Key Issues in the Asia Pacific - Empowering Communities in Asia Pacific to build an Affordable, Inclusive, Open and Secure Internet

Cybersecurity

Cybersecurity is a growing concern, especially in the era of Internet of Things (IoT) and proliferation of automation. There is urgency to increase technical capabilities and address gaps that may arise from innovation, including risk mitigation strategies and incident response capabilities. Most cybersecurity measures in the Asia Pacific (APAC)[1] region are yet to catch up with the exponential growth of Information and Communication Technologies (ICT) infrastructure and online services, particularly in developing economies. When we think about securing the Internet, it usually means ensuring network security and stable operation, maintaining the integrity, confidentiality and availability of network data, effectively responding to network security incidents, preventing cybercrime and the ability to trace malicious activities.

Multiple stakeholders play a key role by working together to mitigate cybercrime. Law enforcement, security research centres, and the technical community comprising CERTs[2], network operators and IT professionals, amongst others, are critical to ensure a safe Internet environment for users. Collaboration between relevant agencies and the technical community is needed to ensure practical, reasonable and fair solutions to security issues. In this regard, the meeting recognised the Pacific's efforts[3] to establish CERTs in Papua New Guinea, Tonga, and Vanuatu as they will play a critical role in incident response and developing technical and forensic[4] capabilities in the region. Having a regional multi-stakeholder forum in conjunction with technical and academic meetings or conferences is an effective way to include the technical community[5] to discuss a feasible plan for cybersecurity policy. A transparent multi-stakeholder approach to identify and address key risks is a positive way forward to addressing cybersecurity issues within the Asia Pacific region.

The future stability and security of the Internet highly depends on the successful implementation of policies, guidelines and best practices, and by addressing the increased implementation of few major issues like IPv6, DNS Security Extensions(DNSSEC)[6] and routing security[7].. Increased effort is required to develop, implement and revise minimum standards and best practices that address identified key risks for end users, organisations, and critical Internet infrastructure. Existing cybersecurity standards such as ISO 27000 security Series standards, encryption standards etc. can be referenced as guidelines. Critically, the development and implementation of policies and best practices must be balanced with the protection of individual

---

[1] Merger 5. Cybersecurity capacity for nations in the Asia-Pacific: https://ftp.asia/data/public/ee2c7f
[2] Ibid
[3] Ibid
[4] Ibid
[5] WS. 38 How can we enhance the collaboration between Tech and IGF communities in APAC?: https://ftp.asia/data/public/e9cff2
[6] 52% of the countries have adopted DNSSEC in the Pacific (Pacific IGF: https://participate.icann.org/p3gf484cgqm/).
[7] Merger 7. Know Your Net – Enabling A-Z competences with Net Tech in the Pacific: https://ftp.asia/data/public/8f32a4

privacy rights. When developing standards, emphasis should be placed on understanding local culture and norms[8] which may result in different perceptions of threats to security within the APAC region.

Key cybersecurity issues raised were on the impact of emerging technologies such as IoT, and continued access to Whois, which is a system critical for incident response purposes. With billions of IoT devices, applications and services already in use, and more coming online, IoT security is of utmost importance[9]. Poorly secured IoT devices and services could serve as entry points for cyber-attacks[10], threatening the safety of individual users and compromising sensitive data. Such attacks on Internet infrastructure can affect the delivery of services such as healthcare and basic utilities. Action against cybersecurity threats such as IoT-based Distributed Denial of Service (DDoS) attacks need to be collectively taken by IoT device manufacturers, service providers, users, standards developing organizations (SDOs), policymakers, and regulators to protect the critical Internet infrastructure[11]. Additionally, it is important to increase awareness, that CERTs have continued access to Whois, as public accessibility might be restricted due to privacy considerations. Not only the technical operators but the end users also need to be trained on security techniques and methodologies as a preventive and proactive measure.

At the APrIGF there was wide acceptance that to mitigate security concerns and fight cybercrime, there is an urgent need to propagate cybersecurity education, awareness and strengthen the technical capabilities[12]. This demands more capacity building programmes and activities to strengthen the knowledge and capabilities of the technical operators. More dialogue and discussion around addressing cybersecurity gaps are also required.

Online Privacy and Protection

Privacy and data protection are critical issues. It is important to protect and respect the rights of users while ensuring digital security as a whole and prevent data-driven discrimination. In addition, 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 and women online[13]. The Internet community should take a proactive approach (contributing to the efforts of regulators and legislators to strengthen online privacy and data protection), and also collaborate with agencies and organisations which are trying to combat ‘hate speech’.

[8] Merger 5. Cybersecurity capacity for nations in the Asia-Pacific: https://ftp.asia/data/public/ee2c7f
[9] WS43. Securing continuity and availability of your IOT, beyond malicious hacking: https://ftp.asia/data/public/d0ae8e
[10] Ibid
[11] Ibid
[12] Merger 7. Know Your Net – Enabling A-Z competences with Net Tech in the Pacific: https://ftp.asia/data/public/8f32a4
[13] WS91. Privacy in the Digital Age & the Rule of Law: Mapping Privacy/Data protection and ICT Legal Frameworks in the Global South: https://ftp.asia/data/public/9e3e65

Emerging national and regional personal data protection laws, regulations and non-tariff measures (NTMs) have strengthened privacy considerations, especially those that have extraterritorial enforceability that affect the Asia Pacific region[14]. As tensions between contractual compliance obligations and national legislation arise, capabilities in monitoring legislation as it progresses must be improved to avoid multi-stakeholder processes being trumped by regulatory processes[15]. Private entities, especially social media platforms play a significant role in ensuring privacy online and refraining from compromising privacy rights of users[16]. Privacy by design needs to be emphasized along with informed consent standards and provisions for data access should be developed via a multi-stakeholder approach and rooted in human rights principles and the internationally recognized right to privacy[17].

As cross-border data-flow increases with the proliferation of online services[18], differing levels of protection in relevant jurisdictions and general lack of user awareness, the highest level of privacy protection should be guaranteed as a default safeguard and international minimum standards should be created.

Data protection is an evolving concept for the Pacific region, and while national data protection laws (such as the Online Safety Bill for Fiji[19]) are important to safeguard collection and use of personal data[20], capacity building initiatives are also needed to educate end-users on the value of protecting the use of personal information online.

Access and Empowerment

The immense potential of the human capital in Asia Pacific beckons for reliable, robust, and high-speed access to the Internet in order to excel in the digital age. Enabling access not only involves building infrastructure or connectivity, but also refers to other aspects such as access to knowledge and information, affordability, accessibility, inclusion, diversity, digital literacy etc[21]. Resources and support that help to empower access need to be considered. The key to socio-economic progress in the developing societies is quality education, and the delivery of education resources requires an accessible, affordable and open Internet. Often the last mile

[14] Merger 1. Cross-border Data & Contents Regulation in Asia Pacifc Region: https://ftp.asia/data/public/b9190c
[15] WS89. "Whois" collected, disclosed and protected: How we care about protecting data privacy?: https://ftp.asia/data/public/7bd735
[16] WS91. Privacy in the Digital Age & the Rule of Law: Mapping Privacy/Data protection and ICT Legal Frameworks in the Global South: https://ftp.asia/data/public/9e3e65
[17] Ibid
[18] Merger 1. Cross-border Data & Contents Regulation in Asia Pacifc Region: https://ftp.asia/data/public/b9190c
[19] The Fiji Government has recently introduced an Online Safety Bill that will see irresponsible social media users paying up to $20k in fine and face imprisonment of up to five years if investigated by the Online Safety Commission and found guilty. This bill will impact on hateful and harmful electronic communications and the posting of intimate visual recordings that would impact women and children as victims. (http://www.parliament.gov.fj/bills/ - Online Safety Bill 2018; http://www.parliament.gov.fj/wp-content/uploads/2018/03/Bill-7-Online-Safety-.pdf , amendment: http://www.parliament.gov.fj/wp-content/uploads/2018/05/Amended-Draft-of-Bill-No.-7-Online-Safety-Bill.pdf)
[20] Merger 2. Case Studies of Censorship, Surveillance, and Transparency Reporting in Asia : https://ftp.asia/data/public/9f2fe2
[21] Pacific ICT Plenary: Challenges and Opportunities of Connectivity in Small Island States: https://ftp.asia/data/public/a6d0e2

connectivity becomes a major barrier to access, especially in the landlocked and small island developing countries[22].

The use of emerging low cost network solutions such as Community Networks not only provide access but also empower the local communities to become an active part of the Internet operations[23]. The provision of Internet access should be backed up by meaningful local content and demand-driven solutions that propel Internet usage in the country. Governments, more particularly in the Pacific sub-region[24], should be encouraged to play an assistive role by creating an enabling Policy environment, conducive business incentives[25], expanding universal access, improving digital literacy and offering capacity building initiatives. At the same time, Internet shutdowns and restrictions are detrimental to the freedom of expression and right of universal access to Internet[26].

By engaging youth[27] and marginalized communities into the Internet development process can lead to a more inclusive and equitable Internet access for all users.

Similarly, it is imperative to devise a comprehensive disaster management plan, including Internet accessibility before and after the disaster, in order to save human lives and improve emergency response time[28]. It is the collective sentiment of the Asia Pacific community that the right balance of facilitative Policies, lucrative business models, smart users and awareness campaigns can bridge the digital divide that exists in the region.

Digital Economy and Emerging Internet Technologies

Digital Economy has been taking over everyday life, not only with e-businesses but also with emerging technologies. In the coming years, it is expected that the digital trade and e-commerce will be the key enablers of the global economic growth and will change the ecosystem of the traditional trade[29]. Innovation of emerging Internet technologies will also help improve and accelerate global trade.

Disruptive innovations such as Blockchain, cloud computing, IoT, Artificial Intelligence (AI), etc. have the potential to redesign our interactions in business, politics and society and change existing economic structures and financial ecosystems. However, as they inevitably challenge traditional national borders, international cooperation is needed to align these emerging technologies and the existing social system. Algorithm discrimination, AI ethics and competing

[22] WS76. Least Developed Countries and Issues of Access: A Land Locked or Island Country Perspective: https://ftp.asia/data/public/24b784
[23] WS47. Community Networks – Internet access for the community by the community: https://ftp.asia/data/public/3025aa
[24] WS.8 Effective eGovernment for empowering Pacific Citizens: https://ftp.asia/data/public/152289
[25] Pacific ICT Plenary: Challenges and Opportunities of Connectivity in Small Island States: https://ftp.asia/data/public/a6d0e2
[26] Merger 6. Internet Restrictions in Asia Pacific Region and How to Mitigate: https://ftp.asia/data/public/16fe92
[27] WS. 28 Youth Participation Fills in Gaps, Niches Too: https://ftp.asia/data/public/f757a5
[28] WS. 85 Preparing for Natural Disasters: https://ftp.asia/data/public/5d21b4
[29] WS.105 Digital Trade and Development: https://ftp.asia/data/public/899f99

concerns of data privacy, censorships and surveillance that uses emerging technologies need to be weighed against technology as a tool to benefit society[30].

The development of all the new technologies contribute to the development of the markets. In facilitating this development, all stakeholders need to balance economic development with fostering innovation and civil rights involved in this social improvement through new technologies. Progress of each economy toward the UN Sustainable Development Goals by 2030 also requires national strategies that integrate social and economic measures which can embrace all these emerging technologies[31]. Good national governance and legislation are prerequisites for successful economic development, not to mention supranational cooperation.

Digital economy also inherently involves problems with data ownership and poses some novel questions concerning cross border data flow and data localization[32]. International businesses and enterprise as well as individuals will face complicated compliance issues involving foreign jurisdictions, and some countries have already enacted strict data localization laws which ensure the national governance of the data of their nationals. The emerging trends on the Internet seems to go against the primary ethos of the Internet – the one Internet, and the Internet communities in general are pushing back against the localization of data and balkanization of the Internet as a whole[33].

Governments around the world, instead, can provide an environment which help free flow of data with transnational laws, which will ultimately assist the enterprises to nurture the new technology innovation and cultivate talents. This will also ultimately bind the humanity as a whole by leaving rooms for open discourses and dialogues. MLATs and other regional agreements[34] are now being drafted also to make sure collaborative works of different jurisdictions to govern the data transactions and the Internet society in general. Regional cooperation can be one of the ways to ensure the related level of trans-border digital economy which will ultimately benefit the society with innovations and foster peace through trade.

Diversity and Inclusion

Diversity and inclusiveness are fundamental principles of Internet governance and key to shaping our sustainable future where everyone's voice is heard. Capacity building efforts in engaging women, youth, people with disabilities, and other marginalised groups, including indigenous people and non-English speaking population are important and should be

[30] Ibid
[31] Ibid
[32] Merger 1. Cross-border Data & Contents Regulation in Asia Pacific Region: https://ftp.asia/data/public/b9190c
[33] Ibid
[34] Ibid

encouraged[35]. The digital economy, including e-commerce and innovative technologies, can contribute to the empowerment of women and marginalized groups[36].

Efforts must be made to make the Internet more hospitable, safe and open to everyone. Online content should be available in all languages wherever possible, including encouraging the development and use of Internationalized Domain Names (IDNs). Online accessibility and the availability of services online particularly for people with disabilities remain a priority[37].

Development of content on the Internet should include accessibility as part of the agenda as such accessibility features can add to the user experience[38]. This could be achieved with various technological developments such as voice assistants and character recognition software. More can be done to involve people actively in developing inclusive technologies and online content. Further, inclusion should also shape the technology in a way that allows diverse social cultures to accept and adopt the Internet easily. The Internet community should work with different communities such as the education authorities to develop programmes for digital literacy[39] in all languages. While designing and implementing capacity building programs, particularly when engaging youths[40], factors such as age and usage interests of the target groups should be accounted for and leveraged upon to expand their usage of the Internet[41].

Policies should effectively encourage building skills and ensure the Internet remains an open and safe environment for users[42]. Policy reforms are needed to ensure gender-inclusive access to the Internet, increasing digital literacy, enhancing ICT skills and Science Technology Engineering and Math (STEM) studies, and building networks amongst women. Economic incentives to encourage diversity in the workforce should be explored. Focus is needed on building trust online, including better legislation and enforcement of laws against online abuse and harassment[43]. More consideration should be given to safeguard the wellbeing of vulnerable groups such as children[44].

The Internet should be easily accessible to the diverse social cultures to adopt, using the Internet to bolster their various communities. Thus, universal acceptance and internationalization and localization practices should be widely promoted as norms on the Internet.

---

[35] Merger 4. Taking Internet Governance to the Masses: Through Communication, Engagement and Capacity Building: https://ftp.asia/data/public/34f6f2
[36] WS.30 Responsibilities of Internet Platforms for Tackling Online Abuse Against Women & Other Marginalized Groups: https://ftp.asia/data/public/91d3b3
[37] WS.44 Putting digital accessibility policy into practice – Case studies from Vanuatu and Asian countries: https://ftp.asia/data/public/cbc97e
[38] Ibid
[39] WS. 83 Digital literacy, libraries and information services: supporting the community on the platform of the Internet': https://ftp.asia/data/public/9602e6
[40] WS. 28 Youth Participation Fills in Gaps, Niches Too: https://ftp.asia/data/public/f757a5
[41] WS. 94 Empowering Change with Data: Measuring Youth Digital Mobility: https://ftp.asia/data/public/9e69f9
[42] Merger 4. Taking Internet Governance to the Masses: Through Communication, Engagement and Capacity Building: https://ftp.asia/data/public/34f6f2
[43] WS.30 Responsibilities of Internet Platforms for Tackling Online Abuse Against Women & Other Marginalized Groups: https://ftp.asia/data/public/91d3b3
[44] Ibid

Multi-stakeholder Participation in Internet Governance

Collaborative multi-stakeholder participation is acknowledged globally as the most productive approach to outreach and capacity building for Internet governance[45]. However, the full benefits of the multistakeholder model that encourages multiple perspectives provided by voices of all ages and backgrounds, can be hindered somewhat by some Pacific cultures, due to their traditionally hierarchical approach to discussions and decision-making. This was evident in a discussion about eGovernment[46] and the reticence displayed by Pacific governments to encourage citizens to access government information online or to invite them to engage in online discussions about government decisions. Lack of internet access is a form of control of information by some governments.

Exposure to the Youth Internet Governance Forum (YIGF) by young Pacific Island participants[47] highlighted that their need for increased access, education and capacity building that would enhance their understanding of the Internet itself, was an essential pre-requisite to their understanding and engaging in discussions related to even basic Internet governance concepts. Internet governance should be a natural progression through the school curriculum. Many APrIGF Pacific participants admitted that they were unaware of what the Internet was and how it worked, let alone how its governance was managed. This made it more difficult for them to contribute to discussions with their Asian counterparts on topics concerning the wider Asia Pacific region.

Capacity building efforts are critical in order to encourage new participants in events such as the APrIGF, but, different approaches need to be identified to spread the awareness about Internet governance more effectively within different communities. Creating ways to encourage newcomers to speak up and tell their stories would be a good start. Transforming complex and technical Internet governance issues into understandable language for all, would also not only increase greater understanding but also encourage more participation[48]. In addition, the benefits and expectations of these multi-stakeholder discussions and forums must be clear and effectively conveyed.

When knowledge is lacking, engagement doesn't really happen. True engagement can come about through an academic education but with regards to Internet governance, enhanced learning is also being encouraged within the Asia Pacific region through participation in Schools of Internet Governance (SIGS)[49], Internet Governance Academies (IGAs), and national and regional IGFs. All of these opportunities introduce new learning and capacity building through the multi-stakeholder model and create new networks at regional and local levels for participants from diverse backgrounds, encouraging greater knowledge and the sharing of best

[45] Merger 4. Taking Internet Governance to the Masses: Through Communication, Engagement and Capacity Building: https://ftp.asia/data/public/34f6f2
[46] WS.8 Effective eGovernment for empowering Pacific Citizens: https://ftp.asia/data/public/152289
[47] Youth Internet Governance Forum 2018 Vanuatu: http://aprigf.vu/yigf-agenda/
[48] Merger 4. Taking Internet Governance to the Masses: Through Communication, Engagement and Capacity Building: https://ftp.asia/data/public/34f6f2
[49] Asia Pacific Alliance for Schools & Academies of Internet Governance (APASA): http://apasa.asia/

practices. Fellowships offered by I* (I-star) organisations[50] are welcomed within the Asia Pacific region to usher new leaders and newcomers into the Internet ecosystem. Attracting participants to these learning platforms at local or regional level will facilitate more multi-stakeholder participation that can increase individual contributions from the Asia Pacific region at the global IGF level.

[50] I* organisations: https://www.apnic.net/community/ecosystem/iorgs/