ASIA-PACIFIC CYBER INSIGHTS

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

THE GLOBAL CONFERENCE ON CYBERSPACE 2015

The GCCS is the fourth iteration of the International Cyberspace Conference process which began in London 2011, with subsequent sessions in Budapest 2012 and Seoul 2013. This multistakeholder process aims to build a focused dialogue on principles for governing behaviour in cyberspace and set out an agenda for further work.

The GCCS conference in The Hague aims to ensure that the internet remains free, open, and secure by setting out three key objectives the conference will seek to support:[1]

1. Support of practical cooperation in cyberspace.
2. Promote capacity building and knowledge exchange in cyberspace.
3. Discuss norms for responsible state behaviour in cyberspace.

GLOBAL CONFERENCE ON CYBERSPACE 2015

Annotated Agenda

- **PLENARY FOCUS SESSION 1:** International peace and security
- **PLENARY FOCUS SESSION 2:** A secure place for business and people
- **LAUNCH OF THE GLOBAL FORUM ON CYBER EXPERTISE**
- **PLENARY FOCUS SESSION 3:** Fast forward, economic growth and development in cyberspace
- **PLENARY FOCUS SESSION 4:** Privacy

ACKNOWLEDGEMENTS

We would like to thank the Ministry of Foreign Affairs of the Kingdom of the Netherlands, the Embassy of the Kingdom of the Netherlands in Canberra, and the GCCS2015 team for their support and ongoing enthusiasm for our efforts to bring Asia–Pacific perspectives to the Global Conference on CyberSpace.

Thank you to the Institute of Strategic and International Studies Malaysia for their partnership in hosting the Kuala Lumpur workshop and for our partners on the ground in The Hague for helping to launch our paper. And of course a special thank you to all the participants and contributors to our Asia-Pacific Insights project who lent us their time and expertise to help amplify the diverse viewpoints of our region.

1 https://www.gccs2015.com/gccs/all-about-gccs2015

ASIA–PACIFIC CYBER INSIGHTS: REGIONAL PERSPECTIVES ON THE GLOBAL CONFERENCE ON CYBERSPACE 2015

At the leading edge of social media and mobile internet adoption, incorporating 47.5% of global netizens and growing fast, the Asia–Pacific is a rich and vibrant environment for the growth of cyberspace.[2]

The region incorporates some of the most mature cyber actors in the world as well as some of the least connected. Governments throughout the region are becoming increasingly aware of the importance of cyberspace, however the capabilities, needs, and priorities of each state lie across a wide spectrum. Asia–Pacific cyber perspectives are far more diverse and dynamic than the dominant narratives coming from the 'cyber great powers' and it is important that the region's distinct voices are heard in international cyber discussions.

This report aims to give insight into the wealth of cyber perspectives across the Asia–Pacific and amplify the regional voice on the key themes and questions of the Global Conference on CyberSpace 2015 (GCCS) in April 2015. To achieve this the Australian Strategic Policy Institute's International Cyber Policy Centre partnered with the Institute of Strategic & International Studies Malaysia to host a multistakeholder workshop to gather and collate the expertise of a broad cross-section of Asia–Pacific cyber experts. With generous support from the Ministry of Foreign Affairs of the Kingdom of the Netherlands, the workshop brought together participants from government, the private sector, academia, think tanks, non-governmental organisations (NGOs), as well as regional and international organisations from 12 Asia–Pacific countries.[3]

The following represents a collation of the thoughts and perspectives from the workshop and subsequent discussions. It is based on the key themes and questions of the GCCS and structured around the GCCS agenda. The intention was not to achieve consensus but instead accurately portray the points of convergence and divergence across the region. Throughout the process the recurring themes of clarity, capacity, and responsibility emerged as ways to ensure a more reliable, secure, and stable cyberspace.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE INTERNATIONAL CYBER POLICY CENTRE

In partnership with GCCS 2015 The Netherlands

ISIS MALAYSIA

www.aspi.org.au/icpc @ASPI_ICPC

Authors: Klée Aiken and Jessica Woodall

2 http://wearesocial.net/blog/2014/01/social-digital-mobile-apac-2014/

3 Australia, China, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, South Korea, Singapore, US, and Vietnam.

Plenary Focus Session 1: International peace and security

GCCS Session goals:[4]

- Supporting, solidifying, and increasing the coherence of the emerging global consensus.
- Moving the international debate forward through clarification and new ideas.
- Broadening participation in the international debate.

Asia–Pacific background:

International peace and security in the cyber domain is fraught with challenges. Difficulty of attribution, low cost of entry, and a high level of ambiguity in this space make cyber an attractive tool for nefarious actors, both state and non-state. This region has seen its share of international cybersecurity incidents with hacktivists trading salvos as tensions rise in the South China Sea, between India and Pakistan, China and Hong Kong, to name a few. State-driven cyber-attacks emanating from North Korea have targeted South Korea and the US while espionage efforts have upset relations between Australia and Indonesia. While the source of attacks remain a point of contention, what is clear is that cyber malfeasance is now a regular component of larger regional disagreements.

While this regional picture may appear bleak, there are plenty of opportunities to improve stability in cyberspace. An increasing number of bilateral dialogues that cover cyber issues and the inclusion of cyber in multilateral forums all contribute to building international assurances and reduce the risk of conflict. Growing investment in confidence building measures also opens avenues for practical engagement to promote stability rather than conflict in cyberspace.

Select issues:

- Although international peace and security has traditionally been the domain of the state, the lines between state and non-state are becoming increasingly blurred, especially in cyberspace.
- Non-state actors, motivated by political disagreements, who target private sector entities complicate the divide between criminal activities, activism, and national security.
- Civilian and military reliance on shared information and communications technology (ICT) infrastructure and the collateral damage and uncontained spread of malware from cyber-attacks that target them complicates the legal and operational understanding of legitimate targets.

4 Derived from February 2015 GCCS preparatory document.

- The conflation of debates around cybersecurity, cybercrime, privacy, espionage, freedom of expression, and other issues has been counterproductive to the development of mature policy and dialogue.
- Conflicts in cyberspace, whether state or non-state driven, do not exist in a vacuum and generally reflect wider pre-existing tensions.
- The lack of agreed upon definitions for critical cyber terminology often result in actors 'talking past each other' increasing the risk of misunderstandings and miscalculation.

Key takeaways:

- While the state is not the only actor in international peace and security, it remains the main actor in this space and an important catalyst to promote stability in international cyber relations.
- For any agreement on terminology to hold legal weight it requires codification. This implicitly requires treaty-level agreements and therefore the state.
- To increase clarity in state-to-state relations, governments should regularly produce cyber strategies or white papers that publicly outline understanding of and intentions in cyberspace.
- Establishing state responsibility to ensure their territories are not used for unlawful use of ICTs is a positive application of state sovereignty in cyberspace.
- Military declaratory policies that define government stances on cyber activities reduce the risk of miscalculation and escalation of tensions.
- The establishment of bilateral, regional, and/or international frameworks to guide interactions between states, similar to the Code for Unplanned Encounters at Sea, can help prevent conflict escalation especially during a crisis.
- While the establishment of shared definitions for key cyber terminology is a useful endeavour to improve clarity, building a glossary of how each state defines critical terms may be a more practical effort, at least in the interim.
- Different modes of interaction (i.e. bilateral, multilateral, intergovernmental) and different forums (i.e. APEC, ASEAN, UN) provide unique channels for engagement. Each avenue provides differing opportunities and it would be prudent to at best coordinate, but at least, ensure cross-awareness between these efforts. This would help promote a complimentary division of labour and avoid duplication of efforts.
- Confidence building measures (CBMs) offer a practical means for regional risk reduction. Starting with the basics should not be undervalued; the establishment of a database defining clear national points of contact, policy desktop exercises, and other efforts can go a long way to build trust, mitigate risk, and build international assurances.

- Rules of the road in cyberspace can be developed at the international level, but also at the regional, and even local levels.
- Compiling lists of encouraged and discouraged state behaviours in cyberspace could help establish a baseline from which international norms can be built.
- A focus on the stability of cyberspace, rather than on cyber conflict will highlight common ground and provide more fruitful avenues for cooperation and collaboration.

Plenary Focus Session 2: A secure place for business and people

GCCS Session goals:[5]

- Facilitating a new and constructive discussion on the roles and responsibilities of consumers, businesses and governments in securing cyberspace (thereby broadening the debate to involve new stakeholders).
- Exploring and considering international solutions against criminal safe havens.

Asia–Pacific background:

With over 61% of the world's population, 3,500 different spoken languages and an assortment of different political systems, the Asia–Pacific is a culturally diverse region.[6] Information communications technologies has presented immense opportunities for growth, but also new challenges. Mobile phones have provided online access to a new generation, one that had taken it up with gusto. In 2005, for every 100 inhabitants in the Asia–Pacific only 23 had mobile internet access. By 2014, this number rose 287% to 89 in every 100.[7]

Lack of end-user awareness, online crime and a lack of harmonised legal structures and capacity are shared challenges associated with the rapid uptake of new technologies. But due to the varying points of socio-economic development and online ecosystems across the region, the scale and prioritisation of these issues vary greatly.

Select issues

- Domestic agencies within some national structures lack effective coordination on cyber issues. This can inhibit internal coherence, with negative flow-on effects for international cooperation and engagement.

---

5 Derived from February 2015 GCCS preparatory document.
6 http://www.unescap.org/stat/data/syb2011/I-People/Population.asp
7 http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

- The debate in the Asia–Pacific remains largely 'stuck' on cybercrime issues whilst the wider global discussion has expanded to include issues such as international law and norms relating to state activities in cyberspace.
- There are different interpretations of who bears the risk of cyber-attacks and who is responsible for countering this threat.
- There may be little capacity to enforce cyber laws, or no interest to do so, even in countries that have drafted cyber legislation.
- The Council of Europe Convention on Cybercrime (the Budapest Convention) is a divisive topic in the Asia–Pacific region. Some countries like the convention but are unable to accede due to the strict entry rules. Others object to the convention because it was formed without Asian regional input or concerns around certain provisions such as metadata retention.
- Cross-border private sector collaboration can be a complex issue. Cooperation is often strong on issues such as spam, but some countries are frustrated by a lack of ISP assistance on content control issues.
- It is difficult to combat cybercrime on a government-to-government level due to varying levels of capability and legal definitions that exist across the region.
- The occurrence of private sector 'hacking-back' was raised as an emerging issue in cyberspace. This is a noteworthy issue in the Asia–Pacific as government capabilities and responses to crime can pale in comparison to the capabilities possessed by large corporations.
- Public awareness and basic cyber hygiene efforts need to be improved.
- As businesses increase their reliance on the internet for basic operations and to reach customers it is imperative they play a bigger role in wider cyber discussions.
- High uptake in mobile technology creates a different cyber environment in the region, with its own unique characteristics and threat picture.
- With a large population new to the digital space, people are often the weakest link in the Asia–Pacific; therefore a strong public education push is needed.
- There is a lack of mechanisms to address 'bulletproof hosting' and where network operators are unwilling to address malware on their own systems.

Key takeaways:

- Improve domestic co-ordination on cyber issues. Establish effective communication channels between the agencies and departments with a stake in cyber issues.
- The private sector is a useful vehicle to help improve public cyber hygiene, especially where government efforts are lacking.
- Partnerships across academia, the private sector, civil society, and government can help pool best practice and address a wide range of common cyber issues.
- Start with the least controversial issues, build consensus, and then expand from there.

  Shared overarching cyber goals may include:
  - Maintain the stability and security of cyberspace
  - Ensure that critical national infrastructure is secure
  - Ensure the public is safe from fraud
  - The need for cooperation to combat cybercrime
  - Confidence building measures are needed for conflict prevention.
- Governments also have a responsibility to prevent infrastructure within their jurisdiction from being used for unlawful purposes.
- Countries unable to accede to the Budapest Convention due to capacity restraints, can use the provisions as a template to establish de facto cybercrime frameworks.

Global Forum on Cyber Expertise: A global platform for cyber capacity building

GCCS Session goals:[8]

- Harness global commitment to promote sustainable cyber capacity building and provide new funding streams for cyber capacity building.
- Promote a policy dialogue and mutual exchange of experiences and expertise to formulate requirements as well as best practices on cyber capacities in key areas.
- Take stock of, build on, and complement current initiatives.

8 Derived from February 2015 GCCS preparatory document.

Asia–Pacific background:

The Asia–Pacific region presents a multifaceted capacity building picture. It is home to many of the UN's least developed countries and several more in their developmental and economic adolescence. These are the countries that have, and will continue to benefit the most from technical, policy, legislative, organisational and law enforcement capacity building efforts. While the region is also home to global leaders in cyber best practice, in the past it has been difficult to match their expertise in a practical manner with those in need of specific training and mentorship.

The picture has often become more complex when factoring in the resulting well-intentioned, but often overlapping and uncoordinated efforts.

Capacity building currently exists in the Asia–Pacific primarily in the CERTs–CERTs and technical arenas and via wider bilateral programs driven by a handful of countries, companies, and NGOs in the region. In addition to building capacity, these programs have successfully served to help build confidence and transparency between those involved.

To improve capacity building outcomes, these efforts need to be both expanded to encompass policy, legislation, and governance issues, and coordinated to ensure they are fulfilling actual needs in a systematic way.

Select issues:

- Historically, capacity building efforts have been focused on ICT development and enabling a digital economy, without prudent attention to developing policy and legislation to govern the space.
- Varying levels of development and different capacity building needs across the region make universal capacity building models ineffective.
- A lack of coordination between existing capacity building measures results in a duplication of initiatives, gaps in meeting key needs, and sometimes conflicting or cross-cutting efforts.
- Capacity building initiatives often lack a long-term strategy, resulting in one-off impacts that lack sustainability and limit wider impact.

Key takeaways:

- Cyber capacity building initiatives should maintain a transparent and consistent overarching narrative, but must have the flexibility to tailor approaches to each particular circumstance.
- Capacity building efforts to build holistic cyber policies and structures must be pursued with the same vigour as those pursuing economic growth.
- Regional capacity building can be mapped to show those countries with specific needs and those who are ready and willing to share best practice, helping to ultimately match the two.
- Capacity building should not be limited to state-based programs but should draw on the expertise of the private sector, think tanks, civil society, and academia.
- Tailored programs that address the needs of smaller communities and nations and are written in local languages need to be developed.
- Efforts should be directed towards establishing national cyber crisis expert teams. CERTs are a logical starting point.
- Building whole-of-government cyber legislation and coordination should also be a crucial top-level target of capacity building.
- When building capacity, policy and technical goals need to be kept realistic and built in a strategic manner.
- To promote sustainability, skills building initiatives should prioritise training trainers, rather than focusing on one-off skills training.

Plenary Focus Session 3: Fast forward, economic growth and development in cyberspace

GCCS Session goals:[9]

- To facilitate an innovative and constructive discussion on how governments, businesses and society can prepare themselves for the ever increasing integration of the digital economy in the physical world.
- To provide insights into the way governments can achieve digital innovation and economic growth.

9 Derived from February 2015 GCCS preparatory document.

Asia–Pacific background:

The online environment has presented vast and exciting opportunities for business in the Asia–Pacific. Digital innovation is driving growth across Asia, contributing to economic prosperity and providing new development opportunities. The internet has opened new markets for products and services, simplified corporate processes and helped to expand fledgling operations across the region and the globe. The internet has removed the tyranny of distance, fundamentally changing how we interact with the world and carry out business.

The online world has also given society a new voice. Those in the region can now more readily connect with diaspora communities, friends and families across the world. It presents a medium for like-minded people to gather and share their knowledge, experience and opinions.

But at the same time an expansion in the Asia–Pacific online footprint has come with an increased exposure to risk. The explosion in new internet users across the region has seen public education fall dramatically behind digital uptake. This has presented challenges for online safety and end-user security in the Asia–Pacific.

Select issues:

- Economic and social collaboration between the public and private sectors is lacking.
- The private sector often limits its involvement on cyber issues to government-initiated workshops and discussions.
- In some countries there are no established rules around the issue of active cyber defence and the right to 'hack back'.
- Many companies avoid publicly disclosing they have experienced a network compromise as they do not want to suffer real or perceived reputational damage.
- Corporations are often targeted by politically motivated attacks. Often it is not because of the data they hold, but because they are seen as representative of a certain state or government industry.
- There has been a blurring of issues where private sector information security problems have become merged with strategic security. For example, the Sony hacking incident where a compromised corporate network became fused with the national security of the US.

Key takeaways:

- The private sector has the responsibility to more actively drive policy, governance, and technical activities in their own right.
- Financial drivers are the easiest and most important starting point for government–private sector cyber relationships. Increased economic growth is in the interests of all involved.
- The private sector can help with education and awareness campaigns to its large customer base, and more broadly into society.
- There needs to be an open discussion around the appropriate boundaries for active cyber defence and 'hacking-back'. This is particularly important in developing countries where official online crime fighting agencies and CERTs may lack the capacity of private sector companies.
- Private sector companies need to be both more involved, and increasingly invited to participate in national-level drill exercises; particularly those that involve critical national infrastructure.
- Mandatory breach reporting laws can assist law enforcement to understand the scope of cybercrime issues affecting the private sector, and help to slow the proliferation of online threats.

Plenary Focus Session 4: Privacy

GCCS Session goals:[10]

- Emphasizing the importance of a debate on privacy protection at an international level.
- Facilitating a constructive and forward-looking debate on this issue with all stakeholders.
- Addressing roles and responsibilities of different stakeholders through policy recommendations.

Asia–Pacific background:

Civil liberties in cyberspace represent an area of particular divergence in the region. Encompassing issues of human rights, sovereignty, culture, security, and privacy, the diversity of approaches to civil liberties online reflects the diversity of social and political structures in the Asia–Pacific.

10 Derived from February 2015 GCCS preparatory document.

Cyber provides countless privileges to governments, private sector organisations, and individuals, but it also presents obligations. This dichotomy is where different approaches to privacy and freedom of expression online stem. For some countries in the region the need for social harmony is used to justify limiting online privacy, while others cite national security when controlling online content. In many cases cybercrime legislation or anti-terror efforts are used to rationalise content control efforts. Even in countries that have stronger protections of civil liberties, the business commoditisation of personal data has raised significant concerns over privacy and individuals' control over their data.

Select issues:

- The challenge of balancing privacy and security, security and innovation, and privacy and monetisation are key dilemmas governments across the Asia–Pacific must consider when forming cyber policy.
- As activities that are illegal offline are most often illegal online, framing the discussion of content control and privacy as cyber issues often blurs the wider socio-political context in which such measures are taken.
- In some states there is genuine disagreement over the universality of the right to freedom of expression, which is often seen as a threat to social harmony and stability.
- A lack of shared conceptualisations of key cyber terms can lead to skewed policy dialogues, most clearly evident in the expansion of the usage of cybercrime to rationalise efforts to curb privacy and freedom of expression.
- Differing approaches to privacy laws pose a challenge as states attempt to enforce legislation across borders, especially evident in take-down requests directed at private sector entities located in other jurisdictions.
- The business use of data has resulted in a slew of legal and ethical challenges to privacy and the ownership of one's data, but at the same time these business models allow free access to online tools and platforms that would otherwise be cost prohibitive.

Key takeaways:

- When developing information sharing frameworks and legislation, it is important to remain conscious of the flow-on privacy implications for businesses, their clients and customers.
- While civil liberties are a sensitive issue and it is often easier to initiate discussion on less controversial topics, they should not be built into an unassailable problem. These issues must not be tackled as an 'all-or-nothing' affair, instead an incremental approach can be taken to achieve progress.

- Additionally an 'all-or-nothing' approach to civil liberties marginalises regional partners, often leading to adverse reactions undermining wider opportunities for cooperation.
- The privacy debate is not one that exists solely in the online space and its dynamics largely reflect the same issues and concerns in the offline space. This must be considered when approaching privacy issues online, especially from an international perspective.

ICPC PARTING THOUGHTS

This compilation of Asia–Pacific views genuinely represents how divergent and contradictory regional cyber perspectives can be. The key takeaways, collected from cyber experts from across the region, suggest ways forward for the region and international community to meet the goals and intentions of the Global Conference on CyberSpace. While the scale of the challenges may vary widely across the region, each government, business, and citizen faces fundamentally similar hurdles. Despite headlines of cyberwar, espionage, and crime, there is more common ground to be found than not.

In discussions on Asia–Pacific cyber perspectives, clarity, capacity, and responsibility emerged as recurring themes on how to ensure a more reliable, secure, and stable cyber ecosystem.

Clarity is critical to break through the default secrecy and ambiguity that has come to define cyberspace. Building clarity around governance structures and doctrine that shape regional cyber policies would go a long way to reduce the risk of conflict and miscalculation. The regular publication of cyber white papers or strategies, the defining of military doctrine in cyberspace, establishing counterpart points of contact, and the translation of national terminology each removes unnecessary opacity and sets the foundation for dialogue and cooperation on cyber issues.

The need to improve capacity across the region was an area of unanimous agreement. Whether in the policy space, in technical skills building or in the construction of ICT infrastructure, there is a shared recognition of cyber as a catalyst for growth and the need to ensure sustainability and security in its expansion. Identifying the needs and expertise of actors across the region and matching partnerships in a complimentary way is critical to 'bridge the digital divide' and improve whole-of-system prosperity and stability.

In discussing the key challenges facing cyberspace, a lack of accountability was a constant refrain. While it remains contentious whether responsibility to secure systems and prevent malicious use of cyberspace lies with the state, network operators, service providers, individuals, or a combination of each, the establishment of accountability is critical to spur action.

Holding the state accountable for preventing the use of national infrastructure for malicious purposes; placing onus on the individual to practice good cyber hygiene; and ensuring the private sector fosters a secure environment for its clients and customers, together can offer the benefits of connectivity to the Asia–Pacific whilst reducing risk.

The region requires pragmatic and flexible cyber policy approaches to grapple with the breadth of challenges that cyberspace presents. Clarity, capacity, and responsibility are strong goals to pursue in the Asia–Pacific, but in a region so economically, politically, socially, and culturally diverse the path forward is fraught with hurdles. At the same time this makes it an ideal testing ground for the critical challenges of cyberspace; and it is home to its own creative approaches to cyber challenges that offer best practice for the global community.

Acronyms and abbreviations

GCCS Global Conference on CyberSpace 2015
ICT information and communications technology
NGOs non-governmental organisations

ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.aspistrategist.org.au


A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
INTERNATIONAL
CYBER POLICY
CENTRE