Asia Pacific Regional Internet Governance Forum
2017 Bangkok Synthesis Document

1. ## Background

   First published in 2015, the Asia Pacific Regional Internet Governance Forum (APrIGF) Synthesis Document aims to identify relevant Internet governance interests within the Asia Pacific region and to reflect the discussions which take place at the APrIGF conference[1] each year. Building on the APrIGF Synthesis Document from APrIGF 2015 Macao[2] and APrIGF 2016 Taipei[3], the process for the 2017 Synthesis document now includes two webinars[4] each followed by public comment periods[5] to collect wider input from the Asia Pacific Internet community across all stakeholder groups to build a more comprehensive and collaborative open document detailing the significant deliberations which took place during the APrIGF 2017 Bangkok.

2. ## Purpose

   The Synthesis Document aims to collect the contributions and outputs of participants at the APrIGF meeting (as well as those within the broader APrIGF community through remote participation and dissemination on the mailing list and online platform). The APrIGF Multistakeholder Steering Group (MSG)[6] and the Drafting Committee[7] accept that the Synthesis Document cannot be fully representative of the very diverse Asia Pacific region. Nevertheless, they anticipate that the development of this Synthesis Document can help drive active participation in the Internet Governance Forum (IGF) process and demonstrate the value of the annual APrIGF meeting as a platform for voices, views and thoughts in the Asia Pacific region as a contribution to relevant global, national, local and international forums on Internet governance.

3. ## Introduction

   In December 2015, the United Nations General Assembly (UNGA) reviewed the outcomes of the World Summit on the Information Society (WSIS+10) and as part of the WSIS+10 outcome[8], renewed the IGF mandate for another 10 years. In its resolution[9], the UNGA called for the '*close alignment between the [WSIS] process and the 2030 Agenda for Sustainable Development*' and highlighted the

---

[1] APrIGF main website: http://aprigf.asia/
[2] APrIGF 2015 Macao Synthesis Document: http://2015.rigf.asia/macau-synthesis-doc-file/
[3] APrIGF 2016 Taipei Synthesis Document:
http://aprigf.asia/documents/APrIGF_2016_Taipei_Synthesis_Document.pdf ; Appendix II:
http://aprigf.asia/documents/2016appendixii.pdf
[4] Webinar 1: 11 July 2017, Webinar 2: 16 August 2017
[5] First Input/Public Comment Period 6-19 July 2017; Second Public Comment Period, 16-31 August 2017
http://comment.rigf.asia/
[6] APrIGF Multi-stakeholder Steering Group: http://aprigf.asia/msg.html
[7] APrIGF Synthesis Document Drafting Committee: http://aprigf.asia/drafting-committee.html
[8] WSIS+10 outcomes: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf
[9] Ibid.

contribution of Information and Communications Technologies (ICTs) towards achieving the Sustainable Development Goals (SDGs)[10].

4. In June this year, the IGF Multistakeholder Advisory Group (MAG) held their second open consultation and meeting[11]. The MAG recognized the importance of the intersessional work done in the National and Regional Initiatives (NRIs) and strongly supported continuing the intersessional work on 'Policy Options for Connecting the Next Billion(s)' in Phase III. These initiatives, along with Dynamic Coalitions (DCs) and the Best Practice Forums (BPFs) as well as the National and Regional Initiatives (NRIs), will be given space to hold sessions at the annual global IGF meeting to be held on 18-21 December 2017[12] in Geneva, Switzerland.

5. The Asia Pacific Regional Internet Governance Forum (APrIGF) serves as a platform for discussion, exchange and collaboration at a regional level. It also aims to aggregate national and local IGF discussions, promote a progress discourse, and ultimately advance the Internet governance development and understanding in the Asia Pacific region.

6. **Key Issues in the Asia Pacific region – Ensuring an inclusive and sustainable development in Asia Pacific: A regional agenda for Internet governance**

7. **I. Access, Empowerment and Diversity**

8. More than half of the global Internet users belong to the Asia-Pacific region but the true benefits of bridging the access gap can be realized only if it leads to socio-economic empowerment of the multifaceted human capital in the region[13]. Therefore, access infrastructure should be backed by inclusive strategies that are responsive to the increasing connectivity demand and to support the research and deployment of technologies and solutions. Moreover, policies and processes should be adopted to bridge the digital divide; improve network resilience to disasters[14] in order to create a holistic approach towards eGovernance[15] and to push back against Internet shut-downs[16].

9. Community networks and public access to ICTs[17] have the potential to help improve digital literacy and access to information resources that support education and life-long learning. These networks also facilitate safe, meaningful, non-discriminatory access by all users, including women and children and those within marginalized and underserved communities. Youth-driven initiatives[18] leverage

---

[10] UN 2030 Agenda for Sustainable Development: https://sustainabledevelopment.un.org/post2015/transformingourworld

[11] Summary of 2nd Open Consultation and MAG meeting, : https://www.intgovforum.org/multilingual/content/igf-2017-second-open-consultations-mag-meeting-0

[12] IGF Geneva 2017 – "Shape Your Digital Future!" https://igf2017.swiss/

[13] WS. 57 Connecting the Unconnected in Developing Asia for a Sustainable Digital Economy: http://igf.asia/WS_57

[14] WS. 38 "Cry for help!" - rapidly reconnecting the disconnected in disasters Rapid Restoration of Access to Telecommunications (RREACT) : http://igf.asia/WS_38

[15] WS. 27 Evolving an Open e-Governance Index for Networked Societies: http://igf.asia/WS_27

[16] WS. 94 Engaging with the #KeepItOn Movement: Fighting Internet Shutdowns: http://igf.asia/WS_94

[17] WS. 74 Community networks and public access to ICT: http://igf.asia/WS_74

[18] WS. 41 Youth-driven Internet Governance related Initiatives: http://igf.asia/WS_41

information technology to drive social change and better empower the next generation of Internet leaders in the region. Access to the next billion of Internet users is being enabled by innovative technologies such as IPv6[19], Internationalized Domain Names (IDNs)[20] and Email Address Internationalization (EAI)[21]. In parallel, it is important that inclusive policy measures are taken such as the universal acceptance of IDNs in order to support, preserve, and enhance their individual and collective uniqueness, and the language, geographic and cultural diversity that these new users will bring to the Internet.

10. ## II. Capacity Building

11. Capacity building is critical to bridge the digital divide across the Asia Pacific, especially in underserved and developing countries. Empowerment of diverse communities to develop, deploy and use ICTs more effectively enables them to stay informed and understand their digital rights and responsibilities. These communities can, therefore participate and enhance the Internet ecosystem. Capacity building strategies at the local, regional and global level that address the needs of marginalized communities from underserved regions (including the small island developing states) are key towards digital inclusion, and should incorporate security and privacy.
Capacity building developed on the basis of an inclusive and multistakeholder approach is particularly important for ensuring cybersecurity, privacy, and a safer Internet. Thus, it is a necessary initiative for Asia Pacific to build a robust and empowered Internet community. New users from all walks of life and representing a wide range of stakeholder groups (including but not limited to the technical community, rights activists, policy makers, legislators, online business owners, people with disabilities, common users, and in particular women, youth and students) will be drawn into the Internet governance ecosystem. Capacity building initiatives and programs will accelerate the growth of this community in Internet governance, leading to a strengthened Internet infrastructure, well-informed policies, active Internet community, and more empowered and engaged users.

12. Fellowships offered by I* (I-star) organisations[22] are welcomed within the Asia Pacific region to usher new leaders and newcomers into the Internet ecosystem. Schools of Internet Governance (SIGs), Regional IGFs and IG Academies are creating new networks at regional and local levels for participants from diverse backgrounds, encouraging greater knowledge sharing and diverse perspectives. A variety of approaches help to increase participants' understanding of the complexity of different Internet governance issues and build a better appreciation of the roles, responsibilities, and perspectives of different stakeholders. In the case of SIGs, Asia-Pacific has made major strides through multiple regional, subregional and national initiatives. Nevertheless, there is still more effort required in underserved areas of Asia Pacific. The greatest challenge that exists for any capacity building initiative is funding and sustaining these programs, however, it is also important to ensure that the courses consider the diversity of language and culture, as well as the background knowledge and skills of participants.

---

[19] Merger 3. National policies and Industry strategies on IPv6 in the Asia Pacific region: http://igf.asia/merger3
[20] WS. 35 Developing a Diverse and Inclusive Internet Through Internationalized Domain Names: http://igf.asia/WS_35
[21] WS. 1 Universal Acceptance : An Elixir to Inclusive and Multilingual Internet: http://igf.asia/WS_1
[22] I* organisations: https://www.apnic.net/community/ecosystem/iorgs/

13. ## **III. Security – Cybersecurity, Privacy and Safer Internet**

Cybersecurity, the protection of online systems from damage and disruption, is critical not just to the stability of cyberspace, but also increasingly important to the physical world. Collaboration and capacity building[23] are needed to mitigate[24] and prevent cyber security incidents[25] within and beyond the Asia Pacific region, and the setting of global encryption standards is encouraged[26].

14. ***Legislation and Policies Governing ICTs***

Across the Asia Pacific region, legislation[27] has been developed to govern various aspects of the Internet. Legislation that traditionally govern offline spaces is also used in tandem with these specialised legislation to address violations. These provisions must respect internationally recognised human rights and standards for restrictions (for example, and not limited to, the Council of Europe's Convention on Cybercrime[28]). Particularly, states should be urged to reconsider the manner in which mutual legal assistance agreements (MLATs)[29] are currently implemented. The right to privacy, access to justice and rule of law must be upheld when data of individuals are shared by states.

15. A three-part test of legality, legitimacy and proportionality must be ensured to be passed for all relevant jurisdictions in the investigation or prosecution. An oversight of the process must be required from all participating stakeholders. Data about requests should be made available to the public, for the interest of transparency[30] and accountability.

16. Advances in data encryption require due consideration for an expiration date of protection measures and mechanisms, so contemplated regulations can stand the test of time[31]. Similarly, the mobile and IoT industries also face challenges of time and expiration[32] and regulatory measures can

---

[23] WS. 25 Supporting National Computer Emergency Response Teams for Improving Cyber Security http://apps.2017.rigf.asia/submission/proposaldetail?id=47: Specific suggestions include: Infographic on cybersecurity and CERT for laypeople, codifying case studies of cybercrime and comparing model/traditional penalties (anonymizing the victims) for cybercrime eradication training programs.

[24] WS. 25 Supporting National Computer Emergency Response Teams for Improving Cyber Security http://apps.2017.rigf.asia/submission/proposaldetail?id=47

[25] WS. 29 Cyber Security Incident Role Play http://apps.2017.rigf.asia/submission/proposaldetail?id=51

[26] WS. 83 Upgrade Required: Obfuscation and cryptographic http://apps.2017.rigf.asia/submission/proposaldetail?id=113

[27] WS. 97 Trends in Cybercrime Law: Common legislative: http://apps.2017.rigf.asia/submission/proposaldetail?id=128

[28] Convention on Cyber Crime: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[29] WS. 98 Examining MLAT Alternatives for Asian Economies: http://apps.2017.rigf.asia/submission/proposaldetail?id=129

[30] WS. 80 Algorithmic Transparency: Understanding why we are profiled in a certain manner http://apps.2017.rigf.asia/submission/proposaldetail?id=109

[31] WS. 83 Upgrade Required: Obfuscation and cryptographic http://apps.2017.rigf.asia/submission/proposaldetail?id=113: To address the issue of expiration of encryption technology, a suggestion was made that the regulation should address this and make the regulation future-proof, at least to the life span of a human.

[32] WS. 83 Upgrade Required: Obfuscation and cryptographic, see ibid for link: People rely heavily on the devices and networks that they use, and they don't have the technological/administrative/legal permission to upgrade/update/patch these devices by themselves. An observation is made that safe behavior on vulnerable device is not safe.

balance consumer protection with the responsibility that Internet-connected manufacturers and software-developer will take in making their devices secure for a reasonable time period.

17. ***Privacy, data encryption, and data protection***
Privacy and data protection are critical issues now, especially as they may come into conflict with freedom of expression, and can result in data-driven discrimination[33]. It is important to protect the right of users to secure communications with the role that encryption plays in this protection, as well as in ensuring digital security as a whole.

18. While expectation of privacy may vary by cultures, comprehensive protection mechanisms must meet internationally recognised right to privacy and be linked to consent and agency. Considering the nature of cross-border data transfer for online services, differing levels of protection in relevant jurisdictions and general lack of user awareness, the highest level of protection should be guaranteed as a default safeguard and international minimum standards should be created. These protections should also take into account the rapid development of technology that may make current data encryption, data-masking and obfuscation techniques obsolete in the future.

19. In this context it should be noted that the protection of children[34] and youth[35] from illegal and harmful online content is an important issue not only for the Asia Pacific region. It is vital for all stakeholders to cooperate and collaborate on effective policies and frameworks to uphold the freedom of expression online, free flow of information, and the protection of children and youth online. Capacities of children and young people should also be strengthened so that the approach is not entirely protectionist and gives agency to the users as well.

20. ## IV. Digital Economy and Enabling Innovations
Digital trade and e-commerce are key enablers for the development of the global economy[36], yet they inevitably challenge traditional national borders. Disruptive innovations such as Blockchain[37] have the potential to redesign our interactions in business, politics and society. The digital economy and trade cannot be successful without trust[38], the free flow of information, and appropriate domestic and global rules. To realize the potential growth of the digital economy, free trade agreements[39] should be reviewed in light of the growing trend of limiting free flow of information and/or requiring data localization, as well as source code disclosure unless there is a legitimate

---

[33] WS. 80 Algorithmic Transparency: Understanding why we are profiled in a certain manner
http://apps.2017.rigf.asia/submission/proposaldetail?id=109
[34] WS. 37 Detecting and removing child sexual abuse material. How is APAC doing?
http://apps.2017.rigf.asia/submission/proposaldetail?id=60
[35] WS. 36 Inclusive and multilateral approach to protect the youth
http://apps.2017.rigf.asia/submission/proposaldetail?id=59
[36] WS. 57 Connecting the Unconnected in Developing Asia for a Sustainable Digital Economy:
http://apps.2017.rigf.asia/submission/proposaldetail?id=83, WS. 67 Towards Sustainable Development in Asia Pacific: Mobile Internet and Access to Knowledge in the Marketplace -
http://apps.2017.rigf.asia/submission/proposaldetail?id=94
[37] WS.81 Blockchain: Do we need killer applications before the realization of decentralized Internet governance? -
http://apps.2017.rigf.asia/submission/proposaldetail?id=111
[38] WS. 48 Enable Innovation and Trust in Internet Economy: Toward an Interoperable Online Authentication and Identification Infrastructure - http://apps.2017.rigf.asia/submission/proposaldetail?id=72
[39] Merger 4. Trade Rules for the Digital Economy: Asia's Agreements at the WTO and RCEP -
http://apps.2017.rigf.asia/submission/proposaldetail?id=56

public policy reason. Coordinated multistakeholder collaboration and thorough discussion among all other stakeholders with active government participation is indispensable to realizing the benefits of the digital economy to all.

21. **IV. Human Rights and the Internet**

Respect for human rights is fundamental to the achievement of the Sustainable Development Goals (SDGs)[40]. Therefore, human rights agreements should apply to the Internet environment as set out in the WSIS Geneva Declaration of Principles[41], Tunis Agenda for the Information Society[42], and other international conventions and declarations[43]. These areas include access and development, freedom of expression[44], right to assembly and privacy, the right to information, education, health, culture, as well as a broad range of other rights[45]. Laws, policies, and practices on the security of network and information systems, data protection, surveillance, anonymity, intermediary liability[46] and cyber-crime must protect human rights and meet international standards for guarantees. The application of human rights should also consider cross-cutting issues of gender, disability, age and sexuality[47]. These issues were the subject of intense scrutiny and debate by all stakeholders at the APrIGF meeting.

22. *Gender digital divide and ending online gender-based violence*
The gender digital divide is a continued and critical concern in efforts to address disparity in Internet access in the region. Meaningful and equal access includes addressing issues related to connectivity as well as the persistent disparities in literacy and income, barriers in the form of social and cultural norms as well as online gender-based violence.

23. Taking effective action to counter gender-based violence online is important in ensuring that the Internet fulfils its potential as a positive driver for change and development, as well as in helping to construct a safe and secure environment for women and girls in every sphere of life[48]. Gender-based violence can, among other things, limit women's ability to take advantage of the opportunities that ICTs provide for the full realization of women's human rights, act as a barrier to access[49] that can exacerbate the gender digital gap, violate women's human rights, and reproduce

---

[40] UN 2030 Agenda for Sustainable Development:
https://sustainabledevelopment.un.org/post2015/transformingourworld
[41] WSIS Geneva Declaration of Principles, 12 December 2003:
http://www.itu.int/net/wsis/docs/geneva/official/dop.html
[42] WSIS Tunis Agenda for the Information Society, 18 November 2005:
https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[43] Universal Declaration of Human Rights: http://www.un.org/en/universal-declaration-human-rights/ ,
[44] WS. 88 Unshackling Expression: A pathway to decriminalise the Internet -
http://apps.2017.rigf.asia/submission/proposaldetail?id=118
[45] WS. 93 The whole truth: Bringing Economic, Social and Cultural Rights into perspective -
http://apps.2017.rigf.asia/submission/proposaldetail?id=123
[46] The Manila Principles (https://www.manilaprinciples.org/) have been drafted by a multistakeholder group and published and consulted at the RightsCon 2015 (https://www.rightscon.org/past-events/). More work needs to be done to put the Manila Principles into practice.
[47] Merger 2. Content Moderation and Online Harassment:
http://apps.2017.rigf.asia/submission/proposaldetail?id=135
[48] WS. 63 Surveillance from a Feminist Perspective: http://apps.2017.rigf.asia/submission/proposaldetail?id=89
[49] WS.4 Access to rights online: Digital gap for disenfranchised and marginalized communities -
http://apps.2017.rigf.asia/submission/proposaldetail?id=22

gender stereotypes and discrimination. It is important that all stakeholder groups participate in addressing the issue of online gender-based violence[50] through a range of strategies such as the framework of human rights, including capacity building, more effective complaints and redress mechanisms, inclusive decision-making processes, and/or appropriate legislative and policy-based responses.

24. *Internet shutdowns and blocking*

Uninterrupted access to the Internet is essential for the free exercise of rights online. Network shutdowns and blocking have serious economic consequences and impede the right to information, expression, assembly and association among other rights as well. Any disruptions to the access to mobile and Internet services must comply with strict standards established in national legislation and must meet the threshold of legality, necessity and proportionality laid down in the International Covenant on Civil and Political Rights[51].

25. *The Right to be Forgotten*

The Right to be forgotten[52] as a principle must be approached with caution. Significant and competing issues relating to its extraterritorial application, digitised media archives and the integrity of historical records, the rights of individuals and media freedoms must be weighed carefully. Moreover, emerging jurisprudence on this subject competes with public interest as it imposes a burden of proving public interest on people searching for information or intermediaries facilitating that search such as libraries, educational institutions, archives and search engines.

---

[50] WS. 22 Hack to fight online violence - http://apps.2017.rigf.asia/submission/proposaldetail?id=44

[51] International Covenant on Civil and Political Rights: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[52] Merger 1. Publicness and the Right to be Forgotten: the Debates Begin: http://apps.2017.rigf.asia/submission/proposaldetail?id=132

26. **Appendix 1 – Process and Participation**

27. This APrIGF 2017 Bangkok Synthesis document[53] has been developed from input received during the open call for contributions before the APrIGF, at the APrIGF event both onsite and remotely, as well as comments received during the two public input periods[54]. Two webinars[55] preceded both public comment periods to further engage the APrIGF community on the purpose and process of the Synthesis document. This document is finalized by the Drafting Committee on 6 December 2017 for publication.

---

[53] A Draft 0 framework for this document was circulated on the APrIGF Multistakeholder Steering Group (MSG) and Synthesis Document Drafting Committee mailing lists and posted publicly to solicit input, was based on the submitted and accepted workshop proposals for the APrIGF containing placeholders for topics to be discussed at the APrIGF event. Draft 1 incorporated comments and input from the series of "Synthesis Document Discussion" sessions at APrIGF 2017 as well as input received on the online public commenting platform during both public input periods, and was published for a second public input period to garner wider input.

[54] Public input period 1 (6 – 19 July 2017): https://comment.rigf.asia/asia-pacific-regional-internet-governance-forum-2017-bangkok-synthesis-document-draft-0/ ; Public input period 2 (24 August – 10 September 2017): https://comment.rigf.asia/

[55] Webinar 1 (11 July 2017): https://2017.aprigf.asia/2017/07/11/webinar-1-asia-pacific-regional-internet-governance-forum-2017-bangkok-synthesis-open-input/; Webinar 2 (24 August 2017): https://2017.aprigf.asia/2017/08/22/webinar-2-for-synthesis-document-2017/