation, GDPR)對於資料跨境傳輸採取原則禁止，例外許可(林政君編譯，2018)，相關條款載於「第五章個人資料移轉至第三國或國際組織」，例如：

- 第 45 條：個人資料移轉至第三國或國際組織，僅於執委會決定該第三國、第三國內的領域或特定部門，或國際組織，確實有充足的程度保護時，才可以傳輸，且不須獲得任何特別授權(財團法人金融聯合徵信中心，2017)。

#### 4. CPTPP

《跨太平洋夥伴全面進步協定》(The Comprehensive and Progressive Agreement for Trans-Pacific Partnership, CPTPP)電子商務專章之相關規定如：

- 第 14.11 條與 14.13 條明定各國應允許包含個資在內的電子資料跨境移轉，以及不得要求計算設施(Computing Facilities)在地化。但同時也允許各締約國可以基於達到「正當公共政策目標」，例如涉及國家安全或具體公共利益等，而得另行特別規範；且各締約國也認同各國基於保障通訊傳播的安全與機密性而各自訂有相關法規。

#### 5. WTO 之 TiSA 草案

世界貿易組織(WTO)之《服務貿易協定》(Trade in Services Agreement, TiSA)草案中的電子商務章節訂有相關條款(徐程錦，2016)，例如：

- 第 2 條：不得禁止其他成員國的服務提供者，於進行業務目的時，做資料的跨境傳輸。
- 第 8 條：不得以設立或使用本國境內計算設施，作為允許來自其他成員的服務提供者在本國提供服務的條件。

## 6. APEC 之 CBPR 體系

亞太經合會(Asia-Pacific Economic Cooperation, APEC) 透過「跨境隱私保護規則體系」(Cross Border Privacy Rules System, CBPR System)，從建立一套跨國安全可靠隱私保護系統角度，促進資料在 APEC 會員國間的自由流通，營造有利區域內跨境數位貿易發展的環境。

APEC 會員國加入 CBPR 體系需要通過下列三個階段的審核：

- (1) 申請個資隱私保護執法機關成為「跨境隱私合作協議」(Cross-Border Privacy Enforcement Arrangement, CPEA) 成員
- (2) 申請個資保護體制的審核認可
- (3) 申請認證機構 (Accountability Agent) 的審核認可

截至 2018 年 12 月，我國已經完成前兩個階段的審核，成為 CBPR 體系的成員，預計 2019 年國內即會出現 CBPR 認證機構，開始受理企業的認證申請。企業一旦通過認證，將有助於爭取 APEC 會員國的市場商機。

### (四) 提案內容

- 提案名稱：資料跨境流通與資料在地化對我國的挑戰
- 提案單位：國家通訊傳播委員會綜合規劃處
- 主持人：黃文哲／國家通訊傳播委員會法律事務處副處長
- 與談人：余若凡／國際通商法律事務所合夥律師  
吳國維／NII 產業發展協進會顧問  
陳在方／交通大學科技法律學院助理教授  
陳幼臻／Google 臺灣公共政策與政府事務總監  
何明誼／台灣人權促進會專案經理

- 簡介&討論議題

麥肯錫顧問公司 2016 年的研究指出，資料跨境流通對全球經濟成長的貢獻已經超過傳統的貨物貿易，單是 2014 年就為全球帶來 2.8 兆美元的收益。不過，自從 2013 年史諾登揭發美國政府秘密監控全球網路後，限制資料跨境流通與要求「資料在地化 (Data Localization)」相關政策逐漸席捲全球。根據美國資訊科技與創新基金會(ITIF)統計，目前全球至少有三十多個國家與地區實施相關政策，當中也包含許多歐美先進國家在內。

綜觀各國實施「資料在地化」相關政策的原因，主要包括為了維護民眾隱私、確保打擊犯罪時能取得資料、保護本國產業發展與稅收、提升國家安全等。雖然這些政策的論述基礎與成效仍待討論與檢驗，但是所伴隨的潛在風險，如阻礙數位經濟成長與創新、損害消費者權益、增加企業 IT 支出、加速全球網路分裂，甚至淪為威權國家監控人民與打壓異己的利器等，已經引發國際社會的疑慮。

另一方面，部分國際經貿協定與組織則是推動資料跨境的自由流通，避免數位保護主義升高。例如：我國正積極爭取加入的《跨太平洋夥伴全面進步協定》(CPTPP)，其電子商務專章中即規定成員國不得要求計算設施 (Computing Facilities) 在地化 (惟同時也允許成員國可基於「正當公共政策目標」而另行規範)；世界貿易組織 (WTO) 之服務貿易協定 (TiSA) 亦研商如何禁止會員國限制資料跨境流通；亞太經合會 (APEC) 也透過建立「跨境隱私保護規則體系」(CBPR system)，以減少資料跨境流通的障礙。

但值得注意的是，國際經貿規範日益涉及網路治理的情形，也引發許多國際網路治理社群的擔憂，因為有別於網路治理的所有多方利害關係人 (multi-stakeholder) 共同、公開、平等的參與精神，國際經貿規範的制定方式是採不透明且只有政府代表能參與的政府間 (intergovernmental) 模式。

我國《個人資料保護法》與《數位通訊傳播法》(草案)雖然沒有具體要求「資料在地化」，但是基於兼顧維護安全與隱私，對資料的跨境流通訂

有基本原則與規範。面對國際間資料治理政策的立場分歧，我國需要透過國內多方社群的溝通對話，充分了解相關利弊得失，以凝聚政策共識。

本場座談將探討以下問題：

1. 「資料在地化」的定義與範圍為何？
2. 各種實施「資料在地化」的原由是否合理？
3. 「資料在地化」政策可能對我國的政經與社會等層面產生哪些影響？
4. 如果世界各國都實施「資料在地化」可能對全球網路發展產生什麼影響？
5. 國際經貿規範論及「資料在地化」等治理議題，對我國正反面影響為何？

## (五) 座談內容

- 時間：107 年 7 月 13 日(五) 11:15~12:45
- 地點：中華電信學院板橋所 701 室
- 座談內容
  - 民主陣營與極權陣營對於資料跨境流通問題，於 2003 年的 ITU 會議即展開諸多爭辯。近年來，中國大陸與俄羅斯更是實施明確的「資料在地化」政策，但是這會大幅限制貿易的自由。因此，法規如何兼顧安全、隱私與經濟發展，成為國際間的重要議題。例如：TiSA (服務貿易協定)電子商務章節的第 2 條、第 4 條與第 8 條，明確規定不得要求計算設施的在地化，且資料要能跨境自由流通，以確保自由貿易；CPTPP 也有類似內容。相較於許多先進國家對於資料跨境傳輸採取「原則禁止，例外許可」立場，例如近期上路的歐盟 GDPR 第 45 條；我國則是從民國 84 年的《電腦處理個人資料保護法》即採取最開放的態度，即使是目前的《個人資料保護法》，也是「原則許可，例外禁止」(第 21 條)，放眼全球只有紐西蘭和我國

採取相同立場。我國迄今尚未援用上述條款宣告任何國家是個資的禁止傳輸國，其原因包括找不到中央目的事業主管機關出面處理。但由於不是所有國家都具備完善的個資保護法規，因此，已經成立專案辦公室的國家發展委員會，未來是否會處理相關問題，仍有待觀察。因應數位經濟等趨勢發展，通傳會遵循現代貿易規範的精神，兼顧我國使用者的權益保障，訂定《數位通訊傳播法》草案，當中第 21 條有相關規定，過去也有諸多討論，大家可透過網路搜尋。

- 此議題隨著企業雲端化、產業數位化而日益重要，並可分成「是否允許資料自由流通到其他國家」與「是否要求資料儲存在當地」兩個面向，其影響也各有不同。有些國家要求的在地化是指資料的儲存、處理，有些是指資料中心，有些是要求備份或存取。由於雲端服務的本質就是跨越國境，因此，服務提供者面臨如何遵循不同國家的不同法規問題，企業用戶則是不知如何選擇服務提供商，個別使用者不知自己的個資被儲存與備份在哪裡，而政府則是面臨跨境治理的挑戰。所幸國際間對於資料的跨境傳輸已有更多共識，即使是歐盟 GDPR 的原則禁止，也有更多的空間可以允許跨境傳輸。不過，「資料在地化」則較缺乏共識，中國大陸與俄羅斯是主張在地化的極端，美國反對，歐盟有討論但未付諸實施，德國是要求報稅資料在地化，南韓是要求地圖在地化。我國是出口導向國家，產業又以中小企業為主，如果各國都實施在地化，將不利我國中小企業發展，因此，建議可以參考日本做法，強化個資法的執法（2016 年修法），以及參加國際協議與合作。
- WTO 規定只能越來越開放，不能低於原先的承諾。而我國個資法雖然採取開放態度，但是在符合公共利益的前提下，可以援用第 21 條，要求課稅資料或備份資料的在地化。
- 當前服務與技術的創新，來自資料可以在全球流通運算與使用，難

免引發個資保護的疑慮，但 Google 深信創新與個資隱私保護是可以兼顧，也會善盡資料守門人的義務。要求「資料在地化」的原因包括資料隱私性、資料安全性、執法需求、保護主義等，但是這些主張往往又自相矛盾。以增進安全為例，重點應在於預防單一的脆弱點，若只將資料儲存在一個地方，反而更不安全，因為一旦遭受駭客攻擊或自然災害，將會影響服務運作甚至難以復原。再以保護主義、經濟角度為例，根據歐洲國際政治經濟中心 2014 年的研究，實施資料在地化會導致印度 GDP 減少 0.8%、印尼減少 2.3%、南韓減少 0.5%；反之，若促進資料跨境流通，則有助於各國中小企業打入國際市場。

- 臺灣如果想實施「資料在地化」，首先要思考目的為何，又是否有其他方法可以達到相同目的。從政治面來看，中國大陸與俄羅斯實施在地化法規，是在其聲稱擁有數位主權與數位國土的基礎上。再從經濟面來看，由於我國市場僅占全球的 1%~1.5%，一旦在地化的成本（法遵、設備、場地、人力等）大於獲利時，企業將選擇撤出或出走，但卻仍然可以擁有臺灣市場，就如同目前 Amazon 零售商在臺灣沒有設立辦公室，卻還是可以將產品從日本銷售來臺的模式一樣。中國大陸的網路是個封閉社會，中共透過「網路長城」阻斷民眾連結 Google、Facebook、Youtube 等世界各國民眾經常造訪的網站，中共並於 2017 年的烏鎮峰會（世界互聯網大會）公開表示樂於免費提供「網路長城」給其他國家，而許多以國安為由、想掌控網路的國家政府，確實也想要「網路長城」。「資料在地化」會造成每個國家的網路區塊化，世界經濟論壇（World Economic Forum, WEF）於 2016 年即發佈有關網路分裂的報告。而一旦在地化成為全球趨勢，將對今日的 one Internet 帶來巨大改變，目前發展情勢令人悲觀。總之，我國討論「資料在地化」應該分項目仔細討論，以免未蒙其利先受其害。而需要在地化的資料，例如健保資料即為一例。

- 中國大陸的「網路長城」已被美國列為非關稅貿易障礙，可以觀察後續美國將如何處理此問題。另外，在地化與跨境傳輸分屬 2 個題目，很多國家對金融資料的跨境傳輸採取一定限制)。
- 對於今日討論「資料在地化」議題存有疑慮。但從使用者角度而言，「資料在地化」的好處是可以知道自己的資料存放在哪裡，這是人民一項很重要的權利。Airbnb 於中國大陸實施《網路安全法》之前，即已經將資料儲存在中國大陸境內，至今我們仍無法得知臺灣民眾的資料是否也被儲存在中國大陸，但如果答案是，民眾是否會安心？另一方面，如果資料是儲存在臺灣，民眾又會比較安心嗎？畢竟我們至今仍然沒有成立個資法的專責獨立機關。政府、警政單位、大企業、中小企業對於「資料在地化」有許多不同的考量，但對一般民眾來說，只要上網能連到全世界即可。
- 人民沒有相信政府的義務，唯有人民不停地提出挑戰，政府才會進步。鼓勵自由貿易是我國向來的國家政策，迄今也沒有任何部會限制資料的跨境傳輸。但是除了基因與醫療資料、比特幣等有其他相關法規的限制外，我們也要思考是否有其他種類的資料需要於個資法第 21 條中討論，以在隱私保護與自由貿易之間取得平衡。)
- 贊同前面與談人提出的「資料在地化」並非達成目的的最好方式、應分項仔細討論等意見。美國與歐盟對資料跨境傳輸的立場不同，歐盟 GDPR 採取原則禁止，美國則是原則許可。從國際經貿規範的角度來看，我國現行的法規制度沒有問題，而未來如果要修法，則要注意是否違反 CPTPP 規定，以免妨礙我國申請成為會員國。CPTPP 源自美國推動的 TPP，因此，要求會員國應允許資料的跨境傳輸，且不得要求在地化，但同時也保留可以採取例外限制的空間，例如基於正當保護措施、不超過政策目的、不造成歧視結果等。

## • 現場問答

(1) 提問 1

- 問題：我國可以允許資料的跨境傳輸，同時也可以要求「資料在地化」，這兩者並不互相違背，也有待進一步討論。但是，臺灣的蘋果用戶資料可能儲存在雲上貴州，其他如 FB、LINE 等資料則不知道儲存在哪裡。另外，企業要的是彈性、獲利（不可能在世界各國都建資料中心）、不犯法（一旦可能違法就不在當地設辦公室）。經營臺灣金融市場的雲端業者就知道，臺灣本土銀行的資料不能放在國外，Google 正因為在彰濱工業區設有資料中心而成為這項業務的獲利者。
- 回應：個人對於「資料在地化」沒有特定立場，而是認為應該就資料的種類、政策目的，以及能否達成，做仔細討論，如健康醫療資料就應儲存在臺灣，加拿大也是採取相同措施。此外，也要評估臺灣在國際談判上是否有籌碼，以及實施在地化與否的利弊得失。另外，日本花 2 年時間和歐盟談判，讓符合日本個資法的企業即可符合歐盟 GDPR，我國也應成立個資法的專責機關，解釋相關法規疑慮。
- 回應：「資料在地化」並不是好的政策，要考量的層面很多，希望未來能有更多討論，勿讓臺灣淪為網路孤島。

(2) 提問 2 (網路治理論壇暨 yIGF 學員)

- 問題：是否可透過加密等技術，避免資料外洩？
- 回應：技術可以增進安全，降低被駭機率，Google 雲端服務提供獎金給成功的駭客，凸顯 Google 對其服務的安全信心。
- 回應：全球資訊網協會 (The World Wide Web Consortium, W3C) 已要求資料中心應賦予使用者知道其資料儲存地點的權利。
- 回應：有關個資可攜的問題，GDPR 已有規範，我國尚無此概念，

未來可要求國發會重新檢視，以落實大法官對於個資自覺概念的解釋。至於民眾能否知道資料被存放的地點，《數位通訊傳播法》草案中有隱私權政策與資訊揭露的要求。

## (六) 小結

本場座談中，多方社群代表各自從不同角度分享他們對「資料在地化」議題的看法。綜合來看，多數與談人對「資料在地化」措施抱持疑慮，認為它並不是達成「資料在地化」所宣稱的政策目標（如提升資訊安全、保護隱私等）的最好方式，甚至指出如果我國實施「資料在地化」，可能會帶來政治面與經濟面的負面衝擊。不過，也有幾位與談人表示，健康醫療等資料確實有「資料在地化」的需求，而且 CPTPP（跨太平洋夥伴全面進步協定）同時也賦予各成員國可以採取例外限制的空間，因此，我們需要針對不同的資料種類、政策目的、是否有其他替代方案等層面問題，做更進一步的深入討論。

## (七) 會議剪影

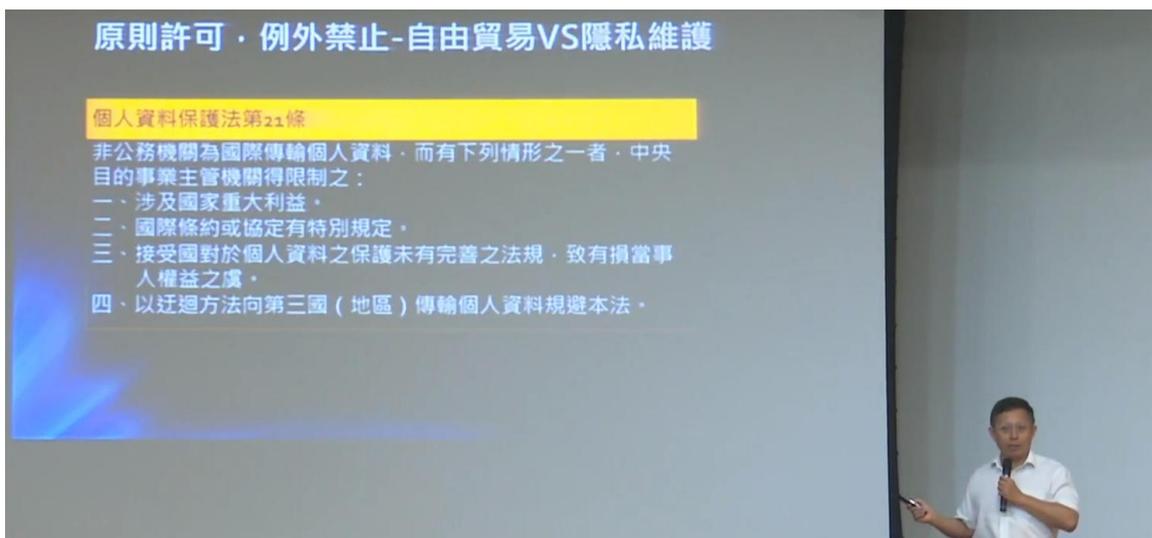




圖18. 「資料跨境流通與資料在地化對我國的挑戰」座談照片

## (八) 參考文獻

- 于國欽 (2018)。APEC 跨境隱私保護 台列成員。工商時報，2018/12/11。  
<https://www.chinatimes.com/newspapers/20181211000315-260205>
- 林玫君編譯 (2018)。簡介歐盟一般資料保護規則(GDPR)之跨境傳輸例外條款。經貿法訊第 233 期(2018.5.25)。  
<http://www.tradelaw.nccu.edu.tw/epaper/no233/5.pdf>
- 徐程錦 (2016)。《服務貿易協定》談判中的網際網路相關問題。  
<https://read01.com/ddO3oo.html>。
- 財團法人金融聯合徵信中心 (2017)。歐盟個人資料保護規則。金融與徵信叢書 NO. 77。
- 國家發展委員會 (2018)。我國申請加入 APEC 「跨境隱私保護規則」(CBPR) 體系成功通過 第一階段審查。

[https://www.ndc.gov.tw/News\\_Content.aspx?n=114AAE178CD95D4C&s=F663B94CC2669E6E](https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&s=F663B94CC2669E6E)

- ASG (2015). DATA LOCALIZATION A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION.  
<https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf>
- Cory, N. (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? ITIF.  
<https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>

## 二、國際參與分享座談

### (一) 會議簡介

#### 1. 會議資訊

- 主題：從臺灣、區域與全球看當前網路治理發展
- 時間：107 年 9 月 27 日 (四) 19:00~21:00
- 地點：伯朗咖啡松江店 4 樓 (臺北市松江路 332 號)
- 主題簡介與議程

在網路與實體世界交織融合的數位時代，不論是電信業者推出的上網方案是否合理、政府如何開放或管制共享經濟、網路平臺如何蒐集利用個人資料、社群媒體如何杜絕假新聞的散播，或是新興科技如 AI 或區塊鏈將如何改變人類社會等，這些問題不但與我們個人的使用權益與基本人權息息相關，而且也是目前國內外網路治理正在探討的重要議題。

其實聯合國早從 2006 年起，即每年舉辦網路治理論壇 (IGF)，讓全球

的多方利害關係人 (multi-stakeholder)，也就是政府、民間企業、技術社群、公民團體，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，以強化全球網路安全穩定地持續運作。儘管 IGF 會後並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，意外地帶動區域型 IGF 與國家型 IGF 的蔚為風潮。根據聯合國統計，全球各地的 IGF 已從 2011 年的 37 個，大幅增加為 2017 年的 97 個。

區域型 IGF 在亞太地區即為亞太區網路治理論壇 (APrIGF)，自 2010 年起已分別於香港、新加坡等地舉辦，包括臺北主辦 2016 年的會議。而國家型 IGF 在我國則為臺灣網路治理論壇 (TWIGF)，自 2015 年起每年舉辦一次會議，並於 2017 年正式轉型為完全由民間自籌經費的自發性組織。

今年我國的 TWIGF 大會主題為「臺灣的數位蛻變與未來：危機與挑戰」，已於 7 月中旬圓滿落幕；亞太區的 APrIGF 大會主題為「讓亞太區社群建立一個可負擔、包容、開放與安全的網路」，也於 8 月中旬在萬那杜舉辦完畢；而聯合國的 IGF 則訂於 11 月中旬在巴黎召開，預計將聚焦討論資安、隱私、新興科技、人權等層面問題。

本次座談會將掌握 2018 年網路治理年度盛會的精彩重點，從臺灣、區域與全球看當前網路治理發展，包括回顧臺灣網路治理論壇 (TWIGF) 的討論成果，分享亞太區網路治理論壇 (APrIGF) 的參與經驗，並展望聯合國 IGF 的重要議題。

表7. 「從臺灣、區域與全球看當前網路治理發展」座談會議程

時間	主題	講者
19:00-19:10	開場致詞	紀效正／通傳會綜合規劃處副處長 陳文生／NII 協進會執行長
19:10-19:30	引言報告：2018 臺灣與全球 IGF	梁理旋／NII 協進會副執行長、TWIGF 秘書處

	1. 我國 TWIGF 精彩回顧 2. 聯合國 IGF 議題簡介	林郁敏／NII 協進會資深經理
19:30-20:30	座談討論：2018 亞太區 APrIGF 參與分享	主持人： 吳國維／NII 協進會顧問、TWIGF MSG 主席 與談人： 陳映竹／台灣經濟研究院助理研究員 周冠汝／網路治理研習營學員、基金會專案人員 薛福仁／網路治理研習營學員、數位志工 (講師)
20:30-21:00	QA&交流	

資料來源：本計畫規劃

## 2. 活動宣傳

本次座談建置活動網站(<https://www.nii.org.tw/events/igf/>)，提供會議簡介、議程、場地等資訊，以及線上報名功能 (圖 19)。

宣傳方式主要透過臉書社團—臺灣網路治理論壇(Taiwan IGF) 和網路治理研習營 (IG Camp) 發佈活動訊息，貼文如下圖 20 所示。兩社團於本次活動期間共約有 2,200 位成員。另外，也發文至通傳會，邀請相關人員報名參加，以及將活動訊息以電子郵件寄送給同意收取網路治理相關活動的訂閱者。



圖19. 「從臺灣、區域與全球看當前網路治理發展」座談會網站頁面



圖20. 「從臺灣、區域與全球看當前網路治理發展」座談會臉書社團宣傳

### 3. 出席概況

本次座談共計包括學者、研究人員、律師、公務人員、調查官、產業界人士、大專學生等共 46 人報名，最後有 38 人到場，出席狀況良好。與會者在交流時間踴躍提問，並積極與講者討論，互動交流相當熱絡。

## (二) 開場與引言報告

### 1. 開場致詞

NII 協進會執行長陳文生首先介紹座談會的議程，以及 QA 交流時間的 2 種提問方式，包括現場舉手發問，以及在 slido 網站上匿名提問。接續由通傳會綜合規劃處副處長紀效正致詞，他表示現代人的生活與網路已無法分割，網路是實體空間延伸出來的虛擬空間，許多問題與你我都息息相關，需要大家去關心。紀副處長提到網路社群媒體大量散布假新聞的問題日益嚴重，但是用「假新聞」(fake news) 這個流行語來指稱不確實的新聞報導並不適當，應該要用「不實訊息」(disinformation)。此外，許多民眾以為網路上的「不實訊息」是由通傳會做審查，但其實網際網路並非由單一部會主管，除了媒體要自律之外，應該要由大家共同管理這個珍貴資源。

### 2. 引言報告：TWIGF 精彩回顧

- NII 協進會副執行長梁理旋

TWIGF 於 2015 年成立，是一個將網路多方利害關係人聚集在一起溝通互動的平臺，自 2017 年正式轉型為完全由民間自籌經費的自發性組織，除了建立 TWIGF 臉書社團、舉辦年度大型論壇外，每 1~2 個月還舉辦小型座談會。

2018 年的年度論壇於 7 月 13 日~14 日舉辦，共有 16 場座談，260 人與會，Youtube 累積觀看次數達 1,700 次。除了國內政府、技術社群、公民團體、民間企業等積極參與外，更有來自國際主要網路公司、社群網站、通

訊軟體平臺，以及國際組織的共襄盛舉，顯示 TWIGF 受到國內外相關社群的重視。

TWIGF 特點在於它是多方社群共同申辦的活動，針對各種網路治理的相關議題進行對話，期盼大家加入 TWIGF 臉書社團，並踴躍提案 2019 年的座談。

表8. 2018 TWIGF 座談題目

子題類別	題目 (共16場次)
電信與網路政策	<ul style="list-style-type: none"> <li>資料跨境流通與資料在地化對我國的挑戰</li> <li>監控、審查、與數位權利保護：從網路透明報告談起</li> </ul>
網路安全	<ul style="list-style-type: none"> <li>雲端管轄權?--跨境數據取證之困境與突破</li> <li>群眾媒體Live秀挑戰網路治理-直播這檔事！</li> <li>5G行動通信網路之資安挑戰</li> <li>從臉書個資外洩檢視政府開放資料個資保護</li> </ul>
數位經濟	<ul style="list-style-type: none"> <li>GDPR: Balancing Privacy with Stakeholder Needs for Data (ICANN申辦)</li> <li>數位經濟下的競爭法課題</li> <li>區塊鏈及虛擬貨幣的治理模式課題</li> <li>如何讓臺灣的網路環境更具有國際競爭力</li> </ul>
數位包容	<ul style="list-style-type: none"> <li>網路封鎖：對抗網路侵權的可行之道？</li> <li>從數位促進影響:量度青年數碼移動力 (DotAsia申辦)</li> </ul>
新興科技議題	<ul style="list-style-type: none"> <li>區塊鏈技術在台灣的應用、發展與未來</li> </ul>
共通及其他議題	<ul style="list-style-type: none"> <li>如何在臺灣建構網路治理機制的環境</li> <li>台灣女性在 ICT 相關產業的就業機會與未來</li> <li>網路治理在校園</li> </ul>

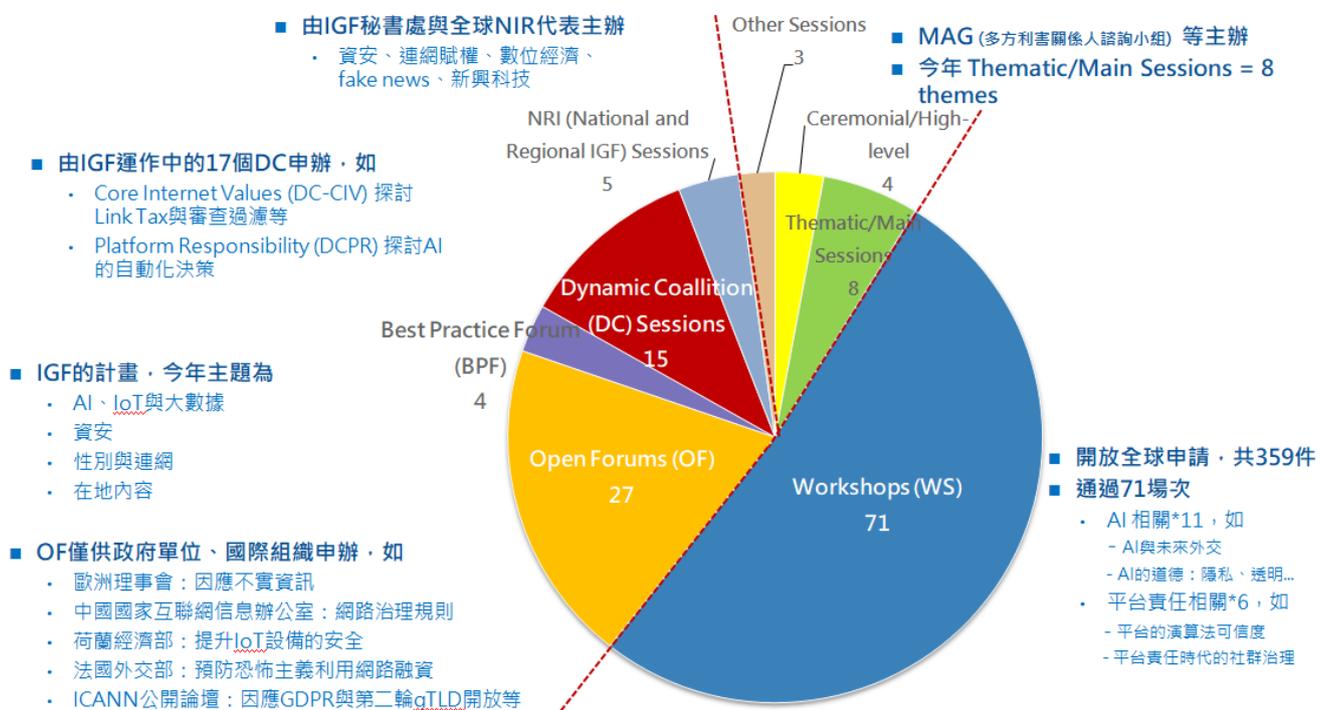
資料來源：TWIGF 秘書處

### 3. 引言報告：2018 聯合國 IGF

- NII 協進會資深經理林郁敏

2018 聯合國 IGF 於 11 月 12 日~14 日在法國巴黎召開，大會主題為「網路信任」(Internet of Trust)，討論主題分為 8 大主題與 55 個子題，共計 137 場會議。這些主題與子題是 3~4 月期間 IGF 徵求全球社群意見後彙整而成。

IGF 會議可分成主場次(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) 等許多不同類型。當中的座談是開放給全球申請，今年共有 300 多件申請案，最後有 71 件獲得通過，討論最多的是人工智慧和平臺責任相關議題；開放論壇只有政府單位和國際組織可以申辦，如這次歐洲理事會與法、荷、中等國政府都有申辦；而最佳典範論壇則是最後會提供建議給大家參考。



資料來源：本計畫彙整

圖21. 2018 聯合國 IGF 會議類型與討論議題

雖然臺灣不是聯合國的會員國，無法親臨現場參與會議，但是仍可透過遠端參與，同步在線上提問。因此，期許國內各界能多關注聯合國 IGF 與亞太區 APrIGF，才能聽到多元不同聲音，了解真正的世界潮流與國際趨勢。

### (三) 座談討論：2018 APrIGF 參與分享

- 主持人：吳國維／NII 協進會顧問、TWIGF MSG 主席
- 與談人：
  - 陳映竹／台灣經濟研究院助理研究員
  - 周冠汝／網路治理研習營學員、基金會專案人員
  - 薛福仁／網路治理研習營學員、數位志工（講師）

主持人和與談人們分享 2018 年 8 月份前往萬那杜參加 APrIGF 的經驗與心得，重點包括：

#### 1. 跨越語言障礙

- 英文為國際會議所使用的語言，有些國家在英語表達上有困難，或是對某些口音與用字較為陌生，以致形成溝通障礙。所以，相當程度的語言能力，是有效溝通的第一道門檻。

#### 2. 跨越社群障礙

- APrIGF 主要目的為跨社群的溝通與合作，但是技術社群和其他社群經常覺得無法與對方溝通，因此，應考量使用對方能理解的語言來對話。
- 每個國家重視的議題不同、對問題了解的層次也不同，如何理解對方已知的知識，然後站在不同立場進行討論，是需要努力的。
- 如何突破同一社群的同溫層、尊重其他社群的利害關係人，進而達到溝通的目的，仍是需要學習的課題。

#### 3. 萬那杜的上網問題

- 萬那杜為許多小島組成的島國，大學教育仰賴遠距教學，但是當地

網路速度卻是又慢又貴。臺灣人習以為常的網路吃到飽、免費 WIFI 等，對當地人來說是難以想像。

#### 4. 積極參與網路治理

- 網路治理議題與數位時代的生活息息相關，需要大家共同關心與解決問題。而參加國際會議時，應主動提案、擔任座談講者，或是至少把握在會議中發言的機會。

### (四) QA & 交流

本次座談的問答交流採現場發問與網路提問兩種方式，網路提問於 slido 網站進行，兩者合計共有十多個問題。惟因時間有限，僅就以下問題討論交流。

#### 1. 臺灣在亞太國家中參與網路治理的情況？

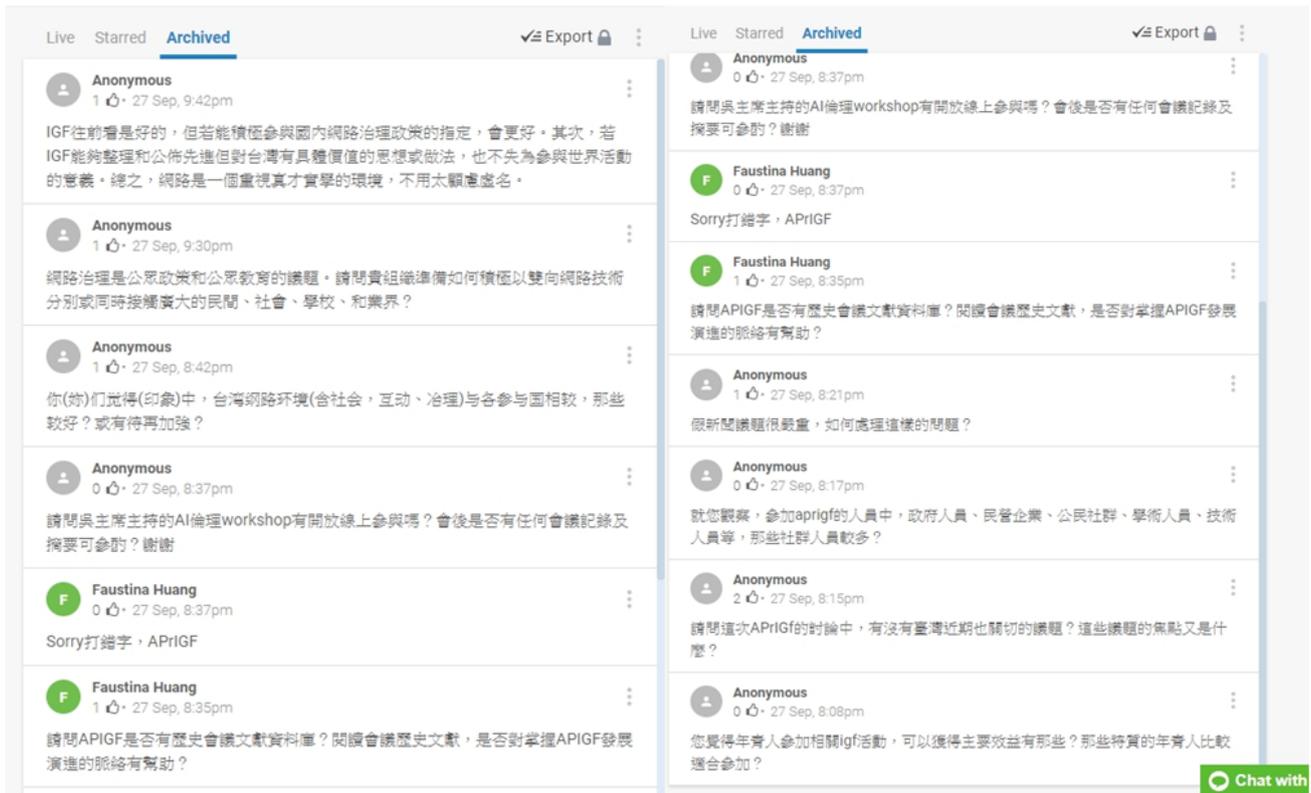
- 就 TWIGF 年度論壇與雙月會議活動的參與狀況來看，臺灣在亞太地區的表現是不錯的，而且臺灣政府官員願意主動參加 TWIGF，與其他利害關係人共同溝通討論，這在亞洲其他國家很少見到。

#### 2. 哪一個社群的 APrIGF 參與者最多？

- 社群參與人數的多寡不是重點，而是參與的程度如何。
- 由於許多人身兼不同的利害關係人身分，因此，在國際會議發言時，可以自行決定，只要聲明此次發言是代表哪一個社群或單位，讓大家知道你的立場即可。

#### 3. APrIGF 是否有歷年會議的文獻資料？

- APrIGF 網站上有每年會議的摘要報告，並自 2015 年開始由大會產出綜合報告 (Synthesis Document)，記錄當年各大議題的討論成果，並於聯合國 IGF 做報告分享。



資料來源：Slido 網站

圖22. 「從臺灣、區域與全球看當前網路治理發展」座談會線上提問

## (五) 小結

本次座談內容顯示，我國的國內網路治理參與情況，從 TWIGF 年度論壇與雙月會議活動的出席率與問答互動來看，在亞太國家當中堪稱表現相當不錯，尤其政府官員也願意主動和其他多方社群溝通討論。至於 APiGF 的參與，重點並不在於現身出席，而是要朝向主動提案、主動發言、擔任講者等，能夠和國際進行互動交流的方向努力。

## (六) 會議剪影



圖23. 「從臺灣、區域與全球看當前網路治理發展」座談會照片

### 三、歐盟《防止散播線上恐怖主義內容法案》

#### (一) 概述

有鑑於歐盟近期發生的多起恐怖攻擊事件中，皆發現恐怖份子利用網路策劃攻擊行動，歐盟執委會 (European Commission, EC) 於 2018 年 9 月 12 日提出《防止散播線上恐怖主義內容法案》(Regulation on preventing the dissemination of terrorist content online)，要求網路平臺業者必須在接獲政府主責單位刪除命令的 1 個小時內完成作業，否則最高將可處全球年度營業額 4% 罰鍰。

此法案目前尚待歐洲議會與歐洲理事會的採認。而依據歐盟的法規種類說明，Regulation 一旦獲得採認，無須再經由各國立法程序，即可適用於所有歐盟成員國 (EC, n.d.)。

線上「恐怖主義內容」是歐盟線上「違法內容」當中的一個類別。歐盟執委會表示，由於「恐怖主義內容」一旦散播出去，會立即產生安全性風險，因此，特別就此提案立法；至於「違法仇恨言論」等其他有害的違法內容，則是持續透過各種措施，全面遏阻它們的擴散。

根據歐盟相關文件，上述詞彙的定義如下所列：

- 線上「違法內容」

所有不符合歐盟或成員國法規的資訊，包括恐怖主義、兒童性虐待、「違法仇恨言論」、商業騙局與詐欺、侵犯智慧財產權。

- 線上「恐怖主義內容」

涉及煽動或提倡進行恐怖份子的犯罪行為、宣傳恐怖組織的活動、提供實施恐怖主義罪刑的技術指導等資料，包括文字、圖像、錄音、影片等。

- 線上「違法仇恨言論」

由歐盟刑法等法規所訂定，係指針對種族、膚色、宗教、血統與民族，或人種等個人或族群的特徵，公然煽動去施加暴力或仇視敵對。

歐盟線上「違法內容」的類別與主要因應措施彙整如下表 9 所示。由於範圍相當廣泛，因此，本篇僅探討當中與國家社會安全有關的線上「恐怖主義內容」與「違法仇恨言論」。

表9. 歐盟線上「違法內容」類別與因應措施

線上違法內容類別	因應方式	說明
恐怖主義內容	制定新法	有鑑於恐怖分子利用網路策劃多起歐盟的恐怖攻擊事件，且恐怖主義內容一旦上網會立即產生安全風險
違法仇恨言論	採業者自律並追蹤成效	2016 年啟動的《對抗線上違法仇恨言論行為準則》已獲相當成效，70% 仇恨言論於接獲通知時即刪除，而需進一步評估的案件中有 80% 於 24 小時內處理完成
兒童性虐待	目前正評估成效	已有《對抗兒童性虐待指令》(Directive on combating sexual abuse of children)；目前非營利組織 WePROTECT Global Alliance (我們保護全球聯盟)，及由歐盟共同成立的 INHOPE (International Association of Internet Hotlines, 國際網路兒童色情檢舉熱線聯盟) 持續展現執行成效
侵犯智慧財產	修改法規	正推動法規改革--《著作權指令》(Copyright Directive)
	採業者自律	針對仿冒商品，近期已發布相關指南(guidelines)，另外也有多個相關的合作備忘錄 (MOU)
商業詐騙與詐欺	推動合作方案	已有《不公平商業行為指令》(Unfair commercial practices directive)、《消費者權益指令》(Consumer

線上違法內容類別	因應方式	說明
		rights directive)；目前正推動如消費者保護聯合行動 (Consumer Protection Joint Actions)等合作方案

資料來源：本計畫彙整

## (二) 政策發展與目標

### 1. 政策發展

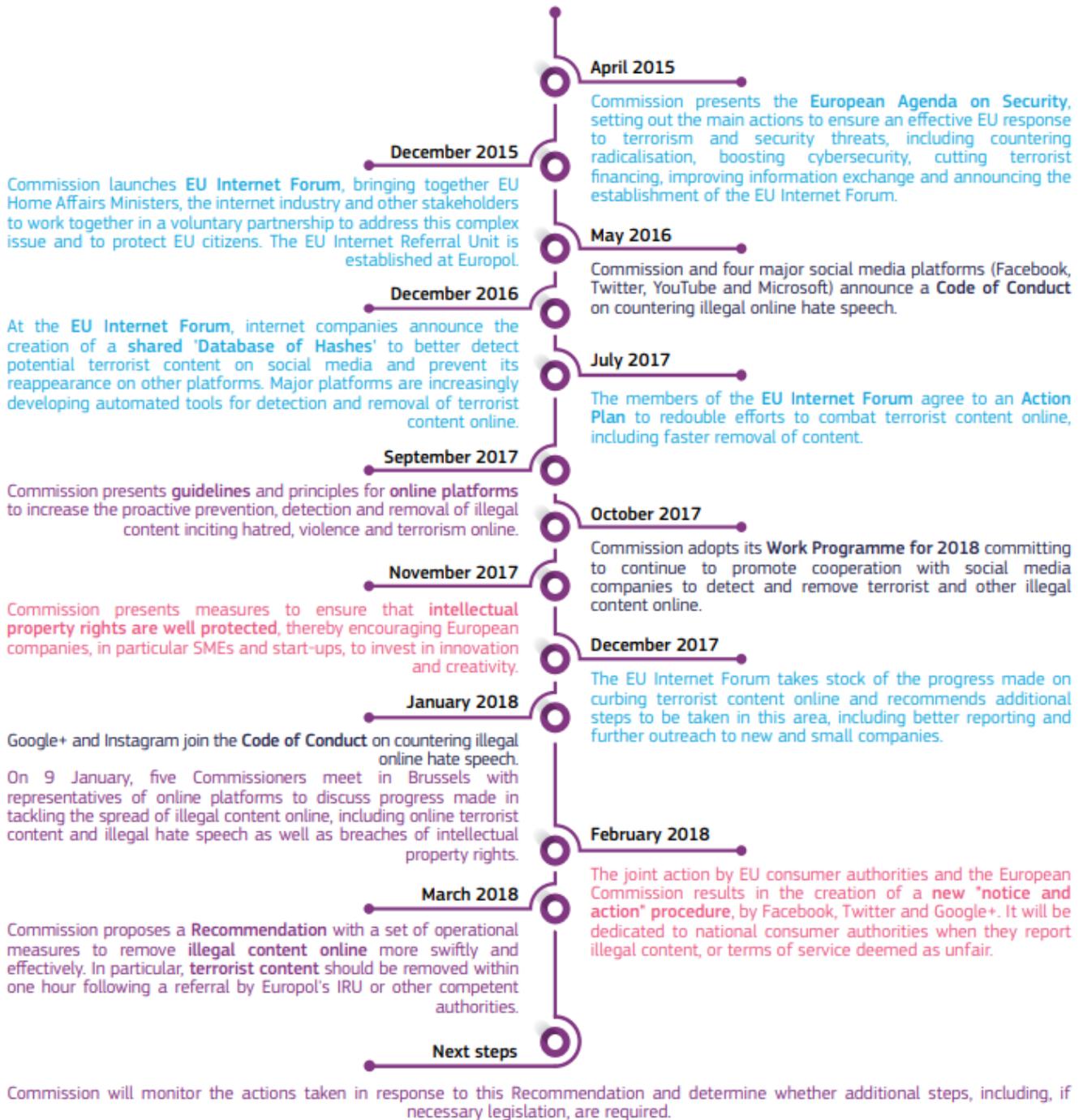
歐盟執委會自 2015 年即著手因應線上「違法內容」問題，其政策措施發展如圖 24 所示 (至 2018 年 3 月)。主要措施包括：

- 2015 年 12 月歐盟官方、網路平臺業者與其他多方社群，於歐盟網路論壇 (EU Internet Forum) 建立自主合作夥伴關係，討論複雜的線上「違法內容」議題；後續並於歐洲刑警組織 (European Police Office, Europol) 中，設立轉介處理線上「違法內容」的單位。
- 2016 年 5 月 31 日歐盟執委會與 Facebook、Microsoft、Twitter、YouTube 共同推出《對抗線上違法仇恨言論行為準則》(Code of Conduct on countering illegal online hate speech)，相關業者承諾於 24 小時內檢視刪除要求，並於必要時進行刪除。
- 2017 年 9 月 28 日歐盟執委會發布《打擊線上違法內容，強化線上平臺責任通告》(Communication on Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms)，透過非強制性規範，要求網路平臺業者強化自律措施，對煽動仇恨、暴力與恐怖主義等違法內容，進行主動偵防與刪除。
- 2018 年 3 月 1 日歐盟執委會發布《有效打擊線上違法內容建議措施》，內容包括明確的通知與刪除程序、有效的工具與偵防技術、

加強確保基本權益的保護措施、與主管當局緊密合作等；並特別針對「恐怖主義內容」，建議於接獲正式通報的 1 小時內進行刪除。

- 2018 年 4 月至 6 月期間，歐盟執委會就整個線上「違法內容」相關問題，進行利害關係人的意見蒐集，包括對歐盟的社會大眾展開意見徵詢與隨機抽樣問卷調查、向各成員國主管機關及網路平臺業者諮詢等，主要結果包括：
  - 整體而言，大多數的利害關係人認為線上「違法內容」是嚴重的社會問題，但也指出，如果立法要求刪除違法內容，應同時具備確保言論自由等基本權益的保障措施。
  - 社會大眾意見徵詢共回收 8,749 份個人意見，結果顯示 75% 認為網路是安全的、33% 曾經見到違法內容、幾乎所有人都認同言論自由的重要性、18% 認為採取進一步措施是重要的。
  - 隨機抽樣問卷調查共回收 33,244 份樣本，結果顯示 65% 認為網路不安全，90% 表示阻止違法內容的散播是重要的。
  - 成員國主管機關普遍認為，雖然業者自律有些效果，但是對於「恐怖主義內容」需要賦予具約束力的責任。而這項看法也和歐洲理事會 2018 年 6 月會議的結論相同。
- 2018 年 9 月 12 日歐盟執委會提出《防止散播線上恐怖主義內容法案》，主席容克 (Jean-Claude Juncker) 表示，1 個小時是恐怖主義釀成最嚴重災害的關鍵時間，因此透過新法案以回應歐盟民眾對安全的期許。歐盟執委會並指出，2016 年啟動的《對抗線上違法仇恨言論行為準則》已獲相當成效，且目前主要網路平臺業者包括 Facebook、Microsoft、Twitter、YouTube、Instagram、Google+、Snapchat、Dailymotion，都已簽署加入這項行為準則。

## TIMELINE – WHAT HAS THE COMMISSION DONE TO COUNTER ILLEGAL CONTENT ONLINE?



資料來源：EC, 2018

圖24. 歐盟執委會因應線上「違法內容」措施發展 (截至 2018 年 3 月)

## 2. 預期目標

### (1) 《防止散播線上恐怖主義內容法案》

此法案旨在透過對網路平臺業者訂定最低限度的義務，在不侵犯基本權益下（例如言論與資訊自由等），為防止網路服務遭到恐怖主義的濫用，提供一個統一的法律框架，增進網路平臺業者的法規遵循明確性，提升使用者對線上環境的信任，以確保歐盟數位單一市場能在一個開放與民主的社會順利運作。

### (2) 《對抗線上違法仇恨言論行為準則》

此準則係為網路平臺業者對抗線上「違法仇恨言論」散播的自律規範，同時亦作為簽署準則的業者，確保會快速處理刪除通報的具體承諾。

## (三) 實施重點

### 1. 《防止散播線上恐怖主義內容法案》

#### (1) 法案特點

《防止散播線上恐怖主義內容法案》具有包括限時 1 小時刪除、所有平臺皆有法律責任、祭出重罰等下列 7 項特點：

- 限時 1 小時內刪除

「恐怖主義內容」於上線後 1 小時即開始快速傳播，因此，網路平臺業者必須於接獲政府主責單位刪除命令的 1 小時內，完成刪除作業。

- 訂定「恐怖主義內容」的明確定義

「恐怖主義內容」係指涉及煽動或提倡進行恐怖份子的犯罪行為、宣傳恐怖組織的活動、提供實施恐怖主義罪刑的技術指導等資料。

- 所有平臺皆有法律責任

為確保網路服務不會遭到恐怖主義的濫用，所有平臺業者都須負有法

律責任。至於是否要採取主動性的積極措施(如使用新工具)，則視該平臺被用來散播「恐怖主義內容」的風險有多高而定。

- 加強合作

合作架構的成員包括網路平臺業者、成員國(政府)，以及歐洲刑警組織。當中，網路平臺業者與成員國必須指派全年無休的聯絡窗口，以追蹤刪除命令或轉介通知的執行情況。

- 強化保障措施

網路平臺業者必須提供有效的投訴機制，並要儘速恢復被無理刪除的內容，如有使用自動偵測工具，也要進行人工監督與驗證；而政府主責單位應該完備有效的司法補救措施；內容提供者則擁有質疑撤銷命令的權利。

- 提升透明度與課責

網路平臺業者與政府主責單位必須提供年度透明度報告(說明如何處理「恐怖主義內容」)與定期報告(說明所採取的預防措施)，以確保落實透明度與監督。

- 祭出重罰

歐盟成員國必須對沒有履行刪除命令的網路平臺業者，施以有效、對等、懲戒性的罰鍰。在系統性失效的情況下，最高可處前一年的全球年度營業額4%罰鍰。

## (2) 分工與合作

針對上述特點中的「加強合作」，根據《防止散播線上恐怖主義內容法案》，合作架構成員的各方主要工作如下：

- 網路平臺業者

- 實施「辦理刪除命令與轉介通知」的穩健程序。
  - 指派全年無休的聯絡窗口，以在收到刪除命令的 1 小時內迅速刪除內容，並與政府主責單位聯繫。
  - 確保備妥人工監督等保障措施，以避免內容遭自動化工具誤刪。
  - 備妥有效的申訴程序，讓使用者在自認為內容遭到誤刪時，可以提出申訴。
  - 與政府主責單位針對「恐怖主義內容」的刪除措施與預防上傳，進行合作；當涉及危害公共安全時，應立即通報執法單位。
  - 在服務條款中，明訂防止散播「恐怖主義內容」的政策，並將因應此問題所採取的行動，列入發布的年度透明度報告中。
- 成員國（政府）
    - 確保該主責單位具有辨識線上恐怖主義文宣的能力，且當需要時，能夠迅速發出刪除命令或轉介通知。
    - 與其他成員國及歐洲刑警組織協調，確保線上「恐怖主義內容」的證據已經標記，同時避免國家層級調查的重複與介入。
    - 備妥合適的上訴程序，讓網路平臺業者與內容提供者在自認為遭受不公平的刪除命令時，可以提出申訴。
    - 於全面考量本法案相關因素後，裁定違法網路平臺業者的罰鍰。
  - 歐洲刑警組織 (Europol)
    - 將「恐怖主義內容」轉介給網路平臺業者處理。
    - 協調刪除命令與轉介通知，以避免重複作業。
    - 當網路平臺業者不確定該向哪個成員國警示與恐怖主義犯行有關的證據時，扮演聯絡窗口的角色。

- 提供專家支援予成員國與網路平臺業者。

## 2. 《對抗線上違法仇恨言論行為準則》

《對抗線上違法仇恨言論行為準則》的主要重點如下：

- 使用者通報

協助使用者通報違法仇恨言論 (提供通報系統，並進行教育宣導)。

- 評估依據

當收到通報要求刪除內容時，網路平臺業者依據其政策與社群守則，並於適當情況下，同時依據各成員國與歐盟的遏止散播種族主義與仇外主義相關法規，進行評估。

- 作業時程

大多數使用者通報需於 24 小時內完成評估，並於必要時予以刪除。

### (四) 相關爭議

針對歐盟提出《防止散播線上恐怖主義內容法案》，全球主要網路平臺業者表示支持歐盟對抗恐怖主義的目標。Facebook 指出，他們的目標和歐盟執委會一樣，也不允許自家平臺上有恐怖主義，並且已經迅速且大規模地刪除恐怖主義文宣，還自認為可以做得更多；YouTube 也表示，他們贊同歐盟迅速刪除「恐怖主義內容」的要求，而這也是他們在這方面投入大量人力與科技的原因 (BBC News, 2018)。

不過，媒體與學者從法規衝突、引發網路審查與監控、危害言論自由、侵犯人權等層面，對此法案提出質疑或反對意見；而歐盟執委會則是強調此法案與其他歐盟法規的一致性、具有充分保護基本權利的措施，以及沒有網路審查的問題等。相關爭論與歐盟的說明詳如下表 10 所示。

表10. 歐盟《防止散播線上恐怖主義內容法案》的爭論與說明

爭議點	各界質疑或反對意見	歐盟執委會的說明
法規衝突	TechCrunch 與財富雜誌 (Fortune) 報導指出，此法案與歐盟《電子商務指令》(E-Commerce Directive)衝突，因為後者禁止成員國要求網路平臺業者監控使用者所傳輸或儲存的資料(Lomas, 2018; Meyer, 2018)	由於散播「恐怖主義內容」的風險尤為巨大，本法案可以例外排除歐盟架構，因此，成員國要求網路平臺業者實施主動性措施並不會違反《電子商務指令》15 之 1 條(EC, 2018c)
引發網路審查與監控	TechCrunch 報導認為，此法案鼓勵網路平臺業者發展自動偵測工具、進行主動性措施、刪除「恐怖主義內容」等，形同要求網路平臺業者執行事先過濾(Lomas, 2018)	本法案是在充分尊重歐盟基本權利的基礎上訂定的，並強化保障基本權利的措施，尤其是保護言論與資訊自由，同時也確保合法內容不會遭到刪除，因此，沒有網路審查的問題 (EC, 2018b)
危害言論自由	TechCrunch 報導指出，何謂「恐怖主義內容」其實很主觀，此法案所訂定義無可避免將會鼓勵刪除模糊地帶的內容，進而連帶衝擊言論自由(Lomas, 2018)	
侵犯人權	紐約大學法學院教授 FionnualaNíAoláin (2018) 認為，此法案對恐怖主義的寬鬆定義，將衝擊法律所保障的言論、宗教活動、政治參與的自由；且法案對網路公司課以諸多責任，卻沒有充分闡明人權與法治的義務、補救機制，並且還過度擴大安全框架	

資料來源：本計畫彙整

## (五) 小結

本篇介紹歐盟針對線上「違法內容」當中的「恐怖主義內容」，推動新法《防止散播線上恐怖主義內容法案》；對「違法仇恨言論」則是持續實施業者自律的《對抗線上違法仇恨言論行為準則》。兩者皆是旨在能夠迅速處理明顯與可能的違法內容，避免因為司法程序冗長而讓這些內容不斷地散播，並造成實質傷害。而儘管歐盟在因應線上「違法內容」的整體政策發展過程堪稱周延，且前述法案也獲得全球主要網路平臺業者的正面回應，一旦涉及強制性法規的介入時，仍然不免招致網路審查與監控、危害言論自由、侵犯人權等抨擊。

近來國內也有意針對網路上的不實消息（常以「假新聞」統稱）推動立法或修法，包括《國家安全法》、《社會秩序維護法》、《刑法》等法規，都列入盤點名單(蘋果日報，2018a)。惟在尚未定義問題範圍時，已經引發各界將不同問題混為一談且各持正反立場的情況。例如，有學者專家基於既有的《社會秩序維護法》、《刑法》已足以懲處毀謗、散播謠言等情狀而反對立法(張理國，2018；今周刊，2018)；但也有學者因為來自中國大陸的惡意不實訊息已危害國家社會安全而建議修法(蘋果日報，2018b)。因此，歐盟區隔問題且循序漸進的政策發展，或可作為我國參考。

### 1. 界定問題範圍與相關法規

歐盟基於「違法行為不分實體世界與網路世界」(What is illegal offline is also illegal online)理念，首先將網路上的各種問題內容，區分為違反既有法規的線上「違法內容」，以及有問題但不違法的「不實訊息」(過去稱為「假新聞」)。前者又可分為恐怖主義、仇恨言論、兒童性虐待、商業騙局與詐欺、侵犯智慧財產權等類別，並有各自不同的既有法規規範；後者則將於下一篇進行探討。

### 2. 立新法規為最後手段且限縮範圍

歐盟並非一開始就採取強硬的立法措施，而是從業者自律著手，包括從 2015 年開始展開多方社群溝通對話，之後針對其中的「違法仇恨言論」推動行為準則 (2016 年)，接續再就整個線上「違法內容」提供業者自律的方向性原則 (2017 年)與操作性的建議措施 (2018 年)，並進行多項多方利害關係人的意見蒐集 (2018 年)，直至 2018 年 9 月才正式宣布針對當中有立即性安全威脅的線上「恐怖主義內容」推動新法。

## (六) 參考文獻

- 今周刊 (2018)。假新聞的處罰條文，其實一直都是存在的！  
2018/6/12。  
<https://www.businesstoday.com.tw/article/category/80392/post/201806120016/假新聞的處罰條文，其實一直都是存在的！>
- 張理國 (2018)。學者也反對假新聞立法恐涉選前議題設定。中國時報 2018/10/3。  
<https://www.chinatimes.com/newspapers/20181003000575-260118>
- 蘋果日報 (2018a)。「政府不應單方定義假新聞」政院擬修法打假學者：恐限制新聞自由。2018/9/19。  
<https://tw.appledaily.com/headline/daily/20180919/38129591>
- 蘋果日報 (2018b)。學者陳秉訓：建議修《國安法》正視網路時代變遷。2018/9/18。  
<https://tw.appledaily.com/new/realtime/20180918/1432260/>
- Slow and Insidious Erosion of Fundamental Rights. Just Security.  
<https://www.justsecurity.org/61086/european-counter-terrorism-approaches-slow-insidious-erosion-fundamental-rights/>
- BBC News (2018). Google, Facebook, Twitter face EU fines over extremist posts. BBC News. <https://www.bbc.com/news/technology-45495544>
- EC (2018a). State of the Union 2018: Commission proposes new rules to get terrorist content off the web.  
[http://europa.eu/rapid/press-release\\_IP-18-5561\\_en.htm](http://europa.eu/rapid/press-release_IP-18-5561_en.htm)

- EC (2018b). State of the Union 2018: Commission takes action to get terrorist content off the web - Questions and Answers.  
[http://europa.eu/rapid/press-release\\_MEMO-18-5711\\_en.htm](http://europa.eu/rapid/press-release_MEMO-18-5711_en.htm)
- EC (2018c). Regulation on preventing the dissemination of terrorist content online.  
[https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf)
- EC (2018d). A Europe that protects: Countering terrorist content online.  
[https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-terrorist-content\\_en\\_0.pdf](https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-terrorist-content_en_0.pdf)
- EC (2018e). Illegal Content on Online Platforms.  
<https://ec.europa.eu/digital-single-market/en/illegal-content-online-platforms>
- EC (2018f). Commission Recommendation on measures to effectively tackle illegal content online.  
[http://europa.eu/rapid/press-release\\_MEMO-18-1170\\_en.htm](http://europa.eu/rapid/press-release_MEMO-18-1170_en.htm)
- EC (2018g). Countering illegal hate speech online.  
[http://europa.eu/rapid/press-release\\_MEMO-18-262\\_en.htm](http://europa.eu/rapid/press-release_MEMO-18-262_en.htm)
- EC (2018h). Summary report of the public consultation on measures to further improve the effectiveness of the fight against illegal content online.  
<https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-measures-further-improve-effectiveness-fight-against-illegal>
- EC (2018i). A Europe that Protects: Countering Illegal Content Online.  
<https://ec.europa.eu/digital-single-market/en/news/europe-protects-counterin-g-illegal-content-online>
- EC (n.d.). Type of EU Laws.  
[https://ec.europa.eu/info/law/law-making-process/types-eu-law\\_en](https://ec.europa.eu/info/law/law-making-process/types-eu-law_en)
- Meyer, D. (2018). Here Comes Another EU Law Threatening Google and Facebook With Enormous Fines. Fortune.  
<http://fortune.com/2018/09/12/eu-juncker-terrorist-propaganda-google-facebook/>

- Schechner, S. (2018). Tech Firms Face Prospect of Fines in Europe Over Terror Propaganda. The Wall Street Journal.  
<https://www.wsj.com/articles/eu-backs-fines-for-tech-firms-over-terror-propaganda-1536744963>

## 四、歐盟《處理線上不實訊息之歐洲作法通告》

### (一) 概述

為了因應不實訊息(disinformation)<sup>4</sup>的擴散與衝擊，確保歐洲的價值觀與民主制度，歐盟執委會於 2018 年 4 月 26 日發布《處理線上不實訊息之歐洲作法通告》(Communication -Tackling online disinformation: a European approach)，提出業者自律、支持獨立的事實查核機制、鼓勵優質新聞、宣導媒體識讀等對抗不實訊息散播的措施。

而網路平臺業者與廣告業者亦於 2018 年 9 月 26 日作出正式回應，共同公布完整的自律規範標準—《歐盟不實訊息實踐準則》(EU Code of Practice on Disinformation)，承諾將從政治性廣告的透明度、關閉假帳號等層面，打擊不實訊息的散播。

歐盟《處理線上不實訊息之歐洲作法通告》是歐盟執委會在進行公眾意見徵詢、專家研議等多項多方利害關係人程序後而彙整發布的，並將「不實訊息」定義如下：

為了經濟利益或故意欺騙大眾，而去創造、呈現與散播可查證的虛假或誤導性訊息，並可能造成公共傷害。公共傷害包括對民主政治、決策過程，以及公共事務的威脅。不實訊息不包括錯誤報導，諷刺和模仿調侃，或有明確標

---

<sup>4</sup> 歐盟於 2018 年 4 月以前，以「假新聞」(fake news) 泛稱「不實訊息」問題。本篇對 2 個詞彙的使用，係依據歐盟的原始文件用詞。

識的黨派新聞與評論。

歐盟執委會表示，「假新聞」(fake news)只是整個複雜「不實訊息」的一部分，雖然部分歐盟成員國正在研究推動立法，但是現有的法規尚未涵蓋假新聞與不實訊息，因此，兩者都不構成違法行為。

歐盟執委會並指出，高達 83% 歐洲人認為不實訊息已威脅民主發展。適逢歐洲議會選舉將於 2019 年登場，因此，歐盟提出因應措施，並期許業者的自律準則能有助於在兼顧歐洲自由多元的基本原則下，實現透明、公平、值得信賴的線上活動。然而，如果業者自律的成效不彰，未來仍不排除採取立法監管。

## (二) 政策發展與目標

### 1. 政策發展

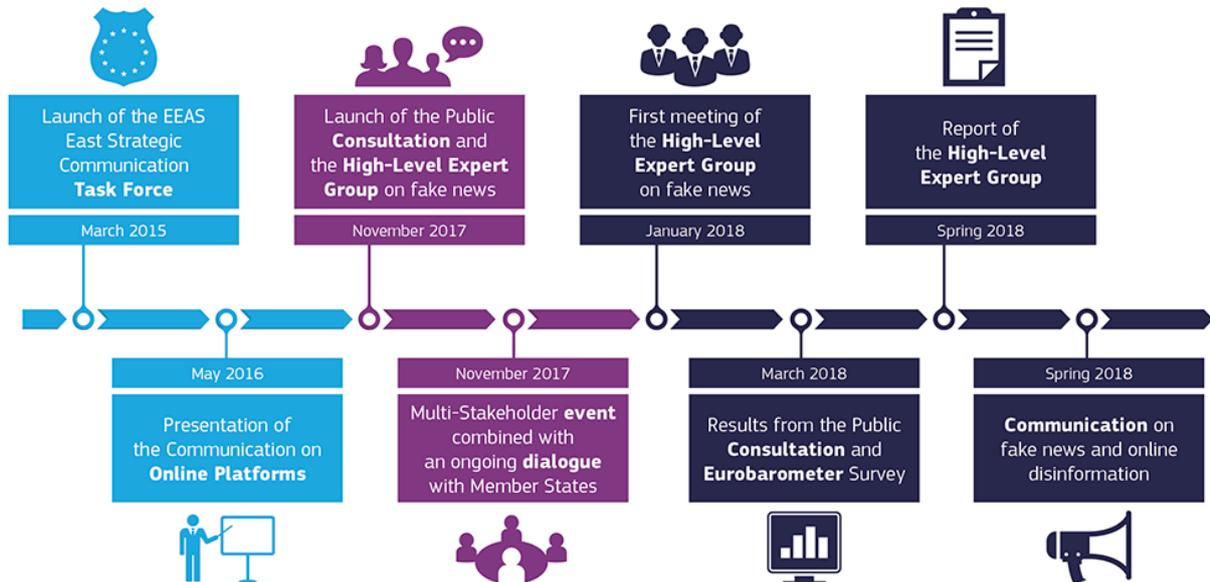
歐盟自 2015 年即開始因應不實訊息的衝擊，其政策發展如圖 25 所示(至 2018 年 4 月)。以下說明近一年來主要的政策發展過程：

- 2017 年 11 月至 2018 年 2 月進行公眾意見徵詢，主要結果如下：
  - 線上問卷調查：共收到 2,986 份回覆問卷，所有人都認為假新聞很可能會對社會造成傷害，尤其是在政治、移民、少數族群、安全方面；且目前社群媒體在協助使用者查核事實方面做得不夠；而因應策略方向應為多方利害關係人、多面向與業者自律，且事實查核與全面性的媒體識讀都是必要的措施；但無論如何，都要確保言論自由等基本權益，且不能直接或間接導致網路審查。
  - 電話訪談：共訪問 2 萬 6 千多位受訪者，83% 認為假新聞會危害民主，85% 表示假新聞在自己國家造成問題，68% 指出每周至少看到一次假新聞。
- 2017 年 11 月 13 日至 14 日舉辦多方利害關係人會議，以確定假新聞

的問題範圍，並評估社群媒體已實施方案的有效性，進而研商進一步行動的核心原則。

- 2018 年 1 月成立高階專家工作小組(High-Level Expert Group, HLEG)，成員來自公民團體、社群媒體、新聞媒體、記者、學者等共 39 位代表，並於 2018 年 3 月 12 日提出對抗假新聞與不實訊息報告，主要內容包括以「不實訊息」而非「假新聞」來描述當前問題，並提供強化網路新聞透明度、推動媒體識讀等多管齊下的政策建議。
- 2018 年 4 月 26 日發布《處理線上不實訊息之歐洲作法通告》，揭示因應不實訊息的原則(如資訊的透明度、多元化等)，以及呼籲業者自律、宣導媒體識讀等行動方案。
- 2018 年 5 月 29 日召開「線上不實訊息多方利害關係人論壇」(Multistakeholder Forum on Disinformation Online)，分成工作小組與意見小組(Sounding Board)。前者由網路平臺業者與廣告業者組成，負責訂定《歐盟不實訊息實踐準則》；後者由事實查核單位、學術界、媒體、公民團體等組成，負責評估準則內容並監督執行狀況。
- 2018 年 9 月 26 日網路平臺業者與廣告業者共同公布完整的自律規範標準《歐盟不實訊息實踐準則》，承諾將從政治性廣告的透明度、關閉假帳號等層面，打擊不實訊息的散播。
- 2018 年 10 月 16 日止，包括 Facebook、Google、Twitter 等業者，以及互動廣告歐洲辦公室(Interactive Advertising Bureau Europe)等商業協會已經簽署自律準則，並各自提出相關工作項目與時程表。

# Tackling Fake News in the EU



資料來源：EC, 2018

圖25. 歐盟處理假新聞與不實訊息的政策發展(至 2018 年 4 月)

## 2. 預期目標

歐盟執委會認為，由於不實訊息的問題複雜且數位環境是快速發展，因此，其因應政策應該是全面的、不斷地評估情勢，並根據演變來調整政策目標，而且不該期望單一方案可以解決所有挑戰，也不能無所作為。據此，歐盟《處理線上不實訊息之歐洲作法通告》訂定下列 4 項總體目標暨原則：

### (1) 透明度

改善資訊的來源、製造、贊助、傳播、鎖定目標族群的透明度，以利民眾評估所看到的線上內容，並揭露操弄輿論的可能意圖。

### (2) 多元化

透過支持優質新聞、媒體素養，以及平衡訊息創造者和散播者的關

係，維持資訊的多元化，以促進公民具有批判性思考進而能做出明智的決策。

### (3) 可信賴

藉由提供誠信標示（尤其是信賴標誌）、改善訊息的可追溯性，以及認證有影響力的訊息提供者，以強化訊息的可信度。

### (4) 全面性

打造全面性的解決方案，有效的長期解決方案有賴認知推廣、更多的媒體識讀，以及政府部門、網路平臺業者、廣告商、查核者、記者、媒體集團的共同合作。

## (三) 實施重點

### 1. 《處理線上不實訊息之歐洲作法通告》

歐盟《處理線上不實訊息之歐洲作法通告》提出的因應措施主要如下：

#### (1) 由業者訂定實踐準則

網路平臺業者應該訂定對抗不實訊息的實踐準則，以確保贊助內容的透明度、說明演算法功能、有助於第三方查核、便於使用者接觸不同觀點的新聞來源、識別並關閉假帳號、處理自動化機器人問題、讓事實查核者與政府單位可以持續追蹤線上不實訊息。

#### (2) 建立獨立的事實查核歐洲網絡 (network)

從歐盟成員國的國際事實查核網絡單位中，挑選恪守其守則者，以建立橫跨整個歐洲的共同作業方法，交流最佳措施，並作最廣泛的事實澄清。

#### (3) 建置對抗不實訊息的歐洲線上平臺

建置橫跨歐盟地區資料存取、蒐集與分析的線上平臺，以支援事實查核者與相關學術研究者的工作。

#### (4) 強化媒體識讀

鼓勵事實查核單位與公民團體組織，提供媒體識讀教材給學校與教師，並舉辦歐盟的媒體識讀週活動，以協助歐洲人能以批判性眼光識別線上內容與不實訊息。

#### (5) 支援歐盟成員國對選舉的因應能力

協助歐盟成員國確保因應選舉的能力，對抗日益複雜的線上不實訊息、網路攻擊等網路威脅。

#### (6) 鼓勵主動建立線上識別系統

鼓勵業者主動建立線上識別系統，以改善訊息提供者的可追溯性和識別性，提升線上訊息內容與來源的信任與可靠性。

#### (7) 支持優質與多元的訊息

歐盟成員國應擴大對優質新聞的支援規模，以確保多元且永續的媒體環境。歐盟執委會並將向新聞媒體徵求提案，以製播歐盟事務的優質新聞。

#### (8) 協調策略性的傳播政策

歐盟執委會將研擬策略性傳播政策，結合歐盟及成員國當前與未來因應不實訊息措施，規劃對抗對歐洲錯誤描述與不實訊息的宣導活動。

## 2. 《歐盟不實訊息實踐準則》(業者自律規範)

《歐盟不實訊息實踐準則》係由主要的網路平臺業者與廣告業者共同訂定，以做為業者自律的標準規範，其內容分為 5 個類別共 15 條承諾。

表11. 《歐盟不實訊息實踐準則》業者承諾事項

類別	承諾條款
安全廣告投放	1. 訂定政策和流程，例如限制廣告服務的範圍或付費展示的位置，並與事實核查組織合作，以阻斷廣告與營利的不實訊息。
政治性與議題性廣告	2. 遵守歐盟與成員國的法律規定，並在簽署的準則中簡述所有廣告應與編輯內容有明確區分。當廣告出現在新聞或編輯內容時，應以容易辨識是否為付費傳播的方式呈現。
	3. 公開披露政治性廣告（係指支持／反對候選人或公投的廣告），包括贊助者的身份與金額。
	4. 制定合理的公開披露「議題廣告」方法，包括定義「議題廣告」，但此定義不含政治討論與政治觀點的報導，以及商業廣告。有鑑於對言論自由的影響，鼓勵簽署者與專業的利害關係人共同探討兼顧實現透明度與維護基本權利的方法。惟相關工作不應干涉廣告自律組織的領域。
誠信的服務	5. 針對與所提供服務有關的身份識別及濫用自動機器人問題，訂定明確的政策，並在歐盟內實施。
	6. 制定不允許使用自動化系統的政策，並在平臺上公開該政策。
賦權消費者	7. 針對能夠幫助民眾在觸及可能錯誤的線上新聞時能做出明確決策的產品、技術與計畫，進行投資，包括與新聞體系合作發展有效的信賴指標。
	8. 針對能夠在搜尋、訂閱，或其他自動播放管道，優先排列出相關、真實且權威訊息的技術，進行投資。
	9. 針對能夠讓民眾更容易找到公共利益主題不同觀點的事物或工具，進行投資。

類別	承諾條款
	10. 與公民團體、政府、教育機構，以及其他利害關係人合作，共同支持推動提升批判性思考與數位媒體識讀。
	11. 鼓勵市場採用有助於消費者了解為什麼會看到特定廣告的工具。
賦權研究社群	12. 支持善意去追蹤並了解不實訊息影響的獨立作業，包括由歐盟執委會促成建立的獨立事實查核網絡。支持方式包括分享受隱私保護的數據、進行聯合研究，或與學術界和公民團體合作。
	13. 不禁止或阻止（外界）對其平臺上的不實訊息與政治廣告進行善意研究。
	14. 鼓勵對不實訊息與政治廣告進行研究。
	15. 召開年度活動，以促進學術界、事實核查社群、價值鏈成員之間的討論。

資料來源：EC, 2018

自願簽署實踐準則的業者與商業協會可就上列 15 條承諾事項，逐一勾選各自承諾要達成的項目，並提供里程碑與時程表，範例如下圖 26 Google 簽署內容的部分截圖所示。之後意見小組（由事實查核單位、學術界、媒體、公民社會等所共同組成）會對簽署者展開為期 12 個月的成效評估。

COMMITMENTS		NEXT STEPS AND MILESTONES TO BE ADDED TO THE BLUEPRINT FOR ACTION		
<b>Scrutiny of ad placements</b>		<b>Date</b>	<b>Milestone</b>	<b>Description</b>
Commitment 1	a. X b. X c. X d. X	26 September 2018	Signing the Code of Practice	The final Code of Practice to be signed by members of the Working Group
		October 2018	Assigning of independent third party organization (TPO) monitor	This organization will review the transparency reports of signatories to assess compliance to the code
<b>Political advertising and issue-based advertising</b>		October 2018	European Commission and multi-stakeholder forum members raise awareness of the CoP to get other signatories to join the CoP	
Commitment 2	X	Autumn 2018	Relevant signatories start to provide programs and/ or products to ensure access to authoritative (EU election-related) content and safety of the elections	
Commitment 3	X	December 2018	TPO submits report reviewing KPIs	As envisioned in the KPIs
Commitment 4	X	December 2018	European Commission publishes progress report	
<b>Integrity of services</b>		Early 2019	Network of independent fact-checking organizations launched and meeting facilitated with signatories to discuss collaboration	The Commission's communication envisions the creation of an independent network of fact-checking organizations
Commitment 5	X	Early 2019	Commission examines TPO report	The Commission will review the TPO report and communicate its views ahead of the May 2019 elections
Commitment 6	X			
<b>Empowering consumers</b>				
Commitment 7	X			
Commitment 8	X			
Commitment 9	X			
Commitment 10	X			
Commitment 11	X			
<b>Empowering the research community</b>				
Commitment 12	X			
Commitment 13	X			
Commitment 14	X			
Commitment 15	X			

資料來源：EC, 2018

圖26. 《歐盟不實訊息實踐準則》簽署範例-- Google

#### (四) 相關爭議

歐洲消費者聯盟(Bureau Européen des Unions de Consommateurs, BEUC)批評歐盟執委會礙於沒有對政治廣告展開正式研究，而採取三心二意的立場；並認為讓平臺業者加入處理問題的作法並不合適，因為他們正是投放挾帶假新聞廣告的獲利者 (Stupp, 2018；BEUC, 2018)。

此外，由歐盟執委會召集的「線上不實訊息多方利害關係人論壇」的意見小組（由事實查核單位、學術界、媒體、公民團體等組成）更是直接抨擊業者自訂的《歐盟不實訊息實踐準則》沒有達到預期的有效性與可課責性，可說「根本不算是自律規範」，因為「它缺乏共通的方法、沒有明

確且有意義的承諾、沒有可量測的目標或 KPIs (關鍵績效指標, Key Performance Indicators)、無法監控過程, 以及沒有遵循或執行的工具」。意見小組也因此要求歐盟執委會與第三方進行審核, 以衡量所謂的實踐準則當中所列的意旨是否被付諸實行, 並評估它是否符合歐盟《處理線上不實訊息之歐洲作法通告》所訂定的目標。

## (五) 小結

本篇介紹歐盟針對現行法規沒有規範的不實訊息 (包括假新聞), 提出《處理線上不實訊息之歐洲作法通告》, 並實施業者自律 (且由業者自訂實踐準則)、強化媒體識讀等多項因應措施。本計畫將歐盟因應的各種線上內容問題及其政策措施, 包括前一篇文章的線上違法內容, 一併彙整成下表 12。

表12. 歐盟因應線上內容問題的類別與政策措施

歐盟因應的線上內容問題	線上違法內容	內容類別	總體因應政策	各別因應政策／措施	說明
	違反歐盟與成員國現有法規	恐怖主義	2017《打擊線上違法內容, 強化線上平臺責任通告》	制定新法	提案《防止散播線上恐怖主義內容法案》
		仇恨言論 (含暴力)		採業者自律並追蹤成效	自 2016 年實施《對抗線上違法仇恨言論行為準則》
		兒童性虐待		目前正評估成效	已有《對抗兒童性虐待指令》; 並有政府支援組織與民間團體推動相關工作
		侵犯智慧財產	2018《有效打擊線上違法內容建議措施》	修改法規	正推動《《著作權指令》》法規改革
		商業詐騙與詐欺		採業者自律	已針對仿冒商品發布相關指南; 多個相關的合作備忘錄
				推動合作方案	已有《不公平商業行為指令》、《消費者權益指令》; 目前正推

歐盟	線上	內容類別	總體因應政策	各別因應政策／措施	說明
					動如消費者保護等合作方案
	線上不實訊息	虛假、誤導性訊息  (不含錯誤報導, 諷刺和模仿調侃, 或有明確標識的黨派新聞與評論)	2018《處理線上不實訊息之歐洲作法通告》	由業者訂定實踐準則	實施促進贊助內容的透明度、識別並關閉假帳號等措施
	現有法規尚無規範			建立獨立的事實查核歐洲網絡	建立歐盟共同作業方式, 交流最佳措施, 並作最廣泛的事實澄清
				強化媒體識讀	鼓勵事實查核單位與公民團體組織, 提供媒體識讀教材給學校, 並舉辦歐盟的媒體識讀週活動
				支持優質與多元訊息	擴大對優質新聞的支援規模、徵求新聞媒體製播歐盟事務的優質新聞
				協調策略性的傳播政策	研擬策略性的傳播政策, 規劃對抗歐洲不實訊息的宣導活動
				其他: 建置對抗不實訊息的歐洲線上平臺; 鼓勵主動建立線上識別系統	建置歐盟地區資料存取、蒐集與分析的線上平臺; 鼓勵業者主動建立可識別與追溯訊息提供者的線上系統

資料來源：本計畫彙整

上表 12 顯示，歐盟首先將網路上的各種問題內容，區分為違反既有法規的線上「違法內容」，以及有問題但不違法的「不實訊息」，然後分別訂定總體因應政策與各別因應措施。因此，本計畫已於上一篇建議我國先界定問題範圍與相關法規。

而針對本篇所探討的不實訊息問題，歐盟在因應政策發展上，有下列 2

個特點：

### 1. 經由多方程序制定總體政策方向

歐盟在經由公眾意見徵詢（線上問卷調查與電話訪談）、多方利害關係人會議討論、專家工作小組政策研議等多項廣泛性與專業性的多方利害關係人程序，並採納相關意見或建議後，才發布《處理線上不實訊息之歐洲作法通告》，確立不實訊息的定義，制定總體政策目標暨原則，並據此提出因應措施。

### 2. 實施多管齊下且長短期兼顧的因應措施

歐盟執委會指出，面對複雜的不實訊息，沒有單一方案可以解決所有問題，因此，於集結多方利害關係人智慧後，提出軟硬兼施（實施業者自律但又不排除立法）、長短期兼顧（如強化媒體識讀、建立獨立事實查核網絡）、涵蓋所有多方利害關係人責任的多管齊下措施。

如上一篇所述，近來我國也準備著手因應網路上的不實訊息／假消息／假新聞等相關問題，目前行政院正在盤點國內相關法規與行政措施，且不排除設立跨部會工作小組（徐政璿，2018），而立法院也已有修法的提案<sup>5</sup>。雖然我國面臨的情境與問題和歐盟有所差異，但是，若能參考上述歐盟相對完整且嚴謹的作法，對於問題的釐清與定義，應能發揮相當助益，進而共同集思廣益，找到最佳的總體政策方向與完整有效的因應措施。

## （六）參考文獻

- 呂文玲（2018）。網路散布假新聞、假消息之法制研析。

<sup>5</sup> 邱志偉等 19 位立委於 107 年 5 月提出「社會秩序維護法第六十三條條文修正草案」請審議案，新增「未經查證在網路散播傳遞假新聞、假消息，足以影響公共之安寧秩序者」，可處 3 日以下拘留或 3 萬元以下罰鍰。葉宜津等 17 位立委於 106 年 10 月提出「國家安全法增訂第二條之二條文草案」請審議案，增訂第 2 條之 2，將網路領域列為國安範疇。

[https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=175893&fbclid=IwAR1\\_FguPmpQm\\_38AyBIHKforFBZMUESXtL1WWFt08XvzZ-nrlfA7s4rLaTc#](https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=175893&fbclid=IwAR1_FguPmpQm_38AyBIHKforFBZMUESXtL1WWFt08XvzZ-nrlfA7s4rLaTc#)

- 胡元輝 (2018)。總統要打假訊息歐盟模式值借鑑。蘋果日報 2018/10/11。 <https://tw.appledaily.com/headline/daily/20181011/38149140/>
- 徐政璿 (2018)。行政院：參考國外經驗 成立跨部會小組防範「假新聞」。東森新聞雲 2018/11/4。 <https://www.ettoday.net/news/20181104/1298071.htm>
- 通傳會 (2018)。公告自即日起受理 107 年度媒體識讀教育研習活動補助申請。 [https://www.ncc.gov.tw/chinese/news\\_detail.aspx?site\\_content\\_sn=566&is\\_history=0&pages=0&sn\\_f=38779](https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=566&is_history=0&pages=0&sn_f=38779)
- BEUC (2018). Disinformation: BEUC and Sounding Board members reject Code of Practice. <https://www.beuc.eu/press-media/news-events/disinformation-beuc-and-sounding-board-members-reject-code-practice>
- EC (2018a). Code of Practice on Disinformation. <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>
- EC (2018b). Statement by Commissioner Gabriel on the Code of Practice on Online Disinformation. [http://europa.eu/rapid/press-release\\_STATEMENT-18-5914\\_en.htm](http://europa.eu/rapid/press-release_STATEMENT-18-5914_en.htm)
- EC (2018c). Roadmaps to implement the Code of Practice on disinformation. <https://ec.europa.eu/digital-single-market/en/news/roadmaps-implement-code-practice-disinformation>
- EC (2018d). Factsheet on Tackling online disinformation. <https://ec.europa.eu/digital-single-market/en/news/factsheet-tackling-online-disinformation>
- EC (2018e). Tackling online disinformation: a European Approach. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>

- EC (2018f). Fake news and online disinformation.  
<https://ec.europa.eu/digital-single-market/en/fake-news-disinformation>
- EC (2018g). EU Code of Practice on Disinformation  
[https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=54454](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454)
- EC (2018h). Synopsis report of the public consultation on fake news and online disinformation.  
<https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-fake-news-and-online-disinformation>
- EC (2018i). Tackling online disinformation: Commission proposes an EU-wide Code of Practice.  
[http://europa.eu/rapid/press-release\\_IP-18-3370\\_en.htm](http://europa.eu/rapid/press-release_IP-18-3370_en.htm)
- Stupp, C. (2018). Commission threatens to legislate on ‘fake news’ ahead of 2019 EU election.  
<https://www.euractiv.com/section/digital/news/commission-threatens-legislation-on-fake-news-ahead-of-2019-eu-election/>
- The Sounding Board (2018). The Sounding Board of the Forum on Disinformation Issues Their Unanimous Final Opinion on the So-called Code of Practice.  
<https://www.euractiv.com/wp-content/uploads/sites/2/2018/09/Joint-Press-Statement-Sounding-Board-Issues-Opinion-on-Code-of-Practice-EMBARGO.pdf>

## 五、歐盟《著作權指令》法案

\*本篇內容特別邀請黃勝雄博士撰文分析

### (一) 概述

歐洲議會於2018年9月12日通過《著作權指令》(Copyright Directive)，當中最重要條文是第11條及13條。第11條屬於出版商與論文提供者新

的獲利模式，當 Google 等網路平臺公司連結到這些具著作權內容時，出版商們可要求付費許可，簡稱連接稅(Link Tax)。第 13 條要求 YouTube 及 Facebook 等網路平臺公司需防止其用戶上傳受著作權保護的內容，簡稱上傳過濾機制(Upload Filter)。這些平臺必須主動與著作權所有權人合作，防止平臺用戶上傳受著作權保護的內容。《著作權指令》仍需經由 2019 年 1 月歐洲議會最終投票完成決議。

## (二) 政策發展與目標

歐盟《著作權指令》目的在於更新網際網路時代的網路版權法規。這一項法案從討論開始到議會初步表決通過，都充滿許多爭議。原本在 2018 年 7 月，由於第 11 條的連接稅與第 13 條的上傳過濾機制，這兩項關鍵條款遭受批評，而被歐洲議會議員拒絕。不過，9 月的歐洲議會中，因為修訂部分內容條款而獲得歐洲議會同意批准，投票結果為 438 票贊成，226 票反對。

雖然《著作權指令》仍然需在 2019 年 1 月由歐洲議會進行最終投票，但是歐盟專家表示，該指令不太可能在最終表決被否決。

《著作權指令》完成最終審議後，再由歐盟各成員國實施，這些成員國在解釋條款內容時，可能有相當落差，導致不同國家在實施政策產生很大差異。

## (三) 實施重點

歐盟《著作權指令》中最重要且最具爭議的條款是第 11 條和第 13 條。第 11 條旨在為出版商提供一種新的營運模式，當 Google 等公司連接到出版商的內容時，允許出版商要求付費許可。第 13 條要求 YouTube 和 Facebook 等網路平臺阻止用戶上傳受著作權保護的內容。

本指令的支持者表示，著作權第 13 條不會被濫用，並且會提供豁免權

給如 GitHub (開放原始碼軟體平臺)或維基百科等網站。但是，反對者認為這些規定是災難性的，就第 11 條而言，這個設計在 Google 新聞等共享文章平臺已經嘗試多次並且一再失敗，更可能導致著作權業者的濫用。

多年來，出版業者一直在免費贈送他們試圖保護的內容。事實證明他們推動的方向錯誤，他們將大量的網路觀眾推向平臺業者，產出利潤豐厚的廣告收入。出版業者嘗試實施訂閱制度也遇到了困難。例如，英國媒體太陽報在 2013 年推出付費專區，但僅幾年就放棄了訂閱制的想法。網路新聞的模糊商業模式使出版業者的案例變得複雜。

沒有明確資料說明歐洲議會的著作權提案將對出版業者帶來多少收入。歐洲議會的委員會宣稱，德國出版業者估計其網路收入將增長 10%。雖然這不能算是微不足道，但是反對者指出，這個數字仍不足以拯救這個產業。幾十年來，出版商的商業模式依賴於將資訊匯集到單一來源。例如報紙是一站式商店，不僅用於時事與分析，還用於電影列表及房地產、汽車和工作的分類廣告。隨著 eBay 和 Google 等網路競爭媒體出現後，出版業者已失去大部分廣告市場。

《著作權指令》第 13 條受到批評者嚴厲指責。該條文要求網路平臺主動與著作權所有權人 (rightsholders) 合作，阻止用戶上傳受製作權保護的內容。要滿足第 13 條法令要求的唯一方法，就是 YouTube 或 Facebook 等網路平臺服務提供者必須將所有使用者上傳到網路平臺的資料，完整掃描編碼建立內容資料庫。這項作法將為小型平臺服務提供者產生難以置信的沉重負擔。而內容過濾技術可能還會被作為廣泛的內容審查機制，這也是維基百科 (Wikipedia) 創辦人 Jimmy Wales 和全球資訊網(World Wide Web) 發明者 Tim Berners Lee 強烈反對此條款的主要原因。

長期使用網際網路的人對《著作權指令》第 13 條的措施可能並不陌生。第 13 條的預期方法與 YouTube Content ID 作業模式相當類似，只是將 Content ID 模式複製並且擴散到全球網際網路。歐洲議會成員 Axel Voss 在

《著作權指令》中具有主導作用，他表示該指令條款內容未提到網路過濾器，條款內容只表示「使用可行技術」來防止具著作權內容被侵權問題。《著作權指令》最新修訂版本包含網路百科全書等網站豁免權，但 Axel Voss 表示無法預測哪些網路平臺會受到此法案的影響。

《著作權指令》的支持者表示，目前反對指令的說法都是美國大型科技公司肆無忌憚的因素造成，大型科技公司急於控制網路平臺，而現行法律和指令的修正好可作為證據，《著作權指令》不會被大型業者濫用，包括指令第 13 條提供 GitHub 和維基百科等網站的豁免權，以及僅是超連結或不受約束文章的分享，都是許可範圍。

儘管存在這些分歧，但顯然的，如果《著作權指令》在 2019 年 1 月獲得歐洲議會的最終批准，它將對歐盟和世界各地的網路產生巨大的顛覆性影響。《著作權指令》在歐盟各不同國家究竟如何被詮釋與落實尚未可知，但權力的平衡與轉變是明確的方向，就是網路大型科技公司正逐漸失去對網際網路的控制權。

#### (四) 相關爭議

德國報紙出版商協會主席 Mathias Döpfner 曾表示：「如果不能確保智慧財產權受到保護，代表出版商對數位轉換的未來沒有任何看法。任何不這樣說的人，若不是說謊就是為了分散注意力」。在出版商強烈要求網路平臺對保護著作權內容負有責任的氛圍下，歐洲議會通過了相當具爭議的《著作權指令》。

《著作權指令》第 13 條要求網路平臺提供者使用可行的技術措施，防止違反著作權的內容上傳到網路上。YouTube Content ID 管理機制就被外界視為本條文所呈現的「可行技術」。然而 YouTube Content ID 內容管理機制曾發生許多具有爭議的案例。有一位使用者錄製一段早晨包含鳥鳴的影像上傳到 YouTube，但是從 YouTube 播放時發現背景的鳥鳴聲消失了，

經過向 YouTube 公司反應，YouTube 比對 Content ID 發現背景鳥鳴聲與 Rumblefish 公司鳥鳴聲內容著作權的 Content ID 相同，因此演算法自動將鳥鳴聲刪除。在 YouTube 平臺內容曾發生許多類似案例。YouTube Content ID 管理因此受到許多人權團體批評，認為這是 YouTube 自動監視與控制用戶的審查工具。因此，所謂的技術可行措施自然會讓許多人有相同疑慮。

《著作權指令》第 13 條對小型平臺提供者是很大挑戰，如果小型平臺提供者必須配合實施內容上傳自動過濾技術，那麼不僅小型業者須負擔沉重的營運成本，而且還可能做得非常糟糕讓服務不堪使用。強制要求平臺業者建構內容過濾技術，等於鼓勵小型業者盡可能地過濾掉任何可能的內容，因為業者沒有任何誘因讓可能無辜內容通過過濾機制篩選。

美國 FOSTA 停止性交易法案(全名為《允許各州及受害者對抗非法網路性交易法案》，Allow States and Victims to Fight Online Sex Trafficking Act)就是這種情境的案例。FOSTA 法案原意在打擊網路性交易，法案增加平臺業者管理性交易內容的義務。但是當法案通過後，知名的雲端服務提供者 Cloudflare 立即停止提供 Switter 網站網路服務，然而 Switter 其實是一個性工作者友善的網站而非性交易網站。因為管制措施使網路服務提供者沒有誘因讓可能無辜的內容通過過濾而去冒犯違法風險。

## (五) 小結

近年來，基於網路管理的理由，國家政府對網路內容或資訊進行過濾或篩選的做法，日益普遍。網路中介者 (Intermediary)<sup>6</sup> 對於網路內容提供者及閱讀者應承擔的責任，也逐漸引發各領域的討論。

網際網路發展多年以來，網路中介者維持網路自由開放精神，以中立角色提供服務。馬尼拉原則 (Manila Principles) 即是由全球多家網路中介

---

<sup>6</sup> 包括網路服務提供者 ISP (Internet Service Provider)、網路內容提供者 ICP (Internet Content Provider)、或搜尋引擎業者(Search Engine)。

者共同合作訂定的網路自律規範，其重點包含網路中介者應避免對第三方內容承擔責任；沒有司法機關命令，不得對內容進行限制；內容限制請求必須清晰明確，並且依照正當程序；法律、內容限制命令與實務作法必須通過必要性比例原則的檢驗；法律、內容限制政策與實務作法必須遵循正當程序；透明度與問責機制必須建立在法律、內容限制政策和實務作法中。

在網際網路朝大眾傳播媒介模式發展的趨勢下，網路中介者的重要性也日益增加。網路中介者基於技術演進與網路使用環境發展使然，逐漸介入網路內容過濾。例如執行垃圾郵件過濾、實施惡意軟體過濾等，這些非惡意內容管制或許可能視為合乎公眾期望的介入措施。但網路使用者不免關心網路中介者是否可能進一步介入內容傳輸順序，甚至影響言論自由。確保網路使用者不需經由網路中介者同意，隨時能與不特定的大眾直接溝通，是健全網路發展的首要目標。

網路空間裡的終端使用者受我國憲法言論自由保障。網路使用者的言論自由和資訊取得自由應受到保障，同時也應保障網路中介者一定程度的編輯裁量權。即便擁有市場主導力量的中介者可能成為私人審查的危險，也不因此管制中介者所應具備的編輯裁量權。

網路中介者可以發揮協助使用者選擇其感興趣的資訊內容，不同的網路中介者在資訊編輯立場上可能有所不同，基於不同立場所實施的過濾與箝制才是公眾應關注的焦點。編輯裁量權在新聞自由領域被視為媒體言論自由保護底線的原則之一，掌握編輯裁量權的網路中介者可以有效促進網路使用者存取其想取得資訊內容的能力，或阻絕不想看到的內容。美國聯邦最高法院指出，政府不應偏好特定類型言論，這也是網路中立性原則的基本要求。

歐洲議會通過的《著作權指令》以第 11 條的連接稅制度，與第 13 條的上傳過濾機制，最為關鍵。這 2 項條款對臺灣的影響分析與建議如下：

### (1) 第 11 條對臺灣影響有限

《著作權指令》第 11 條的连接稅，雖然看似對出版商有益，但是，目前尚未出現成功的商業模式，這樣的成效值得商榷，而且對臺灣的出版業者、著作權所有權人，或閱讀者，影響程度都是有限。

### (2) 第 13 條不利臺灣網路業者，內需市場者可未來再導入可行技術

針對《著作權指令》第 13 條的上傳過濾機制，由於目前國際大型網路平臺多已建置相關機制，如 YouTube 的 Content ID 系統已經使用類似做法，可以某種程度保護著作權所有權人，因此，短期內對於網際網路市場的影響不大。不過，臺灣網路業者多為中小型業者，要導入上傳過濾機制的建置成本與營運成本都相當高，其結果可能是著作權所有權人尚未獲益，網路業者先蒙其害。同樣地，這些合規要求對網路新創公司也會造成營運成本增加。因此，臺灣的中小型或新創網路業者，如果目標市場是在內國內，可以待市場成長後，再逐步導入經濟可行的技術。

### (3) 歐盟《著作權指令》可能不易落實，凸顯政策規劃須兼顧各方權益

在法規設計構面，歐盟《著作權指令》飽受網路社群的質疑與批評，政策規劃者除了考量保護著作權所有權人的權益外，也需評估保障私有權利所投入的公共成本，並且必須兼顧閱讀者權益。即使如歐盟這樣的先進社會，本法案並不易取得全體利害關係人的共識，未來可能面臨各會員國不易落實的情境，值得作為臺灣著作權相關法規設計時的借鏡與參考。

## (六) 參考文獻

- 劉靜怡 (2011)。網路內容管制與言論自由。月旦法學雜誌 192 期。頁 63-80
- Vincent, J. (2018). EU approves Controversial Copyright Directive. The Verge. From <https://www.theverge.com/2018/9/12/17849868/eu-internet-copyright-refor>

m-article-11-13-approved?fbclid=IwAR17nDwo92BABoH7qtPBNHp8uVzAolDiUXFA0WfYG9Rr\_brqTPCx8zVjQ1s

- Manila Principle. (n.d.). manilaprinciples.org. From <https://www.manilaprinciples.org/zh-hant>
- Messieh, N. (2012). A copyright claim on chirping birds highlights the flaws of YouTube's automated system. The Next Web. From <https://thenextweb.com/google/2012/02/27/a-copyright-claim-on-chirping-birds-highlights-the-flaws-of-youtubes-automated-system/>
- Politico. (n.d.). Plan to make Google pay for news hits rocks. From <https://www.politico.eu/article/plan-to-make-google-pay-for-news-hits-rocks-copyright-reform-european-commission/>

## 六、法國與歐盟爭取全球網路治理領導角色

### (一) 概述

法國總統馬克宏 (Emmanuel Macron) 於 2018 年 11 月 12 日在第 13 屆聯合國 IGF 開幕演說時，呼籲以創新思維，建立一個加州式與中國式以外的網路治理模式，一個包含所有利害關係人在內的新形態多邊合作。他並率先提出《巴黎籲請信任與安全的網路空間》(Paris Call for Trust and Security in Cyberspace) 倡議，以及法國政府將派遣團隊進駐 Facebook 共同打擊仇恨言論的創舉。因此，也被媒體解讀為試圖在網路空間扮演核心領導角色。

歐盟執委會與歐洲議會也在 14 日的 IGF 發表聯合聲明，指出歐盟大力支持多方模式的網路治理，並將扮演帶領網路治理論述與強化 IGF 的角色。

### (二) 政策發展與目標

#### 1. 法國推動新治理模式

法國總統馬克宏於 IGF 的開幕演說指出當前網路正遭逢三個嚴重且迫切的威脅，而且我們也對網路抱持錯誤的預設。所謂的威脅包括來自國家策劃與犯罪意圖的攻擊；極端分子與獨裁政權散播仇恨、恐怖主義、顛覆民主的言論；以及網路平臺巨擘為其利益讓使用者觸及偏頗內容。錯誤的預設則是指我們誤以為網路只能有下列 2 種模式存在：

- 加州式的網路：由強大的全球私人企業主導網路發展，(政府)沒有規範，完全由業者自主管理。
- 中國式的網路：由強大的獨裁政權完全監控，並驅動創新，是一種霸權。

面對這些情勢，馬克宏強調，正確地規範網路已經刻不容緩，我們需要以創新思維打造一個政府、網路業者、公民團體與所有利害關係人能夠適當進行規範的新途徑，以及包含所有利害關係人在內的新形態多邊合作，以建立一個自由、開放、安全的網路空間，否則將有動搖民主基石的風險。

馬克宏並拋磚引玉，提出下列國際新倡議，以及法國政府新創舉：

- 《巴黎籲請信任與安全的網路空間》倡議：呼籲所有人共同合作對抗線上惡意活動、技術與行為，強化網路的信任與安全。目前已有超過 370 個機構簽署倡議，當中 50 多個為國家政府，其餘為民間企業、工商組織、公民團體、學校等單位。
- 法國政府將進駐 Facebook 共同打擊仇恨言論：法國政府將於 2019 年上半年派遣官方團隊進駐 Facebook，雙方共同發展對抗挑釁與仇恨言論的具體措施，以確保主要平臺業者為其網站上的第三方內容實施高品質的管理規則。

此外，馬克宏也表示，IGF 不能淪為一個只是辯論與思考的會議，而是需要改革成為能夠產出具體建議的地方，因此，繼 2017 年瑞士 IGF 首度提

供（主場次）重點結論後，2018 年巴黎 IGF 與 2019 年柏林 IGF 也會持續推動 IGF 改革。

其實馬克宏於 2018 年 5 月的一場演說上，就提出有別於美國與中國大陸的管理科技公司的「**第三種方式--歐洲模式**」。他認為，歐洲在法規上有其地位，不只是 GDPR 隱私議題，而且還有課稅、網路霸凌、保護獨立工作者等方面。而當務之急即是如何建立「**調合創新與公共利益的歐洲模式**」（Dillet, 2018）。此外，馬克宏也正在歐盟推動課徵數位稅等網路法規。

美國網路媒體 VentureBeat 分析指出，法國展現強大且令人驚訝的倡議。隨著國際地緣政治局面不斷變化，法國正在尋求重新回到國際舞臺的中心位置，並試圖在解決當前混亂的網路空間方面，扮演核心領導角色。

## 2. 歐盟引領多方模式發展

歐盟執委會與歐洲議會於 2018 IGF 聯合聲明中指出，此次 IGF 會議適逢和紀念第一次世界大戰停戰一百周年的「巴黎和平論壇」幾乎同時登場，凸顯和平、安全、穩定的訴求，也必須包含數位領域。然而，當前網路已出現極端化、分裂，以及違背多方原則的新情勢，且民主程序與機構正因為不實訊息的散播、藉由社群媒體活動干擾選舉等因素，而飽受威脅，顯示平臺業者於預防濫用的角色、確保使用者能掌控自己的資料，以及全球合作共同對抗網路威脅，將是未來幾年的迫切挑戰。

為此，歐盟執委會與歐洲議會認為，我們需要更強大有效的網路治理，而歐盟所大力支持的網路治理，是採取多方模式，並且以 IGF 作為討論平臺。不過，IGF 也必須被賦權，讓它不只是個討論新興議題的平臺，而且也能尋求共通原則與政策標準。

歐盟執委會與歐洲議會強調，帶領網路治理論述與強化 IGF 功能是歐洲責無旁貸的責任與義務。2017 年 IGF 提供的日內瓦公報(Geneva Messages, 為主場次的重點結論) 已經跨出第一步，相信 IGF 在歐盟國家連

續 3 年的主辦下，將會有進一步發展。

### (三) 實施重點

#### 1. 法國推動新治理模式

馬克宏對於他所謂的「歐洲模式」著墨不多，目前只強調是一種「調合創新與公共利益」的模式，是一種既非美國的無為而治，也不是中國大陸嚴格管控的模式。因此，以下僅介紹他所提出的新倡議與新創舉。

##### (1) 《巴黎籲請信任與安全的網路空間》倡議

《巴黎籲請信任與安全的網路空間》倡議為一份呼籲大家共同承擔責任，改善網路空間信任、安全與穩定的宣言，並藉由強化多方利害關係人取向、廣泛合作等方式，承諾達到下列 9 個目標：

- 強化對惡意線上活動的預防與復原
- 保護網路的可連接性與完整性
- 共同合作以防止選舉過程遭受干擾
- 共同打擊線上盜版侵權
- 防止線上惡意程式與技術的擴散
- 改善數位產品與服務的安全性
- 強化所有人的網路衛生 (cyber hygiene)
- 打擊非官方組織發動的線上傭兵活動與攻擊行為
- 共同合作以強化相關的國際標準

目前已有超過 370 個單位簽署這項倡議，包括 50 多個國家政府，以及微軟、Google、Facebook、Intel、三星、富士等 200 多家民營企業，以及近

百個工商組織、公民團體、大學等單位。不過，網路科技強國的美、中、俄等國並沒有簽署。

簽署者並同意於 2019 年的巴黎和平論壇與柏林 IGF 集會，以追蹤相關成效與進展。

## (2) 法國政府將進駐 Facebook 共同打擊仇恨言論

法國政府和 Facebook 達成協議，將於 2019 年上半年派遣團隊進駐 Facebook，以探究其對抗仇恨言論的內容政策、管理措施、處理流程等細節（例如如何進行標註、如何識別／決定／移除有問題的內容、自動化工具的演算法是否公正等），進而共同發展具體措施，遏止網路上仇恨、挑釁、歧視等不當內容的散播。

根據雙方協議內容，法國政府的進駐時間為 6 個月，期間內 Facebook 將授權這些官員可以取得相關的內部政策與工具。Facebook 表示，這是共同管理公共科技的新模式。法國總統馬克宏也重申，我們需要有中美兩國以外，規範科技的第三種方式 (Dillet, 2018b)。

## 2. 歐盟引領多方模式發展

歐盟執委會與歐洲議會認為，歐盟國家從 2017 年起連續 3 年主辦 IGF，將會為網路治理帶來進一步發展。例如 2017 年由瑞士政府主辦的 IGF，首度於會後發布日內瓦公報，提供 2 個高階主題場次與 6 個主場次的重點結論，已經跨出改善 IGF 的第一步；而 2018 年會後所發布的巴黎公報，更是動員超過百位學生志工，以及許多法國多方社群，將 2 個高階主題場次、8 個主場次，以及 71 個座談討論，彙整成 8 個主題的重點結論，作為本次會議的「非約束性原則」；相信 2019 年的柏林會議將有更具體產出。

其實歐洲新聞媒體 Politico Europe 於 2017 年已報導，歐盟的網路規範已經從隱私保護拓展到網路內容、反壟斷、向課稅等層面。而在當前美國退出全球領導地位的局勢下，許多國家會追隨歐盟的帶領 (Scott, 2017)。

## (四) 相關爭議

### 1. 《巴黎籲請信任與安全的網路空間》倡議

對於法國總統馬克宏提出這項倡議，微軟總裁史密斯 (Brad Smith) 表示，資訊科技已被用來威脅民主，而民主社會需要提出因應，因此，他讚賞馬克宏的領導能力，並認為獲得廣大支持的巴黎倡議是邁向數位和平的重要一步。

不過，由於網路科技強國的美、中、俄，以及發動網路攻擊的主要國家中國大陸、伊朗與北韓都沒有簽署這項倡議；加上倡議內容沒有從法律層面要求履行任何原則，而且對於違反承諾者也沒有任何罰則，因此，此倡議也被視為只是「象徵網路空間需要外交與合作」或是「無法發揮作用的公關噱頭」(Matsakis, 2018；Cimpanu, 2018)。

### 2. 法國政府將進駐 Facebook 共同打擊仇恨言論

儘管法國總統馬克宏形容這是政府與企業攜手合作對抗仇恨言論的全球實驗性創舉，不過，美國的社會主義平等黨透過自家的世界社會主義網站 (World Socialist Web Site, WSWS)，抨擊馬克宏其實是在實施網路審查計畫，且真正的審查目標並不是外國的極權主義或仇恨言論，而是法國國內的政治反對派。WSWS 還指出，自從 Facebook 與 Google 於 2017 年開始實施大規模的網路審查以來，整個歐洲和美國都一樣，皆是將矛頭對準政治反對者，都是在破壞言論自由與民主權利 (Lantier, 2018)。

## (五) 小結

本篇介紹法國總統馬克宏提倡美 (加州)、中兩國以外的第三種網路治理模式，也就是「調合創新與公共利益的歐洲模式」。他並拋磚引玉提出《巴黎籲請信任與安全的網路空間》新倡議，以及法國政府將派遣團隊進

駐 Facebook 共同打擊仇恨言論的新創舉；而歐盟也發表聲明，表示強力支持多方模式的網路治理，並要扮演帶領論述的角色。

我國《數位通訊傳播法》草案亦強調多方利害關係人參與。面對全球網路治理取向（方式）的發展變動，本計畫建議如下：

- 密切關注歐美多方模式發展，找出我國最合宜的多方模式

美國與歐盟都是以多方取向（方式）來治理網路。長期以來，網路的發展因為網路源自美國的歷史性因素而由美國主導，並向全球灌輸「網路有其特殊地位，不能以國家通訊傳播與貿易政策加以管理」概念，而這也符合美國的政治與經濟利益 (Huston, 2018)。不過，隨著網路發展成為攸關國家競爭力的關鍵、美國退出國際網路治理領導角色、網路遭到各種勢力的濫用等演變，歐盟轉向對網路空間祭出越來越多的管制措施，如同馬克宏所稱，歐洲模式是要「調合創新與公共利益」。然而，不論是美國或歐盟模式，他們的主張不一定符合我國的利益或處境。因此，我國應該密切關注歐美多方模式的變動，並透過國內多方社群討論，找出對我國最合宜的多方模式。

## (六) 參考文獻

- 大紀元 (2018)。【新聞看點】矽谷高管缺席 互聯網大會降級。2018/11/9。 <http://www.epochtimes.com/b5/18/11/8/n10839388.htm>
- 法廣 (2017)。第四屆世界互聯網大會在烏鎮召開 中國輸出網絡監控模式引發擔憂。2017/12/3。 [trad.cn.rfi.fr/中國/20171203-第四屆世界互聯網大會在烏鎮召開-中國輸出網絡監控模式引發擔憂](http://trad.cn.rfi.fr/中國/20171203-第四屆世界互聯網大會在烏鎮召開-中國輸出網絡監控模式引發擔憂)
- 法廣(2018)。烏鎮互聯網大會與中國對網絡自由的威脅。2018/11/7。 [trad.cn.rfi.fr/中國/20181107-烏鎮互聯網大會與中國對網絡自由的威脅](http://trad.cn.rfi.fr/中國/20181107-烏鎮互聯網大會與中國對網絡自由的威脅)
- 陳曉莉 (2018)。超過千名 Google 員工連署抗議傳聞中的中國過濾版搜尋引擎。iThome, 2018/8/17。 <https://www.ithome.com.tw/news/125316>

- 新唐人電視臺 (2018)。【禁聞】世界互聯網大會 矽谷高管為何集體缺席。2018/11/22。 <http://ca.ntdtv.com/xtr/b5/2018/11/10/a1398766.html>
- 新華網 (2015)。習近平在第二屆世界互聯網大會開幕式上的講話（全文）。2015/12/16。  
[http://www.xinhuanet.com/politics/2015-12/16/c\\_1117481089.htm](http://www.xinhuanet.com/politics/2015-12/16/c_1117481089.htm)
- 新華網 (2018a)。習近平向第五屆世界互聯網大會致賀信。新華網，2018/11/7。  
[http://www.wicwuzhen.cn/web18/news/mtbd/201811/t20181107\\_8683498.shtml](http://www.wicwuzhen.cn/web18/news/mtbd/201811/t20181107_8683498.shtml)
- 新華網 (2018b)。第五屆世界互聯網大會開幕 黃坤明宣讀習近平主席賀信並發表主旨演講。2018/11/7。  
[http://big5.xinhuanet.com/gate/big5/www.xinhuanet.com/politics/leaders/2018-11/07/c\\_1123677318.htm](http://big5.xinhuanet.com/gate/big5/www.xinhuanet.com/politics/leaders/2018-11/07/c_1123677318.htm)
- 賈開(2016) 網際網路全球治理的中國方案。學習時報 2016.10.14。  
[http://big5.qstheory.cn/gate/big5/www.qstheory.cn/international/2016-10/14/c\\_1119717403.htm](http://big5.qstheory.cn/gate/big5/www.qstheory.cn/international/2016-10/14/c_1119717403.htm)
- Cadell, C. (2018). China's Xi calls for global cooperation to create 'fairer' internet. Reuters, 2018/11/7.  
<https://www.reuters.com/article/us-china-cyber/chinas-xi-calls-for-global-cooperation-to-create-fairer-internet-idUSKCN1NC0CG>
- Cimpanu, C. (2018). US, Russia, China don't sign Macron's cyber pact. ZDNet, 2018/11/12.  
<https://www.zdnet.com/article/us-russia-china-dont-sign-macrons-cyber-pact/>
- Clover, C. (2016). Xi Jinping pushes China's vision for the worldwide web. Financial Times, 2016/11/16.  
<https://www.ft.com/content/482bcfd0-abd0-11e6-9cb3-bb8207902122?mhq5j=e1>
- Dillet, R. (2018a). Macron defends the European way of tech regulation. TechCrunch, 2018/5/24.

<https://techcrunch.com/2018/05/24/macron-defends-the-european-way-of-tech-regulation/>

- Dillet, R. (2018b). Facebook to let French regulators investigate on moderation processes. TechCrunch, 2018/11/12.  
<https://techcrunch.com/2018/11/12/facebook-to-let-french-regulators-investigate-on-moderation-processes/>
- EC (2018). Internet Governance Forum 2018: Joint Declaration from European Commissioner Mariya Gabriel and Members of the European Parliament.  
<https://ec.europa.eu/digital-single-market/en/news/internet-governance-forum-2018-joint-declaration-european-commissioner-mariya-gabriel-and>
- France Diplomatie (2018). Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace.  
<https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in>
- Freedom House (2018). The Rise of Digital Authoritarianism: Fake news, data collection and the challenge to democracy.  
<https://freedomhouse.org/article/rise-digital-authoritarianism-fake-news-data-collection-and-challenge-democracy>
- Gan, N. (2018). China reasserts its right to manage the internet its own way. South China Morning Post, 2018/11/8.  
<https://www.scmp.com/news/china/politics/article/2172045/chinas-top-leaders-absent-internet-conference-draws-less>
- Huston, G. (2018). Has Internet Governance Become Irrelevant? CircleID, 2018/10/28.  
[http://www.circleid.com/posts/20181026\\_has\\_internet\\_governance\\_become\\_irrelevant/](http://www.circleid.com/posts/20181026_has_internet_governance_become_irrelevant/)
- IGF (2018). IGF 2018 Speech by French President Emmanuel Macron.  
<https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-frenc>

h-president-emmanuel-macron

- Lantier , A. (2018). Macron and Facebook announce joint social media censorship plan in France. WSWS, 2018/11/14.  
<https://www.wsws.org/en/articles/2018/11/14/macron14.html>
- Matsakis, L. (2018). The US sits out an international cybersecurity agreement. Wired, 2018/11/12.  
<https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/>
- O'brien, C. (2018). France leads effort to save internet from itself with 'Paris Call' and Facebook embed. VentureBeat, 2018/11/13.  
<https://venturebeat.com/2018/11/13/france-leads-effort-to-save-internet-from-itself-with-paris-call-and-facebook-embed/>
- Paulson, H. M. (2018). Remarks by Henry M. Paulson, Jr., on the United States and China at a Crossroads.  
[http://www.paulsoninstitute.org/news/2018/11/06/statement-by-henry-m-paulson-jr-on-the-united-states-and-china-at-a-crossroads/?mod=article\\_inline](http://www.paulsoninstitute.org/news/2018/11/06/statement-by-henry-m-paulson-jr-on-the-united-states-and-china-at-a-crossroads/?mod=article_inline)
- Politico (2018). Emmanuel Macron's 'arms control' deal for cyber warfare.  
<https://www.politico.eu/article/macron-unites-europe-business-to-fight-cyber-foes/>
- Scott, M. (2017b) Europe's tech ambition: To be the world's digital policeman. POLITICO, 2017/8/20.  
<https://www.politico.eu/article/europe-tech-ambition-to-be-world-digital-policeman/>

## 七、美國商務部公開徵詢國際網路政策優先議題

### (一) 概述

美國商務部的國家電信暨資訊管理局(National Telecommunications and

Information Administration, NTIA) 於 2018 年 6 月 4 日至 7 月 17 日，向所有利害關係人公開徵詢對「未來國際網路政策優先議題」的意見和建議，以作為 NTIA 後續的施政重點。

NTIA 表示，由於網際網路和數位通訊對美國的創新產業、社會發展、教育、公民和文化生活有重大影響，因此，他們將鼓勵網路及相關經濟的發展與創新，列為最優先的施政要項，並據此進行這一次的政策公開徵詢，詢問有關資訊自由流通與管轄權、多方利害關係人取向(方式)的網路治理、隱私與安全，以及新興科技與趨勢，共 4 大類 23 個問題，最後收到 91 件來自多方社群與個人的回覆意見。

## (二) 政策發展與目標

### 1. 政策發展

NTIA 指出，由於電信與資訊攸關一個國家的公共福利、國家安全與國際競爭力，為了維持有效的相關國家政策，近年來他們將網路通訊的發展與創新視為基礎任務。另一方面，川普政府在 2017 年國家安全戰略 (2017 National Security Strategy) 亦強調，資訊的開放流通及網路的互通互連，與美國經濟的繁榮息息相關，美國提倡公開且互通的通訊，降低全球資訊與服務的交流障礙。爰此，NTIA 向美國各界廣徵對國際網路政策的意見。

NTIA 並進一步說明此次徵詢以下 4 大類問題的原由。

#### (1) 資訊自由流通與管轄權

NTIA 表示，資訊的自由流通攸關網路言論自由與全球經濟的持續成長。然而，有些國家以看似合法的理由 (如保護隱私、徵稅、執法需求) 限制資訊的流通，此舉已傷害基本人權，並危及網路所提供的社會經濟與教育機會。另外，越來越多國家的法院做出迫使美國公司移除全球線上資訊的判決，但是，在某個國家所審查的資訊可能是另一個國家要保護的言

論，此類管轄權爭議凸顯無國界的網路和國家主權之間產生的緊張局勢。

## (2) 多方利害關係人取向 (方式) 的網路治理

NTIA 提倡以多方利害關係人取向 (方式) 來治理網路與發展政策，並支持 ICANN、IETF (Internet Engineer Taskforce, 網際網路工程任務小組)、RIRs (Regional Internet Registries, 區域網際網路註冊機構) 等採用多方取向 (方式) 的組織。NTIA 還以身作則，以多方取向(方式)將全球 DNS 的管理民營化，於 2016 年 10 月完成 IANA (網路號碼指派機構, Internet Assigned Numbers Authority) 監管權移交給 ICANN。此外，NTIA 自聯合國 IGF 成立以來，即積極參與這個全球性，且由多方社群訂定議程的網路公共政策對話平臺。

## (3) 隱私與網路安全

NTIA 認為網路安全風險會威脅國家安全，及經濟成長與創新。面對這個全球性的問題，必須透過國際協調加以因應，所以，NTIA 在 OECD (經濟合作暨發展組織, Organization for Economic Cooperation and Development)、APEC (亞太經合會)、IGF 等場合，提倡由業界主導的資訊安全風險管理措施。至於隱私與資料保護，NTIA 主張各國保護民眾隱私的不同作法不應妨礙全球商務發展，並因此與聯邦貿易委員會 (FTC) 等相關部會共同推動可通用的隱私制度與機制，例如 APEC 「跨境隱私保護規則體系」(Cross Border Privacy Rules System, CBPR System)，以及歐盟-美國隱私盾協議 (E.U.-U.S. Privacy Shield Arrangement)。

## (4) 新興科技和趨勢

NTIA 提倡能幫助企業家與創新者在全球市場開發新數位產品與服務的政策，也因此時常需要商討網路寬頻接取服務、數位素養、智財權和技術標準等議題，這些也是近十年來國際上熱烈討論的議題。而未來幾年的焦點將在於人工智慧對社會與經濟的衝擊、自動化與網路新商業模式對勞動市場的改變，以及區塊鏈應用的快速成長。

## 2. 政策目標

NTIA 透過此次公開徵詢，向有興趣的利害關係人，包含私人企業、技術社群、學術界、政府單位、公民團體和個人，徵求國際網路政策的相關意見和建議，所收到的回覆有助於美國政府找出全球網路領域中最重要的議題，以利 NTIA 有效地運用其資源與專業，優先處理這些議題。

### (三) 徵詢問題與回覆

#### 1. 徵詢問題

NTIA 所徵詢的 4 大類 23 個問題，詳如下表 13 所示。

表13. 美國 NTIA 徵詢國際網路政策優先議題之題目

類別	子題
資訊自由 流通與管 轄權	1. 網路資訊自由流通的挑戰有哪些？
	2. 哪些國外法律和政策限制了網路資訊的自由流通？對美國企業和一般使用者的影響是甚麼？
	3. 其他國家是否曾作出將國家法律援用於全球網路的相關判決？其對美國企業的實際影響為何？對使用者的影響又是甚麼？
	4. 網路言論自由的挑戰有哪些？
	5. 為了保護網路言論自由，全球所有利害關係人，包括政府、企業、技術社群、公民團體和使用者的角色應該為何？
	6. NTIA 在協助降低網路資訊自由流通的限制，和保護網路言論自由方面，可以扮演甚麼角色？
	7. NTIA 可以在哪些國際組織或場域中，最有效率地提倡資訊自由流通和言論自由？

類別	子題
	8. NTIA 如何能進一步協助對網路管轄權的挑戰？
多方利害關係人取向(方式)的網路治理	9. 多方利害關係人取向是否能繼續建立一個讓網路成長繁榮的環境？如果是，為什麼？如果否，為什麼？
	10. 是否有多方利害關係人取向最能發揮效用的公共政策領域？如果有，是哪些領域以及為什麼？是否有多方利害關係人取向無法發揮功效的領域？如果有，是哪些領域以及為什麼？
	11. 在網路治理的多方利害關係人中，現有的課責架構是否足夠？如果否，為什麼？可以做哪些改善措施？
	12. IANA (網路號碼指派機構) 監管權的移轉是否應該撤回？如果是，為什麼以及如何做？如果否，為什麼？
	13. 有關 ICANN 與 GAC (政府諮詢委員會)，NTIA 應優先考慮的事情是甚麼？
	14. 是否有 NTIA 須繼續進行的其他 DNS (網域名稱系統) 相關事務？如果是，請描述。
	15. 是否有參加 IGF 的阻礙？如果有，該如何降低阻礙？
	16. 針對 IGF 的架構、組織、規畫流程、或議程上，是否有可改進之處？如果是，有哪些？
	17. NTIA 可採取哪些行動來幫助提高對 IGF 的認知，以及促進利害關係人的參與？
	18. 在網路治理中，多邊組織的角色是甚麼？
隱私與網路安全	19. 網路安全威脅如何傷害國際貿易？又這些威脅的因應措施如何傷害國際貿易？
	20. 哪些國際場域最合適討論數位隱私的問題？在這些國際場域中，NTIA 應該優先處理哪些隱私議題？

類別	子題
新興科技和趨勢	21. 哪些新興科技和趨勢應該是國際政策的討論焦點？請舉出明確的例子。
	22. 關於新興科技和趨勢的討論應該在哪些國際場域舉行？哪些國際場域是最有效力的？哪些是最沒有效力的？
	23. 目前有哪些最佳典範來推廣新興科技的創新和投資？這些最佳典範是否為通用的？或是取決於國家經濟發展的程度？NTIA 應該如何推廣這些最佳典範？

資料來源：NTIA, 2018；本計畫彙整

## 2. 整體回覆概況

NTIA 共收到 91 份多方社群與個人提出的回覆 (NTIA, 2018b)。國家法律評論 (National Law Review) 彙整整體回覆概況如下 (Pierce, 2018)：

### (1) 資訊自由流通與管轄權

回覆者普遍對於跨境資料流通的限制感到擔憂，並反對資料在地化，認為會對資料流通帶來不必要的限制，且會對小型企業造成負擔，因為他們沒有足夠的資源在每個國家配合維運。另外，技術社群和公民團體希望 NTIA 關注全球日益增加的對線上內容進行管制的要求，他們表示，管制仇恨言論或恐怖主義內容，可能會對合法言論帶來嚴重後果。

### (2) 多方利害關係人取向(方式)的網路治理

多數的科技業者和貿易團體支持以全球性、多方利害關係人的取向(方式)，來治理網路，並認為 NTIA 應該維持 IANA 監管權的移轉，以利網路治理的多方利害關係人取向(方式)更加茁壯。

### (3) 隱私與網路安全

雖然公民團體普遍不認為 GDPR 可以作為其他想要規範個資國家的典

範，但他們也表示，應該注意網路使用者日益增加的隱私權需求，尤其在大數據和物聯網時代。產業界則質疑 GDPR 能否在其他管轄權實施，但也擔心被遺忘權可能在歐洲以外的地區被採用，因此，他們建議 NTIA 鼓勵以合作及多方利害關係人流程，來決定保護資料的方法，切勿扼殺創新。而在網路安全方面，許多技術社群和公民團體都反對讓加密資料提供後門程式以便政府取得內容，因為這會降低加密保護資料的功能。

#### (4) 新興科技和趨勢

多位回覆者指出，人工智慧(AI)、機器學習(Machine Learning, ML)，以及物聯網 (IoT) 都是要關注的新興科技，並期望 NTIA 鼓勵這些新興科技朝向負責、道德的方向發展，包含將對經濟與人權的衝擊納入考量。

### 3. 多方社群個別意見

本計畫另外從所有回覆文件中，挑選 5 個具有代表性，且分屬不同類別的多方社群，彙整其回覆重點 (表 14)，以了解不同社群的立場，相關比較將於下一節說明。這 5 個多方社群為技術社群的 ICANN (由董事會提交回覆)與 ISOC (網際網路協會)；公民團體的電子前哨基金會 (Electronic Frontier Foundation, EFF)；學術界的喬治亞理工學院網路治理計畫 (Internet Governance Project)；以及代表 Facebook、Twitter、Google 等美國主要網路公司的網路協會 (Internet Association, IA)。

表14. 多方社群回覆 NTIA 徵詢國際網路政策優先議題

1. 資訊自由流通與管轄權					
多方 社群 問題	產業界	學術界	技術社群		公民團體
	網路協會 (IA)	網路治理計畫 (IGP)	網際網路協會 (ISOC)	ICANN 董事會	電子前哨基金會 (EFF)
1. 資訊自由流通的挑戰?	例如不平衡的版權管理制度、資料流通的限制、中介機構責任罰款、封鎖網站、沉重關	政府實施網路主權與控制權、將監督網路內容的責任施加於各大	封鎖疑似非法或不合宜的內容、限制加密或視其為非法行為、強	n/a	n/a

1. 資訊自由流通與管轄權					
多方 社群 問題	產業界	學術界	技術社群		公民團體
	網路協會 (IA)	網路治理計畫 (IGP)	網際網路協會 (ISOC)	ICANN 董事會	電子前哨基金會 (EFF)
	稅等	網路平臺	迫資料在地化		
2. 限制資訊自由流通的國外法規?	詳本協會對 2017 國家貿易評估報告 (2017 National Trade Estimate Report) 中，有關數位貿易障礙的評論	n/a	n/a	n/a	n/a
3. 以國家法規判決全球網路的案例?	義、荷、俄羅斯等國法院判決平臺業者須為第三方內容負責的案例，造成業者財務支出增加，或得關閉某些網站功能，甚至中斷整個網站	歐盟 GDPR 中的被遺忘權迫使以美國為主的搜尋引擎提供移除連結的功能，將嚴重限制取得有事實根據的資訊、讓有心人士濫用來逃避責任	歐盟 GDPR 和加拿大法院判 Google 刪除某搜尋結果(Equustek 案)，開啟境外強制執行國家法規先例，不同法律相互抵觸將阻礙全球科技發展、製造監管競爭與網路分裂、使網路無法運作	n/a	n/a
4. 網路言論自由的挑戰?	巴西正評估國外公司能否自由流通資訊，國會也預計通過類似被遺忘權，要求網路服務業者移除被認為無關或過時的訊息。在泰國，若有人在網路發表對皇室或國家不敬的言論，將遭處刑責。這些威脅言論與資訊自由的挑戰，阻擾美國企業進入市場	資料在地化、內容審查、智慧財產權、網路安全、中介機構責任等法規或政策，皆會阻礙資訊自由流通和言論自由	n/a	n/a	包含美國在內的各國政府，皆不重視網路言論自由，政府代表通常較關切智慧財產權擁有者的利益
5. 各利害關係人於保護言論自由的角	當使用者、內容業者和企業，被賦予自由開放的資訊流通時，網路才得以興盛、促進社群交	n/a	n/a	n/a	網路的特色為去中心化，在網路層僅有少數的中心管制點，但也

1. 資訊自由流通與管轄權					
多方 社群 問題	產業界	學術界	技術社群		公民團體
	網路協會 (IA)	網路治理計畫 (IGP)	網際網路協會 (ISOC)	ICANN 董事會	電子前哨基金會 (EFF)
色?	流與跨境商業活動，因此，支持資訊自由流通能消除貿易障礙，讓美國網路業者在國外自由運作				製造審查與限制的機會。一個中心化的網路將會失去原有獨特的價值和優勢，所有關係人都應該保護言論自由
6. NTIA 在促進資訊與言論自由可扮演的角色?	NTIA 應成為資料自由流通和言論自由的擁護者，持續與美國貿易代表署和聯邦政府其他機構協調努力，確保相關阻礙不會再增加	由於貿易協定常被少數特殊利益團體支配，建議 NTIA 透過更開放的多方取向，提供建言給貿易協調單位，如在 WTO 發起爭端解決流程以反制中國的網路長城(中國全面封鎖網路顯然違反 WTO 相關規定)、建議加入 CPTPP 以對越南的資料在地化法規提出異議	建議 NTIA 檢視美國網路政策的意涵。網路的全球性和去中心化的本質，應被保護和維持，以確保使用者皆能連網和獲益	n/a	NTIA 為美國 GAC 代表，其立場應基於廣大的公眾利益，而非只代表註冊商和執法單位，並應於 ICANN 會議前，和其他多方社群討論相關議題，且將保護言論自由視為 GAC 首要工作。
7. 提倡資訊與言論自由最有效率的國際場域?	WTO 正研商消除數位貿易障礙問題，NTIA 應協助美國貿易代表署，以確保政府立場符合網路業者需求；NTIA 也應在世界智財權組織提倡美國政策，包含平衡版權保護、版權的避風港原則和中介機構責	ICANN 新章程明定不得將其域名管理權延伸至對網站內容的監管，NTIA 應善用 GAC 代表的身分，維護新章程(與第 6 題合併回覆)	n/a	n/a	n/a

1. 資訊自由流通與管轄權					
多方 社群 問題	產業界	學術界	技術社群		公民團體
	網路協會 (IA)	網路治理計畫 (IGP)	網際網路協會 (ISOC)	ICANN 董事會	電子前哨基金會 (EFF)
	任保護等，以鞏固美國在數位貿易的領導地位				
8. NTIA 如何協助網路管轄權的挑戰?	與歐盟持續溝通，以免衝擊美國企業 (摘自第 3 題的回覆)	提倡網路空間為全球共享資產，不應受國家主權籍制，並與 ITU、OECD 和 G20 合作推廣此概念(與第 6 題合併回覆)	n/a	n/a	n/a

2. 多方利害關係人取向的網路治理					
多方 社群 問題	產業業	學術界	技術社群		公民團體
	網路協會 (IA)	網路治理計畫(IGP)	網際網路協會 (ISOC)	ICANN 董事會	電子前哨基金會 (EFF)
9. 多方取向能否持續建立網路繁榮的環境?	為使美國企業持續成長創新，成為全球化企業，應該繼續採取目前的多方取向治理網路	多方取向仍是讓網路蓬勃成長的重要一環，網路必須受到保護，免於被任一國家所侵佔	網路複雜的生態系統，其政策制定必須是協作、包容、透明的，以及採用多方取向，規範須由多元的社群訂定，以服務各種需求	在執行 IANA 職責上，ICANN 與其他組織共創一個單一、可互通、全球性的網路。IANA 得以運作良好是因為全球的網路營運者和使用者自願性地支持	用多方取向管理和監督網路基礎設施仍然是目前最佳選擇，NTIA 應盡力使此方式更為公平且平衡，更關注資源較少的利害關係人、公民團體和非商業用途族群
10. 多方取向最能發揮效用的公共政策領域?	多方取向很適合網路政策的發展，因為它鼓勵使用者和營運網路基礎設施的技術社群，實際參與政策制定	當治理範圍為跨國或全球性時，如網路安全議題，多方取向最能發揮效用。但若過度重視流程和代表類型，恐淪為缺乏效率與效能	如加拿大的加強 IoT 安全措施、NTIA 的 IoT 安全升級和修補程式、《非洲網路基礎建設安全指	ICANN 多方社群不斷努力因應 GDPR 對 WHOIS 的衝擊，期能兼顧法規遵循與儘量維持 WHOIS 既有功能	n/a

2. 多方利害關係人取向的網路治理					
多方 社群 問題	產業業	學術界	技術社群		公民團體
	網路協會 (IA)	網路治理計畫(IGP)	網際網路協會 (ISOC)	ICANN 董事會	電子前哨基金會 (EFF)
			導方針》等		
11. 現有多方取向的課責架構是否足夠?	n/a	雖然 ICANN 課責機制因新章程的制定而有所改善，但 ICANN 組織(如執行長和幕僚)經常剝奪社群制定政策的權力，違反由下而上的多方取向，且 ICANN 董事會也沒有盡到監督管理責任	n/a	由各個支援組織(SO)與諮詢委員會(AC)代表組成的提升 ICANN 課責跨社群工作小組(CCWG)達成共識建議，加強多方社群的能力，使董事會負起責任，讓董事會的行為和決策符合 ICANN 使命和章程	ICANN 政策制定流程對資源充足者較有益，大型智財權擁有者的聲音通常蓋過公民團體和小型企業組織，因此 ICANN 須確保全體利害關係人的實質參與
12. IANA 監管權移轉是否應撤回?	不該取消，否則將會破壞美國的可信度和地位，讓極權主義政府為掌控全球網路關鍵資源而爭鬥，造成網路分裂，限制商務和言論自由	不該取消，因為公然將全球性的設施國有化，勢必引起整個網路社群的強烈反抗，ICANN 的適法性將被摧毀，更給了中、俄等極權國家推翻多方取向的正當理由，並建立另一個網路系統	不該取消，因為此移轉展現協力管理網路關鍵資源的適法性，更鞏固多方取向，且移轉後的運作符合安全穩定與公平分配的期望	不該取消，因為移轉過程設有加強監督與課責的機制，而移轉後的維運也獲得客戶的高度滿意	不該取消，否則將造成網路分裂。網路不屬於任何一個特定的政府或利害關係人，它是屬於全體人類的資產
13. NTIA 應優先考慮的 ICANN 與 GAC 事務?	強烈維護美國的利益，並確保 ICANN 對所有利害關係人負責	改革 GAC，GAC 應回歸原先設定的諮詢委員會(AC)身份，避免有些政府意圖將 GAC 變成替代性支配政策制定的工具	n/a	n/a	改善 ICANN 和 GAC 中，多方利害關係人取向的平衡
14. NTIA	n/a	支持美國憲法所保護的言論自由、維護	n/a	n/a	n/a

2. 多方利害關係人取向的網路治理					
多方 社群 問題	產業業	學術界	技術社群		公民團體
	網路協會 (IA)	網路治理計畫(IGP)	網際網路協會 (ISOC)	ICANN 董事會	電子前哨基金會 (EFF)
應續推 的其他 DNS 事 務?		ICANN 的新章程			
15. 參 加 IGF 的阻 礙?	本協會支持 IGF 持續作為全球討論網路政策的重要平臺 (摘自第 9 題回覆)	IGF 因須採聯合國會議規格辦理而花費驚人,但政府部門只公關式地參加官方單位申辦的 Open Forums、主場會議毫無討論重點、MAG 成員遴選不透明、議程評選標準偏頗、非聯合國成員國民不能報名出席會議... , IGF 正搖搖欲墜,恐淪為可被其他會議取代的一般性論壇,如 GCCS、RightsCon、WSIS Forum 等。IGP 和許多團體正評估是否持續參與	n/a	n/a	n/a
16. IGF 待改進 之處?	n/a	建議 NTIA 支持修改 MAG 成員的遴選程序與座談評選方式,讓多方社群決定	n/a	n/a	n/a
17. NTIA 對 IGF 與多方 參與的 認知推	n/a	鼓勵企業、政府和公民團體將 IGF 作為協商網路治理的平臺(摘自第 17 題回覆)	支持並確保 IGF 成為全球網路治理生態系統的重要環節。NTIA 在 2017 年採多方	n/a	n/a

2. 多方利害關係人取向的網路治理					
多方 社群 問題	產業業	學術界	技術社群		公民團體
	網路協會 (IA)	網路治理計畫(IGP)	網際網路協會 (ISOC)	ICANN 董事會	電子前哨基金會 (EFF)
廣?			取向處理 IoT 安全升級，已成典範應與國際分享		
18. 多邊組織最佳典範，以及於網路治理的角色?	多邊組織應推動最佳典範，以及教育其會員國接取網路的益處	n/a	n/a	n/a	n/a

3. 隱私與網路安全					
多方 社群 問題	產業界	學術界	技術社群		公民團體
	網路協會 (IA)	網路治理 計畫(IGP)	網際網路協會(ISOC)	ICANN 董事會	電子前哨基金會 (EFF)
19. 網路安全威脅對國際貿易的傷害?	n/a	n/a	加密可維護言論自由、貿易、隱私和使用 者信賴，應成為資訊交換與儲存的規範，所有 試圖從法律或技術去 限制使用加密，都會對	n/a	n/a
20. 最適合討論數位隱私的國際場域，及 NTIA 優先議題?	支持 NTIA 在 OECD 和 IGF 參與政策制定，並以彈性且健全方法，保護線上隱私和網路安全。NTIA 的首要工作是對消費者和企業維持管理的一致性，以及跨境法規的可預測性	n/a	守法公民和網路安全產生負面影響。因此，美國政府不應降低或限制加密的使用。	n/a	針對 WHOIS 資料庫如何符合 GDPR 規定，目前 ICANN 正在研議具共識的政策，NTIA 不宜介入，但仍應將保護隱私列為參與 ICANN 的重要優先議題

4. 新興科技和趨勢					
多方	產業業	學術界	技術社群	公民團體	

社群 問題	網路協會 (IA)	網路治理 計畫(IGP)	網際網路 協會(ISOC)	ICANN 董事會	電子前哨基 金會(EFF)
21. 國際政策應討論的新興科技?	新興科技發展迅速，任何相關趨勢和科技的討論，都應全面了解其主要的工程特性，以及發展成熟的時間框架，而非用傳統工業的角度來檢視網路新興科技	n/a	n/a	n/a	n/a
22. 最適合討論新興科技的國際場域?	n/a	n/a	n/a	n/a	n/a
23. 推廣新興科技創新與投資的最佳典範?	新興科技的創新與投資有賴國家層級的框架帶動，以吸引企業的投資動機，並提供數位科技商業取向的基本保護	n/a	n/a	n/a	n/a

資料來源：本計畫彙整

#### (四) 相關爭議

綜合 NTIA 提出的徵詢問題與原由說明，以及上表 14 所彙整的美國多方社群意見，可發現美國與其他國家之間，以及美國的不同多方社群之間，對下列議題抱持不同看法。

##### 1. 國際間的網路管轄權與法規衝突

NTIA 與美國多方社群指出，以國家及區域法規來判決或規範全球網路的案例越來越多，凸顯各個國家主權對網路管轄權的爭議與緊張局勢，以及不同國家之間的法規衝突。如果不能妥善解決，將會阻礙全球科技發展、破壞網路提供的成長機會、製造監管競爭、殘害人權與言論自由、造成網路分裂與無法互通運作等問題。而被美國多方社群點名可能引發這些問題的法院判決與法規案例包括：

- 法院判決案例

- 義<sup>7</sup>、荷<sup>8</sup>等國家的法院判決平臺業者須為第三方內容負責，造成業者財務支出增加，或得關閉某些網站功能，甚至中斷整個網站。
- 加拿大<sup>9</sup>最高法院判決 Google 必須將某個侵權網站，從全球的搜尋結果中刪除，開啟於境外強制執行國家法規的先例，並引發單一國家法院判決卻影響全球資訊存取的爭議。
- 區域法規案例
  - 歐盟 GDPR 中的被遺忘權迫使以美國為主的搜尋引擎提供移除連結的功能，將嚴重限制存取有事實根據的資訊。
- 國家法規案例
  - 許多國家實施資料在地化、封鎖網站、內容審查、中介機構責任、限制加密、網路安全等相關政策或法規。

面對國際間的網路管轄權與法規衝突問題，美國多方社群除了建議 NTIA 持續與歐盟溝通，以及在國際上提倡「網路空間不應受到國家主權箝制」的概念外，似乎也沒有更具體有效的解決辦法。

## 2. 國內不同社群的歧見

### (1) NTIA 於 GAC 的基本立場

NTIA 為美國政府參與 ICANN 事務的 GAC (政府諮詢委員會) 代表。

---

<sup>7</sup> 義大利 Torino 初審法院於 2017 年 4 月 7 日判決 Youtube 因未及時將侵權的電視劇下架 (雖然違法內容由第三方上傳而非 Youtube)，而須賠償電視劇所有權人 Delta TV 25 萬歐元 ([Delta TV v. Google and YouTube](#)，案號：1928)。

<sup>8</sup> 花花公子雜誌於荷蘭的出版商 Sanoma，控告荷蘭 GS Media 旗下網站 GeenStijl 於 2011 年提供未經授權的照片連結，並引誘讀者點擊。荷蘭最高法院認為事涉歐盟《著作權指令》條文解釋問題，而將全案移送歐盟法院。歐盟法院於 2016 年 9 月 8 日裁定 Sanoma 可以請求法院禁止其他以營利為目的之機構對 Sanoma 照片提供連結 ([GS Media BV v. Sanoma Media Netherlands BV and Others](#)，案號：C-160/15)。

<sup>9</sup> 加拿大最高法院於 2017 年 6 月 28 日判決 Google 必須將侵犯 Equustek Solutions 公司權益的 Datalink 公司，從全球網站的搜尋結果刪除。此案原本已判決 Datalink 敗訴，Google 並據此刪除加拿大境內 345 個與 Datalink 相關的搜尋網頁。不過 Datalink 持續在境外網路銷售 Equustek 山寨貨品，Equustek 因此提出上訴並獲得勝訴 ([Google Inc. v. Equustek Solutions Inc.](#)，案號：36602)

公民團體認為，既然 NTIA 身為政府代表，其立場應該是基於廣大的公眾利益，且應於 ICANN 會議前和其他的多方社群討論相關議題，而非只是代表註冊商和執法單位的權益。

### (2) 多方利害關係人取向 (方式) 的改善

雖然美國多方社群都支持以多方利害關係人取向 (方式) 來治理網路，且一致認為不能撤回 IANA 監管權的移轉，不過，公民團體強調，多方社群在 ICANN 的參與上並不公平，其政策制定流程對資源充足者較有益，且大型智財權擁有者的聲量遠大於公民團體與非商業使用族群，因此，建議 NTIA 應促使多方取向更為公平與平衡。

### (3) IGF 的功能與參與

相較於產業界和技術社群支持 IGF 持續成為全球討論網路政策的重要平臺，學術界 (網路治理計畫) 表示，他們和許多團體都正在評估是否持續參與 IGF，因為 IGF 的辦理費用驚人，但是並沒有達到全球多方社群有效討論議題的會議目的，例如政府部門只是公關性地參加官方單位申辦的會議、許多場次毫無討論重點、多方利害關係人諮詢小組(MAG)的成員遴選不透明、議程的評選標準偏頗、非聯合國成員的國民不能報名出席會議等問題，以致 IGF 恐怕淪為可被其他會議取代的一般性論壇，如 RightsCon (世界數位人權大會)、GCCS (全球網路空間會議，Global Conference on Cyber Space)、聯合國 WSIS (資訊社會世界高峰會，World Summit on the Information Society)等。

## (五) 小結

本篇介紹美國商務部透過公開意見徵詢方式，了解美國多方利害關係人對「未來國際網路政策優先議題」看法，以作為後續施政的重點。此次徵詢有關資訊自由流通與管轄權、多方利害關係人取向 (方式) 的網路治

理、隱私與安全，以及新興科技與趨勢，共 4 大類 23 個問題，最後收到 91 件回覆意見。徵詢結果顯示，整體而言，美國多方社群普遍反對限制資料自由流通的相關措施、支持多方利害關係人取向（方式）的網路治理、擔憂歐盟以外的國家也援用 GDPR 當中的被遺忘權條款，以及認為 AI 與機器學習是必須關注的新興科技。至於日益嚴重的國際網路管轄權與法規衝突問題，美國多方社群除了建議 NTIA 持續與歐盟溝通，以及在國際提倡「網路空間不應受到國家主權箝制」概念外，似乎也沒有更具體有效的解決辦法。

本計畫綜合 NTIA 提出的徵詢問題與原由說明，以及美國多方社群的回覆意見，提出下列建議：

### **1. 參考美國網路政策主張，透過多方取向(方式)決定我國政策立場**

針對資訊自由流通、隱私與安全議題，美國所主張的保護基本人權與言論自由，亦是我國與西方民主國家向來所要捍衛的民主價值。不過，誠如代表美國主要網路公司的網路協會所指「限制言論與資訊自由流通，會阻礙美國網路業者進入當地市場；反之則能讓美國網路業者在國外自由運作」，凸顯美國上述網路政策主張的背後，應有強大的經濟利益考量。

每個國家的經濟利益甚至是公共利益，都有其獨特且複雜的政經社會文化考量，以致近來我們看到歐盟的網路政策發展已經和美國漸行漸遠。因此，儘管美國的網路政策主張具有相當參考價值，但是我國的網路政策立場，仍然應該透過多方取向(方式)，由我國的多方社群共同討論決定，如此才能找出最符合我國公共利益的政策立場。

### **2. AI 與自動化為未來重要治理議題，啟動討論以因應數位衝擊**

NTIA 在此次公開徵詢文件中指出，網路治理未來幾年的焦點將是人工智慧對社會與經濟的衝擊、自動化與網路新商業模式對勞動市場的改變，以及區塊鍊應用的快速成長。而美國多方社群的回應也強調 NTIA 應該鼓勵這些新興科技朝向負責、道德的方向發展。

行政院已推出「臺灣 AI 行動計畫 (2018-2021)」，以帶動我國未來經濟發展邁向新階段為目標。我國對於新科技的發展，向來偏重經濟產值，鮮少關注它對整體社會所帶來的挑戰，而這次似乎也不例外。隨著國際網路治理會議對 AI 與自動化的討論日益熱絡，我國也應該著手展開相關研究與討論，除了在消極面避免發生某部會因為不察網路時代的國際政策趨勢而被批評為「無知與失職」的憾事外，在積極面更是應該透過及早規劃與準備，以帶領我國因應未來數位轉換的衝擊。

## (六) 參考資料

- EFF (2018). Re: International Internet Policy Priorities.  
[https://www.ntia.doc.gov/files/ntia/publications/public\\_interest\\_comments\\_on\\_noi\\_final.pdf](https://www.ntia.doc.gov/files/ntia/publications/public_interest_comments_on_noi_final.pdf)
- ICANN Board of Directors (2018). Re: International Internet Policy Priorities.  
[https://www.ntia.doc.gov/files/ntia/publications/2018-07-13\\_icann\\_board\\_ntia\\_noi\\_comments.pdf](https://www.ntia.doc.gov/files/ntia/publications/2018-07-13_icann_board_ntia_noi_comments.pdf)
- IA (2018). Re: International Internet Policy Priorities.  
[https://www.ntia.doc.gov/files/ntia/publications/ia\\_comments-international\\_internet\\_priorities.pdf](https://www.ntia.doc.gov/files/ntia/publications/ia_comments-international_internet_priorities.pdf)
- IGP (2018). Re: International Internet Policy Priorities.  
<https://www.ntia.doc.gov/files/ntia/publications/igp-comments.pdf>
- ISOC (2018). Re: International Internet Policy Priorities.  
[https://www.ntia.doc.gov/files/ntia/publications/isoc\\_comment-ntia-noi-2018-07-17.pdf](https://www.ntia.doc.gov/files/ntia/publications/isoc_comment-ntia-noi-2018-07-17.pdf)
- NTIA (2018a). Notice of Inquiry on International Internet Policy Priorities.  
<https://www.ntia.doc.gov/federal-register-notice/2018/notice-inquiry-international-internet-policy-priorities>
- NTIA (2018b). Comments on International Internet Policy Priorities.

<https://www.ntia.doc.gov/federal-register-notice/2018/comments-international-internet-policy-priorities>

- Pierce, J. (2018). NTIA's International Internet Policy Priorities for 2018 and Beyond, National Law Review.  
<https://www.natlawreview.com/article/ntia-s-international-internet-policy-priorities-2018-and-beyond>

## 八、俄羅斯號召金磚國家另建網路系統

\*本篇內容特別邀請黃勝雄博士撰文分析

### (一) 概述

美國是領導網際網路發展的國家，無論在網路技術、網路關鍵資源數量，以及網路關鍵基礎設施的掌控，都領先全球其他國家。隨著網際網路應用與服務日益廣泛，網際網路已不僅是數位科技議題，也是數位經濟、政治與外交等多方領域的重要議題。因此，網際網路治理受到越來越多國家的重視。於是俄羅斯於 2017 年底號召金磚國家（巴西、俄羅斯、印度、中國大陸、南非）建立一個獨立、替代性、只由他們專屬共享的網際網路，以合力擺脫美國對全球網際網路的控制權。

### (二) 政策發展與目標

網際網路的網域名稱根伺服器 (DNS Root Servers) 是掌控網際網路關鍵資訊系統。現有網域名稱根伺服器是由美國加州登記的 ICANN (網際網路名稱與號碼分配機構) 所管理。全球共有 13 組英文字母組成的網域名稱根伺服器。美國政府在 2016 年將 IANA (網路號碼指派機構) 的治理功能移轉給 ICANN 子公司 PTI (Post Transition IANA) 負責營運。DNS Root A 根伺服器一直是委由美國 Versign 公司負責營運。

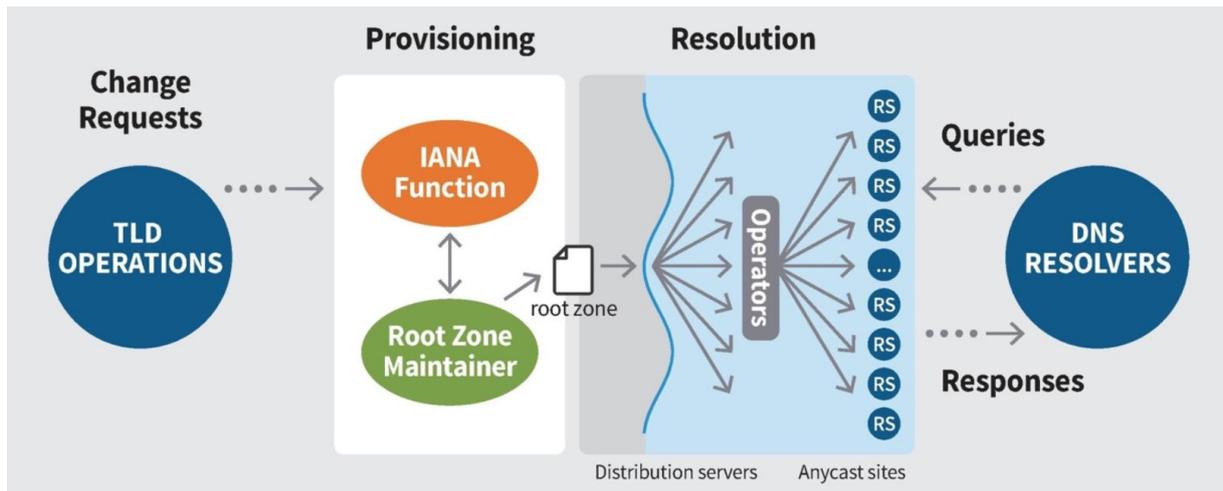


圖27. Internet DNS Root System 註冊與解析

俄羅斯政府認為，管控全球網際網路大權的 ICANN 由美國政府管轄，這對於網際網路的治理是一大危機。其中尤其以 Root (A)網域名稱根伺服器的角色最為關鍵。從俄羅斯政府角度，如果美國與俄羅斯發生軍事衝突，美國政府只要將俄羅斯的國家頂級網域名稱 .RU 從網域名稱根伺服器的域名檔 zone files 移除，俄羅斯立刻從全球網路空間中消失。全球無法解析任何 .RU 網域名稱，無法與任何 .RU 網站連線或通訊。

俄羅斯普丁總統的網路顧問表示，俄羅斯已經做好充分準備，隨時可以將俄羅斯的網路從國際網路分離。俄羅斯國安會要求政府為金磚國家(巴西、俄羅斯、印度、中國大陸、南非)國家籌劃獨立運作的替代性網際網路(alternative Internet)，此設計將導致全球網際網路運作機能更脆弱。普丁總統要求這項任務規劃期限為 2018 年 8 月。俄羅斯國安會委員表示，西方國家提升網路空間的攻擊能力以及提高實施攻擊作業的準備度，使得俄羅斯國家安全備受威脅。這個任務也代表著將建構獨立不受國際控制的 DNS 根伺服器，新的 DNS 根伺服器系統將提供給巴西、俄羅斯、印度、中國大陸與南非使用。俄羅斯自從 2014 年起，就已經考慮脫離全球網際網路獨立運作。

### (三) 實施重點

網路攻擊事件不斷發生，北約擴張和選舉干涉，俄羅斯和美國之間的緊張關係已開始上升，俄羅斯規劃建構俄羅斯版本的網際網路來取代現有網際網路。俄羅斯版的網際網路計畫可能於2018年啟動。對俄羅斯而言，長期以來感受網際網路受美國控制的隱憂，建構新的替代性網際網路被視為解決此隱憂的方案，此方案同時也可讓政府對網路內容進行不同等級的監督與管理。

建構一套替代性網際網路，就資訊技術上而言或許不複雜，但是專家表示，建構替代性網際網路系統可能會帶來商業和經濟災難。俄羅斯的網路政策方向顯示，無論美國川普總統與俄羅斯普丁總統之間的對話有多熱絡，兩個冷戰時期的對手在網路空間仍舊存在敵對關係。

如果俄羅斯要建構一個替代性網際網路幫助政府控制內容，替代性網路也失去原有網際網路優勢，至少從經濟層面評估替代性網際網路無法取代原有網際網路，最多就是成為政府控制網路內容的工具。俄羅斯與巴西，印度，中國大陸和南非等金磚國家討論發展替代性網際網路的議題。

俄羅斯政府認為，建構替代性網際網路系統是國家安全問題，擁有一個獨立的替代性網際網路可能也會增加俄羅斯政府對民眾的審查，監視和網路作戰能力。電子前哨基金會(Electronic Frontier Foundation)的 Mitch Stoltz 表示，透過獨立的 DNS 根伺服器，俄羅斯可以取消某些網站的訪問，引導人們到其他虛假網站，甚至可以對全球 DNS 系統發起攻擊，而不會給自己帶來風險。這是一個相當龐大的計畫，世界上每臺電腦和手機以及連接網際網路的設備，都必須設定來與特定的替代性 DNS 根伺服器連線。要建立一個真正獨立的網際網路，俄羅斯政府將不得不重新配置俄羅斯境內所有與網際網路連接的設備，以便使用替代性網際網路系統來取代原有網際網路系統。

現代網際網路始於美國政府研究計畫，現今由 ICANN 維護。ICANN 由美國政府建立，作為一個非營利組織運作。普丁在2018年3月接受媒體

訪問時指出，網際網路所有治理工具都在美國境內，美國控制所有工具。都柏林城市大學 (Dublin City University) 助理教授 Tanya Lokot 表示，過去幾年，俄羅斯的替代性網際網路計畫已在國家安全相關資料中出現。越來越多的經濟與國防安全計畫與網際網路結合在一起，他們希望可加強保護自己國家的基礎設施。

Tanya Lokot 表示，俄羅斯的努力與新的反極端主義法律有關，這些法律旨在進一步消除極端意見。它是更嚴厲打擊不同言論的工具，政府可以監控所有人民在網路上的言論。俄羅斯媒體宣稱，莫斯科已經建構一個替代性伺服器來收集 ICANN 根伺服器登記的所有頂級網域名稱。

許多網路專家提出警告，創建替代性網際網路的舉措充滿了弊端。瑞典國防研究局副研究主任 Carolina VendilPallin 表示，俄羅斯商界正在反對第二個網際網路的構想。這個計畫的誕生是因為擔心俄羅斯可能會受到西方切斷網際網路的威脅，或作為一種新形式的制裁。

俄羅斯擁有超過 1 億的網際網路用戶。要準確地說明俄羅斯網際網路流量究竟有多少比例瀏覽國外網站是很困難的，但推測是 10% 到 30% 之間。在此同時，俄羅斯政府一直在努力掌握網路技術。2018 年 5 月，俄羅斯政府試圖阻止大約 1,500 萬俄羅斯人使用通訊軟體 Telegram，並承認這項措施意外地阻止了數百個不相關的網站。

#### (四) 相關爭議

俄羅斯一直號召金磚國家成立獨立的網際網路，建構自己的 DNS 根伺服器。金磚國家認為，現有根伺服器由美國 ICANN 控制是相當嚴重的危機。目前全球有 13 組 Root Servers。美國政府在 2016 年已將 A DNS 根伺服器治理權轉交由 ICANN 管轄的子公司負責營運。

網路治理專家 Wolfgang Kleinwächter 認為，擔心美國控制 DNS 根伺服器的顧慮是多餘的。即使美國政府刪除俄羅斯頂級國家網域名稱 .RU 所

屬的網域名稱 zone 檔案，但網域名稱檔案複本仍存放在其他 12 組英文字母的網域名稱根伺服器及成千上萬組 Anycast 鏡像伺服器上。要完全從所有網域名稱根伺服器與鏡像伺服器移除 .RU 頂級網域名稱可能性十分低。

ICANN 技術長 David Conrad 說明許多人擔心美國政府對 ICANN 施壓控制網際網路，例如控制俄羅斯頂級國碼 .RU 網路連線，但是這樣做的效果相當有限，對美國或網際網路完全沒有好處。網際網路存在的基礎是基於信任，一旦失去使用者的信任，替代性網際網路根伺服器立刻會風起雲湧地產生。網際網路以全球為市場，替代性網際網路根伺服器所帶來的傷害將遠大於利益。

除了俄羅斯外，中國大陸呼籲俄羅斯等金磚國家承諾網路主權概念，由政府採取適當方式控制國家網路。中國大陸在網路白皮書已經提出，在國家領土內政府有權控制與規範網際網路的權利。北京也計畫提升網路作戰能量以對抗網路空間日益高漲的威脅。

中國大陸在內部網路的國際出口建立了一個大型防火牆--防火長城(The Great Firewall of China)，防火長城技術嚴重限制了民眾對國外網站的連線。但即使是防火長城系統的主要設計者，也必須努力解決許多防火長城面臨的技術問題。2016 年，中國大陸政府防火長城工程師方斌星在大學演講期間無法連上特定網站。這個情境反映出提供替代性網際網路最大風險就是「完全失去連接網際網路的能力」。一旦替代性網際網路發生這樣的疑慮或狀況時，建構在替代性網路之上的所有電子商務、數位金融、數位服務等將不被使用者所信任。而一個不被信任的系統就失去存在的價值，這一點是替代性網際網路面臨的最大挑戰。

## (五) 小結

網際網路在我國已有多年的發展歷史，政府從早期的電子化政府、

eTaiwan、mTaiwan 等資通訊國家型計畫都投入大量資源與研究能量在網路的基礎建設與創新應用服務，使我國資通訊網路發展有優異的表現。

隨著資訊安全重要性逐漸提升，我國也開始關注網際網路關鍵基礎設施發展。部分網路服務業者逐步導入國際 DNS 根伺服器來提升網路服務效能。目前包含中央研究院、中華電信公司、是方電信公司都有提供網際網路 DNS 根伺服器服務。

我國也是少數早期參與 ICANN 會議的參與者，包含臺灣網路資訊中心、中央研究院、中華電信公司等都曾派員參加 ICANN 會議的討論。我國資通訊相關基礎設施都是以全球網際網路架構為依歸進行部署與營運。

然而，俄羅斯、中國大陸疑慮美國掌控網際網路關鍵基礎設施，例如 DNS 根伺服器。此議題需從幾個構面考量。首先，網際網路並非單一國家或單一政府所掌控，而是採網際網路治理是多方利害關係人取向(方式)，由不同利害關係人社群依其最佳實務規範與政策流程訂定網際網路治理政策。IETF (網際網路工程技術小組, Internet Engineer Taskforce) 專責網際網路通訊協定與技術的規劃與發展。IP 位址政策與分配由各區域網路治理機構負責，在亞太地區即是亞太網路資訊中心 (Asia Pacific Network Information Centre, APNIC)。頂級網域名稱的註冊與政策由 ICANN 負責。在多方利害關係人模式運作下，單一政府機構很難影響整體網際網路的運作機制與相關政策。

如許多網路專家所提，網際網路根伺服器包含 13 組字母 (A-M) 組成的主節點 DNS 根伺服器，各主節點 DNS 根伺服器又具備數量龐大的 Instance 備份伺服器。在如此多重備援的架構之下，即便任何一部主節點 DNS 根伺服器故障或被人為操控，並不會影響其他主節點 DNS 根伺服器或 Instance 備份伺服器運作。因此，對於單一政府即可操控整體網際網路架構的疑慮是過度擔憂。

建構替代性網際網路面臨的技術或限制可能遠大於我們所想像。想像

替代性網際網路系統取得現有網際網路 DNS 根伺服器所記錄的頂級網域名稱資料，面臨第一個問題就是如何確保替代性網際網路的網域名稱資料與現有網際網路資料一致。當發生資料不一致時，就會造成無法解析及無法上網的情況，這將對建構上層的電子商務與網路服務產生重大損失，極可能對數位經濟造成難以估計的衝擊。這是替代性網際網路面臨的最大挑戰，也是倡議替代性網際網路論述者難以克服的問題。

替代性網際網路投入的計畫規模龐大，帶來的商業價值極其有限，甚至造成重大經濟衝擊。考量我國整體資通訊基礎建設成長軌跡，維持現有全球一致的網際網路發展方向不僅符合我國產業與社會最大利益，更能發揮我國資通訊產業優勢，在完整的全球資訊架構下建構我國資通安全與國家安全。

## (六) 參考文獻

- DW News. (n.d.). Russia moves toward creation of an independent internet. <https://www.dw.com/en/russia-moves-toward-creation-of-an-independent-internet/a-42172902>
- Lynch, J. (2018). Is Russia about to launch a parallel Internet? Fifthdomain. <https://www.fifthdomain.com/international/2018/07/12/is-russia-about-to-launch-a-parallel-internet/>
- RT News. (2017). Russia to launched independent internet for BRICs nations. <https://www.rt.com/politics/411156-russia-to-launch-independent-internet/>
- Beyond, R. (2018). Why do Beijing and Moscow embrace cyber sovereignty. [https://www.rbth.com/opinion/2017/03/22/why-do-beijing-and-moscow-embrace-cyber-sovereignty\\_725018](https://www.rbth.com/opinion/2017/03/22/why-do-beijing-and-moscow-embrace-cyber-sovereignty_725018)
- The Moscow times (2018). Russia is ready for a shutdown of the Internet. <https://themoscowtimes.com/news/russia-is-ready-for-a-shut-down-of-the-internet-putins-adviser-60704>

## 肆、國際參與及交流

### 一、邀請國際專家訪臺

#### (一) 專家簡介

本計畫邀請國際重要網路技術標準與政策專家 Mr. Fred Baker 於 6 月 17 日至 22 日訪臺，並安排拜會總統府國家安全會議、行政院資通安全處、通傳會等 3 個單位，以及至「第 30 屆 TWNIC IP 政策資源管理會議暨第一屆台灣網路維運論壇」公開演講等行程。

Mr. Baker 任職思科系統公司 (Cisco Systems) 院士超過 20 年，期間並擔任網際網路工程任務小組 (IETF) 主席、網際網路協會 (ISOC) 主席、美國聯邦通信委員會 (FCC) 技術諮詢委員會委員等多項職務，且完成 60 個網路技術規格標準 (RFCs)。此外，他在美國還擁有十多項技術專利。主要職務經歷如下：

- 現任職務
  - ICANN 根伺服器諮詢委員會 (Root Server System Advisory Council, RSSAC) 委員 (2017~迄今)
  - 網際網路工程任務小組(IETF) 之 IPv6 運作工作小組 (IPv6 Operations Working Group) 共同主席 (2005~迄今)
  - 網路系統協會(Internet Systems Consortium, ISC) 董事 (2003~迄今)
- 主要經歷
  - IETF 主席 (1996~2001)；IETF 之網路架構委員會 (Internet Architecture Board, IAB) 等多個工作小組之主席 / 負責人 (1990~2017)
  - 思科系統公司 (Cisco Systems) 院士 (1994~2016)

- 寬頻網路技術諮詢小組 (Broadband Internet Technical Advisory Group, BITAG) 技術工作小組顧問 (2012~2016)
- RFC 系列監督委員會 (RFC Series Oversight Committee, RSOC) 主席(2011~2013)
- 美國聯邦通信委員會(Federal Communications Commission, FCC) 技術諮詢委員會(Technical Advisory Council, TAC)委員(2005~2009)
- 網際網路協會 (ISOC) 主席 (2002~2006)；董事 (2006~2008)

## (二) 拜會總統府國安會

- 時間：107 年 6 月 20 日 (三) 10:00~11:00
- 地點：總統府國家安全會議諮詢委員李德財辦公室
- 與會者：李德財委員、國安會研究人員、Mr. Fred Baker、陳文生執行長、本計畫同仁
- 會議摘要 (Mr. Fred Baker 建議事項)

### 1. 研究 TLS 1.3

過去曾推行以網際網路安全協定(Internet Protocol Security, IPsec)作為 IPv6 安全計畫的一部分，但是後來發現傳輸層安全協定(Transport Layer Security, TLS) 是更為常見的工具。IETF 2018 年 3 月通過 TLS 1.3 版，1.3 版與 1.2 版不同之處在於，每次開起一個新的連線，就會得到一個新的金鑰，因此，可讓網路傳輸更為安全，建議相關人員好好研究 TLS 1.3。

### 2. 研究 MANRS

建議網路服務業者研究 MANRS (Mutually Agreed Norms for Routing Security，路由安全共同協議規範)，它是由業者相互同意發展出的路由安全規範，包含以下四項基本且能實際執行的措施：

- 過濾：網路營運者必須要制定清楚的路由政策，確認自己的路由

公告、客戶和鄰近網路的公告都是正確的，才能預防錯誤路由訊息的散布。

- 反欺騙：確認來源位址的正確性可以大幅降低分散式阻斷服務攻擊 (DDoS attack) 的傳播和影響，基本上，網路營運者應該要執行反欺騙來預防有錯誤來源位址的封包進出網路。
- 協調：網路營運者必須在路由資料庫中持續維護可使用的且最新的聯絡資訊，才能促進業者間相互的溝通和協調。
- 全球性的驗證：進行全球性的路由資訊驗證可以限縮路由事件的範圍，因此，公布你的數據資料，讓其他人來驗證。

### 3. 積極參加 IETF 會議

網際網路工程任務小組(IETF)是一個負責網際網路標準的開發和推動的組織，每年在歐洲、北美和亞洲舉辦三次會議，每次約有 1000 至 1500 人與會。以通訊樞紐來說，臺灣在亞洲地區佔有十分重要的地位，希望鼓勵更多臺灣 IoT 製造商參加 IETF。

### (三) 拜會行政院資安處

- 時間：107 年 6 月 20 日 (三) 14:00~15:00
- 地點：行政院資通安全處會議室
- 與會者：徐嘉臨副處長、資安處人員、Mr. Fred Baker、陳文生執行長、本計畫同仁
- 會議摘要 (Mr. Fred Baker 回覆提問)

#### 1. 5G 資安問題

評估 5G 通訊的安全性時，我們必須認知，3G 或 4G 出現的資安問題，極有可能也會出現在 5G，如果某個攻擊在舊的範例中被認定為有效，我們

必須假定它仍會在新的範例中，以不同的方式出現。

在眾多資安問題中，必須特別注意 stingray (一種手機信號攔截器，又稱基站模擬器)，它是一種中間人攻擊。5G 是圍繞著許多微處理器而建構的，stingray 基本上是一種微型基地台(femtocell)，用來瓦解或監控 5G 網路，以這種中間人攻擊來看，幾乎可以產生任何一種網路問題。

## 2. IPv6 攻擊

對於日前一一份報告聲稱一起對 Neustar 的 DNS 服務發動的 DDoS 攻擊，是第一個經由 IPv6 的 DDoS 攻擊，其實這也許不該歸類為 IPv6 攻擊，而是屬於 IPv6 網路中的 DNS 攻擊，因為它並沒有任何 IPv6 的性能，如擴充標頭 (extension header) 等。

## 3. 關鍵基礎設施管理

關於如何降低關鍵基礎設施營運衝擊，首先，是建議與供應商合作，他們很關心相關的網路設備攻擊事件。其他則是常見的建議如：關閉不使用的裝置、使用 SSH (Secure Shell，安全外殼協定)，以及不要重複使用密碼等。另外，可以留意一些安全架構，如線上信任聯盟 (Online Trust Alliance, OTA) 的 IoT Security Framework (物聯網安全架構)、美國國家標準暨技術研究院 (National Institute of Standards and Technology, NIST) 或是美國國土安全部 (The Department of Homeland Security, DHS) 的安全架構。此外，設備供應商和網路營運者應該可以自己選擇要使用的架構，並提供合規的文件。還有，要定期更新並使用最新的軟體或韌體，包含最新的修補程式、開源軟體等。最後，每年請稽核專家針對政府網路、網路服務供應商和網路交換中心的網路、企業網路等，提出關鍵基礎設施的認證，檢視其資通信政策和實務情形。

## 4. 工業控制系統

討論工業控制系統的資安議題，可以參考 NIST 的相關意見。然而，要解決的問題不會只有一個，也不會只有一種解決方法，資訊安全是一個普遍性的問題，必須有通盤的考量，一個微小且看似無意義的失誤有可能會造成重大的影響。

#### (四) 公開演講

- 時間：107 年 6 月 21 日 (四) 10:25~11:05
- 地點：集思交通部會議中心 201 會議室
- 會議名稱：第 30 屆 TWNIC IP 政策資源管理會議暨第一屆台灣網路維運論壇 (TWNOC)
- 演講主題：網路未來的挑戰
- 演講摘要

##### 挑戰 1：政策 (域外適用法規)

從政治層面來看，某個國家/區域的立法會影響到另一個國家/區域，稱為域外適用法規(extra-territorial law)，例如歐盟 GDPR、網路中立性，以及歐盟近日提出的智慧財產權規定等。個人認為這並不是好的發展。

##### 挑戰 2：安全問題

邊界閘道器協定 (Border Gateway Protocol, BGP) 基本上是一種信任制度，訊息在彼此間流通，但是信任鍊橫跨各大洲，缺乏可靠的資源數據，因此，信任鍊成了一個問題，例如我們常看到的域名劫持。

網際網路協會 (ISOC) 目前推廣 MANRS (路由安全共同協議規範)，它的要素是過濾路由和某些數據、反欺騙措施、協調和全球性的路由驗證，強烈建議企業一同加入 MANRS，以發展或加強現有的自發性網路營運規範。

### 挑戰 3：位址 (IPv6 佈署)

Google 測量用戶使用 IPv6 連線的比例，有 47 個國家已經達到 5% 以上，包括 2018 年流量大幅成長的臺灣，但與亞洲國家相較仍低於印、馬、日、泰、越等國。全球第一名是比利時，其原因為比利時政府告訴業者，不論你使用甚麼位址，都要能夠追蹤到用戶，所以業者開始積極佈署 IPv6。另一個影響 IPv6 佈署的因素是企業本身，例如數據中心 Mythic Beasts 向使用 IPv4 位址的用戶收費，使用 IPv6 位址則是免費，導致使用者轉換到 IPv6。因此，是否轉換 IPv6 主要的是法規與費用。

### 挑戰 4：前線佈署 (IoT)

MQTT (Message Queuing Telemetry Transport，訊息佇列遙測傳輸) 是一個輕量、可靠的二進制通訊協定，它的訊息內容很精簡，非常適合用於網路頻寬有限的 IoT 裝置。MQTT 底層是 TCP/IP，所以 IoT 裝置可以沿用既有的網路架構和設備，只是在網路上流通的訊息格式與應用程式的處理機制不同，它的設計是發佈/訂閱模式(Publish/ Subscribe pattern)，能對特定裝置訂閱主題，並盡可能以節省資源的方式確保發送到訂閱的客戶上。

其他保護 IoT 系統安全的方式還包括可參考線上信任聯盟 (OTA)、美國國家標準暨技術研究院 (NIST)，或是美國國土安全部 (DHS) 等單位的安全架構。

但最重要的還是定期更換密碼，以及更新軟體修補程式。IoT 的安全政策與措施應和其他安全系統相容，並要使用最新的軟體與修補程式、使用加密技術，且不要直接將 IoT 裝置連網，而是應先做好安全防護

## (五) 拜會通傳會

- 時間：107 年 6 月 21 日 (四) 15:00~17:00
- 地點：國家通訊傳播委員會 805 會議室

- 與會者：詹婷怡主委、陳耀祥委員、通傳會處室首長與長官、Mr. Paul Wilson、Mr. Fred Baker、陳文生執行長、黃勝雄執行長、吳國維顧問、本計畫同仁
- 會議摘要

本場會議首先由 APNIC 總裁 Mr. Paul Wilson 演說全球 IPv6 發展趨勢。他引用 APNIC 的研究指出，目前全球 IPv6 使用率已從 2014 年的 2.7% 成長為 18%。就經濟體來看，有 20 個國家比全球平均值高，當中又以比利時為第一名 (58.75%)，而八大工業國 (G8) 中也有 6 個達 18% 以上。

但是，Mr. Wilson 也表示，IPv6 使用率高的國家並非都是已開發國家或富足的經濟體，如烏拉圭的比例就高於全球平均值。臺灣目前的使用率為 12%，在過去六個月大幅攀升。東亞國家則仍緩慢發展，包括中國大陸，但預期一兩年內，中國大陸的使用量將大幅增加。

Mr. Wilson 認為，政府對於提高 IPv6 使用率的影響不高，關鍵還是 ISP 的商業考量。接下來的五年，IPv6 使用率會持續增加，業者的相互競爭也會帶動 IPv6 發展，但如果有些業者因為缺乏資金而不去佈署 IPv6，將可能會產生新的數位落差，因此，及早計劃與行動才是上策。

而 Mr. Fred Baker 則是針對通傳會的提問做回覆，主要包括：

## 1. WHOIS 與 GDPR

WHOIS 記載域名註冊者的聯絡資訊，假設沒有 WHOIS，若發生網路安全問題或恐怖攻擊時，要追溯所有者的資訊會很耗時。但 WHOIS 的確與歐盟 GDPR 規範相牴觸，可能的替代方案也許是讓聯絡人自行聯繫提出查詢的一方，這樣一來，個人可識別的資訊不會被這項服務所揭露，而是由被識別的人或公司來揭露，然而這並非是個完美的解決方法。

## 2. IP 分裂化與封包重組

自 1992 年來，IETF 可以找到 2352 個草稿在談分裂化(fragmentation)，顯見 IETF 參與者對此議題十分關心。但越來越多人認為問題應該留在較高的層級去處理，例如傳輸層，讓 TCP (Transmission Control Protocol，傳輸控制協定) 或 UDP (User Datagram Protocol，使用者資料電報協定) 送出較小、且在網路層不具有功能的數據段。IETF 絕對不希望有 IP 分裂化，因為一定會有資訊在傳輸過程中遺失，分裂的封包會造成許多問題。

### 3. 政府分裂化

政府分裂化的確會影響網際網路的完整性，俄羅斯總統普丁想要將.ru 從根區域移除，防止俄羅斯境外的人使用，因此築起高牆，但真正受影響的是被牆關住的人，他們需要兩套系統（俄語和另一個與外面世界溝通的系統），這其實對他們的資金流動和經濟能力是有害的，因此，不建議臺灣以國家安全為由來築起網路高牆。

### 4. 網路自由

如同現實社會，網路世界也會有人濫用我們的自由，我們可以有補償措施，或是去降低發生機率，但是無法完全消滅網路所帶來對個人權力的損害。不過，科技若使用得當，是可以減低這些損害，建議參考的網路安全協定包括相互驗證、DNSSEC、MANRS，這些都可以幫助我們避免走進所謂的網路暗巷，也可以讓我們只和可信任的人溝通。

### 5. IETF 對域名安全的建議

IETF 通常會建議使用 DNSSEC 以及區域簽章(signing of zones) 來加強域名安全，讓 DNS 區域伺服器、遞迴解析器和使用 DNS 資源紀錄者確認是否有簽章的存在，如果有簽章但不能驗證資源紀錄，則不要使用它。舉例來說，A 寫了一封電子郵件，然後產生一組數位簽章，並將該簽名附於信末，之後寄給 B，B 收到信後先利用 A 的公鑰解開該信的數位簽章，B 即可以確定該信的確是來自 A，所以數位簽章可以提供安全性。

## 6. ISP 的網路安全規範

很少有政府或國家級管理機構，要求或命令 ISP 具備特定的網路安全防禦措施，但是可能會採取鼓勵性的方法。ISOC 目前推廣 MANRS，可作為最佳典範，強烈建議政府推動企業加入 MANRS，來改善基礎建設的可靠性和安全性。再者，也要鼓勵企業更重視消費者端的安全性問題，這可以藉由在採購時，就具體指定路由安全的規格來達成。

## 7. 網路安全系統設計

2018 思科網路安全報告指出，採用多家資安供應商的產品或服務似乎更安全，但實際上可能因防護工具彼此不易整合，反而造成更大的危機，因此，使用一致的工具也許會更容易去管理。只是任何一種工具都有它的優點和缺點，所以要使用適切的工具才能發揮它的功用。

## 8. 物聯網安全

線上信任聯盟 (OTA) 的安全架構和美國國家標準暨技術研究院 (NIST) 或是美國國土安全部 (DHS) 是類似的，因此以 OTA 架構來維護物聯網安全是一個好的開始。但最重要的還是使用最新的軟體和定期更新密碼，如果安裝新的裝置，一定要強迫使用者安裝密碼。如果按照架構去施行，基本上可以排除 80% 的問題。

## 9. 多方利害關係人治理方式

每個利害關係人有自己的長處和短處，例如業界最了解科技方面的知識，但是除了行銷以外，沒有足夠權力去影響或推動任何事情；政府雖然有權力，但是經常用在不明智的地方；公民團體在推動某些議題上很有力，但是對於要達成不同目標很難有實質上的進展。因此，不同利害關係人之間沒有高低之分，多方利害關係人機制是迫使大家坐下來聆聽彼此的想法並且產生對話，最後達成某些共識。

## 10. ISO 與資通安全管理法

沒有任何一種國際標準可以保證永遠安全無虞，它只能確認同樣的錯誤不會重複發生。臺灣在 5 月份通過《資通安全管理法》，公務機關每年須訂定資通安全維護計畫，應稽核其所屬或監督機關的資通安全維護計畫實施情形，並訂定資通安全事件的通報及應變機制，建議對於年度資通安全維護計畫必須要做相關分析，例如發生這個等級的事件後，我們做了甚麼反應，以及引起甚麼樣的影響等。

## 11. 網路中立性

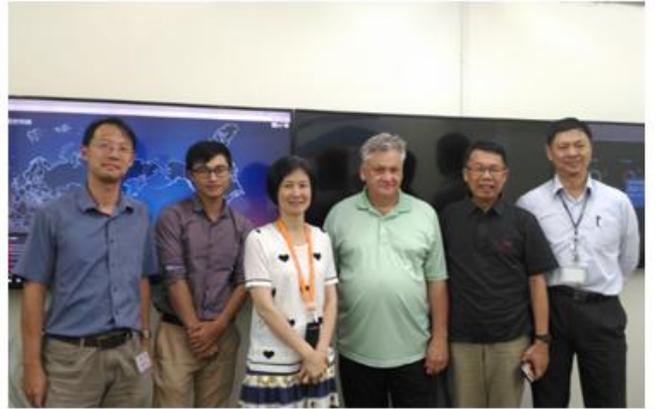
今年 (2018) 美國聯邦通信委員會(FCC) 廢除網路中立政策，其實 FCC 在 2010 年通過的開放網路指令(Open Internet Order) 是正確的，只是錯誤點在於它從 1934 年的通訊法案去做爭論。也因此，原則已經是存在的，只要從正確的法律角度提出論點即可。

### (六) 會議錄影與剪影

#### 1. 會議錄影

本計畫聘請專業攝影師拍攝 Mr. Baker 公開演講 Future Challenges of the Internet 內容。錄影檔可於 YouTube 觀賞，網址為 <https://www.youtube.com/channel/UC9XuqZJU4H0ARFkU8h9wzxxw/videos> (同圖 13)。

## 2. 會議剪影



拜會行政院資安處



公開演講(第 30 屆 TWNIC IP 政策資源管理會議暨第一屆台灣網路維運論壇)



拜會通傳會

圖28. 國際專家 Mr. Fred Baker 訪臺照片

## 二、2018 亞太區網路治理論壇 (APrIGF)

### (一) 會議簡介

#### 1. 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)。

#### 2. 會議資訊

2018 APrIGF (第 9 屆) 於 8 月 13 至 16 日於萬那杜的維拉港召開，主辦單位 (Local Host) 為萬那杜政府資訊總監辦公室 (the Government Chief Information Officer, OGCIO) 與電信與無線通訊監管機構 (Telecommunication and Radiocommunications Regulator, TRR)，共吸引來自 40 多國、超過 300 人實地與會，包括我國亦有十多人出席本次會議。

本次大會主題為「讓亞太區社群建立一個可負擔、包容、開放與安全的網路」 (Empowering Communities in Asia Pacific to build an Affordable, Inclusive, Open and Secure Internet)，座談主題則涵蓋下列六大類別：

- 網路安全
- 線上隱私與保護

- 上網&賦權
- 數位經濟與新興科技
- 多元化
- 多方參與網路治理

APrIGF 的會議型式包括會前入門課程、正式會議、青年論壇、週邊會議等，本年度的正式會議共計 30 場，議程請詳 <http://aprigf.vu/agenda/>，本計畫人員所參與之場次如下表 15 所示。

表 15. 2018 APrIGF 參與場次

主題	場次名稱
會前能力建構	Capacity Building Day for Fellows, General Newcomers & Youth IGF Participants 補助學員、首次與會者、yIGF 學員之能力建構日
開幕	Opening Ceremony 開幕典禮
上網&賦權	Pacific ICT Plenary: Challenges and Opportunities of Connectivity in Small Island States 太平洋 ICT 全體會議：小型島國連線的挑戰與機會
	WS. 94 Empowering Change with Data: Measuring Youth Digital Mobility 以數據促進影響：量度青年數位移動力
	WS. 85 Preparing for Natural Disasters 為自然災害作準備
	WS. 8 Effective eGovernment for Empowering Pacific Citizens 賦權太平洋公民有效的 e 化政府
	Merger 4 Taking Internet Governance to the Masses: Through Communication, Engagement and Capacity Building 透過溝通、參與與能力建構讓大眾了解網路治理
網路安全	WS43. Securing continuity and availability of your IoT, beyond malicious

主題	場次名稱
	hacking 確保 IOT 的持續可用，超越駭客的惡意攻擊
多元化	WS. 30 Responsibilities of Internet Platforms for Tackling Online Abuse Against Women & Other Marginalized Group 網路平臺對女性及其他邊緣團體遭線上辱罵的處理責任
多方參與 網路治理	WS. 4 Sharing Best Practices and Concerns of NRIs in Asia Pacific Region 分享亞太地區 NRIs 最佳典範與疑慮
	Introducing the UN High Level Panel on Digital Cooperation: Mapping Digital Cooperation in the Asia Pacific Region 聯合國數位合作高階小組簡介：描繪亞太區域的數位合作
	WS. 9 AP* 2018 Community Update 2018 亞太區相關社群的最新近況
	WS. 28 Youth Participation Fills in Gaps, Niches Too 青年參與網路治理填補落差及生態環境
	WS. 38 How can we enhance the collaboration between Tech and IGF communities in APAC? 如何促進亞太地區的技術社群與 IGF 社群合作?
線上隱私& 保護	WS. 6 Biomedical Big Data in Asia Pacific Region - Privacy, Public Medical Policy Development and Its Future for the Community 亞太區的生物醫學大數據：隱私與公共醫療政策的發展與展望
	Merger 1 Cross-border Data & Contents Regulation in Asia Pacific Region 亞太地區的跨境資料與內容管制
	Merger 2 Case Studies of Censorship, Surveillance, and Transparency Reporting in Asia 亞洲的審查、監控、透明度報告個案研究
yIGF	Youth IGF 青年網路治理論壇
閉幕	Closing Plenary 閉幕典禮

### 3. 與會人員與目的

本計畫共計 3 人飛抵萬那杜參與 2018 APrIGF，包括吳國維顧問，以及研習營所選拔的 2 位優秀學員。當中，吳國維顧問並主持其中一場座談會議；2 位優秀學員則分別參加一般會議與 yIGF 課程活動。他們此行除了分享臺灣網路治理的經驗、了解亞太地區近來最關切的議題及討論重點之外，2 位優秀學員也從中學習更多的網路治理相關知識，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。

## (二) 重要討論

本屆論壇有不少討論聚焦於太平洋島國的地理文化特殊性所引發的網路議題。本報告從上表 15 本計畫所參與的場次中，摘錄與我國較為相關的重點以提供國內參考。

### 1. 開幕

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

Mr. Masango 介紹聯合國數位合作高階小組 (UN High Level Panel on Digital Cooperation) 的成立目的，是為了加強推動各利害關係人在數位空間的合作，其聯合主席包含阿里巴巴創辦人馬雲，成員則有 Dr. Vinton G. Cerf 等 20 名專家，預計將產出一份具有全球觀點的最終報告。

#### (2) 網路之父 Dr. Vinton G. Cerf

Dr. Cerf 以「未完成的網路」(The Unfinished Internet) 為題發表專題演說。他指出，網路應該能夠提供使用者可負擔的上網費率、商業發展所需的基礎設施、人類終身學習的社會效益、遭遇天然災害時的持續維運等。然而，只談連線問題是不夠的，因為網路發展至今已產生許多問題與挑戰，有賴我們跨越企業、國家的界線，共同努力去面對與解決。這些問題包括

IPv6 的佈署、IoT 的安全隱私與信賴、惡意軟體對自駕車等自動化系統的入侵、不實資訊的散佈等。Dr. Cerf 並強調，我們應該培養思考能力、建立數位素養，而工程師於設計軟體時，也必須拿出倫理道德與責任感。

## 2. 上網&賦權

### (1) WS. 85 Preparing for Natural Disasters

「為自然災害作準備」座談由日本 JPRS 公司(The Japan Registry Services，日本註冊服務公司)申辦，主持人及與談人包括日本技術社群代表、萬那度官員、我國清華大學電機系呂忠津教授、紐西蘭 ISP 業者等。

面對颶風、火山爆發、地震及其所衍生的海嘯等天然災害，日本技術社群代表認為，企業應考量災後的遠距工作環境，以及如何解除電子鎖、如何維持網路與 email 的運作等問題。

在災害監測方面，萬那杜官員表示，他們已將火山及氣象監測的即時資料上網。而研究領域包括以物聯網技術提高主動防災能力的清大呂忠津教授則表示，為了建立防救災警報系統，政府應負責建置及蒐集相關數據，並透過監測資料的開放，吸引產業投入防災技術發展，讓基礎設施與數據的價值達到最大化。

此外，紐西蘭 ISP 業者也呼籲必須正視如何傳遞正確災害訊息的問題，因為災後可能產生網路謠言。他並指出，由於地震發生頻繁，地震通知 APP 可以設定為一定規模以上才啟動通知。

### (2) WS. 8 Effective eGovernment for Empowering Pacific Citizens

「賦權太平洋公民有效的 e 化政府」座談由庫克群島網路行動團體(Cook Islands Internet Action Group)申辦，我國的台灣經濟研究院(以下簡稱台經院)陳映竹助理研究員為與談人之一。此會議將所有的與會者分成「有 e 化政府的一般民眾」、「無 e 化政府的一般民眾」、「政策制定者」三個

組別，各組先進行討論，最後再提出小組報告，其重點如下：

- 「有 e 化政府的一般民眾」組別

該小組所列舉的 e 化政府服務項目包括：

- 新加坡：如停車 APP、記錄人生大事的 Moments of Life，但其代價為放棄部分隱私。
- 日本：部分地區有 J Alert 海嘯警示服務，但仍有錯誤情形；政府草擬政策時，會讓民眾在網路上討論，廣徵民意。
- 臺灣：如實價登錄查詢、eTag (黏貼於車上的國道電子收費系統之電子標籤)、公共政策網路參與平臺等，尤其後者還有修改網路報稅系統等成功案例。
- 澳洲：如開放資訊包含提供鄰居的施工內容，若有意見也能反對鄰居施工；還有醫療資料提供跨院傳輸的服務。

小組成員並指出，既有的 e 化服務項目仍有諸多事項尚待改進。例如民眾不知道有該項服務、資料難以查詢、資料過時、網站的用字遣詞令民眾難以了解、服務不友善 (文件只提供 pdf 檔，必須列印後再手寫) 等。

- 「無 e 化政府的一般民眾」組別

尚無 e 化政府的與會者們所期待的 e 化服務，例如能透過網路辦理出生證明、結婚證明、商業許可證明等。

- 「政策制定者」組別

該小組指出，建立 e 化政府之前，需先釐清服務的對象為誰、提供什麼服務、哪些現有服務可以推動到線上，以及配套資源是否足夠等問題。萬那杜與會者以線上繳稅為例，表示納稅人需要有銀行帳號作為各種支付方式的基礎，但是可能有些納稅人沒有銀行帳戶。不過，也有太平洋某島國官員表示，政府基於國安考量，對於推動 e 化服務會有所猶豫。

### **(3) Merger 4 Taking Internet Governance to the Masses: Through Communication, Engagement and Capacity Building**

「透過溝通、參與與能力建構讓大眾了解網路治理」座談由印度公民團體 CCAOI (The Cyber Café Association of India, 印度網路咖啡協會) 申辦，主持人及與談人包括 ISOC (Internet Society, 網際網路協會)、APNIC (Asia Pacific Network Information Centre, 亞太網路資訊中心) 等技術社群與公民團體代表。

針對如何加強社群參與網路治理，ISOC 亞太辦公室主任 Rajnesh Singh 指出，網路不是只有社群媒體，它已經與我們的生活息息相關，每個人對於形塑網路都能有所貢獻。雖然網路治理對不同族群來說有不同意義，但是每個人的聲音都需要被聽見，而 ISOC 也致力建立多元化的參與，並提供相關的學習資源。

APNIC 主管強調，網路是倚賴建設電塔、衛星等基礎設施才得以形成，APNIC 提供許多技術能力建構課程，讓使用者了解網路的實際運作，也搭起技術社群與使用者的橋梁，讓每一位公民能更有效率地參與公共事務。

ISOC 殘障分會的代表則表示，APrIGF 之類的會議對殘障人士來說，有些難以親近，其原因包括不易抵達會議城市、會場缺乏無障礙設施、討論的議題令人生畏等。因此，如何讓網路更具包容性，以及如何將政策落實，是大家要思考的問題。

## **3. 網路安全**

### **(1) WS. 43 Securing continuity and availability of your IoT, beyond malicious hacking**

「超越駭客的惡意攻擊，確保 IoT 的持續可用」座談由斯里蘭卡的政策研究非營利組織 LIRNEasia (Learning Initiatives on Reforms for Network

Economies Asia，亞洲網路經濟學習改革倡議)申辦，主持人及與談人為 ISOC 代表、荷蘭研究人員、萬那杜官員等。

首先，有關如何提升 IoT 安全，與談人們表示，未來 IoT 產品將比全球人口多，其安全問題可分為直接侵害到使用者的「內部安全」，以及裝置被用來對外攻擊其他人的「外部安全」，因此，IoT 的安全有賴製造者、使用者、政策制定者，三方共同努力。當中，製造端可以採用 OTA (Online Trust Alliance，線上信任聯盟) 的安全架構；使用者則需要製造者及政策制定者提供相關資訊，建立對產品的認知。例如，產品說明書教導消費者修改預設密碼，或是仿照節能產品標示 ABCD 等級，讓使用者在購買產品時可以權衡安全程度與售價高低。不過，也有與談人表示，開發中國家的消費者向來以便宜為優先選擇，此種狀況也應該納入政策考量。

另外，在 IoT 與原始碼相關問題方面，雖然與會者們無法確定 WTO 是否會基於保護商業機密考量，而規定不得檢查原始碼；不過，對於政府是否該檢查 IoT 原始碼，與會者們呈現意見分歧。有些人認為，輸入產品數量眾多，監管機關沒有能力檢查所有的原始碼，因此，應該回歸製造者的自我管制；但也有些人主張，政府對此是責無旁貸。

至於現有 IoT 產品是否多為開放原始碼，與談人們並不清楚目前的產品狀況。不過，他們也指出，使用開放原始碼並不代表安全性就會比較低，例如微軟的非開放原始碼產品也經常遭受攻擊，因此，關鍵還是在於製造公司是否把開放原始碼以對的方式運用在對的地方。

#### 4. 多元化

##### (1) WS. 30 Responsibilities of Internet Platforms for Tackling Online Abuse Against Women & Other Marginalized Group

「網路平臺對女性及其他邊緣團體遭線上辱罵的處理責任」座談由澳洲新南威爾斯大學申辦，主持人及與談人包括澳洲學者、印度與尼泊爾的

公民團體代表等。

澳洲學者表示，言論自由建立於尊重他人的基礎上，而許多騷擾案例凸顯騷擾方的言論自由反而比受害的邊緣團體更多，因此，言論自由不是反對網路平臺進行審查的理由，且平臺審查也不會影響言論自由。

其他的與談人也多認為，平臺業者應該為欺凌辱罵等危害人權的內容，負起責任，從立法層面與實務上的偵測與補救措施，要求平臺業者加強管制仇恨言論。以德國 Twitter 為例，業者所刪除的問題內容往往是轉推而非原始貼文，加上砍掉的帳號也只是虛假帳號，以致成效有限。不過，與談人們也指出，平臺業者也要公開審核標準，避免侵犯言論自由。

至於究竟應該如何要求平臺業者負責，有些與會者認為，民間企業受利益所趨而非正義，平臺業者沒有誘因公開他們的演算法，也無法以國際公約加以約束，加上不同文化脈絡對欺凌（如身體裸露）有不同看法，因此，談論平臺的課責，應根據企業的利害要點進行分析，才有實踐的可能。

## 5. 多方參與網路治理

### (1) WS. 4 Sharing Best Practices and Concerns of NRIs in Asia Pacific Region

「分享亞太地區 NRIs (國家型與區域型 IGF 推動) 最佳典範與疑慮」座談由本計畫吳國維顧問以 TWIGF 名義申辦並擔任主持人，與談人為亞太各國 NRIs 代表。

與談人們首先分享各國 IGF 的辦理情形，其概況如下表 16 所示。

表16. 亞太各國 IGF 辦理概況

國家 IGF	會議形式	資金來源	熱門議題
臺灣	有些國家有全國	有些來自政府，有	假新聞、區塊鏈、隱私

國家 IGF	會議形式	資金來源	熱門議題
日本	性論壇，有些沒有；日本則分為 IGF Japan 與 IGCI 兩個論壇	些來民間企業(如 TWIGF)	假新聞、資料、IPv6
南韓			假新聞、政治介入、AI
紐西蘭			網路安全、線上濫用行為、數位經濟
印尼			數位轉型、數位經濟、數位主權
其他			--

接續則討論 IGF 與國家型 IGF 的核心價值。與談人普遍認同，IGF 是一個讓多方社群溝通對話的好平臺，每個多方利害關係人都是平等的，雖然討論過程費時，最後也沒有產生正式協定，但是網路議題本來就非常複雜，不可能由單一的利害關係人做決定。

不過，也有與談人指出，不能單靠國家型 IGF 來改變世界；再者，過程中也必須有政府的參與，否則就淪為只是一個倡議性的論壇。

另外，有與談人提醒，被聯合國 IGF 秘書處認可的 NRIs，必須是非商業性組織，且論壇的議程須由多方社群共同決定，不能由主辦單位片面主導，所需經費則可尋求企業贊助。對此，吳國維顧問也特別介紹臺灣情況，指出 TWIGF 希望維持其獨立性與中立性，以獲得多方社群的信任，因此，完全沒有政府經費的挹注，且所有經費來源與支出都是公開透明。

至於國家型 IGF 合適採用的溝通平臺，吳國維顧問也提出經驗分享。他表示，雖然很多人對臉書有所疑慮，但是 TWIGF 經嘗試多種平臺工具，並考量當地的使用習慣，最後是以臉書的粉絲社團作為溝通平臺。

## (2) Introducing the UN High Level Panel on Digital Cooperation: Mapping Digital Cooperation in the Asia Pacific Region

「聯合國數位合作高階小組簡介：描繪亞太區域的數位合作」座談係由聯合國 IGF 秘書處代表 Mr. Chengetai Masango，以及網路之父 Dr. Vinton Cerf，兩人共同代表聯合國數位合作高階小組，與與會者進行意見交流。

Dr. Cerf 表示，數位合作需要與法律銜接，並建立常規，例如國家不可干涉網路的公共性。其他與會者則陸續對透明度報告的標準化、封網等議題，提出各自看法，如我國研習營優秀學員周小姐表示，監控議題也需納入數位合作下討論，因為在國家與企業兩種強權的合作下，可能形成國家監控；此外，公民社會的獨立性、公私部門是否達到平權等，也都是多方利害關係人相關主題中，應該探討的議題。

最後，Mr. Masango 將大家的意見彙整成下列 9 大議題，以提供高階小組研議參考，而監控問題，則歸類於隱私與安全大類下的子題。

- 多樣性 (多語言)
- 多方利害關係人 (對話)
- 近用 (費用、頻寬)
- 隱私 (資料永久保存、教育)
- 安全 (斷網)
- 標準與常規 (透明度、可信度與馬尼拉原則)
- 人類發展 (人權)
- 貿易
- 數位會議

### **(3) WS. 38 How can we enhance the collaboration between Tech and IGF communities in APAC?**

「如何促進亞太地區的技術社群與 IGF 社群合作？」座談由日本慶應大學申辦，主持人及與談人包括日本工程師與學生、孟加拉 ISOC 代表、菲律賓資通訊技術部門官員等。

多位與談人表示，政策制定者缺乏技術認知，而技術人員又普遍對政策不感興趣，也不清楚有 IGF 這樣的政策討論平臺，他們傾向以技術解決

問題，也因此，網路政策的制定缺少技術社群的意見。

不過，也有與談人提到，IPv6 佈建即是由技術社群率先推動，而非政策制定。本計畫吳國維顧問則是指出，討論 IPv6 必須從整個生態系統來看，廠商考量的是增加成本能否帶來收益，用戶在轉換期間如果發現跳轉情形也會抱怨，因此，大家應該互相尊重與關心，才能鼓勵技術社群參與交流對話。

其他與會者也建議，將 IGF 會議與技術會議合併辦理，以吸引技術社群參加 IGF，讓不同的利害關係人學習用對方能聽懂的语言討論事情。

## 6. 線上隱私&保護

### **(1) WS. 6 Biomedical Big Data in Asia Pacific Region - Privacy, Public Medical Policy Development and Its Future for the Community**

「亞太區的生物醫學大數據：隱私與公共醫療政策的發展與展望」座談由南韓科學技術院（大學）研究員申辦並主持，與談人包括我國的台灣人權促進會（以下簡稱台權會）何明誼專案經理、台經院陳映竹助理研究員，以及香港資安公司顧問、孟加拉學者等人。

主持人首先指出，許多人沒有察覺自己的健康資料會被日常生活所使用的一些服務記錄下來，如手機軟體、搜尋引擎等，且這些資料被拿來交易或作為商業用途。雖然健康資料的分析也能用於疾病預防、幫助開發中國家改善健康環境等，不過，政府仍應訂定相關法令，保護人民的健康資料與隱私，同時國家之間也要相互合作，共同面對網路安全威脅。

台權會何明誼專案經理表示，臺灣的《醫療法》與《人體研究法》規定，進行人體研究前須取得當事人同意；《全民健康保險法》也規定，健保署執行相關業務時只能蒐集必要資料，並受《個人資料保護法》管制。不過，臺灣並沒有成立個資法的專責單位，而是由行政機關各自認定，以致每個單位的標準不同。例如，健保局在未經國人同意下，便將全國人民

的健保及就醫資料交給學術及非學術單位做研究使用，剝奪人民的資訊自主權，因此，遭到台權會提告。

台經院陳映竹助理研究員則指出，需要教育人民了解誰擁有自己的個人資料，進而學習如何保護個人資料。

香港資安顧問表示，香港也有電子健康紀錄，投保健保者可以同意健保供應商使用其資料，期限為一年但可續約。至於相關資料的研究分析用途，應該是僅限於醫療項目的資料，而非投保者的所有可識別資料。

主持人最後也總結指出，許多國家的醫療資料系統、個資隱私保護法規都尚未健全，有賴各國的多方社群持續努力，促進系統與法規的改善。

## **(2) Merger 1 Cross-border Data & Contents Regulation in Asia Pacific Region**

「亞太地區的跨境資料與內容管制」座談由我國的台經院陳映竹助理研究員以 TWNIC 名義申辦並主持，與談人包括馬來西亞與南韓的研究人員、印度政府資通部門顧問等。

馬來西亞研究員認為，資料的所有權是屬於使用者，而非服務提供者；隨著數位經濟發展，透過立法以保護資料，已是刻不容緩。不過，也有與會者表示，即使完成立法，也無法期待臉書等跨國大企業會遵守太平洋國家的法規。

南韓研究員則列舉近來國際上擴大資料管轄權的法案，如歐盟 GDPR (一般資料保護規範)、美國《雲端法案》、中國大陸《網路安全法》等，尤其後者更直接要求資料必須在地化。印度代表也指出，印度正在討論將資料留在國內的雲端政策，他個人認為，至少備份資料一定要保存在境內。

之後的討論則轉向 IoT 的安全規格問題。與會的德國消保官指出，許多兒童 IoT 產品沒有制定相關標準，從製造到貿易都無從規範。本計畫吳國維顧問表示，IoT 產品若使用便宜的軟硬體將容易被駭，所以，產品在設

計時就應納入隱私保護的考量，政府也應帶頭訂定安全規範；而在國際上，最適合討論 IoT 標準的場域是 IETF (網際網路工程任務小組)會議，近年來 IETF 日益重視隱私議題，也期許更多公民社會成員加入討論。

### (3) Merger 2 Case Studies of Censorship, Surveillance, and Transparency Reporting in Asia

「亞洲的審查、監控、透明度報告個案研究」座談由香港大學申辦，主持人及與談人包括我國的台權會專案經理何明諠、香港學者與業者、韓國公民團體，以及美國學者等。

與談人首先介紹幾個亞洲國家的透明度報告調查結果，例如：

- 香港：通訊監察法規沒有發揮規範政府存取人民網路通訊資料的作用，且政府實施電子通訊監察也缺乏透明度。
- 南韓：業者高度配合政府的撤除內容要求(如刪除扭曲歷史內容)，國營企業、入口網站幾乎是完全配合，其他業者也達 8 成以上。
- 臺灣：索取資料的政府單位主要是警察機關，本地業者對政府要求的配合程度幾乎是 100%，國外業者則為 4 到 6 成。
- 中國大陸：政府結合線下與線上活動，利用大數據分析，對國內外的政治異議者進行監控，同時也透過安全城市計畫對全民監控。如果網路公司沒有遵守政府的審查準則，則會被處罰款或結束營業。

馬來西亞的人權團體代表則介紹一個名為 OONI Probe 的開放原始碼軟體，民眾可以免費下載安裝，以偵測網路連線是否遭到封鎖或審查監視。

最後，與談人們表示，雖然亞太國家中香港、韓國與臺灣的政府會提供監察活動的相關數據，但是對於透明度報告所提出的問題與政策建議，大多沒有處理，因此，也呼籲社會大眾要關切網路審查與監控問題，進而推動法規的調整。

### (三) 結論與建議

#### 1. 減少使用專業術語，降低跨社群的溝通障礙

如何促進技術社群與公民社會參與網路治理的政策討論，是本屆論壇的多個不同場次中，屢次被提及的問題。而與會者們除了提出鼓勵技術社群申辦 APrIGF 座談、秉持相互尊重等建議外，也有人指出，會議中大量使用專業術語與縮寫，已築起參與交流的高牆，而本計畫與會的 2 位優秀學員對此亦感同身受。但其實類似問題於 2017 年 TWIGF 已經被提出。

每個社群本來就有其慣用的語彙與思維，即使是在沒有文化與語言隔閡的國內 TWIGF，不同社群間要以彼此能夠理解的言語，有效地進行網路政策討論，都已是相當不易了，何況是在 APrIGF 這樣的國際場合。因此，未來不論是在國內或國外，多方社群討論網路政策時，都宜儘量減少使用專業術語，避免各說各話，如此才能真正展開溝通對話，為橫跨不同專業領域的網路問題，尋找出最佳的治理方案。

#### 2. 掌握國際趨勢方向，為政策研擬鑑往知來

本屆論壇中各場次對治理議題所提出的主張或建議，有諸多值得我國參考之處。例如，有關網路平臺對於第三方內容責任的討論，凸顯過去賦予網路平臺完全免責的概念，正在逐漸改變，取而代之的是要求平臺業者加強管制欺凌、仇恨等言論的呼聲。至於政府是否該以立法介入的問題，雖然本次會議並未就此特別討論，但從相關報導或分析可看出目前國際上並沒有共識，反對者認為立法會造成平臺業者過度監管而危害言論自由；但支持者主張言論自由不能無限上綱，且社群媒體為了留住客戶並不會進行過度監管。

再如因應自然災害的議題，就有與會者提醒因應網路謠言散佈的重要性。適逢國內近期接連發生災後網路謠言散播事件，例如指稱「蔡總統荷

槍實彈勘災」、「中國大使館安排專車撤離日本關西機場的中國大陸遊客」等，尤其後者甚至引發我國駐外人員輕生的悲劇，因此，如何在災後的第一時間傳遞正確訊息，避免網路謠言不斷地擴散傳播與發酵，應是刻不容緩的課題。

#### (四) 會議剪影



與會者大合照



本計畫吳國維顧問主持座談會議

照片來源：[aprigf.vu](http://aprigf.vu)

圖29. 2018 APrIGF 會議剪影

## 三、ICANN 第 63 次會議

### (一) 會議簡介

#### 1. 會議背景

ICANN (Internet Corporation for Assigned Names and Numbers, 網際網路名稱與號碼指配組織) 為 1998 年於美國加州成立的全球性、非營利、以共識為導向的國際組織，負責網際網路關鍵資源—包括域名系統 (DNS)、IP 位址，以及根伺服器系統 (root server system) 的管理與協調等功能。

ICANN 每年召開三次會議，強調由全球利害關係者參與 (包括政府部門、民間部門、技術社群、網路使用者等)，採取由下而上的共識機制為基礎，制定全球網路管理政策，以促進市場競爭機制，維護全球網路運作之穩定性、可靠性、多元性及安全性。

#### 2. 會議資訊

ICANN 第 63 次會議於 10 月 20 日至 25 日於西班牙的巴塞隆納召開，主辦單位為西班牙經濟暨商務部轄下的國碼註冊管理機構 Red.es，實地與會人數高達 2,360 人。

本次會議為為期 6 天的 ICANN 年度大會，共有開幕、公眾論壇、跨社群論壇、ICANN 內部各社群的會議、各政策制定工作小組會議，以及技術研討會等總計超過 300 場次，當中也包含每兩年舉辦一次的高階政府官員會議 (High-Level Government Meeting, HLG M)，吸引超過 150 名來自世界各國的部會首長與資深官員出席。

本次會議議程請詳 <https://63.schedule.icann.org/>。本計畫參與場次如下表 17 所列。

表17. ICANN63 參與場次

主題	場次名稱
WHOIS 與 歐盟 GDPR	<ul style="list-style-type: none"> <li>•GAC: Overview of WHOIS Compliance with GDPR incl. Report of EPDP Progress</li> </ul> 政府諮詢委員會：WHOIS 遵循 GDPR 綜覽包含 EPDP 進展
New gTLD 政策	<ul style="list-style-type: none"> <li>•GNSO - New gTLD Subsequent Procedures</li> </ul> 通用名稱支援組織 - 新通用頂級域名後續程序 (共 3 場)
政府於 ICANN 角色	<ul style="list-style-type: none"> <li>•HLGM: The Role of Opportunities For Governments in ICANN – Post IANA Transition</li> </ul> 高階政府官員會議：IANA 監管權移轉後政府於 ICANN 的角色機會
ICANN 影響 力	<ul style="list-style-type: none"> <li>•HLGM: The Internet Technological Evolution and the Role and Impact of ICANN</li> </ul> 高階政府官員會議：網路科技的演進以及 ICANN 的角色與影響力
網路政策	<ul style="list-style-type: none"> <li>•HLGM: Global Digital Agenda and Internet Policies</li> </ul> 高階政府官員會議：全球數位議程與網路政策
公共論壇	<ul style="list-style-type: none"> <li>•Public Forum</li> </ul> 公共論壇 (共 2 場)

資料來源：本計畫彙整

### 3. 與會目的

本次會議由計畫吳國維顧問參與，以理解近期 ICANN 所探討的網路治理議題及其討論重點，並提供我國現階段與未來網路治理相關政策參考建議。

## (二) 重要討論

### 1. WHOIS 與歐盟 GDPR

WHOIS 是查詢一個域名或 IP 位址註冊者相關資訊的系統。根據

ICANN 政策規範與合約，每當註冊域名時，註冊者必須提供姓名、地址、eamil、電話等聯絡資訊；而域名管理局則必須提供 WHOIS 公開查詢服務，查詢結果並會顯示註冊者的聯絡資料。因此，WHOIS 被視為違反歐盟 2018 年 5 月 25 日實施的 GDPR（一般資料保護規則）。

為能兼顧符合 GDPR 規範同時保有 WHOIS 服務，ICANN 展開一系列的因應措施，一方面實施臨時條款，對 WHOIS 公開查詢的個資欄位採遮罩處理，另一方面則由 GNSO (The Generic Names Supporting Organization，通用名稱支援組織) 啟動加速版政策發展流程 (Expedited Policy Development Procedure, EPDP)，訂定新的 WHOIS 政策，以在 2019 年 5 月 25 日可以正式啟用。

而在這場 GAC (政府諮詢委員會) 的「WHOIS 遵循 GDPR 綜覽包含 EPDP 進展」會議中，GNSO 說明 EPDP 工作小組將政策制定過程依序分成以下兩個部分：

(1) 確認 WHOIS 服務的 GDPR 法律遵循

先確認存取個人資料的合法事由，並依據列出的事由訂定存取資料的種類。

(2) 訂定取得 WHOIS 資料的措施

依據第三方的存取目的，定義可取得的資料種類，並設計相關認證方式。

GAC 則表示，他們沒有反對 GDPR，但是執法機關的查緝不法工作已經明顯受到影響，EPDP 工作小組與 ICANN 應該尋求解決之道，確保執法機關可以存取 WHOIS 的完整資料。此外，GAC 也指出，現行臨時條款沒有明訂統一的 WHOIS 資料存取模式，且 EPDP 目前的政策規劃可能也沒有包含非公開個資存取模式，這些都會影響執法機關的相關工作，因此，呼籲 EPDP 工作小組設法擴大工作範圍，解決執法機關存取註

冊人資料的相關問題。

## 2. New gTLD 政策

GNSO (通用名稱支援組織) 於 2016 年 1 月成立「新通用頂級域名後續程序政策發展流程」(New gTLD Subsequent Procedures PDP) 工作小組，檢視 2012 年所實施的第一波 new gTLD 開放申請政策是否須進行調整。此工作小組分成 5 個工作主題，分別為整體程序及協助申請、法務／規範／合約責任、字串競爭／反對／爭議處理、國際字元域名／技術／運作、頂級域名使用地理名稱。

本場 GNSO「新通用頂級域名後續程序」會議主要是檢視補充性初步報告 (Supplemental Initial Report) 的內容。ICANN 訂於 ICANN 63 會議結束後發布此份報告，並開始徵求公眾意見。其內容與討論重點如下：

### (1) 字串衝突的最後解決方案：拍賣

報告所列的拍賣方式有公開拍賣、封閉式拍賣、公開招標、隨機抽籤、遞增費用系統等種類。有與會者建議讓申請者自行選擇拍賣方式。至於報告沒有列出的私人拍賣，GNSO 表示，工作小組尚在考慮修正條款內容，規定私下解決字串爭議時，「不允許」某方接受金錢條件而放棄申請。不過，也有與會者認為 ICANN 無權管制自由交易。

### (2) 申請案的公眾意見處理

2012 年的申請程序開放公眾對所有申請案提出意見徵詢，但是沒有如何處理這些意見的相關規定。因此，工作小組認為應建立相關準則，以作為審核委員的評選依據。而與會者也提出應有過濾機器人程式、開放申請者可以回覆所有提問等建議。

### (3) 無法尋得註冊機構

2012 年有部分通過申請的 gTLD 找不到負責營運的註冊機構，此次報

告因此提出由 ICANN 代為選出註冊機構、開放沒有獲得 ICANN 認證的註冊機構提供服務等建議。但是也有與會者對此開放措施表示反對意見。

### 3. 政府於 ICANN 角色

本場高階政府官員會議「IANA 監管權移轉後，政府於 ICANN 的角色機會」主要探討美國商務部於 2016 年 10 月將 IANA (網路號碼指派機構) 監管權移交給 ICANN 後的情勢變化 (如 ICANN 強化既有運作模式與當責機制、政府部門積極投入網路政策立法工作等)，對 ICANN 多方利害關係人運作模式與 DNS 管理等層面的影響。與會各國官員提出的看法如下：

- 巴西

ICANN 為多方利害關係人組織，各國政府不具決策力量，此為 ICANN 獨特之處。雖然參與 ICANN 對政府是一項挑戰，但其涉及議題多元且影響廣泛，因此，各國政府應持續參與，確保其多元化、當責與透明度。

- 比利時

ICANN 有責任確保網路的安全與穩定，它建立聚集多方利害關係人的獨特模式，我們應確保此治理模式持續發揮效用，而且比利時對此模式也很滿意，但仍希望 ICANN 加速改革，並強化 GAC 各成員國的合作。

- 加拿大

加拿大認為多元化、包容與共識決，是多方模式的關鍵原則，而 ICANN 正是以此模式確保網路的開放、安全與相容。如今 GAC 需要繼續與 ICANN 社群合作，以確保遵循 GDPR 並合法存取非公開 WHOIS 資料、推動 New gTLD 未來政策。透過 ICANN 政策發展，我們影響全球網路與未來社會。

- 歐盟

ICANN 是多方治理模式的典範，IANA 監管權的轉移證明此模式的成功。但我們也應該了解，公共政策不是各國政府的專屬責任，雖然各國政

府擁有制定法規的最終權力，但是公共政策對所有社群都有直接的利害關係。因此，各國政府需要和技術及其他社群緊密合作，瞭解各社群的觀點和專家意見。

#### 4. ICANN 影響力

本場會議「網路科技的演進，以及 ICANN 的角色與影響力」為高階政府官員會議，各國政府代表提出的意見如下：

- 美國

安全是美國的最高原則，美國持續在網路安全與隱私議題上努力，以強化企業與大眾對網路的信心，也因此，美國堅持要求 ICANN 社群建立允許合法存取 WHOIS 資料的政策。WHOIS 是執法機關打擊不法與保護消費者及智慧財產權的重要工具，所以，應該允許出於這些目的的合法使用。此外，ICANN 章程亦承諾維護並強化網路的穩定與安全，世界應該信任 ICANN 對網路發展所作出的決策，並透過參與 ICANN 實現我們加強連結與保護數位創新文化的共同目標。

- 日本

網路衍生的新興科技如 AI，將是未來經濟與社會發展的關鍵，但是這些新興科技仍然必須依賴穩定且自由的網路才得以發揮效用，因此，未來 ICANN 的重要性勢必會提升，且日本也支持 ICANN 的多方治理模式。

- 歐盟

歐盟正啟動下世代網路的政策研究，希望藉由技術與合作，打造一個由網路使用者全權掌控、一個以人為本的網路環境。此外，GAC 應該討論如何與其他多方社群密切合作，以推動良好的網路發展。

- 德國

德國強烈支持多方治理模式，因為它是維持網路穩定、開放、安全的

推動力。而為了進一步支持多方治理模式，德國申請主辦 2019 年聯合國 IGF，並確定於 2019 年 11 月在柏林舉行。此外，ICANN 第 69 次會議也將於漢堡舉辦，誠摯歡迎大家熱烈參與。

## 5. 網路政策

本場會議「全球數位議程與網路政策」為高階政府官員會議，各國政府代表提出的意見如下：

- 德國

德國政府日前成立數位化內閣委員會，由首相梅克爾擔任主席一職，主要工作為訂定 AI 國家發展策略、數位政策架構等。此外，也建議政府與業界、學界、公民社會及年輕世代積極交流，廣納各界意見。

- 法國

法國主辦 2018 年聯合國 IGF，本屆大會主題為網路信任，而且法國也支持世界資訊社會高峰會 (WSIS) 主張的多方治理模式。

- 中國大陸

中國大陸將持續追蹤 G20 數位經濟發展暨合作措施，以提升寬頻發展，同時加強投資創業及電子商務，提升網路包容性，並與全世界合作。此外，也會持續發展數位經濟的潛力，包括提倡 AI、大數據等新興科技。

- 英國

ICANN 的多方治理模式將公民社會、企業與政府聚集在一起，為共同目標而努力，是多方治理模式的最佳典範。另一方面，全球至今仍有 50% 人口未連接網路，這是 ICANN 所有多方社群應該正視的議題。

- 日本

日本政府的角色是建立開放安全的網路，其 5 項準則為確保資訊自由

流通、法治、開放、自動化、推動多方治理模式。目前日本政府正推動社會 5.0 計畫，可望解決全球暖化、勞動力不足等問題，而當中網路與 AI 系統將是重要的助力。

- 我國

面對數位經濟發展所伴隨的挑戰，建議政府主動為創新工業提供協助、與所有多方社群合作以確保所有人能從數位經濟中平等獲利、與 ICANN 等國際組織合作以共同建立網路及數位經濟政策。ICANN 主責全球網路安全、穩定及彈性，其政策影響全球的數位經濟發展，因此，ICANN 會議是所有政府相互交流與學習的最佳場合。

## 6. 公共論壇

公共論壇開放所有人向 ICANN 董事會提出與 ICANN 相關的任何問題、評論或建議，提問者不限資格。以下針對 ICANN 此次會議的兩大議題 -- WHOIS / GDPR、new gTLD 政策，摘錄與會者的提問、ICANN 董事的回覆，以及多方社群代表的相關回應。

### (1) WHOIS 與歐盟 GDPR

來自瑞典的國家警察表示，他的職責為處理兒童色情犯罪，過去藉由 WHOIS 循線追查不法份子的資料，如今卻因 GDPR 實施而影響調查進展，因此，詢問統一存取模式的推出時程。

ICANN 執行長暨總裁 Göran Marby 答覆指出，ICANN 並非 WHOIS 資料的管理者，無權提出統一的存取模式，但是會持續向歐洲資料保護局 (Data Protection Authorities, DPA) 尋求法律遵循意見，以提供社群制定相關政策的協助。

還有註冊服務商也就此發表看法。他認為統一存取模式是個好辦法，但是實施難度高，因此，建議 ICANN 社群持續改進相關的流程與技術。

## (2) New gTLD 政策

包括域名系統維運商、註冊管理機構、品牌受理註冊團體等單位都陸續問及有關下一輪 new gTLD 的開放申請時程。他們指出，上一輪的開放決策於 2008 年就獲得董事會通過，但卻直到 2012 年才正式實施；目前已接獲十多個單位有意申請第二輪 new gTLD，但政策進展緩慢，因此，建議董事會允許採用 2012 年的申請指南進行申請。

ICANN 執行長暨總裁 Göran Marby 答覆表示，董事會正在等待政策發展流程 (PDP) 的完成，一旦 PDP 準備就緒並提交給董事會，他們將迅速給予回應。

ICANN 董事 Avri Doria 也表示，申請流程的許多機制尚未建立，董事會正與相關社群討論後續流程，希望儘可能完成各項準備工作，縮短時間落差，以確保 PDP 完成並獲得董事會通過後，就能立即開放申請作業。

## (三) 結論與建議

### 1. 積極參與 WHOIS 新政策討論，確保兼顧我國權益

歐盟 GDPR 生效迫使 ICANN 實施臨時條款，隱蔽 WHOIS 查詢結果的個資相關欄位，以致許多國家政府代表在多場不同會議中，一再重申執法單位對合法存取非公開 WHOIS 資料的強烈需求，甚至連第一線的警察人員都現身說法，凸顯 WHOIS 議題的重要性與迫切性。目前 ICANN 社群正推動制定新法，討論如何在符合 GDPR 前提下，持續提供 WHOIS 的公開查詢與非公開存取服務，其重點涵蓋合法的使用目的、可存取的資料種類、認證方式等細節。

WHOIS 議題的國內主要多方社群包括我國 GAC 代表的交通部郵電司、對 WHOIS 有直接使用需求的調查局與刑事局、須履行 ICANN 合約提供 WHOIS 服務的.taipei 註冊管理局及其註冊服務商 (.tw 為頂級國碼域名，

雖然沒有強制性的履約問題，但.tw 也有提供 WHOIS 服務)，以及代表網路使用者與捍衛個資保護的公民團體等。建議國內多方社群先凝聚共識，釐清我國的實務面需求與公共利益，並在未來幾個月積極參與 ICANN 新政策訂定的討論，以確保 2019 年 5 月 25 日所實施的 WHOIS 新政策能兼顧我國權益。

## 2. 多方治理模式廣獲支持，鼓勵國內援用發展網路政策

本次會議適逢舉辦兩年一度的高階政府官員會議，吸引超過 150 名來自世界各國的部會首長與資深官員出席，且在多場不同主題的高階政府官員會議中，包括我國與歐盟，以及比利時、加拿大、日本、美國、德國、法國、英國等，都公開表示支持 ICANN 與多方治理模式，凸顯 ICANN 在後 IANA 時代的地位更加穩固，以及多方模式治理網路的國際潮流。

誠如歐盟官員所言，雖然各國政府擁有制定法規的最終權力，但是，公共政策攸關所有利害關係人的權益，因此，政府需要聽取多方社群的意見並相互緊密合作。而就參與 ICANN 角度，除了上述的 WHOIS 新政策制定外，第二輪的 new gTLD 開放政策，亦有賴國內多方社群共同研議，以做為我國參與 ICANN 的政策立場。雖然我國於第一輪 new gTLD 開放時，只有申請並通過 .政府、.taipei、.acer、.htc 等 4 個頂級域名，且最後只有 .taipei 實際營運。不過，由於事隔多年，面對國際新一輪的開放政策討論，還是應該重新了解國內多方社群的需求與意向，避免揣測臆斷即形成決策。

#### (四) 會議剪影



開幕典禮 ICANN 執行長致詞



開幕典禮與會者



公共論壇臺上的董事會成員



公共論壇會議與會者



公共論壇排隊發言的與會者



亞太區社群會議

照片來源：ICANN

圖30. ICANN 63 會議照片

## 四、2018 聯合國網路治理論壇 (IGF)

### (一) 會議簡介

#### 1. 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。

#### 2. 會議資訊

第 13 屆 IGF 於 2018 年 11 月 12 日至 14 日於法國巴黎召開，主辦單位為法國政府，會場設於聯合國教科文組織 (United Nations Educational, Scientific and Cultural Organization, UNESCO) 總部，共計有來自全球 143 國、超過 3,000 人與會，遠端參與人數也約有 1,400 人。

本次大會主題為「網路信任」(Internet of Trust)，討論主題涵蓋下列八大類別：

- (1) 網路安全、信任與隱私
- (2) 發展、創新與經濟議題
- (3) 數位包容與連網

- (4) 新興科技
- (5) 網路治理的演進
- (6) 人權、性別與青年
- (7) 媒體與內容
- (8) 技術與維運

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。本年度共計 171 場會議，議程請詳 <https://igf2018.intgovforum.org>。本計畫人員參與場次如下表 18 所示。

表 18. 2018 IGF 參與場次

主題	場次名稱
開幕	Opening Ceremony 開幕典禮
網路治理的 進展	WS. 224 The Past, the Present and the Future for Multi-stakeholderism 多方利害關係主義的過去、現在與未來
	WS. 388 Making National Laws Good for Internet Governance 建立有益於網路治理的國家法律
	OF. 20 Technological Innovation and Internet Governance Rules 科技創新與網路治理規則
新興科技	OF. 21 What future for the Internet? 網際網路的未來是什麼?
	WS. 11 AI Ethics: privacy, transparency and knowledge construction AI 道德：隱私、透明與知識建構
技術與維運	WS. 306 Game Over IPv4: The need of IPv6 for the future of games IPv4 時代終止：網路遊戲的未來需要 IPv6

### 3. 與會人員與目的

本次會議由本計畫吳國維顧問參與，除了擔任「多方利害關係主義的過去、現在與未來」與「AI 道德：隱私、透明與知識建構」2 場座談的與談人和主持人之外，同時也可以了解全球近來最關切的網路治理議題及其討論重點，並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

### 1. 開幕典禮

主辦國法國總統、聯合國秘書長及 UNESCO 總幹事皆出席本次論壇並發表致詞。致詞重點如下：

- UNESCO 總幹事 Audrey Auzulay

數位與 AI 革命所帶來的挑戰需要全體國際社群來共同面對，我們必須解決網路科技所衍生的問題，包含世界連網人口的不平衡、網路所造成社會與性別的不平等，以及網路騷擾與仇恨言論等，UNESCO 會尋求聯合國體系成員的支持，展開國際對話，一起捍衛我們所身處的數位世界。

- 聯合國秘書長 Antonio Guterres

在這具挑戰性時代，要將數位風險轉換成數位機會，IGF 必須與時俱進，以跨領域專家經驗來制定政策、建立共有語言與關係來重新架構現有問題，並加強弱勢族群與發展中國家的聲音。IGF 不能侷限於會中的討論，更需要產出政策與規範性框架來創造更大的影響力，不能讓市場力量這雙無形的手來決定我們的命運，期許與會者能以創新方法來增強網路信任。

- 法國總統 Emmanuel Macron

網路正遭受來自犯罪份子、極端主義、獨裁政權等濫用的嚴重威脅，以正確且創新方式來規範網路已經刻不容緩，需要有包含所有利害關係人在內的新形態多邊合作，因此，法國政府提出《巴黎籲請信任與安全的網路空間》(Paris Call for Trust and Security in Cyberspace) 倡議，並已獲得來

自政府、企業與公民團體的超過 370 份簽署；而且法國政府還將派遣團隊進駐 Facebook，共同打擊仇恨言論，這是前所未見的實驗性創舉。此外，IGF 不該僅限於討論與思考，而是應該改革成為能夠提出具體建議的機構。

## 2. 網路治理的演進

### (1) WS. 224 The Past, the Present and the Future for Multi-stakeholderism

「多方利害關係主義的過去、現在與未來」座談由南韓科學技術院 Ms. Yeseul Kim 主持，與談人包括歐洲網路治理論壇 (The European Dialogue on Internet Governance, EuroDIG) Ms. Sandra Hoferichter、前 ICANN 董事 Mr. Markus Kummer、Mozilla 基金會研究員 Mr. Ayden Férdeline，與本計畫吳國維顧問。

與談人普遍支持多方利害關係人(以下簡稱多方) 主義的網路治理發展。吳國維顧問表示，公開透明是多方主義的核心價值，如同民主制度一樣，雖然並非完美或能解決現今所有問題，但卻是目前處理網路治理議題的最佳方式。尤其現今許多跨國企業在當地營運面臨適法性挑戰(如 Uber 載客服務)，因此，政府在制定政策前，應該聽取多方利害關係人的聲音。

不過，Mr. Férdeline 質疑多方主義的代表性與問責性，認為其政策並非依據實證而制定、過程十分耗時沒有效率，且特定的利害關係人擁有較大權力，以致難以產出公平且公正的結果，如果再不加以改善，政府的權力會越來越重，最後淪為被多邊主義模式接管。因此，建議要平衡多方社群的權力、具備有效的爭議解決流程，以及提升績效表現。

其他與談人則強調，多方模式並非一個靜態完整，而是動態發展中的模式，我們需要持續觀察它自然發展成一個更成熟的形式，而且 IANA (網路號碼指派機構) 監管權的成功移轉也展現此模式對民間社會的開放，因此，現在論定多方模式終將失敗，或注定將被政府法規吞噬，仍猶言過早。

## (2) WS. 388 Making National Laws Good for Internet Governance

「建立有益於網路治理的國家法律」座談由貝魯特社群媒體交流 (Social Media Exchange) 共同創辦人 Jessica Dheere 主持。與談人包含荷蘭外交部資深政策官 Ms. Lisa Vermeer、阿根廷言論自由和資訊取得研究中心 (CELE) 研究員 Ms. Agustina del Campo 等人。

Ms. Vermeer 指出，近年來網路相關立法往往為了加強網路安全、打擊網路犯罪、對抗假新聞與不實訊息等因素，而壓制人權，或是核心決策與立法缺乏一致性，因此，我們應該重新檢視人權，並與政府合作改善問題，以確保立法的合宜性，避免抄襲不良法規。Ms. Santos 則分享巴西的案例，她表示為了維護人權，巴西公民團體透過由下而上的方式，提出一項隱私權法案，且已經成功地獲得立法頒布。

與談人們並討論法規制定過程，以及國家或區域性法規的跨境實施問題。Ms. del Campo 提及網路法規涉及不同部會權責，但大家立場不同，有賴加強協調才能提出和諧的法規。還有臺下與會者讚揚歐盟 GDPR 的制定過程完善且透明，但是，也有與會者從商業角度提出不同看法，認為對跨國企業實施域外適用法規，有時候會造成傷害，如增加法律遵循的成本，反而不利中小型企業的發展。

## (3) OF. 20 Technological Innovation and Internet Governance Rules

「科技創新與網路治理規則」開放論壇由中國大陸國家互聯網信息辦公室主辦，與談人包括中國網絡空間研究院副院長李欲曉和相關學者、APNIC 總裁 Mr. Paul Wilson、亞太頂級域名協會 (APTLTD) 總經理 Mr. Leonid Todorov，歐洲網路治理論壇 (EuroDIG) 共同創辦人 Mr. Wolfgang Kleinwächter，以及巴西 ISOC 副總裁 Mr. Demi Getschko。

中國網絡空間研究院學者表示，現今急需各國分享經驗與加強對彼此的了解，以建構互信的網路世界，由中國大陸舉辦的世界互聯網大會即是

以此為目的，並反映網路為社會國家發展帶來的機會與挑戰，中國大陸也希望更積極參與全球數位發展，並相信每個國家應該決定適合自己的網路治理模式。

Mr. Wilson 稱讚甫結束的世界互聯網大會有良好成果，但是在開啟對話上仍有很大的進步空間，網路開放、封鎖與國家干預等議題仍鮮少被討論，仍缺乏一個能完全信任的對話空間來辯論網路治理議題。

Mr. Todorov 認為，現今的網路治理方式有西方、中國與俄羅斯等三種，但是都無法提供新穎的想法，大多只是對過去的解決方法進行微調而已，他同意聯合國秘書長的看法，未來我們需要更多跨領域的合作。

Mr. Kleinwächter 指出，目前討論的網路主題多為帶有技術成分的政治與社會議題，純技術問題已被政策制定問題所取代，這也引起新的網路治理混亂，建議採用更全面性的方法來檢視普世價值。

幾位臺下與會者則是讚揚中國大陸主辦本場開放論壇，並期盼印度與巴西能效法辦理。最終大家也一致同意網路治理需要更公平開放的討論。

### 3. 新興科技

#### (1) OF. 21 What future for the Internet?

「網際網路的未來是什麼？」開放論壇由歐盟主辦，與談人包括歐盟下世代網路倡議 (Next Generation Internet initiative, NGI) 首長 Mr. Olivier Bringer、歐盟網路未來小組的主任 Mr. Pearse O'Donohue，以及歐洲數位權利協會的 Ms. Maryant Fernández Pérez。

Mr. Bringer 介紹歐盟的下世代網路倡議 (Next Generation Internet initiative, NGI) 是重新想像規劃，建構一個開放、包容、透明、合作的網路，一個健全且去中心化、保護個人資料與隱私的網路，使其成為互通且以人為中心的生態系統，而歐盟也將開發符合這些價值的技術來達成目

標。

Ms. Pérez 提出，對未來網路的想像應該聚焦於信賴與可靠性，因此，首先需和科技巨頭溝通，著手解決許多問題的源頭，也就是網路企業的操縱模式。對此，Mr. Bringer 回應表示，NGI 考量使用者的隱私需求會日益漸增，所以，不僅會試圖找出科技替代方案，也促進更安全、永續的平臺來推廣網路的互通與包容。

## **(2) WS. 11 AI Ethics: privacy, transparency and knowledge construction**

「AI 道德：隱私、透明與知識建構」座談由 APNIC、英國諾丁漢大學、中國大陸清華大學等共同主辦，本計畫吳國維顧問主持，與談人由法國政府代表、中、英學術界代表，以及企業代表所組成。

中國大陸交通大學與清華大學的與談人指出，中國大陸的 AI 研究與發展著重於製造與智慧財產權，因此，強項為 AI 應用，但道德規範則顯得薄弱。對此，英國諾丁漢大學與談人表示，IEEE（電機電子工程師學會）提供政府規範 AI 的建議，而且歐盟與聯合國高階 AI 專家小組也都正在研擬明確的道德規範。

中國微博代表則是分享微博防止網路謠言與假新聞的 AI 系統。他表示，微博開發一個網頁讓使用者回報謠言，也建立使用者信用系統，若使用者的謠言指數太高，他的發言權會被限制。而 Google 與談人表示，改善機器學習的公平性問題，有賴多元化的小組成員共同合作，建立共有的道德規範與框架，因此，Google 今年已推出 AI 的指導原則。

最後，法國國家訊息與自由委員會 (CNIL) 代表分享法國 2017 年的研究報告，歸納演算法與 AI 產生的道德問題有 4 個層面，包括依賴 AI 而失去責任感與控制力、偏見歧視與排他的產生、個人化服務對社群與連線的影響、AI 隱私權與龐大數據引起的挑戰。報告並建議 AI 的道德考量應以

人道主義的觀點為基礎，並要促進公平性。

### **(3) WS. 227 Blockchain for Social and Humanitarian Application**

「區塊鏈在社會與人道主義的應用」座談由巴西學術界的代表所主持，與談人包含技術社群、政府、民間企業、公民團體等多方利害關係人的代表。

與談人們首先分享區塊鏈技術的應用案例，例如印度有藉此促進慈善資金分配透明化的計畫、泰國則是用於解決沒有銀行帳戶民眾的金融交易問題，以及聯合國運用區塊鏈技術追蹤難民動向並提供相關援助等實例。

值得關注的，還有對抗不實訊息的應用案例。來自歐洲國家的技術社群代表指出，美國已有公司著手開發以區塊鏈貨幣經濟為基礎的新聞平台，讓新聞報導免於受到政治與商業廣告的外力介入，並藉由社群成員（讀者）的自律與代幣獎勵機制，促進公平客觀的新聞報導與資訊傳遞。其主要運作方式為社群成員（讀者）可以透過加密代幣直接贊助新聞室<sup>10</sup>；反之，也可以針對偏頗報導發動投票要求關閉該新聞室，一旦得票率超過 50%，該新聞室就會喪失在此平台的執照，且其代幣將會轉贈給發動投票及參與投票的社群成員（讀者）。

不過，與談人們也強調，區塊鏈並不是解決網路問題的萬靈丹，使用之前還是必須進行適當的評估。

## **4. 技術與維運**

### **(1) WS. 306 Game Over IPv4: The need of IPv6 for the future of games**

「IPv4 時代終止：網路遊戲的未來需要 IPv6」座談由 NIC.br (Brazilian

---

<sup>10</sup> 此位社群代表只有說明讀者懲罰新聞室的機制，並未提及讀者亦可獎勵新聞室，此部分係參考境周 2018/4/12 「[擺脫被臉書操控的命運 區塊鏈將成新聞業救星?](#)」報導，以呈現該平台的雙向制度設計。

Network Information Center，巴西網路資訊中心)主辦，與談人包含技術社群、民間企業與政府等多方利害關係人的代表。

技術社群代表表示，許多遊戲平臺尚未採用 IPv6，雖然 CGNAT (Carrier Grade Network Address Translation，電信級網路位址轉換器) 暫時紓解 IPv4 位址枯竭問題，但是每個遊戲玩家都需要 IP 位址，最好的辦法還是要求 ISP 業者與線上遊戲平臺採用 IPv6。不過，有另一位技術社群代表指出，小型 ISP 業者根本不知道如何轉換成 IPv6，且終端用戶的家用路由器沒有預設 IPv6，這些都是線上遊戲業者所面臨的連線問題。對此，有民間企業代表建議對遊戲開發商與網路營運商實施再教育，針對採用 IPv6 的重要性與如何付諸行動進行訓練。

此外，多位與談人表示，IPv6 的性能比 IPv4 強，能夠更快速地取得內容，提供終端用戶更好的使用經驗。他們並認同處理 IPv6 相關問題時，使用多方利害關係人取向是重要的，讓 ISP 業者、線上遊戲產業與政府一起進行討論，可能比強制要求移轉至 IPv6 還有效率。

不過，也有巴西研究人員認為 IPv6 缺乏關鍵性應用，且移轉成本太高，以致難以推行。本計畫吳國維顧問特別就此分享臺灣經驗，指出自從今年臺灣電信業者開始啟用手機的 IPv6 預設連網後，臺灣 IPv6 滲透率已從大約 0.5% 飆升為 24% (2018 年 9 月)，全球排名從六十多晉升為前十名，凸顯手機即是關鍵性的應用，而且支出成本並沒有大幅增加，何況目前 IPv4 售價已經高達每個 15 美元，因此，建議大家從手機的啟用來推動 IPv6 移轉。

### (三) 巴黎公報 (主題結論)

繼 2017 年 IGF 首度於會後發布日內瓦公報 (Geneva Message)，提供該年度 2 個高階主題場次與 6 個主場次的重點結論之後，2018 年 IGF 也於會後發布巴黎公報 (Paris Message)，將 2 個高階主題場次、8 個主場次，以

及 71 個座談討論，彙整成 8 個主題的重點結論，作為本次會議的非約束性原則。以下為摘要簡介，詳細的結論建議可至 <https://www.intgovforum.org/multilingual/content/igf-2018-key-messages> 下載。

### 1. 網路安全、信任與隱私

網路安全至關重要，唯有安全可靠的網路空間才能產生並維持網路的信任。但是網路安全問題隨著新興科技發展而日益複雜，涉及許多不同的層面與利害關係者。本主題針對信任與利害關係人合作、網路外交、資料隱私與保護、演算法、物聯網 (IoTs)、仇恨言論、法律與規範等議題，提供相關建議。例如：多方社群的誠心合作可以在不破壞網路開放自由的情況下，解決隱私與安全問題；了解演算法對人類生活、人權、隱私等層面的風險與影響，有助於找出合適的技術與政策解決方案。

### 2. 發展、創新與經濟議題

如同在 2030 聯合國永續發展議程中所提及的，網路與 ICT 在促進發展上變得日益重要，不但是發展基礎建設的重要因素，更有大幅加強各面向發展的潛能。而隨著社會與經濟試圖駕馭網路的力量，有關發展策略必須是包容、公平、透明，以及考量潛在風險與意外結果的呼聲也越來越多。本主題針對未來工作、永續發展、基礎建設與融資、多方利害關係人取向的數位發展等議題，提供相關建議。例如：經常檢視演算法等科技的應用，相互交流最佳典範與可行的立法框架；大數據的應用應考量發展跨國的治理架構等。

### 3. 數位包容與連網

網路是促進包容的利器，但若沒用在正確的方向，容易導致數位排除，加深各種形式的數位落差。雖然數據顯示連網的費用持續下降，而且全球有超過 70% 的人口已生活在行動網路的範圍內，但是不同的數位落差仍然存在。本主題針對網路接取、數位包容與弱勢族群、社群網絡

(networks)、網路中立、線上教育與數位能力發展等議題，提供相關建議。例如：針對數位包容的根本原因與重要性，需有更多樣的政策觀點；建構多方利害關係人流程必須有跨部門、跨領域的整合方式；使用新科技尋找、了解與處理新的跨世代的議題等。

#### 4. 新興科技

AI、5G、區塊鏈與物聯網能為社會、文化與經濟帶來益處，但治理問題也隨之產生。新興科技大量依賴網路連線，有足夠的人力、物力投入在基礎建設上才能讓新興科技得以繼續發展。本主題針對人工智慧、區塊鏈與加密貨幣、道德等議題，提供相關建議。例如：要使新興科技能服務全人類與促進以人為本的數位化，必須有健全、永續與資訊流通的政策引導；在新舊科技的轉換時期，兩者能互通及相容是必須考量的策略之一；政策趕不上科技，且單一管轄框架下無法規範跨國大企業，因此必須省思「規則是由誰定義」的問題。

#### 5. 網路治理的演進

網路治理問題複雜，有賴多方利害關係人共同參與以找出有效的解決方案。本主題針對擴大利害關係人參與、IGF 的組織與角色、多方利害關係人主義等議題，提供相關建議。例如：IGF 應從國家層級來強化多方社群參與，改善 IGF 在地方、區域與全球的知名度；多方模式必須快速進化，可藉由交流最佳典範等方式協助；網路跨越國界的特性造成管轄與立法的挑戰，而多方模式正是克服此問題的有效方式。

#### 6. 人權、性別與青年

性別不平等必須與其他社會議題(如階級、種族與地域的不平等)共同檢視，AI 演算法衍生的資料監視與偏見也要從性別的角度來審視。本主題針對性別平等、兒少網路安全、民主與數位公民權、難民、青年包容等議題，提供相關建議。例如：超越傳統性別二元性去討論性別議題；性別分

析必須是整體倡議計畫的一部分，並非僅是附加的工作；提高利害關係人對維護兒少網路安全的認知與敏感度；線上社群應建立有效的自治系統，以實現言論自由和線上民主發展。

## 7. 媒體與內容

網路科技對傳播或分享知識的方式產生革命性的變革，不同媒體傳播各式內容，改變人們的想法，左右社會發展方向。如何面對媒體的負面影響與不斷變化的數位內容更顯重要。本主題針對媒體文化與權力、資訊混亂、「假新聞」、選舉和政治過程、在地內容與多語言主義等議題，提供相關建議。例如：政府偕同企業和媒體組織處理媒體與權力來源的關係；由記者和媒體社群（如無國界記者）採取措施來緩解不實訊息的擴散；監測和管理大數據的使用等。

## 8. 技術與維運

網路的基礎建設、路由與協定問題是網路應用層的基礎。然而，以善為出發點的立法，如封鎖非法網站，可能對網路基礎建設造成嚴重意外結果。本主題針對域名系統、網路路由和協定、內容封鎖與過濾、網路中立等議題，提供相關建議。例如：處理有害網路內容需要對話、合作與合法程序；以多方利害關係人取向解決網路立法相關問題；由營運商、監管機構、公民團體和學術界持續對話，以將網路中立應用在 5G 環境。

### (四) 結論與建議

#### 1. 追隨國際議題趨勢，正視 AI 治理挑戰

本屆 IGF 與 AI 相關的座談場次多達十餘場，主要討論 AI 對未來社會的影響、演算法的公平性等道德問題，以及個資與隱私保護等議題，並且提及許多先進國家已經展開訂定 AI 道德規範、發展治理架構等研究，凸顯 AI 治理的重要性。目前我國 AI 相關計畫主要由科技部與教育部主管，研究

內容著重技術領域的開發與應用，對於政經社會文化的研究投入相對有限，因此，我國也應正視 AI 治理問題，調整相關計畫的分配比重或增加新計畫，以追隨國際網路治理的議題發展趨勢，及早因應 AI 即將帶來的治理挑戰。

## 2. 多方取向廣獲肯定，鼓勵我國政策發展公開透明

本屆 IGF 有多場會議論及網路治理的取向(方式)。儘管中、俄等國與會者經常批評多方取向缺乏效率與結果，並宣揚由政府管控的網路主權模式。不過，多方取向(方式)仍然普遍被視為是目前治理網路的最佳方式，因此，建議我國政府訂定網路相關政策時，過程中秉持多方取向(方式)的核心價值--開放與透明，廣納建言並明確答覆各界提問，才能找出最佳的解決方案。

### (五) 會議剪影



圖片來源：IGF 直播影片

圖31. 聯合國 IGF 會議剪影

## 伍、結論與建議

### 一、人才培育

#### 1. 四成錄取者放棄學員資格，如何鼓勵社會參與仍待努力

本次研習營活動提供全程參與的學員（不含公務人員）新臺幣 3 千元整獎學金（TWNIC 支付），以及 2 個出國參加國際會議的名額，作為吸引各界報名並參與活動的實質誘因。

從報名人數 98 人，以及甚至接獲中國大陸的博士研究生來信詢問能否報名並給予交通補助來看，活動訊息獲得相當程度的傳遞。

不過，就實際參與人數而言，經通知聯繫 35 名正取與 10 名備取學員後，最後出席者只有 6 成（27 人），意即高達 4 成（18 人）錄取者放棄學員資格，且當中有 15 人是正在放暑假的大專青年學子。即使是與工作業務相關的公務人員，亦有類似情況，報名成功後又放棄者亦超過 2 成（9 人報名，7 人出席，5 人全程參與）。

以上凸顯，即使在提供實質獎勵誘因下，要讓多方社群與青年學子投入偏向社會參與及貢獻的網路治理，仍屬不易，也有學員表示撥冗 4 天參與的困難。因此，如何鼓勵更多人參與網路治理仍待進一步研議與努力。

#### 2. 大專學員背景知識較為不足，未來課程可採分級並做延續性規劃

本次研習營活動共有 34 名學員出席，包括 16 名大專青年與 18 名多方社群（包含公務人員）。課程進行中，可發現大專青年因為對網路治理議題與 ICANN 事務的背景知識較為不足，以致在議題的分組討論及 ICANN 模擬會議等課程，較無法做深入討論與角色扮演。雖然當中因素也和颱風來襲課程從 2 日縮減為 1 日有關，但是學員間的程度差異性仍然存在，因此，未來或可將課程分成入門與進階，讓有需要的學員先上入門課程，然

後再一起參加進階課程，以增加互動討論的有效性與整體學習成效。

此外，本次研習營活動為第一年舉辦，在籌辦時已考量銜接參與 TWIGF、優秀學員參與 APrIGF，並於 APrIGF 會後舉辦分享交流會議。而未來需進一步將單一活動所聚集的學員能量與熱忱，做延伸性的規劃，讓學員可以持續且長久地參與網路治理。

### 3. 追隨人才培育國際趨勢，於大專院校開設學分課程

網路治理需要學有專精的專業人才投入，才能針對政策議題和多方社群進行深入的討論與交流。然而，這些專業知識涵養並非短天期訓練活動一蹴可幾，而是有賴正規且長期的學校教育才得以奠定基礎。因此，國際上已有許多大專院校開設網路治理學分課程，我國教育部等相關部會也應考量提供誘因，鼓勵國內大專院校開辦此類課程，以培育我國網路治理的專業人才。

國際上的大專院校網路治理課程案例如挪威奧斯陸大學 (University of Oslo) 法律系所「網路治理」碩士課程、日內瓦高級國際關係學院 (The Graduate Institute in Geneva) 跨科系「網路治理與經濟學」碩士課程、瑞士蘇黎世大學 (University of Zurich) 傳播與媒體研究系所「全球網路治理」碩士課程及「網路與全球政治」學士課程、馬爾他大學 (University of Malta) 國際關係研究系所與 Diplo 基金會共同合作的「網路治理」當代外交碩士課程等。

## 二、議題分析與多方參與

### 1. 借鏡歐盟以多方程序循序漸進治理內容，法規介入僅為最後手段

對於網路上各種不當內容的氾濫，歐盟首先將問題區分為違反既有法規的線上「違法內容」(如仇恨言論、恐怖主義等)，以及有問題但不違法的「不實訊息」(過去稱為「假新聞」)，並從 2015 年即展開多方社群的溝通

對話。歷經無數的會議與論壇討論、對公眾與執法機關及網路平臺業者進行意見徵詢，以及召集專家工作小組研議政策等方式，目前歐盟於對抗「違法仇恨言論」，主要是推動行為準則，以敦促業者於 24 小時內將仇恨言論刪除；立法介入的部分，則僅限於有立即性安全威脅的線上「恐怖主義內容」。至於打擊不違法的「不實訊息」，則採取業者自律、強化媒體識讀、建立獨立事實查核網絡等多管齊下措施。

近來我國也準備著手因應網路上的不實訊息／假消息／假新聞等相關問題，目前行政院正在盤點國內相關法規與行政措施，而立法院也已有修法的提案。雖然我國面臨的情境與問題和歐盟有所差異，但是，若能參考歐盟從開始到整個過程中，都持續有多方社群的參與，且循序漸進地發展相關政策，對於問題範圍的釐清與定義，應能發揮相當助益，進而共同集思廣益，找到最佳的總體政策方向，以及完整有效的因應措施。

## 2. 歐盟會員國不易落實《著作權指令》，政策規劃須兼顧各方權益

歐盟《著作權指令》以第 11 條的連接稅制度，與第 13 條的上傳過濾機制，最為關鍵。前者看似對出版商有益，但是目前尚無成功的商業模式，而且對臺灣的出版業者、著作權所有權人，或閱讀者，影響程度都是有限。而第 13 條的上傳過濾機制，由於目前國際大型網路平臺多已建置，因此，短期內對網路市場的影響不大。不過，臺灣網路業者多為中小型業者，要導入上傳過濾機制的建置與營運成本相當高，對網路新創公司而言亦是負擔，其結果可能是著作權所有權人尚未獲益，網路業者先蒙其害。因此，臺灣的中小型或新創網路業者，如果目標市場是在國內，可以待市場成長後，再逐步導入經濟可行的技術。

而在法規設計構面，歐盟《著作權指令》飽受網路社群的質疑與批評，政策規劃者除了考量保護著作權所有權人的權益外，也需評估保障私有權利所投入的公共成本，並且必須兼顧閱讀者權益。即使如歐盟這樣的先進社會，本法案仍然難以取得全體利害關係人的共識，未來可能面臨各會員

國不易落實的情境，值得作為臺灣著作權相關法規設計時的借鏡與參考。

### 3. 從動態發展中尋求我國最佳多方治理模式，把握公開公平原則

法國總統馬克宏提出美（加州）、中兩國以外的第三種網路治理模式，也就是「調合創新與公共利益的歐洲模式」。美國與歐盟都是以多方取向（方式）來治理網路。長期以來，網路的發展因為網路源自美國的歷史性因素而由美國主導，並向全球灌輸「網路有其特殊地位，不能以國家通訊傳播與貿易政策加以管理」概念，而這也符合美國的政治與經濟利益（Huston, 2018）。不過，隨著網路發展成為攸關國家競爭力的關鍵、美國退出國際網路治理領導角色、網路遭到各種勢力的濫用等演變，歐盟轉向對網路空間祭出越來越多的管制措施。

然而，不論是美國或歐盟模式，他們的主張不一定符合我國的利益或處境。因此，我們應該密切關注歐美多方模式的變動，並透過國內多方社群討論，找出對我國最合宜的多方模式。惟多方取向（方式）固然有開放參與及過程公開透明的優點，但同時也常遭到缺乏效率、各多方社群權力不平等抨擊，而國際間也仍在持續尋求改善之道。所以，我國於援用多方取向（方式）時，宜預先保留較長的政策發展時間，過程中也要注意不同社群的平等參與，且對所有提問都應有明確答覆，儘可能做到公開與公正。

### 4. 參考美國資訊自由流通等網路政策主張，惟我國立場應由多方討論

對於資訊自由流通與個資隱私保護，美國政府積極推動 APEC「跨境隱私保護規則體系」（CBPR），以避免各國因為實施不同保護措施而阻礙跨境電子商務發展；美國商務部的公開意見徵詢結果亦顯示，美國多方社群普遍反對限制資料自由流通的相關措施。

我國已獲准成為 CBPR 成員，而且美國所主張的保護基本人權與言論自由，亦是我國與西方民主國家向來所要捍衛的民主價值。不過，美國網路治理發展的主責單位為商務部，其首要之務為促進美國網路經濟發展；

又誠如美國網路協會（代表美國主要網路公司的工商組織）所指，「限制言論與資訊自由流通，會阻礙美國網路業者進入當地市場；反之則能讓美國網路業者在國外自由運作」，凸顯美國上述網路政策主張的背後，具有強大的國家產業經濟利益考量。

每個國家的經濟利益甚至是公共利益，都有其獨特且複雜的政經社會文化考量，以致近來我們看到歐盟的網路政策發展已經和美國漸行漸遠。因此，儘管美國的網路政策主張具有相當參考價值，但是我國的網路政策立場，仍然應該透過多方取向（方式），由我國的多方社群共同討論決定，如此才能找出最符合我國公共利益的政策立場。例如，在本計畫的「資料在地化座談會」上，與談人們論及此政策可能對我國帶來政經面的負面衝擊，但是有些資料（如醫療保健）又有在地化需求，因此，相關問題仍待多方社群做更深入探討，無法一概而論或全盤接受美國或其他國家的立場。

## 5. 俄羅斯另建網路系統可行性低，維持現有系統符合我國最大利益

俄羅斯號召其他金磚國家建立一個獨立、替代性、只由他們專屬共享的網際網路，以合力擺脫美國對全球網際網路的控制權。不過，這項工程面臨的技術或限制，可能遠超過我們的想像。其所面臨的第一個問題，就是如何確保替代性網際網路的網域名稱資料，與現有的網際網路資料一致。一旦發生資料不一致時，就會造成無法解析及無法上網的情況，這將對建構在上層的電子商務與網路服務產生重大損失，極可能對數位經濟造成難以估計的衝擊。

替代性網際網路投入的計畫規模龐大，帶來的商業價值卻極其有限，甚至造成重大經濟衝擊。考量我國整體資通訊基礎建設成長軌跡，維持現有全球一致的網際網路發展方向，不僅符合我國產業與社會的最大利益，更能發揮我國資通訊產業優勢，在完整的全球資訊架構下，建構我國資通安全與國家安全。

### 三、國際參與及交流

#### 1. 積極參與 WHOIS 新政策討論，確保兼顧我國權益

歐盟 GDPR 生效迫使 ICANN 實施臨時條款，隱蔽 WHOIS 查詢結果的個資相關欄位，以致許多國家政府代表在多場不同會議中，一再重申執法單位對合法存取非公開 WHOIS 資料的強烈需求，甚至連第一線的警察人員都現身說法，凸顯 WHOIS 議題的重要性與迫切性。目前 ICANN 社群正推動制定新法，討論如何在符合 GDPR 前提下，持續提供 WHOIS 的公開查詢與非公開存取服務，其重點涵蓋合法的使用目的、可存取的資料種類、認證方式等細節。

WHOIS 議題的國內主要多方社群包括我國 GAC 代表的交通部郵電司、對 WHOIS 有直接使用需求的調查局與刑事局、須履行 ICANN 合約提供 WHOIS 服務的.taipei 註冊管理局及其註冊服務商 (.tw 為頂級國碼域名，雖然沒有強制性的履約問題，但.tw 也有提供 WHOIS 服務)，以及代表網路使用者與捍衛個資保護的公民團體等。建議國內多方社群先凝聚共識，釐清我國的實務面需求與公共利益，並在未來幾個月積極參與 ICANN 新政策訂定的討論，以確保 2019 年 5 月 25 日所實施的 WHOIS 新政策能兼顧我國權益。

#### 2. 追隨國際議題趨勢，正視 AI 治理挑戰以因應數位衝擊

2018 IGF 與 AI (人工智慧) 相關的座談場次多達十餘場，主要討論 AI 對未來社會的影響、演算法的公平性等道德問題，以及個資與隱私保護等議題，並且提及許多先進國家已經展開訂定 AI 道德規範、發展治理架構等研究，凸顯 AI 治理的重要性。

此外，美國商務部於 6~7 月所進行的「未來國際網路政策優先議題」意見徵詢，亦詢問美國多方社群對未來新興科技看法。美國商務部認為，未來幾年網路治理的焦點將是 AI 對社會與經濟的衝擊、自動化與網路新商

業模式對勞動市場的改變等；而美國多方社群的回應也強調，NTIA 應該鼓勵這些新興科技朝向負責、道德的方向發展。

行政院已推出「臺灣 AI 行動計畫 (2018-2021)」，以帶動我國未來經濟發展邁向新階段為目標。我國對於新科技的發展，向來偏重經濟產值，鮮少關注它對整體社會所帶來的挑戰，而這次似乎也不例外。隨著國際網路治理會議對 AI 與自動化的討論日益熱絡，我國也應該著手展開相關研究與討論，除了在消極面避免發生某部會因為不察網路時代的國際政策趨勢而被批評為「無知與失職」的憾事外，在積極面更是應該透過及早規劃與準備，以帶領我國因應未來數位轉換的衝擊。