ASIA PACIFIC REGIONAL INTERNET GOVERNANCE FORUM TAIPEI 2024

SYNTHESIS DOCUMENT

PROCESS

The Synthesis Document aims to document items of common interest relevant to Internet governance in the Asia Pacific region and has developed into one of the highlight innovations of the Asia Pacific Regional Internet Governance Forum (APrIGF) and inspired other national and regional initiatives to develop their own processes.

The 2024 Synthesis Document was drafted, synthesized and published by the 2024 Drafting Committee with the assistance of the APrIGF Secretariat.

Public input was sought during public input period I (15 August – 1 September), APrIGF conference Townhall sessions (21 – 22 August) and public input period II (23 – 31 October).

Comments were collected on the platform: https://comment.aprigf.asia during the public input periods.

2024 DRAFTING COMMITTEE

Saima Nisar, *Co-chair*
Luke Teoh Rong Guang, *Co-chair*
Au Yi Teng, *Security & Trust track lead*
Chanvoleak Ros, *Resilience track lead*
Socheata Sokhachan, *Ethical governance of Emerging Technologies track lead*
Abdullah Qamar
Angela Wibawa
Aviral Kaintura
Byambajargal Ayushjav
Hamna Noor
Jasmine Ko
Jessamine Pacis
John Rojell Y. Elizaga
Lokendra Sharma
Mabda Haerunnisa Fajrilla Sidiq
Md. Saimum Talukder
Nancy Kanasa
Rafi Uddin
Sana Nisar
Unggul Sagena
Zin Myo Htet

For full affiliation information, please see Appendix I

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Asia Pacific Regional Internet Governance Forum (APrIGF) 2024 was held from 21-23 August in a hybrid format, hosted by Taiwan Network Information Center (TWNIC) in Taipei. This marks APrIGF's return to Taipei since the 2016 meeting. The event was held in conjunction with the 2024 Taiwan Internet Governance Forum and the 2024 Asia Pacific Youth Internet Governance Forum.

The overarching theme for APrIGF 2024 is “Evolving Ecosystems, Enduring Principles: Shaping Responsible Internet Governance”. The Internet governance landscape in the Asia Pacific (APAC) region is continually transforming. Internet connectivity and adoption are steadily increasing, yet the challenges around inclusion, safety and security, affordability, and digital rights remain critical. As Internet ecosystem stakeholders diligently work to address these challenges, the core Internet principles of openness, decentralisation, and accessibility for all are still critical today and in the future. With the advent of new and emerging technologies, and the potential for AI to accelerate these new changes, how should we tackle the corresponding governance issues that arise?

The main theme incorporates three high-level thematic tracks, namely ***Security & Trust***, ***Resilience***, and ***Ethical Governance of Emerging Technologies***.

The ***Security & Trust*** *track* addresses key issues in combating misinformation, promoting digital literacy, and safeguarding vulnerable groups in the Asia Pacific region. Cross-regional and sub-regional collaboration with emphasis on developing economies, ethical considerations in fact-checking, strengthening digital education, and supporting a continued multistakeholder approach in Internet governance are highlighted as crucial approaches. Key themes include enhancing media literacy, protecting digital rights, and fostering informed engagement amongst stakeholders like governments, technology players, the technical community, and the civil society.

The ***Resilience*** track addresses the crucial need for a resilient Internet to withstand challenges such as natural disasters, climate change, and geopolitical tensions, particularly in the APAC region. The emphasis is on multistakeholder collaboration to strengthen infrastructure and ensure uninterrupted communication. A key focus is on enhancing the resilience of small Internet Service Providers (ISPs) and addressing the digital divide, particularly in remote areas. The discussions also highlight the importance of aligning governance models with technical standards, adopting eco-friendly technologies, and preventing Internet fragmentation through regulatory harmonisation and inclusive governance. Stakeholders must prioritise a balance between security and the global interoperability of the Internet.

The ***Ethical Governance of Emerging Technologies*** track addresses the rapid advancement of emerging technologies, particularly in the domains of artificial intelligence (AI), machine learning (ML), and digital platforms, which are transforming economies and societies across the APAC region. While these technologies unlock transformative potential, the integration of these technologies into everyday life raises significant ethical concerns, including issues of privacy, data governance, algorithmic bias, and access inequality. Key themes include the importance of creating a regulatory framework that encourages innovation while ensuring the ethical use of emerging technologies, particularly in vulnerable and marginalised communities, and ensuring that advancements in AI and related technologies are accessible to all segments of society is crucial in preventing the widening of existing digital divides.

It is important that the insights and recommendations generated during APrIGF 2024 be actively pursued and implemented. An innovation for this year's Synthesis Document is the Call to Action for Stakeholders that list concrete steps each stakeholder group is urged to commit to as we move towards the WSIS+20 review and IGF mandate renewal next year. Continued collaboration and commitment from all stakeholders will be vital in navigating the complexities of the digital landscape, promoting inclusivity, and safeguarding fundamental digital rights for all communities in the Asia Pacific region, helping shape an Internet ecosystem that upholds enduring principles while embracing responsible innovation.

SECURITY & TRUST

The principle of security and trust emphasises the necessity for robust cybersecurity measures, transparency, and accountability to maintain a trusted and secure Internet environment. As technologies evolve and the Internet ecosystem becomes more complex, safeguarding user data, ensuring information integrity, securing and sustaining stakeholders' trust, and protecting online identities are paramount. This involves addressing cybersecurity risks, data privacy concerns, online safety, and the protection of vulnerable groups – all the while ensuring that the Internet will not be fragmented. A collaborative, multistakeholder approach is essential to develop effective strategies that not only defend against current threats but also anticipate and mitigate future risks. It is imperative to foster an Internet environment where users feel safe and trust the systems they interact with.

The Internet ecosystem is evolving exponentially due to the continuous development and expansion of technologies, platforms, and services; it is also driven by innovation, market demands, and emerging technologies. Diverse stakeholders, technological advancements, and the increasingly dynamic nature of ecosystems have introduced many complex issues for the security and trust of the Internet, making it challenging to ensure robust security measures and maintain trust. How can enduring principles and time-tested approaches, built in a collaborative manner for shaping responsible Internet governance, address complex challenges such as cybersecurity risks, data privacy concerns, information integrity, online safety, online child protection, gender-based violence, and trust in innovation while ensuring the continued smooth and interoperable operation of the Internet?

DIGITAL TRUST, SECURITY & PRIVACY

Building digital trust is crucial for ensuring a secure and inclusive digital ecosystem. Trust is established through transparency and accountability in digital processes and transactions. Mathematical trust, such as that provided by blockchain technology, holds promise for ensuring confidence in digital interactions without a central authority. Health data governance exemplifies the significance of robust data regulations and policies. For instance, economies like South Korea are beginning to utilise big medical data, at the same time underscoring the need for clear regulations to ensure its safe and ethical use.

Biometric Verification and Identity Protection

Implementing biometric verification during SIM issuance is a strong solution to prevent account takeovers via SIM card swapping. This would add a secure layer of identity verification, making it harder for attackers to fraudulently obtain a SIM card. Additionally, holding telecom providers liable if important accounts are hacked due to SIM swapping can incentivise them to enhance security measures, ensuring greater protection for users[1]. This dual approach can significantly reduce the risk of SIM card fraud and protect users' sensitive accounts.

[1] APrIGF, "Defending against Digital Deception: Strategies for Preventing Online Scams and Identity Theft?", proposal form. Available at

Third-Party Authentication in Financial Transactions

There is a very high need for a third-party authentication solution that will ensure that the citizens of an economy can decide and know the receiver of said money. There is an implemented method in Vietnam where if someone is trying to transfer money more than a certain threshold, the bank needs the user to use facial recognition[2] but it can be bypassed with an image, which highlights the need for the technology to be improved. The improved system could be implemented across multiple economies in the Asia Pacific to ensure better security in financial transactions.

Preventing Online Scams and Identity Theft

Educating users about recognising and avoiding scams is as important as developing robust measures (e.g. through multi-actor authentication, biometric verification, and third-party authentication practices securing digital identities) to empower individuals against deceptive tactics. The importance of enhancing digital literacy and providing education about online scams among users cannot be overstated[3]. International cooperation plays a pivotal role in sharing information and countering global scam operations, fostering a more secure digital environment. Collaborative efforts among governments, private organisations, and individuals are essential to effectively combat these threats and enhance digital security.

Balancing Security and Free Speech in Messaging

The rise of online scams and identity theft poses significant risks to digital trust and security. The challenge of preventing messaging scams while protecting privacy and free speech is increasingly complex. In the Asia Pacific region, cybersecurity laws must strike a balance between security and Internet freedom. Mobile communication's widespread usage makes users a prime target for messaging scams. Deploying AI-based content validation, anti-phishing software, and regulatory frameworks requiring sender identification helps combat these scams effectively. For example, regulatory frameworks, such as those implemented in Vietnam[4], which involve rigorous third-party authentication practices, are essential for ensuring secure financial transactions.

Ensuring that these measures have appropriate legal bases, minimal intervention, and respect for privacy while involving third-party oversight, strengthens their implementation and fosters

https://forms.for.asia/proposal/?proposalform=NjYyMjk4YmE2YzEwMy8vMzQvLzE5NDIvLzA= (accessed on 21 October 2024)

[2] The State Bank of Vietnam, “SBV’s guidance on implementation of Decision 2345/QD-NHNN”, news article. Available at https://sbv.gov.vn/webcenter/portal/en/links/cm409?dDocName=SBV604617 (accessed on 21 October 2024)

[3] APrIGF, “Messaging scam and combatting to protect human rights and democracy”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyYmJiODdiMDEwYS8vMzQvLzIwMTAvLzA= (accessed on 21 October 2024)

[4] APrIGF, “Defending against Digital Deception: Strategies for Preventing Online Scams and Identity Theft?”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMjk4YmE2YzEwMy8vMzQvLzE5NDIvLzA= (accessed on 21 October 2024)

user trust. Transparency and accountability are vital in ensuring that government and telecom measures do not infringe on privacy and free speech. Moreover, end-to-end encryption should be encouraged to protect user privacy and data integrity, strengthening overall cybersecurity and reducing the risk of unauthorised access.

Cybersecurity and Human Rights in APAC

In the Asia Pacific region, cybersecurity laws must balance the imperatives of security with the need to uphold Internet freedom. The influence of authoritarian digital governance models in economies like Vietnam, Cambodia, Nepal, and Pakistan poses significant challenges to civil liberties. For instance, these economies have adopted cybersecurity laws that include data localization and digital surveillance provisions, which threaten freedoms of expression and information.

Thailand's legislation exemplifies this struggle, with vague provisions in the Cybersecurity Act 2019[5] and Personal Data Protection Act 2019[6] (PDPA 2019), enacted in 2019, that equates national security with public safety, potentially threatening political freedoms. These laws have been strongly supported by various government agencies in Thailand, reflecting a focus on national security priorities[7]. Conversely, Taiwan's transparent and participatory governance model provides a viable blueprint for achieving security without compromising rights[8]. Taiwan's civic engagement platforms like JOIN[9] and the fact-checking tool Cofacts[10] highlight the benefits of inclusive governance in maintaining trust and security.

Developing robust oversight mechanisms, maintaining strong encryption standards, and implementing gender-responsive policies are essential steps for a secure and inclusive digital environment. Addressing the needs of vulnerable populations, including children and marginalised communities, through responsible data handling and digital literacy initiatives is critical for fostering digital trust and ensuring a safe digital future. Protecting children's privacy on social media and promoting digital literacy are critical steps toward creating a safe digital space for future generations.

In conclusion, addressing digital trust, security, and privacy requires a multifaceted and collaborative approach. Incorporating transparency, accountability, and inclusivity into digital governance, and leveraging advanced technologies responsibly, will build a secure and

[5] Thailand National Cyber Security Agency, “Cybersecurity Act, B.E. 2562 (2019)”, government gazette. Available at https://www.mdes.go.th/law/detail/3572-Cybersecurity-Act-B-E-2562--2019- (accessed on 14 November 2024)

[6] Thailand Ministry of Digital Economy and Society, “Personal Data Protection Act, B.E. 2562 (2019)”, government gazette. Available at https://www.mdes.go.th/law/detail/3577-Personal-Data-Protection-Act-B-E--2562--2019- (accessed on 21 October 2024)

[7] APrIGF Document Platform, “Asia Pacific Regional Internet Governance Forum 2024 Taipei Synthesis Document – Draft 1”, public comment. Available at https://comment.rigf.asia/#comment-1882 (accessed on 17 November 2024)

[8] APrIGF, “Infrastructures of Repression: Cybersecurity and Human Rights in the Asia Pacific”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYzNDgyZTU0Mzc5ZS8vMzQvLzIwNDkvLzA= (accessed on 21 October 2024)

[9] Taiwan National Development Council, “Public Policy Online Participation Network Platform”, website. Available at https://join.gov.tw/ (accessed on 21 October 2024)

[10] Taiwan Cofacts, “Cofacts”, website. Available at https://en.cofacts.tw (accessed on 21 October 2024)

trustworthy digital ecosystem. Efforts to protect data integrity and user privacy, as well as ensure equitable access to digital tools must be ongoing and adaptable to emerging challenges and opportunities in the digital landscape.

MULTISTAKEHOLDER GOVERNANCE & POLICY REFORM

There is a pressing need for stronger participation in the multistakeholder model of Internet governance. This call for more representation, including by community members from the APAC region, arises from the recognition that existing processes that could impact the Internet, such as those leading up to the WSIS+20 Review, may have gaps in inclusivity. Although these processes evolve slowly, proactive engagement is crucial. Stakeholders are encouraged to keep themselves informed of developments and find avenues to contribute, whether by communicating with government representatives, engaging with organisations like ISOC or ICANN, or connecting with local community leaders. The value of having diverse voices in decision-making that could impact the Internet cannot be overstated, as their absence may lead to significant losses in representation and accountability, and possibly a fragmentation of the Internet. Effective collaborative Internet governance must include active participation from all stakeholders, including governments, the private sector, the technical community, and civil society. This participation can lead to a more resilient Internet by ensuring that security measures are not only reactive but proactive.

Successful communication and collaboration among various coalitions are vital. Information-sharing mechanisms, such as mailing lists (e.g., ICANN's WSIS+20 Outreach Network mailing list, APrIGF discuss mailing list), should be utilised to facilitate ongoing discussions and collective efforts in addressing multistakeholder challenges. Active participation in these dialogues could help inform policy-makers, shape policy reform, and enhance understanding across different sectors and stakeholders.

The adaptability of the multistakeholder model is crucial for addressing the complexities of governance in the digital age. Continuous conversations are needed to gather diverse perspectives and expertise, ensuring that policy discussions remain relevant and inclusive. Engaging with both mature and emerging audiences is necessary to raise awareness about governance processes and encourage broader participation in relevant discussions.

Furthermore, it is vital to break down silos that exist within specialised communities, such as technical experts and civil society organisations. Regional and global forums like APrIGF and IGF provide essential platforms for stakeholders to interact and collaborate beyond their usual domains of focus, such as policy, technical expertise, or advocacy. By fostering communication and collaboration, these platforms can facilitate better aggregation of knowledge and resources, ultimately enhancing multistakeholder governance.

Ongoing efforts should be made to assess and document both successful and unsuccessful cases in multistakeholder engagement[11]. This evaluation will provide critical insights into what worked and how to improve what did not, allowing stakeholders to learn from past experiences and adapt strategies accordingly.

Collaborative Governance for a Resilient Internet

The collaborative approach between Global South and Global North is critical in fostering interoperable governance frameworks that can prevent the future fragmentation of the Internet[11]. This collaboration is vital, especially amidst increasing geopolitical tensions, as it encourages cooperation over competition for the next generation of the Internet. The rapid growth of the Internet has led to various challenges, including security risks and cyberattacks. To address these challenges effectively, a multistakeholder governance model that involves both public and private sector actors is essential.

Furthermore, transparency and accountability in data collection practices are paramount. Stakeholders must commit to clear guidelines on data usage, ensuring that online services and products are open about their data practices. Governments can take proactive measures by collaborating with telecommunications operators to launch awareness campaigns that educate citizens on cyber threats and online scams. Combining traditional media, such as television and radio, alongside digital platforms, can enhance outreach efforts.

Investment in digital infrastructure is another critical area requiring policy and regulatory reform. Public-private partnerships, capacity building, and digital literacy initiatives must be prioritised to create a more inclusive Internet. Regional cooperation and knowledge-sharing among stakeholders can foster innovative technologies, ensuring affordable access solutions that empower communities globally. By harmonising regional approaches, we can enhance social media accountability and safety, paving the way for a more secure and resilient Internet.

Harmonizing Regional Approaches for Social Media Accountability

To tackle the challenges posed by social media in the digital age, a harmonised regional approach to accountability and safety is key. This involves the creation of consistent policies and shared frameworks that can be applied across jurisdictions, addressing issues such as misinformation, hate speech, and online harassment. By establishing common standards for content moderation and data privacy, stakeholders can ensure alignment with international human rights principles.

Regional coalitions must facilitate collaboration among governments, tech companies, and civil society organisations to effectively combat the pervasive issues related to online harm. This collaboration should extend to capacity building. For instance, educational programs targeting social media platform users, influencers, and vulnerable groups can help them recognise disinformation and understand its broader societal impacts. Additionally, social media moderators can be trained to better detect and remove gendered attacks in a timely manner,

[11] APrIGF, "NetMundial+10, GDC, WSIS+20 – what else is happening in the world of Internet governance", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyYmU1MTBlZDZiZS8vMzQvLzIwMTUvLzA= (accessed on 21 October 2024)

enhancing the safety of online spaces. The establishment of regional oversight bodies can provide a platform for dialogue, enabling stakeholders to monitor compliance with these standards and ensure that platforms adhere to them. Moreover, investing in digital literacy and public awareness campaigns can empower users to navigate online spaces safely and responsibly.

Legal frameworks must also be adaptable, addressing emerging threats while preserving fundamental freedoms, including the right to freedom of expression. A balanced approach that considers both safety and expression will be crucial in fostering a healthy online ecosystem. By engaging with diverse perspectives from various regions, we can craft solutions that reflect the unique cultural contexts and needs of different communities.

In addition, the accountability of platforms must adopt a risk-based approach[12]. This approach allows for differentiated accountability measures tailored to the unique features and functions of various platforms. However, stakeholders must remain cautious of overly pessimistic risk-avoidance strategies that could inadvertently exacerbate the spread of disinformation. For instance, examining responses to legislative initiatives like Australia's News Media Bargaining Code[13] can inform the development of more balanced and effective policies. Engaging in ongoing research and collaboration among stakeholders will ensure that policies are grounded in data and reflect the complexities of online interactions.

HUMAN RIGHTS, INCLUSION & ADVOCACY

The evolving digital landscape presents unique challenges to human rights, particularly in regions such as the Philippines, Vietnam, Malaysia, and India. There is a pressing need to address the specific threat profiles and contextual nuances that affect these economies. A commitment to enhancing community guidelines and ensuring the availability of essential materials in multiple languages is crucial. While gaps currently exist in translation and accessibility, the potential for artificial intelligence to improve language inclusion and accessibility is promising. Continuous efforts are necessary to make significant advancements in this area.

When it comes to government requests for content removal, it is imperative to uphold a transparent and structured process. Such requests must be rigorously assessed against established community standards, along with comprehensive legal and human rights reviews. This dual commitment to comply with local laws while safeguarding international speech protections illustrates the complexities inherent in navigating governmental pressures. It is essential to maintain global policies and specific mitigation strategies tailored to the unique dynamics of each economy, ensuring that rights are protected effectively.

[12] APrIGF, "Platform Accountability in South and Southeast Asia", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMGI0MzZjZDljYS8vMzQvLzE5MjMvLzA= (accessed on 21 October 2024)

[13] Australian Competition & Consumer Commission, "News media bargaining code", treasury laws amendment bill. Available at https://www.accc.gov.au/by-industry/digital-platforms-and-services/news-media-bargaining-code/news-media-bargaining-code (accessed on 21 October 2024)

Healthcare and human rights defenders represent sectors under significant threat, particularly in the wake of the COVID-19 pandemic and ongoing hybrid conflicts. Cyber attacks on these vital sectors highlight the urgent need for a multistakeholder approach to enhance cyber resilience. Recognising the intersection between healthcare and human rights protection can foster a collaborative environment where both sectors are fortified against emerging threats.

In conclusion, fostering human rights and inclusion in digital advocacy requires ongoing dialogue and engagement among various stakeholders. Establishing connections and collaboration across civil society organisations can bridge existing gaps and reinforce the protections needed for human rights defenders. Continued engagement beyond formal sessions is critical to develop actionable strategies that promote inclusivity and uphold human dignity in the digital age.

Addressing Vulnerable Groups in Digital Spaces

The protection of vulnerable groups in the digital realm necessitates a nuanced understanding of religious affiliations and cultural sensitivities. Content that may be perceived as blasphemous crosses a critical line, demanding condemnation to uphold respect for diverse beliefs. As advocates for human rights, the need for platforms that actively engage human rights defenders is important, especially in urgent scenarios where traditional methods prove ineffective and slow. The lack of prompt responses often leaves marginalised voices unheard. Therefore, raising awareness and promoting adherence to UN guidelines among human rights defenders is essential for effective advocacy.

However, the gap between policy and implementation remains significant, particularly regarding the protection of human rights defenders. While offering innovative solutions, technology also presents challenges as it can be weaponized against those advocating for rights. The ongoing discourse around AI liability highlights the complexities within global governance frameworks. Representatives from major tech companies like Meta and Microsoft[14] revealed that while initiatives exist, safeguarding goes beyond mere statements. A proactive, action-oriented Corporate Social Responsibility framework is critical for these corporations to genuinely secure customers’ rights regarding freedom of expression and digital security. Furthermore, establishing transparent accountability mechanisms among tech companies, governments, and civil society is paramount to prioritising users' rights.

Multistakeholder Engagement and Inclusivity

In discussions surrounding human rights and digital governance, the concept of multistakeholder engagement has often been criticised for falling into tokenism. While companies like Meta and Microsoft[15] participate in dialogues about human rights, genuine

[14] APrIGF, “Digital Frontlines: Safeguarding Human Rights Defenders in the Cyber Age”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMTE5MmRkNTFkYS8vMzQvLzE5MjgvLzA= (accessed on 22 October 2024)

[15] APrIGF, “Digital Frontlines: Safeguarding Human Rights Defenders in the Cyber Age”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMTE5MmRkNTFkYS8vMzQvLzE5MjgvLzA= (accessed on 22 October 2024)

engagement requires involvement at all levels—from planning to monitoring. The voices of human rights defenders, particularly those representing minority communities, must be included in decision-making processes to ensure that policies reflect the realities faced by the most vulnerable.

The exclusion of grassroots perspectives not only undermines the effectiveness of these discussions but also perpetuates a cycle of neglect regarding urgent human rights issues. A commitment to authentic multistakeholderism involves creating platforms for diverse voices, and ensuring their concerns are addressed and integrated into policy development. The example of Taiwan's public platform[16], which encourages government responses to citizen proposals, exemplifies how inclusive mechanisms can enhance accountability and responsiveness. Such initiatives can empower marginalised groups—women, children, and indigenous peoples—by amplifying their voices and ensuring their needs are recognised by authorities.

The importance of addressing the digital divide cannot be overstated. As discussions on a Digital Bill of Rights[17] evolve, key principles must include privacy protections, the right to free expression, access to information, due process, and digital inclusion. By investing in digital infrastructure and promoting digital literacy, governments can help bridge this gap, fostering an inclusive digital environment where all voices are heard and respected.

Combatting Online Harassment of Human Rights Defenders

The ongoing harassment and intimidation of human rights defenders on various online platforms raise critical questions about the accountability of these platforms. While major companies are taking steps to implement safeguarding measures, it is evident that harm is still prevalent on smaller, less regulated platforms. Effective solutions require a holistic approach to combat the organised violence faced by human rights advocates.

Panel discussions often neglect the critical aspect of online safety in conjunction with the physical safety of defenders[18]. This interconnectedness is crucial for creating comprehensive protection strategies. The experiences of defenders in the field during crises are essential to understanding the challenges they face and developing effective responses.

Moving forward, it is imperative that we not only share success stories and best practices but also prioritise the perspectives of those directly impacted by these issues. Learning from the experiences of human rights defenders will inform industry practices, ensuring that their tools and protocols adequately address the threats they face. Comprehensive training programs

[16] vTaiwan, “vTaiwan”, website. Available at https://vtaiwan.tw/ (accessed on 22 October 2024)

[17] APrIGF, “Digital Bill of Rights: A Systematic Bottom-Up Approach Towards Freedom in the Digital Age”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMGRhMDdjOTlhZi8vMzQvLzE5MjUvLzA= (accessed on 22 October 2024)

[18] APrIGF, “BreaktheSilo: Streamlining Gender Safety in the Digital Space”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyYzM0ZTdjYmE3ZC8vMzQvLzIwMzQvLzA= (accessed on 22 October 2024)

focusing on both online and offline safety measures should be implemented to equip defenders with the knowledge necessary to navigate and mitigate risks effectively.

Incorporating a human rights-centred approach into technology development and implementation will promote a safer digital space for all. By fostering a dialogue that includes the voices of defenders, we can work toward building more resilient structures that support human rights in the cyber age.

DISINFORMATION, MISINFORMATION & MEDIA ACCOUNTABILITY

The rapid proliferation of disinformation and misinformation across the Asia Pacific region poses significant challenges to media accountability and the integrity of information ecosystems. Stakeholders recognise the urgent need for enhanced collaboration among fact-checking organisations within the region, particularly in light of autocratic regimes engaging in information operations. These regimes often propagate misinformation, further complicating the efforts of civil society and media actors to uphold truthfulness in reporting.

There is a growing recognition of the importance of training and capacity building initiatives aimed at fact-checkers and media professionals. Initiatives, such as cross-border training programs among fact-checking organisations, have demonstrated potential for fostering a more resilient response to misinformation. For instance, collaborative efforts between Taiwanese and Filipino fact-checking entities have successfully trained community members, enhancing their skills to identify and combat misinformation in local contexts.

Efforts must be made to establish robust networks of fact-checkers across the region, particularly in economies experiencing political upheaval. Notably, the training of fact-checkers from Myanmar prior to the coup illustrates the potential for these initiatives to strengthen media accountability. Despite the challenges posed by political repression and the exile of journalists, recent efforts to reorganise fact-checking communities outside Myanmar have reignited hope for effective responses to misinformation.

The need for a united coalition of fact-checkers in the Asia Pacific is evident, as disparities in resources and attention can hinder effective information verification efforts. Topics like the South China Sea conflict and the systemic spread of misinformation from governments should receive more visibility and scrutiny in regional forums. By amplifying the voices of Asia Pacific fact-checkers and encouraging the sharing of resources, such a coalition can help address blind spots in the global discourse on disinformation and misinformation[19].

The sustainability of fact-checking initiatives remains a critical concern. Funding sources often influence the operations of fact-checking organisations, raising questions about independence

[19] APrIGF, “Charting the Path for a Regional Fact-Checking Coalition in the Asia Pacific”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMjIyMzg2M2E5YS8vMzQvLzE5MzcvLzA= (accessed on 22 October 2024)

and credibility. To navigate these challenges, a commitment to core principles of truthfulness and transparency in funding can fortify the legitimacy of fact-checking efforts.

While fact-checking is not a panacea for the complex landscape of disinformation, it plays a crucial role in detecting false narratives and promoting community engagement. The participation of local communities in fact-checking efforts is essential, as it not only builds trust but also fosters a culture of accountability in media consumption. Ultimately, strengthening media accountability mechanisms will require a multifaceted approach that combines fact-checking, community involvement, and systemic support from regional stakeholders.

Strengthening Fact-Checking Initiatives

Engaging grassroots initiatives alongside larger coalitions ensures that the voices of smaller Pacific economies are not overlooked. For instance, local communities often have a deeper understanding of the misinformation circulating within their regions and can contribute valuable insights to the coalition. Additionally, establishing accountability-based timetables can help track progress and maintain the momentum needed to combat misinformation effectively. Ultimately, empowering local fact-checking organisations through collaboration will enhance their capacity to navigate the complex landscape of disinformation and media accountability[20].

EDUCATION & CAPACITY BUILDING

As the rapid digitization of society progresses, there is an urgent need to build solid pillars of freedom to ensure the digital age does not evolve into an environment of surveillance and control. Major tech platforms like Google, Meta, and TikTok dominate the digital landscape, but there remains a critical need to educate the public about the importance of digital freedom[21], privacy, and autonomy. Capacity building efforts should focus on helping individuals understand the broader implications of relying on these large platforms, as well as the potential alternatives that exist within the free and open-source software movement.

Education on privacy is essential to protecting digital rights, especially as data collection practices become increasingly pervasive. Privacy education should emphasise that privacy is not just about protecting data or preventing identity theft; it is a prerequisite for exercising all other freedoms. This understanding needs to be integrated into curricula from an early age, empowering individuals to navigate digital spaces safely and autonomously.

Moreover, efforts should be made to ensure that individuals are educated about their right to disconnect, as part of their digital autonomy. As digital platforms become more integral to everyday life, the right to disconnect is often overlooked. Communities should be educated

[20] APrIGF, “Gendered Disinformation - Deepening understanding and exploring countermeasures”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyYmU3ODYxOGI3NS8vMzQvLzIwMTcvLzA= (accessed on 22 October 2024)

[21] APrIGF, “Digital Bill of Rights: A Systematic Bottom-Up Approach Towards Freedom in the Digital Age”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMGRhMDdjOTlhZi8vMzQvLzE5MjUvLzA= (accessed on 22 October 2024)

about the importance of maintaining a balance between staying connected and preserving mental health.

Finally, building capacity to understand the legal frameworks that support digital rights is critical. It is necessary to educate policymakers, legal professionals, and the public about laws that can protect digital freedom. For example, initiatives similar to the US Section 230 of the Communications Decency Act[22], which enabled the growth of the early Internet, should be considered for promoting digital freedom and fostering an open Internet. Education and training programs should focus on preparing future generations to advocate for policies that protect against the overreach of big tech and surveillance capitalism.

Strengthening Digital Safety Through Education

Safeguarding user data, ensuring information integrity, and protecting online identities are paramount in today's digital world. While frameworks for privacy and security exist, they can only be fully effective when coupled with education that empowers users to protect themselves online. Capacity building should focus on raising awareness about digital rights and privacy, equipping individuals with the knowledge to identify potential threats and adopt best practices to secure their personal data.

Educational initiatives must address digital literacy at all levels—from students to professionals. Implementing training programs that teach individuals how to navigate privacy settings, recognise phishing attempts, and use encryption tools is essential. Furthermore, awareness campaigns should highlight the importance of transparency and accountability, ensuring users understand how governments and telecom companies may handle their data[23]. Independent oversight bodies can be established to monitor these practices, but individuals also need to be educated about their right to access secure Internet services without geographical, political, or social boundaries.

Targeted capacity building initiatives should focus on training law enforcement, judiciary, and other agencies to tackle cyber diplomacy and enforce global privacy best practices. As seen in Pakistan, where law enforcement agencies can intercept communications for safety purposes, there is a pressing need for capacity building within these institutions to strike a balance between security and citizens' privacy.

In addition to formal education, digital safety programs must involve parents, educators, and office workers. These efforts will foster a generation that not only understands digital risks but is equipped to mitigate them. In this way, the right to safe Internet access will be protected across diverse communities, regardless of age or gender.

[22] Cornell Law School, "Section 230 of the Communications Decency Act of 1996", U.S. Code. Available at https://www.law.cornell.edu/uscode/text/47/230 (accessed on 22 October 2024)

[23] APrIGF, "Digital Bill of Rights: A Systematic Bottom-Up Approach Towards Freedom in the Digital Age", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMGRhMDdjOTlhZi8vMzQvLzE5MjUvLzA= (accessed on 22 October 2024)

Combatting Gendered Disinformation Through Education

Gendered disinformation remains a significant challenge, particularly for women, transgender, and gender-diverse individuals in public spaces. These disinformation campaigns, which often include hate speech, harassment, and doxxing, aim to delegitimize their voices. To address this issue, a comprehensive education program must be integrated into digital literacy initiatives, particularly for young people, educators, and vulnerable communities.

Public awareness campaigns can empower individuals to recognise gendered disinformation and prevent its spread. Workshops, online courses, and educational materials in multiple languages should be developed to train individuals on the tactics used in these campaigns and the real-world impact they have. Schools and universities should integrate gendered disinformation awareness into their curricula, enabling students to understand the broader social implications of such campaigns and how they affect political discourse and cultural inclusion.

Beyond this, governments and civil society must collaborate to counter societal biases against women and gender-diverse people. Policymakers need to be educated on how to regulate emerging technologies, like AI-driven deep fakes, which are increasingly used to target vulnerable communities. Building capacity among policymakers to address these issues will ensure that digital spaces become safer for all.

Bridging Digital Gaps in Remote Areas Through Education

In many areas globally, access to the Internet remains fragmented due to technical and infrastructural limitations. Content Delivery Networks (CDNs) often impose minimum bandwidth requirements for local cache servers, which smaller economies like Bhutan may struggle to meet[24]. As a result, these economies experience restricted access to content, exacerbating the digital divide. To address these disparities, education and capacity building should focus on enabling remote communities to advocate for better infrastructure while developing local solutions to bridge the gap.

Educational programs targeting policymakers in smaller economies can help them better understand the technical requirements for accessing global content, allowing them to negotiate more effectively with CDNs. Simultaneously, community-based training can empower local leaders to create innovative workarounds, such as community-run networks that optimise existing bandwidth.

Moreover, there is a critical need to educate users about how to maximise the utility of limited connectivity. Digital literacy programs should teach individuals how to use lightweight web tools and applications that consume less data, ensuring that even those in remote areas can participate in the digital economy. Capacity building initiatives can also include technical training

[24] BlazingCDN, “Geographic Differences in CDN Performance and How to Address Them”, blog post. Available at https://blog.blazingcdn.com/en-us/geographic-differences-in-cdn-performance-and-how-to-address-them (Accessed on 22 October 2024)

for local IT professionals, enabling them to support and maintain local digital infrastructure, and reducing dependence on external providers.

In addition, creating an environment where citizens can actively engage in advocacy for better digital infrastructure is key. Educational programs should provide communities with the knowledge they need to advocate for Internet rights and digital access at local and international levels, fostering a more equitable Internet for all.

Empowering Vulnerable Groups Through Digital Education

The rise of technology presents both opportunities and risks for vulnerable groups, such as children, women, and marginalised communities. In regions like eastern India, children from shelter homes or marginalised communities are increasingly targeted for trafficking through online platforms. Education and capacity building are critical to safeguarding these populations and preventing exploitation.

A multi-pronged approach to digital education can help protect vulnerable individuals. First, digital literacy must be embedded in school curricula to ensure that children understand the dangers of online interaction, particularly when engaging with unknown parties. Parents and caregivers should also receive training on how to monitor Internet usage and protect their children from malicious actors. Governments need to establish accessible reporting mechanisms so that individuals can easily report suspicious activities, whether in schools, shelters, or communities.

Capacity building for law enforcement and judicial systems is equally important. Training these professionals to handle cases involving cyber exploitation, particularly trafficking, will ensure that they are better equipped to protect vulnerable groups. Local authorities should be educated on global best practices, enabling them to identify and dismantle trafficking networks operating through digital platforms.

Finally, building digital education programs that teach ethical governance is essential. Vulnerable communities must have a safe space to learn about their rights and gain access to information that empowers them to navigate the online world securely. Governments should ensure that these programs reach marginalised populations, giving them the tools to protect themselves while benefiting from the positive aspects of digital technology.

RESILIENCE

For communication infrastructure, services, and data exchange to continue to function dependably in the face of a variety of obstacles, the Internet's resilience is essential. To minimise Internet disruptions, various stakeholder groups must work together in concert. When creating policies that affect the interoperability of the Internet, stakeholders must collaborate closely. The necessity for this has increased due to the significant threats that natural disasters, climate change, and geopolitical tensions pose to the Asia Pacific region's vital infrastructure. Additionally, building resilient Internet infrastructure for small ISPs is essential, as they have a crucial role in providing Internet access to unreached and remote areas. The COVID-19 pandemic has further intensified Internet usage, creating opportunities for collaborative platforms that facilitate interaction among diverse stakeholders.

To build resilience at the design stage of systems, a code of practices governing processes — such as isolation of affected systems and recovery methodologies — should be adopted to mitigate the risks of deploying untested products and processes that could significantly impact system functionality. The role of multinational corporations, as highlighted by incidents like the CrowdStrike outage[25], raises concerns about conflicts of interest, especially when these companies advise governments on critical infrastructure. Governance is needed to separate business models from targeted advertising when such companies manage essential services like digital ID. Furthermore, increased global government participation and dialogue are crucial to creating policies that attract private sector investment in expanding digital public infrastructure.

Data centres are the backbone of the functioning of the Internet and the establishment of the interconnected world. The resilience of the Internet is impacted directly by the resilience built into the data centre infrastructure, where redundancy in the provision of elements and sub-systems ensures seamless operation during disruption. In addition, governance and regulations affecting the data centres need alignment with the Internet governance policies and regulations to achieve service levels and resilience.

Improving digital infrastructure and encouraging sustainable development are essential as the APAC region deals with an increase in cyber threats and disruptions. How can the region improve its digital infrastructure's sustainability, accessibility, and resilience? How can stakeholders minimise the carbon footprint of data centres, optimise energy consumption, and adhere to green standards to promote environmentally friendly technological growth? What cooperative actions might enable enterprises and local communities to mould their digital futures in accordance with socioeconomic priorities? Lastly, how can renewable energy adoption and energy-efficient solutions be successfully promoted and addressed?

[25] Su-Lin Tan, "Asia-Pacific faces fallout from CrowdStrike outage: 'It will continue to happen'", *South China Morning Post*, 26 Jul 2024. Available at https://www.scmp.com/week-asia/economics/article/3271923/asia-pacific-faces-fallout-crowdstrike-outage-it-will-continue-happen (Accessed on 22 October 2024)

RESILIENCE AND SUSTAINABILITY

The focus is on building resilient Internet infrastructure and sustainability in the face of challenges such as natural disasters, geopolitical tensions, and environmental concerns. Key discussions involve ensuring infrastructure like data centres and ISPs that can withstand disruptions while maintaining operations. Regulatory frameworks need to address resilience, particularly during disasters, technical standards to prevent tampering (like DNS), and the integration of eco-friendly practices such as reducing the carbon footprint of data centres. Taiwan’s experience with undersea cables and disaster recovery is a case study of how countries can build stronger infrastructure.[26] There is also a focus on promoting sustainability through green computing and energy-efficient solutions.

Internet Infrastructure and Development

In this era, there is a focus on exploring the balance between national security and the risks of Internet fragmentation. Examining the impact of the European Digital Services Act (DSA), intermediary liability, and the challenges in regulatory harmonisation across diverse communities in the APAC region raises questions on whether over-harmonization could ultimately undermine regulatory resilience. Emphasis is placed on community-driven, collaborative solutions to mitigate fragmentation while protecting digital rights. [27]

Regarding national security, some countries have started to implement their Internet with the support of countries with similar political ideologies. For instance, in Myanmar, the Myanmar E-Governance Master Plan 2030[28] envisages building a primary gateway for integrated national services, however the impact of implementation of this plan will create restrictions and control of citizens data for political purposes.

Additionally, from a small developing country perspective, particularly in Samoa[29], the transformative potential of technologies like satellite Internet constellations can be seen improving connectivity. However, regulatory blocks and infrastructural limitations hinder such advancements. In Samoa and across the Pacific, specific challenges related to regulatory frameworks impact the deployment of technologies like satellite Internet, including stringent regulations that may not accommodate emerging technologies. Overly restrictive or inconsistent

[26] APrIGF, "Strengthening the Digital Resilience of Taiwan: with Special Reference to Undersea Cables", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYxZjc1MWY3YWJmOC8vMzQvLzE5MjAvLzA= (Accessed on 22 October 2024)

[27] APrIGF, "Regulatory Resilience in the Age of Internet Fragmentation", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMTYyMTY2NzJmOC8vMzQvLzE5MzMvLzA= (Accessed on 22 October 2024)

[28] Republic of the Union of Myanmar, Ministry of Transport and Communication, “E-Governance Master Plan 2030”. Available at https://motc.gov.mm/sites/default/files/Myanmar%20e-Governance%20Master%20Plan%202030%20(%E1%80%99%E1%80%B0%E1%80%80%E1%80%BC%E1%80%99%E1%80%BA%E1%80%B8).pdf (Accessed on 22 October 2024)

[29] APrIGF, "Bottom-up Advocacy for a Resilient Internet", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyNzY2YmMwYWQ4NC8vMzQvLzE5NjUvLzA= (Accessed on 22 October 2024)

regulations can promote fragmentation, especially in rural areas that need connectivity most, exacerbating the digital divide and limiting efforts for universal access.

Affordability is a large barrier. Low-income households may not be able to afford to connect to satellite Internet because of various socio-economic factors. A possible solution is to provide the knowledge and capacity to the local communities to implement the community-based Internet[30] with the help of organisations with the necessary expertise.

Taiwan's past experiences with natural disasters, including the 2024 earthquake, can provide important lessons about the resilience of infrastructure. The case study emphasises that resilience is about how quickly systems can recover and return to their regular functions, not about preventing harm. To guarantee that Disaster Recovery (DR) sites remain available, the government or telecom authorities in the nation should create a framework mandating that all ISPs and telecom providers create a Business Continuity Plan (BCP). In order to prevent disruptions to the entire Internet during disasters and to ensure that communication continues, ISPs should also have several routes to their uplinks.[31]

Another important subtopic to highlight is the need for sustainable solutions in subsea cable laying, installation, and maintenance. It would also be useful to explore how digital trade agreements could shape the future resilience of subsea cables[32] and connections. For example, the EU-Singapore Digital Partnership (EUSDP) is a relevant resource, along with similar agreements between Singapore the UK, and Australia, as well as mentions in RCEP/IPEF.[33]

Environmental Impact of the Internet

Building on three years of research and development, and planned to expand to 15 jurisdictions across the Asia Pacific, including several least-developed countries, the EcoInternet Index[34] from DotAsia Foundation continues to investigate how various factors—such as energy, efficiency, and economy—impact the relationship between the Internet and the environment.

Evaluating the environmental impact of the Internet involves more than simply measuring its carbon footprint. Instead, how the growth of the Internet replaces more carbon-intensive traditional activities, offers valuable insights for policymakers. With Internet usage expected to surge, it is crucial to integrate sustainability into climate agendas and action plans.

[30] APrIGF, "Regulatory Resilience in the Age of Internet Fragmentation", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMTYyMTY2NzJmOC8vMzQvLzE5MzMvLzA= (Accessed on 22 October 2024)

[31] APrIGF, "Internet infrastructure resilience during disaster event - Case Study for the 0403 Taiwan Earthquake, and others", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMGUwNzcxOWI1NS8vMzQvLzE5MjcvLzA= (Accessed on 22 October 2024)

[32] APrIGF, "Strengthening the Digital Resilience of Taiwan: with Special Reference to Undersea Cables", proposal form. Available at https://aprigf.tw/programs/strengthening-the-digital-resilience-of-taiwan-with-special-reference-to-undersea-cables/ (Accessed on 22 October 2024)

[33] European Union, “EU-Singapore Free Trade Agreement”, 01 February 2023. Available at https://digital-strategy.ec.europa.eu/en/library/eu-singapore-digital-partnership (Accessed on 22 October 2024)

[34] DotAsia Foundation, "EcoInternet Index.” Available at https://ecointernet.asia (Accessed on 22 October 2024)

Efforts to reduce the Internet's carbon footprint, brings into the spotlight the importance of government intervention and eco-equipment certification in promoting sustainable practices. Additionally, case studies from Japan and New Zealand highlight effective strategies and initiatives that contribute to environmental sustainability in the digital realm. These examples underscore the potential for collaborative approaches to foster a resilient Internet while addressing ecological challenges.[35]

Digital Divide

More than half of the world's population who remain offline are located in South Asia, highlighting the urgent need to bridge the digital gap. Three key policy questions must be addressed: i) Why do most economies in South Asia have over 50% of their population offline despite direct access to submarine fibre? ii) What role can public-private partnerships and regional cooperation initiatives play in accelerating efforts to close these gaps? iii) How can we link digital development with rural development to enhance connectivity and access?

Some of these questions may be answered by governments across the sub-region re-evaluating their national broadband strategies to genuinely connect the unconnected. Many current strategies are merely ticking boxes, overlooking critical issues such as the cost of devices, availability of electricity, and gender disparities. Additionally, the lack of coordination among government agencies in providing services hinders progress.

In countries like Bhutan, a significant digital gap exists, particularly between urban centres like Thimphu and rural areas. The rugged terrain makes it challenging to build and maintain infrastructure, while the cost of Internet services and devices is prohibitive for many. Economic barriers widen this divide, and the lack of local content tailored to Bhutanese users further exacerbates the issue. Innovations such as satellite Internet constellations could potentially improve accessibility in these remote regions[36].

GOVERNANCE FOR RESILIENCY

The Global Digital Compact (GDC)[37] is a recurring topic in discussions on governance to strengthen the resiliency of the Internet - particularly how multistakeholderism and regulations shape the Internet's future and its impact on Internet governance discourse in the Asia Pacific region. Considerations on how national policies might fragment the global Internet lead the debate to examine ways to prevent such fragmentation. Civil society and local stakeholders play a crucial role in shaping Internet governance and advocating for policies that promote inclusivity and resilience. There is continuing discussion on balancing national security with global

[35] APrIGF, "Striving for EcoInternet, towards a resilient Internet", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMjljN2M1MDA0YS8vMzQvLzE5NDMvLzA= (Accessed on 22 October 2024)

[36] APrIGF, "Digital Leap- Enhancing Connectivity in South Asia", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMTM2OWQ1YjJkMC8vMzQvLzE5MzEvLzA= (Accessed on 22 October 2024)

[37] United Nations, document A/79/L.2. Available at https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf (Accessed on 22 October 2024)

interoperability and how emerging technologies, like satellite Internet, fit into a good governance framework.

Level of Censorship

There were proactive concerns about government censorship. The Internet Monitoring Action Project (iMAP)[38] focuses on monitoring censorship activities in South and Southeast Asian countries. While there are solutions available to counter government censorship, disseminating these technologies poses challenges, including additional training for engineers to implement necessary standards. A robust policy and governance framework is crucial, requiring adoption by multiple stakeholders such as governments, ISPs, ccTLD registries, and end users.

One specific technological recommendation is to implement DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT). These protocols encrypt DNS queries, protecting users from eavesdropping and manipulation by third parties, and making it more difficult for intermediaries to monitor or block specific DNS requests, thus mitigating some forms of DNS-based censorship.[39]

Proactive Role of Multistakeholderism

The Global Digital Compact (GDC) has the potential to reshape Internet governance discussions, influencing the future of multistakeholderism and the development of the Internet. Different processes may claim to adhere to the multistakeholder model to varying degrees, presenting challenges that the Internet governance community must address. Since the 2024 APrIGF meeting, the GDC has since been adopted at the Summit of the Future (22 September 2024) annexed to the Pact for the Future[40]. Discussions and clarifications around endorsement and implementation will impact the upcoming WSIS+20 review in 2025.

Bottom-up Advocacy Practices

Power asymmetries among and within stakeholder groups can call into question what “bottom-up advocacy” means. The expertise of each stakeholder group, (technical considerations and capabilities, human rights concerns and frameworks, innovative funding arrangements) should contribute holistically to advocacy practices and decision-making. There are worries that policy and commercial decisions may reinforce power asymmetries between stakeholder groups, which could lead to break down of the legitimacy of the multistakeholder process.[41]

[38] The Internet Monitoring Action Project, "About The Internet Monitoring Action Project (iMAP)", 2024. Available at https://imap.sinarproject.org/ (Accessed on 22 October 2024)
[39] APrIGF, "Enhancing Internet and Web Standards to Address DNS Tampering", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyYmFhMmU2ZWU0Ni8vMzQvLzIwMDYvLzA= (Accessed on 22 October 2024)
[40] United Nations, “Pact for the Future, Global Digital Compact and Declaration on Future Generations” https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf (Accessed on 27 November 2024)
[41] APrIGF, "Bottom-up Advocacy for a Resilient Internet", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyNzY2YmMwYWQ4NC8vMzQvLzE5NjUvLzA= (Accessed on 22 October 2024)

PREVENTING DISRUPTION

Reviews of the strategies used to stop and lessen Internet outages, particularly in light of the possible fragmentation brought on by different regulatory stances, show that harmonised policies can lessen isolation risks and compliance burdens, while regulations that are too restrictive or inconsistent can exacerbate fragmentation. Stakeholder collaboration is emphasised to guarantee the resilience of Internet services, especially in times of crisis. Technical steps to stop censorship and standards tampering, which can impair Internet access and integrity, point towards strengthening DNS security as one solution.

As a result of measures like gateway blocking and international data transfer restrictions, there were increasing worries about Internet fragmentation in the Asia Pacific region. Regional policymakers are facing criticism for enacting laws that could further polarise the area. To standardise standards and save compliance costs, experts and companies suggest implementing universal regulatory frameworks similar to those in the US or the EU. However, critics argue that universal regulations, which primarily serve corporate interests, could jeopardise community resilience and national sovereignty.

Countries like India and Singapore prefer divergent regulations, while Australia and Japan advocate for greater collaboration and consistency. The tradeoffs between national sovereignty and the risks of fragmentation, questions whether universal playbooks can reduce fragmentation or undermine resilience. In addition, the pros and cons of replicating global models versus developing local regulatory frameworks for the APAC region highlight principles that build community resilience while avoiding fragmentation.

There is a delicate balance between maintaining national security and addressing the growing risks of Internet fragmentation. Some of the key issues involve the impact of The European DSA[42], intermediary liability, and the challenges of achieving regulatory harmonisation in the diverse APAC region. The way forward for APAC points to fostering community-driven, collaborative solutions that protect digital rights while reducing the risks of fragmentation in a rapidly evolving digital landscape.[43]

[42] European Union, “The European Digital Services Act (DSA)”, 27 October 2022. Available at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en#:~:text=Digital%20Services%20Act%20(DSA)%20overview&text=Its%20main%20goal%20is%20to,and%20open%20online%20platform%20environment (Accessed on 22 October 2024)

[43] APrIGF, "Regulatory Resilience in the Age of Internet Fragmentation", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMTYyMTY2NzJmOC8vMzQvLzE5MzMvLzA= (Accessed on 22 October 2024)

ETHICAL GOVERNANCE OF EMERGING TECHNOLOGIES

In recent years, there have been unprecedented advancements in literacy rates, globalisation of trade and finance, technological innovation, and rapid population growth. However, these developments have also contributed to widening income inequality and highlighted the need for proactive governance measures to address emerging challenges. Technology is often said to be a neutral tool, but its impact depends heavily on how it is used and who wields it. With every major innovation— the Internet, the dotcom boom, or the modern social media generation—a recurring pattern emerges: dominant players initially rise to monopolise industries but eventually face disruption and decline. It remains to be seen whether new technologies, including AI, will follow this trajectory or retain their influence for a much longer period.

The multistakeholder approach has guided the Internet governance ecosystem for the last nearly two decades. This was not so in the early days of the Internet when governance was primarily the domain of a few key players. In the mid-2000s, the multistakeholder approach gained prominence after the World Summit on the Information Society (WSIS) in 2005 adopted a broader definition of Internet governance from the Working Group on Internet Governance (WGIG) incorporating categories of multistakeholder involvement[44], driven by the need for more inclusive and participatory decision-making processes. Ensuring ethical governance of emerging technologies will require legitimate frameworks where even the most disempowered are included from the beginning.

There is the need to ensure no technology enhances or aids the development of additional barriers and in the utilisation of newly obtained technologies, it is paramount to adopt a human-centric approach to protect basic rights. It is also essential that underserved, underrepresented and marginalised communities are able to reach out through the use of technologies to acquire and participate actively in the digital economy and its related socio-political activities.

PUBLIC PERCEPTION AND AI ACCOUNTABILITY

With approximately 4 billion people expected to vote in elections in more than 64 countries in 2024, the stakes for AI accountability are higher than ever. AI technologies, while offering immense potential, also pose significant risks by amplifying the spread of disinformation and misinformation, which can destabilise societies and undermine democratic processes. These threats, coupled with already fragile societal divisions, necessitate resilient frameworks to govern the use and deployment of AI.

Enhancing public trust in AI systems, particularly in sensitive areas like elections, requires robust accountability mechanisms. Without such measures, public fears about institutional integrity and societal polarisation could worsen. Developers must take responsibility for transparency by disclosing how AI systems function, detailing the data they use, and explaining steps taken to mitigate bias. Meanwhile, regulators should enforce accountability through audits,

[44] Working Group on Internet Governance (WGIG), “Report of the Working Group on Internet Governance”, June 2005. Available at https://www.wgig.org/docs/WGIGREPORT.pdf (Accessed on 22 October 2024)

impact evaluations, and public disclosures. Additionally, citizens should be empowered to challenge AI-driven outcomes that directly impact them. By addressing these challenges collaboratively, society can foster trust and ensure that AI systems serve the public good without compromising democratic integrity.

Information Ecosystems and AI Technology

AI technologies have changed and altered the ways people view information and the way it shapes societies. AI tools and algorithms such as deepfakes and bots prioritise content and spread misinformation on a greater level than ever. Such practices are seen in political content or advertisements; and disinformation practices used in times of elections to influence voting behaviours, affect political debates, can ultimately affect the integrity of democratic institutions.

Frameworks for Inclusive and Ethical AI Governance

In order to alleviate these threats, integrated systems for the development and governance of AI technologies must be inclusive, ethical, and developed in the public interest. Such frameworks are not one-size-fits-all and also need to be localised and tailored to existing social, technological, linguistic, and cultural differences. By rooting AI governance within the specific descriptions of needs and contexts of communities, it is likely that the public will be able to trust the technologies and that benefits AI brings can be equitably shared.

Also, building trust in AI-enabled systems has to do with how the governance system is designed in such a way that enables the AI systems to be accountable. This involves explaining in a simple manner how an AI system makes a decision, how the datasets which are used by the AI models are obtained, and what steps citizens can take when AI outputs that impact their rights and accessing services are produced.

Regional Cooperation for Ethical AI Standards

The methods for advancing AI systems through legal frameworks differ among different jurisdictions in terms of their positions of AI maturity. Legal policy issues and regulatory challenges are broad and complex, with many different vertical and metric scopes.

One of the biggest challenges brought about by AI is the question of trust in technologies that are being deployed across various sectors.[45] Cyber security has become the primary condition for trust as AI may open new avenues in manipulation and attack methods. This has caused new privacy challenges in the relationship between AI and data governance. For machine learning algorithms to be effective, it is essential to have relevant training on data such as AI and Ethics Training, Data Governance and compliance training, etc., to control this learning process to avoid any bias.

[45] APrIGF, “From Innovation to Impact: Responsible AI – challenges and opportunities to tackle online fraud and scams”, themed track proposal form. Available at https://aprigf.tw/wp-content/uploads/2024/08/Proposal-Form-From-Innovation-to-Impact-Responsible-AI-challenges-and-opportunities-to-tackle-online-fraud-and-sca2.pdf (Accessed on 22 October 2024)

Ensuring Inclusivity in AI Development

Inclusive AI development requires the active involvement of a wide range of stakeholders, particularly those from marginalised or underrepresented communities. For example, people with disabilities must have a seat at the table when developing AI systems to ensure their unique needs are addressed from design-phase to final product. AI technologies have the potential to greatly benefit persons with disabilities, but only if they are designed with accessibility and inclusivity in mind.

AI Governance as a Collective Responsibility

In its essence, the governance of AI is a global collaborative multistakeholder effort that involves governments, private corporations, the technical community, and civil society to ensure AI contributes to the positive development of human society.

Governments, tech companies, civil society organisations, and international bodies must collaborate to create policies that ensure AI technologies are not just ethical but also accessible to all. This involves setting standards for accessible AI design, providing support for localised AI development, and ensuring that underserved populations have access to the tools and resources needed to fully engage with AI systems. Thus, a regional approach is necessary to address these disparities and ensure consistent ethical standards across the board. Regional authorities can prove to be an asset in disseminating best practices, regulating harmonisation and initiating AI cross-border collaboration. Through collaboration, the APAC region can ensure that no economy, particularly those that have less developed AI capabilities, is left behind in the race towards ethical AI practices.

DIGITAL RIGHTS, LAWS, AND GOVERNANCE

Digital Sovereignty and Inclusive Policymaking

Economies across the APAC region have enhanced digital sovereignty but this may come at the cost of fragmentation of the Internet and endangerment of digital rights particularly in the regions of control as opposed to transparency. It Is necessary to address the structure and functioning of the legal systems so that these do not allow the rise of digital authoritarianism.

Governance polices and frameworks must be human rights centric with the full multistakeholder participation of all stakeholder groups to avoid policies that tend to favour the elite at the expense of the marginalised sections of society.

TRANSPARENCY AND CONSENT IN DATA USAGE

Need for Consent

Data usage must be limited to what users have authorised, and individuals have the right to control data collection and withdraw if they so choose. For example, in Taiwan, concerns over health data misuse have led the constitutional court to mandate new regulations by 2025.[46] South Korea is similarly grappling with finding the appropriate balance in regulating health data, while in South Asia, India has launched ambitious digital health data programs without yet implementing adequate protections for user privacy.

As data privacy concerns escalate in South and Southeast Asia, the voices demanding accountability of platforms toward regulating social media and communication platforms are getting louder.[54] Singapore is now talking about legislative measures, while Australia is facing voluntary agreements by the industry. Meanwhile, India is taking legislative actions and the effect will be increased transparency and curb harmful content as well. These different approaches reflect a struggle to balance the freedom of expression rights with safety concerns, but what is needed now is better-coordinated governance that strikes a balance between protecting users and building trust on digital platforms.

Advancing data privacy and trust

The countries of the Asia Pacific region need to ensure privacy protection principles are embedded in the legal frameworks to give a high level of protection and encourage innovation. Trust can be built by clearly delineating the legal bounds of data collection and the scope of data use. There should be clear communication of the purpose of users' data, and this can empower users to make informed decisions. This ensures the ethical, transparent, and consensual use of data.

This new wave of digital authoritarianism spurred the development of a Digital Bill of Rights[55]. This Digital Bill of Rights attempts to build a comprehensive framework that safeguards the fundamental rights of users within the virtual space and grants persons protection against state overreach when matters relating to emerging technologies come up. This can serve as a good precedent in instilling privacy, transparency, and consent in pushing for the push for ethical practices in data governance. A rights-based approach leads to a safer and more accountable digital environment.

ACCOUNTABILITY AND ETHICAL DATA PRACTICES IN MULTISECTORAL ENTITIES

The private sector has a vital responsibility to ensure ethical data practices and accountability for the adoption of emerging technologies. In this age where business organisations rely heavily on data, there should be clear and responsible practices around this area. A key issue is the opacity around how these companies gather, disseminate, and utilise individualised information. Consumer confidence calls for a clear establishment of transparency standards.

[46] APrIGF, "Health Data Governance through AI Booming Age : A Journey in Taiwan", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMjQ5MTQ4ZDY3MC8vMzQvLzE5MzkvLzA= (Accessed on 22 October 2024)

Mitigating Bias and Fairness Issues in AI

AI and automated decision-making pose larger ethical issues, especially around bias[47]. Algorithmic bias can adversely affect already disadvantaged groups thus creating a case for frequent audits to check for fairness. Accountability for adverse effects must be embedded in corporate behaviours.

Internal and External Accountability Mechanisms

Enlisting third-party auditors and ethics committees for independent reviews can help enhance accountability as well. These institutions can evaluate the data practices conducted and offer an impartial assessment of potential ethical risks.[48] Companies should be able to monitor their business processes by creating internal teams that will be in charge of data usage and compliance. Specific rules about data utilisation and employing ethics experts can foster compliance with data regulations.

Data Security and Breach Accountability

Data Security cybersecurity is an ever-present challenge, especially with unauthorised access to sensitive data being a major concern. More severe and detailed sanctions and regulations ought to be established so as to ensure businesses become proactive in safeguarding user data.

Monetization of Personal Data

The monetization of personal data raises significant ethical concerns, particularly regarding companies profiting from user information without adequate consent or compensation. Clear guidelines must promote fair data practices, ensuring users retain control over their information and benefit from its use.

Ensuring Accountability, Transparency, and Fairness in Data Governance

Users' rights must be safeguarded through trust building measures such as fair data processing. It is essential to be transparent with users about what data is collected, for what purpose, and how it will be utilised.[49] Data as an Asset for Fairness Ethical data practices can help achieve fairness, especially for the disadvantaged. This can be used to help reduce unequal access to services and biases in decision-based algorithms.[50]

[47] APrIGF, "Health Data Governance through AI Booming Age: A Journey in Taiwan", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMjQ5MTQ4ZDY3MC8vMzQvLzE5MzkvLzA=. (Accessed on 22 October 2024)

[48] Big Data Framework. "Why Data Ethics Matter | Establishing a Data Ethics Framework.", website. Available at https://www.bigdataframework.org (Accessed on 22 October 2024)

[49] European Union, "General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679", law journal. Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed on 22 October 2024)

[50] APrIGF, "Building Holistic Resilience to Address Emerging Ethical and Social Challenges in the Digital and AI Age", proposal form. Available at

Ethical Data Collection, Usage, and Retention

In order to ensure transparency, individuals should be informed of any definite purpose limiting the collection of personal data to such purposes only. This is the case in both the European Union General Data Protection Regulation (GDPR) and the Personal Data Protection Act of Thailand PDPA[51], which was constructed following the GDPR principles. Both mention that the processes of the collection of data are somehow responsible and self-explanatory. Still, challenges have arisen, especially regarding data retention, its safekeeping, and obtaining relevant consent from the user. To avoid breach of such trust and to align with user expectations, organisations are required to limit data collection, offer individuals ways to access and correct inaccuracies, and provide individuals with a clear and strict data retention policy so that no personal data is held for longer than the time limit provided.

Interoperable Data Governance and Accountability

Amending and integrating policies and frameworks based on best-fit working models ensures interoperable accountability mechanisms for data governance. Companies should focus on building mechanisms to manage data responsibly and make sharing information without any limitations possible.

CHILD SAFETY AND DIGITAL LITERACY

As AI, blockchain and IoT change the digital landscape, child online protection and children's digital competence have never been of greater importance. These technologies provide opportunities but also have challenges, particularly in protecting children as users. These challenges can be addressed through ethical governance, transparency, and education for all, to ensure that children's rights are upheld.

Ethical Governance for Child Safety

New technologies raise ethical concerns that involve privacy, data protection, and bias. Governance frameworks for such new technologies should be child-centred and ensure that the security of children is not negotiable and that children are in a safe virtual environment from the start. The holistic integration of children's safety features will require the collaboration of stakeholders like tech developers, educators, and parents.

Digital Literacy: Empowering Children

Digital literacy is a key prerequisite for empowering children to use the Internet for good. This goes wider than just understanding how to use devices – children also need to use critical thinking, understand the principles of privacy, tenets of digital safety, and have respect for other

https://forms.for.asia/proposal/?proposalform=NjYyNjVjMmY5N2M3MS8vMzQvLzE5NTkvLzA= (Accessed on 22 October 2024)

[51] APrIGF, "Building Holistic Resilience to Address Emerging Ethical and Social Challenges in the Digital and AI Age", proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyNjVjMmY5N2M3MS8vMzQvLzE5NTkvLzA= (Accessed on 22 October 2024)

people online. Children have to use the increasing online resources for learning. Schools, parents, and local communities need to have holistic programs and activities that promote active and responsible use of the Internet.[52]

Equitable Access to Technology

Socio-economic disparities, gender inequalities, and infrastructural challenges in the APAC region limit some children's access to technology and safe online environments. Bridging these gaps requires collaboration across governments, the private sector, and civil society. All children, regardless of their background, should be able to access the digital world safely, while being protected from its inherent dangers.

Strengthening Regulatory Frameworks and Building Child-centric Policies

The advancement of Internet technology has added new threats for children including online bullying, scams, and child sexual abuse. Protecting their digital rights is a social responsibility that needs the help of parents, teachers, and lawmakers. In the APAC region, some conflicting cultural norms and socio-economic factors render the safe use of the Internet more challenging. Thus, there is a need to develop contextual solutions that embrace the needs of society.

Child-centred regulation and policies that promote online security need to be built in a multistakeholder manner, with expertise from the civil society and technical community, promulgation of industry-wide initiatives by the private sector, and enforcement of legislation and regulation and cross-jurisdictional cooperation by the governments.

The Role of Regional Cooperation

Regional cooperation is crucial to ensure that all children benefit from a safe and inclusive digital environment in the Asia Pacific region. Stakeholders must regularly engage in dialogue to share experiences, discuss policy challenges, and offer best practices. and collaborate on effective solutions. National and Regional Internet Governance Forums (NRIs) like the Asia Pacific Regional Internet Governance Forum (APrIGF) offer spaces where these conversations can happen.

Securing Children’s Safety: An Ethical Obligation

Ultimately, ensuring the safety of children in the digital age is not just a technical issue, but an ethical one. By prioritising education, collaboration, and governance, a digital world can be built

[52] APrIGF, “Securing Trust: Ethical Governance in Championing Children's Digital Rights”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYzNDZmYWE1NzcwNy8vMzQvLzIwNDUvLzA= (Accessed on 22 October 2024)

[54] APrIGF, “Platform Accountability in South and Southeast Asia”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMGI0MzZjZDljYS8vMzQvLzE5MjMvLzA= (Accessed on 22 October 2024)

[55] APrIGF, “Digital Bill of Rights: A Systematic Bottom-Up Approach Towards Freedom in the Digital Age”, proposal form. Available at https://forms.for.asia/proposal/?proposalform=NjYyMGRhMDdjOTlhZi8vMzQvLzE5MjUvLzA= (Accessed on 22 October 2024)

where children's rights are respected, and children are equipped with knowledge and empowered with agency to thrive to their benefit online.

CONCLUSION

Empowering local communities, fostering ethical practices in fact-checking, and enhancing media literacy are vital in addressing misinformation and disinformation. Digital education, particularly in remote areas and vulnerable groups, must be prioritised to ensure equitable access and protection from exploitation. Multistakeholder collaboration between governments, the technical community, private sector, and civil society is crucial to building resilient, informed communities capable of navigating the digital landscape responsibly.

Building Internet resilience is essential to ensure continuous service amidst challenges like natural disasters, cyber threats, and geopolitical tensions. Key actions include supporting small ISPs in underserved areas, enhancing infrastructure redundancy, and adopting secure protocols such as DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) to protect against disruptions. Multistakeholder collaboration is vital to strengthen physical and digital resilience, ensuring systems can recover quickly from disruptions.

Resilience also requires robust governance frameworks that prevent Internet fragmentation while balancing security with global interoperability. Integrating sustainability into resilience efforts, such as optimising energy use in data centres, will help align Internet growth with environmental goals. A holistic approach combining infrastructure, governance, and eco-friendly practices is critical to maintaining a resilient and open internet across the Asia Pacific region.

Ethical governance of technologies in their inception stages such as AI, blockchain, and IoT is necessary for society to reap the benefits these technologies bring while eliminating possible threats. Developing and deploying these technologies should avoid reinforcing existing inequalities, or creating new ones by design and default toward transparency, fairness, inclusivity, and accountability. It is particularly important for those whose rights have been violated, who have been deprived of access to these technologies in the first place, and for whom the most pressing need is to be able to catch up as a community. In addition, cooperation from both the public and private sectors is essential to ensure that these goals are achieved effectively.

Regional and global collaboration must be promoted to build a robust data governance framework and address the problem of AI bias in order to establish trust and gain public confidence towards the use of technology by all. Ethical governance mechanisms should support the process of true value creation, fundamental rights, the democratic process, and sustainable development for a fair, equitable, and responsible digital world.

The Asia Pacific region stands at a critical juncture in its adoption of emerging technologies. While the potential for innovation is immense, so too are the ethical challenges that must be addressed to ensure that these technologies serve the public good. The discussions at APrIGF 2024 underscore the importance of a balanced approach—one that promotes innovation while protecting fundamental human rights and ensuring that no one is left behind in the digital revolution.

CALL TO ACTION FOR STAKEHOLDERS

In line with this year's theme, "Evolving Ecosystems, Enduring Principles", it is crucial for all stakeholders to take steps to ensure that core Internet principles aren't eroded. This call to actions suggests specific roles and responsibilities within the multistakeholder community in supporting a continued safe, resilient and ethical Internet for all. By promoting digital literacy, implementing policies that prioritise privacy, data protection, digital rights, ethical AI, and cybersecurity, strengthening regional collaborations amongst stakeholders, tackling misinformation, advancing ethical standards, and ensuring equitable access to technology, stakeholders can support an evolving Internet ecosystem that serves communities worldwide and protects vulnerable populations.

GOVERNMENT

1. Strengthen multistakeholder collaboration and consider input on all issues and policies that could affect the governance and development of the Internet and digital policy processes.
2. Implement accessible and culturally relevant digital rights policies and data governance frameworks that emphasise privacy, data protection, child protection, cyberbullying, and citizens' autonomy, ensuring ethical, transparent, and fair collection, storage, and use of personal data while including the right to disconnect.
3. Invest in community-based digital literacy initiatives, particularly in remote and marginalised areas, to empower vulnerable populations. Further, create and enforce regulations that promote internet resilience, especially in areas prone to natural disasters and geopolitical tensions.
4. Form independent commissions to oversee and regulate fact-checking organisations, ensuring they adhere to ethical standards, with periodic audits conducted every two years.
5. Develop and enforce comprehensive regulations for ethical AI deployment, focusing on transparency, accountability, sustainability, and human-centric design to safeguard fundamental human rights, while collaborating with international organisations to establish global standards.

TECHNICAL COMMUNITY

1. Keep informed of Internet-related developments and processes arising from non-technical processes, share expertise, and advise policy-makers on matters relating to operation and governance of critical Internet infrastructure.
2. Engage in peer reviews and technical audits to ensure that AI and machine learning models are thoroughly vetted for bias, fairness, and accuracy before deployment in real-world applications.

3. Develop ethical standards and guidelines for software development to include robust encryption and data protection mechanisms, ensuring fairness, security, and privacy of users' data are built into the core architecture of technologies from the outset.
4. Develop and maintain free, open-source software solutions for identifying and reporting misinformation, while contributing to collaborative platforms that empower communities and stakeholders to innovate ethically in emerging technologies.
5. Disseminate information about data privacy, online security, and best practices for online safety (e.g., strong password management, secure browsing, and avoiding phishing scams) through educational initiatives organised in partnership with local communities.

ACADEMIA

1. Recommend all educational institutions to include media literacy and digital citizenship programs in their curricula and lifelong learning programs, focusing on critical thinking and recognising misinformation.
2. Fund and publish research studies analysing the impacts of gendered disinformation, AI and other emerging technologies, with actionable recommendations for policymakers.
3. Encourage public dialogue through conferences, publications, and open forums to discuss the evolving ethical challenges in emerging technologies and engage the broader public in shaping governance solutions.
4. Collaborate with governments and industry to develop ethical frameworks that guide the responsible innovation and application of AI, ensuring that the technology benefits society as a whole.
5. Develop and implement ethical guidelines for the use of AI in the academic sector to ensure it benefits society.

CIVIL SOCIETY

1. Advocate for the rights and needs of marginalised groups in public discussions, ensuring their concerns are heard and considered in discussions about the ethical deployment of emerging technologies.
2. Create campaigns to educate the public on the dangers of misinformation and the risks and benefits of AI through workshops, social media, and community events.
3. Create and maintain platforms with high transparency for citizens to report misinformation and access resources for fact-checking, such as through SMS, ensuring these are widely promoted across communities.
4. Form local groups to monitor misinformation in their communities, sharing findings with fact-checking organisations and local authorities to enhance accountability.

5. Collaborate with other stakeholders to demand greater transparency and fairness in the digital services they use, holding developers and companies accountable for unethical practices.

PRIVATE SECTOR

1. Keep informed of Internet-related developments and processes, share insights, and advise policymakers on relevant matters, ensuring that the industry-wide practices remain compliant with global standards and relevant laws and regulations.
2. Prioritise fairness and bias mitigation while increasing transparency in AI decision-making by developing open, explainable AI during the design, development, and deployment of AI and other emerging technologies, particularly in critical sectors such as healthcare, finance, and education, where vulnerable groups may be impacted.
3. Commit to regular audits of AI systems, especially in high-stakes areas, to identify and mitigate any unintended negative consequences on marginalised communities.
4. Foster public-private partnerships to promote innovation while maintaining adherence to ethical governance standards, ensuring that technological development does not come at the expense of human rights or societal well-being.
5. Allocate a percentage of their annual profits to support digital literacy programs and initiatives aimed at combating misinformation, and collaborate with local fact-checking organisations to provide funding and resources for their operations, ensuring transparency in content moderation practices.

APPENDIX I

Name	Affiliation	Stakeholder Group	Track
Saima Nisar (Co-chair)	Xiamen University Malaysia	Academia	Ethical governance of Emerging Technologies
Luke Teoh Rong Guang (Co-chair)	Universiti Sains Malaysia, NetMission.Asia	Youth/Students	Ethical Governance of Emerging Technologies
Au Yi Teng (penholder)	Nanyang Technological University	Youth/Students	Security & Trust - lead
Chanvoleak Ros (penholder)	YIGF Cambodia/ Cambodia Development Resource Institute	Civil Society	Resilience - lead
Socheata Sokhachan (penholder)	Netmission.asia	Youth/Students	Ethical Governance of Emerging Technologies - lead
Abdullah Qamar	Virtual university of Pakistan	Academia	Ethical Governance of Emerging Technologies
Angela Wibawa	ICANN	Technical Community	Security & Trust
Aviral Kaintura	National Forensic Sciences University, Delhi Campus	Youth/Students	Security & Trust
Byambajargal Ayushjav	Faro Foundation Mongolia NGO	Civil Society	Ethical Governance of Emerging Technologies
Hamna Noor	APrIGF (FC)	Private Sector	Ethical Governance of Emerging Technologies
Jasmine Ko	DotAsia Organisation	Technical Community	Security & Trust
Jessamine Pacis	Foundation for Media Alternatives	Civil Society	Resilience
John Rojell Y. Elizaga	Polytechnic University of the Philippines - Manila	Youth/Students	Security & Trust
Lokendra Sharma	The Takshashila Institution, Bengaluru	Academia	Ethical Governance of Emerging Technologies
Mabda Haerunnisa Fajrilla Sidiq	The Habibie Center	Civil Society	Resilience
Md. Saimum Talukder	School of Law, BRAC University	Academia	Ethical Governance of Emerging Technologies

Nancy Kanasa	Department of Information and Communication Technology	Government	Ethical Governance of Emerging Technologies
Rafi Uddin	Independent	Youth/Students	Resilience
Sana Nisar	Habib Bank Limited	Private Sector	Ethical governance of Emerging Technologies
Unggul Sagena	SAFEnet	Civil Society	Ethical Governance of Emerging Technologies
Zin Myo Htet	Chiang Mai University/ Youth IGF Myanmar	Youth/Students	Resilience

APPENDIX II

2024 APrIGF workshop sessions:

	Session Title
1	Charting the Path for a Regional Fact-Checking Coalition in the Asia-Pacific
2	Regulatory Resilience in the Age of Internet Fragmentation
3	Digital Frontlines: Safeguarding Human Rights Defenders in the Cyber Age
4	Gendered Disinformation – Deepening understanding and exploring countermeasures
5	NetMundial+10, GDC, WSIS+20 – what else is happening in the world of Internet governance
6	Digital Leap- Enhancing Connectivity in South Asia
7	Securing Trust: Ethical Governance in Championing Children’s Digital Rights
8	Bottom-up Advocacy for a Resilient Internet
9	BreaktheSilo: Streamlining Gender Safety in the Digital Space
10	A Multistakeholder Approach to Safeguarding Information Integrity through Advancing Internet Governance in Asia and the Pacific
11	Platform Accountability in South and Southeast Asia
12	Making AI responsible for financial inclusion
13	Is Asia-Pacific ready for AI? Balancing AI Innovation and Ethical Governance merging with AI for Marginalized: Shaping Responsible AI Governance for Open, Unbiased, and Localized Innovation*
14	Internet infrastructure resilience during disaster event – Case Study for the 0403 Taiwan Earthquake, and others
15	Digital Bill of Rights: A Systematic Bottom-Up Approach Towards Freedom in the Digital Age
16	Messaging scam and combatting to protect human rights and democracy
17	Building Holistic Resilience to Address Emerging Ethical and Social Challenges in the Digital and AI Age
18	Multistakeholderism in the post-GDC era
19	Striving for EcoInternet, towards a resilient Internet
20	Enhancing Internet and Web Standards to address DNS Tampering
21	Contextualising Fairness: AI Governance in Asia
22	Infrastructures of repression: Cybersecurity and Human Rights in the Asia Pacific
23	Strengthening the Digital Resilience of Taiwan: with Special Reference to Undersea Cables
24	Freedom Online Coalition Regional Dialogue – Asia-Pacific

25	Defending against Digital Deception: Strategies for Preventing Online Scams and Identity Theft?
26	ShhorAI: Combating Hate Speech and Fostering an Inclusive Digital Space
27	Health Data Governance through AI Booming Age : A Journey in Taiwan

*merged workshop session