

# 財團法人台灣網路資訊中心因公出國人員報告書

108 年 7 月 30 日

報告人姓名	陳映竹	服務單位及職稱	國際事務委員會委員
出國期間	108 年 7 月 15 日 至 108 年 7 月 20 日	出國地點	俄羅斯海參崴
出國事由	<p>自 2017 年起即擔任亞太區網路治理論壇的多方利害關係人小組成員，本年度以國際事務委員會委員職務出席 APrIGF 2019。</p> <p>今年度同時也擔任兩場工作坊的與談人，並參與今年度的獎助金研究員師徒計畫，與其中三位研究員，針對 APrIGF2019 中數位經濟相關的議程進行討論。</p> <p>本報告書內容：</p> <p>壹、出國目的</p> <p>貳、考察、訪問過程</p> <p>參、考察、訪問心得</p> <p>肆、建議意見</p> <p>伍、其他相關事項或資料</p> <p>(內容超出一頁時，可由下頁寫起)</p>		
授權聲明欄	<p>本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。</p> <p>授權人：</p> <p>(簽章)</p>		

附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。

## 目錄

壹、 出國目的 .....	1
一、 本年度會議簡介.....	1
貳、 考察、訪問過程 .....	4
一、 能力建構日(7月16日).....	4
二、 主要議程日(7月17日至19日).....	7
(一)7月17日 .....	7
(二)7月18日 .....	11
(三)7月19日 .....	15
參、 考察、訪問心得 .....	19
一、 跨國提案合作經驗.....	20
二、 實體國界的限制與網路無國界 .....	21
三、 照片使用與個人資料、隱私保護的爭議.....	22
肆、 建議意見 .....	23
伍、 其他相關事項或資料.....	24

# 壹、出國目的

自 2017 年起即擔任亞太區網路治理論壇的多方利害關係人小組成員，本年度以國際事務委員會委員職務出席 APrIGF 2019。

今年度同時也擔任兩場工作坊的與談人，並參與今年度的獎助金研究員師徒計畫，與其中三位研究員，針對 APrIGF2019 中數位經濟相關的議程進行討論。

## 一、本年度會議簡介

在 2018 年 2 月時，俄羅斯與中國皆提出要主辦 APrIGF 2019 會議之計畫書，由於俄羅斯主辦方 TLD RU 協調中心(Coordination Center for TLD RU)在提案準備上較為完整，同時會議地點也屬於遠東地區，考量中國政府對於網路及言論的嚴格監控，可能對於會議直播參與、線上討論、會議文件傳遞等相關作業不易進行，最後多數人選擇將會議辦於簽證申請不易但設備、網路相對方便的俄羅斯遠東聯邦大學(Far Eastern Federal University，簡稱 FEFU)，主辦單位同時也建議參與者可以住在學校的宿舍群中，並提供機場與校園、市區旅館的接駁巴士，每日提供獎助金研究學員、青年網路治理論壇(Youth IGF)參與者早餐及會議餐點。

本年度的 APrIGF 會議主題為「Enabling a Safe, Secure and Universal Internet for All in Asia Pacific」，並在這個主題下設六個子題：(1) Safer Internet, Cybersecurity & Regulation、(2) Access & Universality、(3) Emerging Technologies & Society、(4) Human Rights Online、(5) Evolving Role of Internet Governance & Multi- Stakeholder Participation 和(6) Digital Economy。

亞太地區幅員遼闊，東亞、南亞、太平洋國家地區的經濟與網路發展不同，但共同的目標都是希望能藉由網際網路相關科技來帶動經濟發展，同時也希望注意個資保護與網路安全議題。

本年度共有 60 個提案，其中包括歐洲著名的智庫 Friedrich

Naumann 基金會也有參與提案。經由議程委員會審核內容、時程安排後，選出 22 個提案，分別安排在三天的主要議程中，由於網路安全還是大家所關心的議題，除了往昔討論網路安全外，本年度也討論了常規、道德、規定、法律等差異性，同時也討論新興科技與資料控管的安全相關議題。在主要議程的前一天安排能力建構日 (Day 0, Capacity Building Day)，提供第一次參與 APriGF 的參與者，能藉由參與能力建構日了解此次的會議主題與討論方向。

表 1 此次入選的工作坊題目

Sub-Theme	Accepted Workshops
<b>Safer Internet, Cybersecurity &amp; Regulation</b>	(1) Child-led research on promoting safer Internet from children’s perspective (2) Protection of Child Online: Importance of Child Safety Complaints Tools (3) Localized Internet: Two Sides of a Coin (4) Cyber Norms in Asia-Pacific (5) A roadmap for studying ICT laws and building a database for Asia (6) Know Your Net – Working Together to Address Internet Security and Standards (7) Digital Security at the Grassroots: Emerging needs and challenges (8) Coping with misinformation in an era of information deluge: Who is Responsible?
<b>Access &amp; Universality</b>	(1) Honey, I shut the internet! Dealing with internet shutdowns in Asia Pacific (2) Universal Acceptance: Opportunities and Risks for Asia-Pacific &

Sub-Theme	Accepted Workshops
	<p>Universality of the Domain Name System (DNS)</p> <p>(3) The Future of Digital Identity and Human Rights</p> <p>(4) Language Diversity in Asia-Pacific: Challenges towards Digital Dividends</p> <p>(5) Community Networks – Connecting the Hardest Half</p> <p>(6) Sharing IPv6 Deployment Experiences among Asia Pacific Countries</p>
<b>Emerging Technologies &amp; Society</b>	<p>(1) The Ethics behind Computing Machines: Raising Awareness of Digital Talents</p> <p>(2) IoT Security – A Differentiator for Consumers</p> <p>(3) Parallel Workshop: Build Concept on AI and Society for good Global</p> <p>(4) Can we apply “multi-stakeholder approach” for governance of crypto assets?</p>
<b>Human Rights Online</b>	<p>(1) Online Resistance Movements and Political Organising Against and Countering Hate Speech in Asia</p>
<b>Evolving Role of Internet Governance &amp; Multi- Stakeholder Participation</b>	<p>(1) Analyzing Perspectives on Youth Participation in the Multi-stakeholder Landscape: A Contextual Follow-Through Session on Motivations to</p>

Sub-Theme	Accepted Workshops
	Sustainability Efforts
<b>Digital Economy</b>	(1) Big tech everywhere: Is this the future of the Internet? (2) Is e-Government an effective mechanism for developing economies

## 貳、考察、訪問過程

因海參崴當地人多不使用英文，為避免獨自一人夜間搭計程車至遠東聯邦大學，所以提前於 15 日自臺灣出發，於仁川機場轉機至海參崴，再搭乘接駁巴士至遠東聯邦校園，也配合接駁巴士時間，自 19 日至海參崴出發於仁川機場轉機返臺。

### 一、能力建構日(7 月 16 日)

能力建構日是為了讓第一次參與 APrIGF 會議的人們能理解網路治理論壇的進行方式、該次會議討論的主題與內容、討論的方向。每年會稍微改變進行的方式。本年度由 MSG 的主席 Rajnesh Singh 開場，向大家簡單介紹本年度的大會主題，同時也提醒大家在拍照上傳至社群網站時，必須取得被拍攝者的共識。由於俄羅斯是歐洲國家，所有參與者皆受到歐洲資料保護規範 (General Data Protection Regulation, 簡稱 GDPR) 所保護，所以在相關照片使用、可辨識的個人資料上，大家都格外注意。

本次將獎助金學員依照子題分為六個群組，並由不同的 Mentor 導師所帶領，所以由六個主題的導師分別簡短地分享本年度的研究方向。由於今年帶領三位獎助金研究員於數位經濟議題，所以也準備了數位經濟議題中，配合本年度也探討了如何讓每個人都能取用網路、安全的討論，關於資料使用、資料保護、資料經濟，歐盟相關法規與

歐洲地區境內希望資料能自由流動的相關議題外，同時也提到亞洲區的亞太經濟合作會議 (Asia-Pacific Economic Cooperation, 簡稱 APEC) 的 Cross Border Privacy Rules System (簡稱 CBPRs)，是期望在保護隱私的框架下能使資料自由流通。

歐洲與亞洲都清楚資料的流通與再使用都能促進經濟發展，但歐盟設置了嚴格的 GDPR，各國也提出相對應的個人資料保護法、隱私保護法、網路安全或資訊安全的相關法律，雖然可以保護消費者、網路使用者個人資料的安全性，但目前也缺乏統一的標準，這些有可能造成新創企業及新科技發展上的阻礙。

同時本年度太平洋國家延續去年電子化政府的提案，今年也有電子化政府的討論，所以政府的數位轉型是否對國家經濟發展產生影響，同時也建議大家多討論應該是要讓科技發展領先於政府法律制定？還是政府法律應該要在科技發展前設下限制？

不過因為時間限制，加上多數參與者後來多在討論關於性別參與、網路取用性的相關的議題，因此只簡單介紹主題方向。

之後則由網路治理生態系中的主要組織與相關單位，讓他們向第一次參與者介紹這些組織在網路生態系中的主要負責工作；今年也安排了去年在聯合國網路治理論壇(簡稱聯合國 IGF)成功提案的 Mariko Kobayashi 教大家如何成功提案，與國際提案時需要注意在講者聯絡上的相關議題。由於時區、個人網路使用習慣、網路安全與隱私保護尺度的不同，國際提案會遇到相當多的挑戰，聯合國 IGF 在議題上的需求會比區域性的需求更具全球性，同時也會有不同的議題考量。

大會同時安排了 MSG 成員之一的 Leonid Todorov，與大家分享如何製作殺手級的簡報，避免大家過於依賴投影片，忽略了網路治理論壇裡最重要的是與現場參與者的互動，也不需要製作太多投影片，避免讓參與者因缺乏互動而缺少參與感，也因為此次的分享，多數工作坊都是以圓桌會議的方式進行，讓大家有更多的討論與互動，較少使用投影片的時間。

同時也安排了中國的薛紅教授，與大家討論電子商務行為中的消

費者保護。在場的參與者與薛教授的互動中，有不少關於中國政府對於個人資訊的控管、監控及與亞洲其他國家之間的互動提問。

16 日的最後一個活動，安排導師們與獎助金研究員們之間的互動。獎助金研究員們必須參與這些工作坊，並寫下自己的心得與觀察，在 APrIGF 2019 結束時，會安排一個段落，讓每個子議題的研究員們會有代表上台分享五分鐘的感想。原本有一位是屬於 Emerging Technologies & Society 組的研究員要更換至 Digital Economy，但由於該子議題今年有四場工作坊，有四個研究員，而 Digital Economy 議程僅兩場工作坊，有三個研究員，為了工作的負擔均衡，該位研究員也接受建議留在原本 Emerging Technologies & Society 組中。

Digital Economy 本次的研究員有三位：

- (1) **Ananya**，來自印度的學生，專業領域於研究賽局理論、財務金融與經濟，同時參與過今年 ICANN 64 神戶會議，認為需要以經濟學的角度來看整個網際網路生態體系與制定網路政策。
- (2) **Mira**，來自印尼的程式設計人員，對於數位經濟有興趣，也有參與過 APNIC 會議。
- (3) **Rose**，來自菲律賓的電信公司。此次參與 APrIGF 2019 主要是擔任其中一場人權與數位身份證的講者。

在 APrIGF2019 開始前一星期，我們四人便已透過即時通訊軟體建立群組溝通，在討論到「網際網路是否應該為公共財？」的議題時，有較多的爭論，尤其是若網際網路若屬於公共財，那麼基礎建設的服務商、網路服務供應商、內容供應業者，是否也不應該收費？那又如何創造數位經濟？在經過討論後，認同網際網路就像是公用事業 (Utilities)，如水、電一樣，使用者需要付費使用，以維持相關事業的正常營運。

我們也談到了歐盟的 GDPR 與歐洲資料流通的資料經濟，由於資料的使用與保護在數位經濟發展中占有重大的地位，但資料不流通也無法藉由研究資料來取得資訊，如何避免資料外洩或是個資被侵犯，

也是一門學問。Rose 提到菲律賓已經有 Data Privacy Act 資料隱私法案，保護個人可辨識資訊(Personal Identity Information)，也提到在 2016 年 5 月選舉時因為選舉委員會(Commission on the Elections，簡稱 Comelec)的網站資料庫遭受攻擊，所以造成 5500 萬筆登記選民資料外洩的情況，也造成至少 2000 萬名菲律賓人民的損失，所以儘管資料在經濟發展中具有重要性，但也要兼顧人民個資與隱私保護。

之後我們也選出了在 APrIGF2019 閉幕式時，由 Anaya 和 Mira 上台分享這三天會議中的心得，由於之前有建立線上討論群組，所以我也請這三位研究員不要只侷限在數位經濟的議程，只要是自己有興趣的議程就去參加，有問題可以線上討論或是和我在同一議程時可以一同討論。

## 二、 主要議程日(7 月 17 日至 19 日)

### (一)7 月 17 日

本日主要議程是早上的開幕式及參與下午的議程。

#### ● Opening Ceremony

俄羅斯聯邦對於多數網路使用者而言，有著相對嚴格的網路監管其網路協調中心主任 Andrei Vorobyev 表示，俄羅斯對網際網路的監管是從 RuNet 作為全球互聯網一部分的立場出發的，並認為透過這樣的方式接觸國際社會，制訂相關的網路策與全球通用技術標準。

其中一位致詞者 Vladimir Solodov 是薩哈(雅庫特)共和國的總理，與大家談論了在俄羅斯聯邦也有著不同的網路發展程度，有些地區的網路建設可能不足，而人口密度也十分低。

今年的 APrIGF 也邀請了聯合國 IGF 秘書處的計畫經理 Chengetai Masango 與大家提到今年將在柏林舉辦的第 14 屆聯合國 IGF，同時也提醒大家關於今年 APrIGF 的主題、產出的文件對聯合國 IGF 的重要性。

在多數的長官向參與者表示歡迎後，現場有一個小型的座談活動，

邀請不同國家的參與者一同討論「Internet Governance in Asia Pacific: The State of Play and Outlook」在這小型的座談會裡，可以快速的了解網路治理在亞太地區不同國家的發展程度，有的國家可能積極的強化其他網路安全、網路事件應變團隊的組成；有些國家，如印度政府主導性較強，多數民眾對於「網路治理」較缺乏認知；有些國家正在努力的推廣由下而上的網路治理討論機制，同時也在強化青年網路治理人才的教育，除了讓他們擁有相關道德的覺知外，也讓他們可以在未來加入網路治理的討論。

在上午的開幕式結束後，APrIGF 2019 活動正式開始。

#### ● **WS14. Know Your Net – Working Together to Address Internet Security and Standards**

以往類似的內容可能是會在 Day 0 的能力建構日討論，但今年議程委員會將活動稍微調整，同時 ICANN 也對該議題進行提案，所以這部份也移至議程中，同時也有機會與俄羅斯的參與者一同討論。由於俄羅斯屬於歐洲國家，所以他們對於歐洲 IP 網路協調中心(Réseaux IP Européens Network Coordination Centre, 簡稱 RIPE NCC)比較熟悉。本場次的提案人是 ICANN 亞太地區的 Joyce Chen 同時擔任主持人，三位與談人則是 APNIC 的總監 Paul Wilson 和網際網路學會(Internet Society, 簡稱 ISOC)的 Naveed Haq 及透過遠端參與的 ICANN 亞太地區的經理 Champika Wijayatunga。

較不同於其他的議程可能偏向人權、政策的探討，這個場次是屬於純技術性的講座，從網域名稱伺服器、IPv4 與 IPv6、網際網路路由(Routing)的安全性探討。

同樣是討論網路安全，我們較熟悉的網路安全可能是在使用者端(企業機房、網路設備、終端消費者)，但在更基礎層部份，包括負責全球域名分配的 ICANN 建議大家在購入域名時，也需要考量域名的註冊商是否有提供域名系統安全擴充(Domain Name System Security Extensions, 簡稱 DNSSEC)；全球 IP 位址發放的五大網路註冊中心

(APNIC、RIPE NCC、ARIN、AFRINIC、LANIC)則都建議大家趕快改用 IPv6，不僅速度較快、位址數目也夠，也較安全；ISOC 則是建議電信商與 ISP 業者使用資源公鑰基礎設施(Resource Public Key Infrastructure，簡稱 RPKI) 與加入 Mutually Agreed Norms for Routing Security(簡稱 MANRS)，在路由資訊交換時也能提高安全性。

同時也討論到了最近 Firefox 和 Google 都預備開始支援 DNS over HTTPS (簡稱 DoH)的服務，用意是為了保護使用者的隱私，避免在域名解析時，被竊聽者竊取或修改使用者的資料，但這也有可能導致駭客透過這樣的服務進行不當的攻擊或造成網路安全的威脅。

在大家簡短的自我介紹之後，大家分為三組進行討論，我則參與了 DNSSEC 推廣的討論。在討論之後，三組則派代表報告該組的結論。在 RPKI 與 MANRS 的討論中，則是建議政府多鼓勵網路服務業者使用這些服務與協議，可以增加安全性並增加彼此的信任程度；而 IPv6 的推廣上，由於許多國家和業者仍不願意更換到 IPv6，而末端消費者並不了解 IPv6 所帶來的好處，所以應該要讓消費者承擔部份的責任，讓他們了解到 IPv6 的好處後，反過來向服務提供者要求他們從 IPv4 更換為 IPv6，

由我上台分享在 DNSSEC 的推廣上，有三個結論：(1)歐洲地區的經濟程度發展不一致，所以可能無法兼顧網路安全與經濟發展，在預算有限的情況下，可能會先選擇網路基礎設施的硬體布建，其次再考慮安全的相關支出。(2)網路服務提供業者在面臨域名加上 DNSSEC 時，多半還會考量到成本因素，對於中小企業而言，可能不會想要多花這樣的成本，同時他們可能也不了解 DNSSEC 在域名保護上的重要性，對許多業者來說，DNSSEC 也許有可能會影響到其網路執行的速度，就算已經縮短至僅有秒數的延遲，但對於某些產業，如期貨業者，可能就會有重大的影響，所以可能會選擇網路速度，而不願加入 DNSSEC。(3)大型的科技公司或是網際網路服務商也許該承擔這樣的責任，並不是說大型科技公司付費提供使用者使用，而是由他們來倡導使用者使用 DNSSEC 來增加安全性，例如先前 Google 便公開表示

若是業者沒有在網站中使用 SSL 加密，不但會在 Chrome 的網址列上顯示不安全，同時也會降低其搜尋引擎結果的排名。這樣的公告引發了許多業者為自己的網站增加 SSL 加密，也能增加一般瀏覽者的隱私與安全性。

最後再由 Joyce Chen 做出總結：(1)政府是否應該要立法或是強制規定業者去使用這類的網路安全或是配合這些網路標準，雖然有很多人會倡導 Security by Design 的觀念，但網路安全應該是屬於基礎的，而不是透過設計的；(2)不止是一般業者、消費者，大型科技公司也應該負擔起宣導的責任，提供較安全的網路使用環境。

由於這部份的資訊較不容易到一般消費端，所以多半會在技術性質較高的政策論壇討論，但也很難得的藉由這樣的機會與 RIPE NCC 的人、遠東大學國際關係學院的副院長一起進行討論。

## ● **WS30. The Ethics behind Computing Machines: Raising Awareness of Digital Talents**

這個場次主要是討論對於在科技快速發展的情況下，如何讓青年數位人才擁有关于道德(Ethics)的認知。在現場的與談人則是先討論了是否能在學校讓老師、教授、在文件上讓學生們有相關的道德認知。

但最主要的是，亞太地區多是以法規、法令來限制程式設計師，且法律制訂者、程式設計人員並不會彼此對話，這也造成了相當大的認知落差。對於政府、法律制訂者多數習慣由上而下的管制，同時就民眾的習慣，也相當依賴政府管制，而不會有所謂的 Social Norms 產生。與談者也提到，如果由政府來制訂 Norms，就如同法規，而不是 Norms，同時有許多政府官員在遇到仇恨言論、被認定是不當的內容時，就會採用斷網(Internet Shutdown)，甚至異想天開的認為阻擋 IP 就可以阻擋這些不當的內容。然而斷網會造成嚴重的網路經濟傷害，可能為了阻斷 20%的不當言論，同時也阻斷了 80%的正常內容，影響了這 80%的用戶。

多數人在現場會認為 Ethics 是可以透過學校教育而內化在學生心

中的，然而當程式設計人員在進入職場後，他們是需要配合公司以營利為導向的工作任務，但許多程式設計人員在工作時，並不是只有「寫程式」而已，不少程式設計人員也會去查詢許多法規，例如專利、著作權的相關法律，在網際網路的歷史上，也有 Google 的程式設計人員要求 Google 停止開發中國的 Dragonfly 計畫，所以程式設計人員是有自己的道德標準而不是只是寫程式的機器而已。

另外也談論了由於未來人工智慧的發展裡，機器學習可能會因為程式人員撰寫時的偏見、歧視或是其學習的資料中有偏見、歧視、仇恨言論時，該如何讓程式撰寫人員避免寫出來的程式有偏見與歧視，這點也在這個場次中有不少討論，但是否能透過學校教導所謂的 Ethics？還是藉由 Social Norms 去影響程式人員？這點並沒有定論，只能確認在不同的立場都有各自的觀點，這也是網路治理論壇重要的原因，讓不同觀點的人在這個平臺上交流意見。

## (二)7 月 18 日

### ● WS17. The Future of Digital Identity and Human Rights

由於亞洲各國政府都陸續改用數位身份證，臺灣也即將全面換發電子身份證，但同樣的議題多年來始終無解。尤其是與談人之一的 Mary Rose Ofianga Rontal 提到了菲律賓 2016 年選舉期間出現的個人資料外洩案，導致 5500 萬筆登記選民資料外洩，也造成人民的恐慌。

由於將人民的個資數位保存，同時中央政府的資料庫也成為了最大的攻擊目標，所以各國政府如何安全保管電子化後的個人資料，不止是網路安全，事後的補救與賠償都是各國政府應學習的態度。

這個場次同時也討論了印度的 Aadhaar 資料庫，由於這個資料庫不止儲存個人資料，更進一步的儲存使用者的生物資訊，包括虹膜、指紋等，同時連結了手機號碼、銀行帳戶等資料，而在人民端的儲存形式也只是一張紙卡，有許多安全上的漏洞，同時因為這樣的連結方式、生物資訊的記錄，若是資料外洩，也可能造成人民的隱私、財產、不可更改的生物資訊被洩漏出去。

現場多數人並不贊成 Aadhaar 資料庫，但在人權團體 Association for Progressive Communications (簡稱 APC)工作的 Gayatri Khandhada 也提出了較客觀的論點。目前反對數位身份證的人，本身通常已具有身份，但對於難民、戰爭受害者來說，他們可能已喪失原本的身份，此時數位身份證可以協助他們擁有身份，也能協助這些人重新進入經濟活動，而不會因為缺乏身份證明，無法參與經濟活動，可能必須為了生活鋌而走險，從事犯罪活動。所以數位身份證並不全然是壞的，而是也有好的面向，但政府如何保護人民的個人資料不會外洩，同時也有完善的補救措施，降低人民的損失，特別是人權中的隱私保護、政府監控、身份被仿造...等，都成了政府在執行數位身份證時需要仔細考量的重點。

## ● WS.20 Cyber Norms in Asia-Pacific

18 日主參與由來自 Australian Strategic Policy Institute 的 Bart Hogeveen 提案的 WS.20 Cyber Norms in Asia-Pacific，同時擔任其中之一與談人。其他的與談人則有：除 Bart Hogeveen 外，還有亞太網路資訊中心(Asia Pacific Network Information Center，簡稱 APNIC)的 Klée Aiken 和 Pablo、印尼雅加達 Centre for Strategic and International Studies Jakarta 研究員 Fitriani 共同討論如何建立亞太地區的 Cyber Norms。由於簽證因素，加上 Bart Hogeveen 同時在新加坡參與 RSA Conference 2019 (Asia Pacific & Japan)，僅有我一個人在現場，但因主辦單位提供了良好的網路，所以其他四位參與者都可以透過網路連線與會。Bart Hogeveen 也透過網路連線主持會議，臨時由秘書處通知，除了與談之外，也負責協助現場的與談控制。

由於 Bart Hogeveen 同時提供了其參與的新加坡資安活動，所以也討論了關於聯合國中十五個國家所討論的 Cyber Norms，我則表達了：1)臺灣無法參與聯合國相關會議，2)臺灣無法參與共同制定 Cyber Norms 的遺憾，3)另外也提出了亞太地區國家政府習慣以法令、規範去管制科技發展，較不容易有 Norms 的出現。

Norms 可以比喻為日常生活中大家的行為準則，如果說是 cyber security 的 norms，則可能是業者、民眾、政府人員之間共同討論出的資安行為準則。

在整體討論可以分為兩個部份，一個是如何建立且由哪些人建立 Cyber Norms？另一部份則是如何實行 Cyber Norms。

2018 年於巴黎舉辦的聯合國 IGF 已有討論關於 Cyber Security Norms，而 APNIC 的成員也多參與其中，同時也在亞太地區國家進行相關的網路與資訊安全的教育訓練活動，幾乎已開始擔負起亞太地區網路安全教育的責任；有部份參與者認為 Intergovernmental 機構之間的合作機制並不透明，期待合作機制可以更透明一些；而 CERT 的模式是屬於明顯的多方利害關係人機制，標準的由下而上的回報機制與合作模式。現場則是討論了聯合國成員國制訂的 Cyber Norms 還是由政府官員代表共同討論制訂的，並不是由下而上或是藉由多方利害關係人機制所討論出來的，但某些政府官員並不了解網路運作的模式與基本的道理，所以由他們進行 Cyber Norms 的制訂，可能會有侵犯人權或過度管制的疑慮。有現場參與者提議可以讓政府人員、技術專家、業者、學者分別各自團體討論後再一起討論 Norms 中的可行性，再一同制訂。

臺灣雖然無法參與聯合國成員一同制訂 Cyber Norms，但也 TWCERT/CC 也積極的參與亞太地區、國際間的資安聯防，而 TWNIC 本身也試圖建立 Cyber Norms。

由於本工作坊在討論之初約有 15 至 20 分鐘在確認網路連線狀態，所以在最後的時間，大家也討論 Norms 是否具有法律效力？如果 Norms 不具有法律效力，對利益優先者而言，可能不會考量 Norms，而是利益優先，不考量人權、侵犯個人隱私；但如果 Norms 具有法律效力，它有可能會阻礙新科技的發展，而它也可能不再是我們所說的日常生活的行為準則，而已成為法律規範。

由於 Cyber Norms 的特性是屬於與時俱進，也是可以隨時討論的，也許明年會再朝網路安全或資訊安全領域討論關於 Cyber Norms 的制

定與落實。

- **WS.37 Is e-Government and effective mechanism for developing economies.**

此場討論則是延續去 2018 年 APrIGF 中關於電子化政府的討論。去年邀請了日本、新加坡、臺灣分享電子化政府的進度，在今年由去年提案者 Maureen Hilyard 繼續針對太平洋上各國政府進行電子化政府或是建立共同的政府入口網站是否有助於太平洋上各國(New Caledonia、Fiji、Samoa、Vanuatu、Cook Islands、Tonga...等國)的經濟發展。

Maureen Hilyard 認為如果有一個共同的電子化政府入口網站，可以協助大家了解政府的政策，同時也許可能協助發展中國家的經濟發展。現場則有來自 Fiji 的講者 Cherie Lagakali 提到 Fiji 和新加坡政府合作，建立了自己的政府網站(<https://www.fiji.gov.fj/>)，民眾可以從網站上了解政府的狀況，也因為是與亞洲電子化政府標竿的新加坡合作，網站上的功能也十分容易了解，甚至還有線上申請公司註冊的功能，都可以在網站上使用。

現場的參與者提到，以非太平洋列島各國國民的身份，他如果想到這些國家，他會希望從網站上了解有哪些對外國移民的福利設施、有沒有幼兒園、托育制度...等。

我則提到如果是針對一個「共同電子化政府入口網站」，可能要先想想哪些觀眾是目標群眾，如果是希望外商投資，可以考慮在網站上提供獎勵投資優惠，但同時也要求外商需要聘用當地國家的民眾或是配合政府政策，協助教育與強化當地的基礎建設，也可以藉此幫助需要的國家改善經濟。

但主要還是需要視這個「共同電子化政府入口網站」的目的是什麼？是要讓各國民眾理解政府政策或參與政府的政策制訂？可能在不同的發展階段有不同的目的，而不是急著一次完成所有的目標，在臺灣發展電子化政府、政府入口網站的過程裡，都曾因為政策實行而

造成政府人員的反感，所以可能分階段實行、理解明確的目的，較有可能成功。

### (三)7月19日

#### ● **WS9. Build Concept on AI society for Global Good Quest for Inclusion**

本日早上與來自南韓 IGF(Kr-IGF)的崔恩彰博士(Eun Chang Choi)、孟加拉 Shah Zahidur Rahman、菲律賓 Aris Ignacio、尼泊爾的律師 Babu Ram Aryal 共同討論人工智慧的治理議題。該場次是由孟加拉的 Shah Zahidur Rahman 提案，用意是藉由學界、技術領域、法律領域……等人共同探討世界各國在積極發展人工智慧的同時，如何對社會帶來正面的影響。

由於人工智慧的發展，就正面效益來說，它可能會讓產業整體大型轉變，進行工作模式的轉型，將會減少人力成本的支出，以教育來說，就不再需要實體教室，學生可以藉由人工智慧的協助在網路上學到相關知識；人工智慧也可以協助人們增加決策的速度，減少人類在閱讀資料與判斷的時間。

上述的各種優點同時帶有缺點，除了可能在未來面臨大量的失業潮外，就目前的應用而言，已有使用人工智慧程式進行履歷表的篩選、候選人的建議，在潛在的程式撰寫者不自覺的意識中可能已存有性別、種族、膚色、宗教信仰……等偏見；也曾經評估人工智慧與勞務機器人的發展，也可能導至教育程度較低的女性無法從事第一線的勞力工作、服務性質工作，也可能導致其生活困難，更因無法接受平等的教育而無求生能力；愛沙尼亞也有人工智慧程式協助辦讀大量的歷史紀錄，2019年六月，法國也通過法案禁止使用人工智慧來研讀與分析過往的案例，以破壞法官審判的公正性；有些國家則使用人工智慧發展具大規模殺傷力的武器；而中國則運用人臉辨識及人工智慧，配合其社會信用評等制度，對人民信用評等或是限制、追蹤人民的活動，讓人民活在恐懼之中。

在研討會中除了大略簡述亞太地區的人工智慧發展狀況外，更深刻的討論了開放資料的使用與人工智慧的責任追究問題，畢竟人工智慧的發展，幾乎是直接挑戰不同國家現行法規，例如 Autonomous cars 若發生意外時，該如何劃分責任？若是 Drones 出事時，該追究誰的責任？不同國家的責任歸咎、標準也不同，也是在此工作坊中觀察到的討論。

由於人工智慧目前的發展進度仍需要分析大量的資料協助機器學習，但在資料的使用上仍然有各國的資料保護法、資料隱私的保護限制，是否應該討論出共同的資料使用框架？由於在 APEC 成員中已有針對跨境傳輸資料隱私保護的 CBPRs(Cross Border Privacy Rules System)資料隱私保護框架，那對於非成員國是否也要遵循？

在工作坊結束後，我們討論著明年是否繼續討論關於人工智慧治理的議題或是針對資料隱私或是使用標準的議題再進行相關的討論，而韓國的崔恩彰博士也表示希望未來有機會來臺灣參與網路治理論壇或是進行相關的分享。

之後與其他參與者稍作交流，與自己帶領的兩位研究員們討論了之後他們在網路治理領域的發展，一位將繼續參與 ICANN 的公開會議，並且也已通過申請成為今年聯合國 IGF 的獎助金研究員，將前往柏林參與網路治理會議；另一位將會繼續在網際網路環境中工作，並參與相關的技術交流活動。

## ● **WS12. Coping with misinformation in an era of information deluge; Who is Responsible?**

午餐時間時，崔恩彰博士邀請我一同參與其主持的不實資訊的工作坊。多數的臺灣參與者都參與了這一場工作坊，在其中分享了臺灣民間與政府合作，澄清不实資訊的各種管道，而技術人員則是討論了如何在技術端攔截不实資訊；也討論了新加坡政府為防堵不实資訊的流傳而進行的言論管制政策，但由於與談人之一也住在新加坡，所以也略有保留。在會中，則是分享去年聯合國 IGF 在巴黎舉辦的主題便

是如何重建信任？不論是目前我們所討論的不實資訊或是自古以有的謠言、流言，都是在歷史上無法避免的，所以政府的公開資訊、澄清管道都是需要建立的，而人民對政府的信心也是需要長時間建立，而非一蹴可及的。

## ● Closing Plenary

最後則是參與閉幕式。今年如同往年，也邀請 NetMission 的工作人員、獎助金的研究員們上臺分享自己負責主題的心得。雖然各國都在發展各種新科技，但資料仍是這些科技的基礎，資料保護除了涉及政策之外，同時也涉及了網路與資訊安全的保護，所以有許多的場次也涉及了法規(資安政策)、人權、科技發展之間的討論。

今年因為主題設定了需要談及包容性，但這部份並不是只有單一的只談經濟發展，同時也包括了整體基礎建設、人才的教育、政府體制的運作方式改變...等。

之後也有聯合國秘書處的計畫經理 Chengetai Masango、APrIGF 秘書處 Jennifer Chung、APNIC 總監 Paul Wilson、Diplo Foundation 的 Tereza Horejsova (遠距參與)、人權團體工作者 Smita Vanniyar，討論「The role of the Asia-Pacific Internet Governance and Multistakeholder Participation in the Global IGF」，即亞太地區的網路治理論壇與如何利用多方利害關係人機制參與全球的網路治理論壇。

全球的 IGF 都是獨立，無垂直關係的，但因為地方、區域、全球性的網路治理論壇都會有相同性的議題，同樣的，也會因為不同文化的關係，多數國家對於「多方利害關係人」的定義不一樣，或是對參與的文化不同，所以自聯合國 IGF 的角度而言，每次辦理聯合國 IGF 要再解釋一次「多方利害關係人機制」也是一種負擔。APrIGF 秘書處 Jennifer Chung 則在討論中提到香港、澳門、臺灣都以多方利害關係人機制成立了網路治理論壇與青年網路治理論壇，2018 年是第一次在太平洋上的國家 Vanuatu 舉辦了 APrIGF，「多方利害關係人機制」也讓 Vanuatu 的網路使用者感到非常實際，也在之後、2019 年舉辦了

他們自己的 Vanuatu IGF，也開始操作「多方利害關係人機制」。每年的 APrIGF 在會議後會產出一份 Synthesis Document，由於 APrIGF 秘書處也是亞洲地區在聯合國 IGF 的 MAG 成員之一，每年她會將這份文件帶至聯合國 IGF 中討論，讓參與者知道 APrIGF 會議中討論的主題與討論。

最後則是由擔任兩年的主席 Rajnesh Singh 告訴大家，今年將重新選舉出新的主席和其中一位副主席，他也會繼續爭取今年與明年的席位，同時也鼓勵本年度參與的獎助金研究員們，在未來也一同競爭 APrIGF 的主席席位。

最後則是由目前的副主席之一，同時也是尼泊爾 IGF 的創辦人 Babu Ram Aryal 向大家宣布，APrIGF 2020 已確定將由尼泊爾舉辦，並與亞太網路治理學校(Asia Pacific School on Internet Governance，簡稱 APSIG)一同於 2020 年五月辦理。

由於每年七月是尼泊爾的雨季，就算是較先進的市區加德滿都會面臨大雨、淹水，所以大會決定將提前於 2020 年五月舉辦，五月在尼泊爾也是較適宜的天氣，同時也不會與其他亞洲國家或是亞太地區、全球性網路治理活動衝突。由於今年有不少參與者因為簽證審核問題、轉機問題無法到現場參與，所以尼泊爾提到簽證是在機場當地海關核發，若是南亞區域合作聯盟(South Asian Association for Regional Cooperation，簡稱 SAARC)的成員國，也可以免簽進入尼泊爾；航班交通也可以自泰國、香港、中國的機場直飛。

## 參、考察、訪問心得

本年度共有 23 個獎助金研究員，7 位男性，16 位女性，多來自南亞與東南亞國家。同時，在這次 APrIGF 裡，來自俄羅斯的參與者非常少，甚至有提供獎助金，他們的參與意願也不高。

APrIGF 的特色之一就是鼓勵無法現場參與的大家都可以透過線上直播參與。2018 年在萬那度(Vanuatu)使用 Adobe Connect 除了要花費長時間的教育訓練，讓當地支援人員學會如何操作，但 Adobe Connect 的操作介面複雜，若是要遠端參與，其行動版本介面對使用者的親和力極低，加上萬那度的網路品質不佳，所以去年許多遠端的講者都無法參與。

今年將線上會議的軟體改為使用 Zoom，讓參與者可以直接透過 Zoom 線上參與，其行動版本的親和力較高，也容易操作。今年度俄羅斯也提供了品質極佳的網路，讓分別處於新加坡、布里斯班、雅加達的講者皆能連線至海參崴，同時與大家進行線上會議並進行互動對談，不會受到地區限制。

今年臺灣有 10 位至海參崴的參與者，不同於在 APrIGF 2017 與 APrIGF 2018，今年臺灣的參與者較往年主動，也多願意與其他國家的參與者互動，尤其是 Youth IGF 與中華民國國家資訊基本建設產業發展協進會(NII)的獎助金學員有不少互動。

因為今年帶領的研究員們一位是聯合國 IGF 的 MAG 成員，另一位則是申請成為將於柏林舉辦的聯合國 IGF 青年大使，她們都鼓勵我去參與聯合國 IGF 或是申請為 IGF 獎助金研究員。當我提到因為臺灣非聯合國成員，無法參與聯合國活動時，她們皆感到不可思議，畢竟網際網路、數位經濟的發展，與是否為聯合國成員無關，同時在網路治理論壇中討論著 Universality 和 Accessibility 卻因為臺灣非聯合國成員，而無法參與討論，她們覺得十分不合理。

不過，儘管臺灣人無法實際參與聯合國 IGF，但目前還是由吳國維老師可以進入聯合國 IGF 會議，而所有人也知道他來自臺灣，另外，

我們也可以自網路會議平台參與，不見得要直接去柏林參加，這點是今年三月前往日本神戶參與 ICANN 64 時與聯合國 IGF 秘書處所確認的。

## 一、 跨國提案合作經驗

由於 APrIGF 是屬於區域性的網路治理論壇，加上亞太地區的幅員廣大，所以在提案時應著重於議題的廣度、深度是否達到區域性平臺討論的標準；與談人的身份是否具多樣化、性別是否均衡；提案人對於時間的安排與工作坊的進行模式；欲達成的目的。這些標準都成了提案是否能通過的重要性。

今年度分別參與了網路安全與新興科技議題。網路安全議題是與澳洲提案者討論過後，一同對於所謂的 Cyber Norms 進行相關的討論，與談人的成員分別來自澳洲的墨爾本和布里斯班、印尼雅加達，再配合臺灣，進行相關的討論。因為持續的參與國際間的網路政策會議，所以對於相關的政策議題也較熟悉。

由於今年度的南韓網路治理論壇(Kr-IGF) 與臺灣網路治理論壇(Taiwan Internet Governance Forum, 簡稱 TWIGF)辦理的日期重覆，在與聯合國 IGF 的網路郵件群組中而有所交流，也在此次受孟加拉的提案人邀請在 APrIGF 2019 中一同擔任論壇的與談人，討論人工智慧治理相關議題，也有不錯的交流，之後也將會於泰國清邁舉辦的 APNIC 48 會議中見面。

網路治理論壇成員之間主要以網路郵件群組在彼此連絡，可以避免有些國家對於通訊軟體、網路社群平台的監管與限制，例如在俄羅斯就無法使用 LinkedIn 但可以使用 Telegram 和 WhatsApp；在馬來西亞無法使用 Medium；在中國可能無法其網路狀態下使用 Google 的服務，所有成員或有興趣的參與者都是透過郵件群組在互相連絡，只有工作人員之間才可能進一步的交換 WhatsApp、Facebook 或是其他社交平台帳號。

提案時需要提供講者名單，臺灣提案者在這點上較為吃虧，若是

提案時的名單皆為臺灣成員，對成員來自於亞洲各國的議程委員會而言，這樣的提案於 TWIGF 提案即可，無區域性討論的必要性。

論壇其他國家的成員，多在其他網路政策活動、學術研討會、網路治理教育活動就認識，也較容易組成多國、多樣化的與談者成員。

## 二、實體國界的限制與網路無國界

此次有不少講者或是 MSG 成員因為無法取得俄羅斯簽證而無法到現場參與，有幾位獎助金研究員同樣因為簽證問題、需要負擔邀請函的相關費用或因健康因素而由其他人員遞補。APNIC 的成員也僅有其總監 Paul Wilson 成功取得簽證得以成行，有不少 APNIC 的職員無法取得簽證現場參與會議，其他也有許多國家的講者也因簽證問題，而無法成行。

在 APriGF 2019 確定於海參崴舉辦後，西伯利亞航空也有了臺灣與海參崴直航的航班，班次不多，且到當地時也已是半夜，在簽證申請上，雖然在會議舉辦前兩週，海參崴表示臺灣可以透過網路申請電子簽證前往海參崴，但網站上仍未有臺灣選項，且當時已在等待相關文件，所有簽證手續已處理近三個月，也來不及改為申請電子簽證。

在與其他獎助金學員交流的過程中，來自印尼的另一位參與者也表示，有時候她如果要參與自己國家其他地區的網路治理活動，可能還要花費比國際行程更高額的交通費用，所以她僅會參與大型的網路政策會議。

遠東聯邦大學提供了良好的網路通訊，所以在會議進行間，無法至現場參與的講者，若處於網路品質不差的環境中，也能順利的藉由網路會議連線參與會議，甚至透過網路連線來主持會議。在這次的經驗裡體會到，若是在網路連線品質穩定的情況下，參與者若能克服不同時區，透過網路連線，也可以節省交通、差旅等相關費用的支出。

### 三、 照片使用與個人資料、隱私保護的爭議

因為會議地點是在大學校區，所以對於出入的人員有嚴格的控管，主辦單位請大家先上傳護照的彩色影本、班機的時間，同時於 19、20 日在機場設有報到櫃檯，參與人員在機場出海關後，就可以直接於機場的報到櫃檯領取自己的名牌。

由於俄羅斯屬於歐洲國家，受到 GDPR 的規範，所以在能力建構日時，主席便要求大家若要上傳照片到社群網站前，需要徵得相片中人物的同意才可以上傳。因此這次除了官方攝影人員外，幾乎沒有太多人在拍照或是上傳照片到社群網站(俄羅斯對於部份社群網站也有管制，會進行言論審查)。

在 19 日時，有現場參與者表示，對於官方攝影人員在拍照時的過度靠近感到不自在，也擔心照片被人誤用，在會後也有激烈的討論。

## 肆、建議意見

亞洲區有兩個網路治理的相關教育組織，一個是位於南韓的亞太網路治理學院(Asia Pacific Internet Governance Academy, 簡稱 APIGA)和亞太網路治理學校(Asia Pacific School on Internet Governance, 簡稱 APSIG), 有些國家也會辦理自己國家的培訓課程。另外像網際網路名稱與數字位址分配機構(Internet Corporation for Assigned Names and Numbers, 簡稱 ICANN)、亞太網路資訊中心(Asia Pacific Network Center, 簡稱 APNIC)、網際網路學會(Internet Society, 簡稱 ISOC)都有相關的教育課程或獎助金, 讓有興趣的人員可以申請參與活動, 並接受教育訓練。

MSG 成員之一的 Aris Ignacio 來自菲律賓, 本身在 Southville International School and Colleges 擔任老師, 今年帶了不少學生一同參與 APrIGF, 在不同的場次中學習相關的資訊, 並與其他國家的人交流。

APIGA 和 APSIGA 這兩個教育單位每年都會培訓不少網路治理的相關人員, 每年也會進行一次的教育訓練招生, 課程內容自網際網路的發展歷史、基礎架構、網路安全與人權等議題; 除了教育訓練之外, 其實最重要的就是學員們的互動, 讓學員彼此可以互相連絡、組織, 交流不同國家的網路治理議題, 進一步到 APrIGF 或是聯合國 IGF 上提案討論。

臺灣雖然在 2016 年辦理了 APrIGF 2016, 但整體對於網路治理的議題可能仍屬於國家層級或是新聞議題層級, 加上參與國際網路治理論壇或教育訓練課程仍需要以英文交流, 所以較少人會主動參與 APIGA 或是 APSIG, 2018 年和 2019 年分別有臺灣參與者至南韓參與 APIGA, 但目前並未見到他們有提案至 TWIGF 或是 APrIGF 中。

在 APrIGF 2019 中, 來自臺灣的參與者皆有發言, 特別是在不實消息的議題上, 提供了臺灣政府與民間的處理方案或合作方式, 臺灣的 IPv6 快速普及, 也成了亞太區國家間討論的議題。未來還希望有

更多來自於臺灣與其他國家合作的提案，除了可以快速讓國際間知道臺灣的經驗外，也能夠增加臺灣在網路治理論壇的能見度。

今年的 TWIGF 有來自 ISOC 的提案人，由菲律賓來臺灣分享政府單位與民間 ISOC 組織合作，擬出網路政策的白皮書。在 APrIGF2019 中，也與一些南韓、新加坡、印尼、尼泊爾的參與者、講者互動，他們希望能來臺灣參與 TWIGF，但也希望臺灣相關單位提供獎助金，協助分攤機票與住宿的費用，也能促進國際交流。

最後，由於個人資料保護的關係，有些人對於自己的隱私保護要求較高，日後國內舉辦會議時，除了在網站上提醒現場會因需要會議記錄，而有官方錄影與攝影外，會議主持人也要提醒大家需要取得被拍攝者的共識及告知用途，才能上傳或公開至社群網站，同時也建議於現場提供「請勿拍攝」貼紙，讓參與者選擇自己是否要接受會議主辦單位的攝影，若不慎入鏡，也可以藉由該標示辨識，將照片移除，這些措施都可以避免日後會議主辦單位與被拍攝者之間的爭議。

## 伍、其他相關事項或資料

1. 官方網站：<https://2019.aprigf.asia> 或 <https://aprigf.ru>

2. 議程表：<https://aprigf.ru/prog/?p=prog>

3. 錄影：<https://aprigf.ru/press/?p=video>

4. 會議討論文件：<https://comment.rigf.asia/>

5. 官方照片放於 Facebook 網址：

[https://www.facebook.com/pg/cctldru/photos/?tab=album&album\\_id=2299454483610834](https://www.facebook.com/pg/cctldru/photos/?tab=album&album_id=2299454483610834)

6. Instagram 網址：<https://www.instagram.com/cctldru/>