SPECIAL REPORT

ASPI

October 2013

A shared agenda for the Seoul Conference on Cyberspace

South Korea, 2013

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

Tobias Feakin, Jessica Woodall, Peter Jennings

This briefing is ASPI's distillation of the thoughts of a group of prominent members of the Australian cybersecurity community. We held a workshop in Canberra on the key panel sessions that will take place at the Seoul Conference on Cyberspace, South Korea, in October 2013.

Several key constituents of ASPI-ICPC were represented at the meeting. They included the Australian Government departments with a stake in cyber issues and members of the private sector, including the banking and IT sectors, defence and security industries and representatives from the wider business community. The aim of the workshop was to provide creative Australian perspectives to take to the Seoul conference. This gathering embodied the multi-stakeholder model championed by the International Conference on Cyberspace process begun in 2011 and demonstrates the Australian cybersecurity community's commitment to ongoing constructive dialogue.

The thoughts in this briefing are intended to stimulate discussion and provide additional areas for collaboration between the public and private sectors across the Indo-Pacific region. In the final analysis, they represent ASPI-ICPC's interpretation of the workshop. Any errors of interpretation are those of the ASPI-ICPC team.

The subheadings in this document outlining the *aims of session* are drawn from the *Annotated agenda for the Seoul Conference on Cyberspace* supplied by the conference organisers.

Session One: Economic Growth and Development

Aims of session

- To discuss the roles of various stakeholders and the impact of the internet economy on global economic growth.
- To explore feasible development models of the internet economy.
- To identify practical steps to provide policy guidance to developing countries on capacity building to implement the internet economy.

Overarching assessment

It is in all nations' best interests that economic growth and development be sustained across the region. The strength of the internet economy is a major factor in that continued growth. If we encourage unconstrained access to an interoperable cyber environment, cyber interconnectedness will spread, boosting the economy. We should aim to build on that interconnectedness by capacity building in a non-competitive and non-discriminatory way across the region. Where a baseline level of technical capability exists, we should aim to provide best practice on the establishment of effective cybersecurity and privacy frameworks.

By remaining focused on practical outcomes, we have the opportunity to increase international technical and trade cooperation with a broader range of nations. Initiating those practical relationships is one of the best ways to share best practice and present the benefits of an open and robust

online economy. By using this model we can ultimately aim to build from economic discussions into talks on wider, more sensitive cybersecurity issues.

Ingredients for a strong internet economy

- Access to the internet via high-speed infrastructure is vital to the growth of the internet economy. There are international development opportunities through public–private partnerships that could help nations reach the minimum standard needed to participate effectively in the online market.
- Policy and legal frameworks are also crucial. Online security, confidence and privacy protection are central for both business and consumer confidence.
- To establish trust internationally, where it's often scarce, governments should state their positions on issues relevant to the internet economy and work actively to establish points of commonality.
- By encouraging co-adaptation, as opposed to starting 'technology races', hypercompetition can be avoided.

Engaging business in the internet economy

- Existing national laws and regulatory frameworks should be made more visible to the international business community to create confidence in consumer protection. The most effective can be used as best practice examples for extending and harmonising consumer rights internationally.
- The economic benefits of creating a secure cyberspace should be presented to encourage countries to make stronger investments in cybersecurity.
- The Australian Signals Directorate's 'top four strategies to mitigate targeted cyber intrusions' could alone avert 85% of targeted cyber intrusions. That list, plus the Australian Department of Broadband, Communications and the Digital Economy's Stay Smart Online Program, could be excellent best practice models for international small and medium enterprises (SMEs).

Australia's stake in the global internet economy

- The National Broadband Network (NBN) gives Australia an opportunity to be a regional leader in the development of new high-speed broadband applications. Similar regional infrastructure developments should be encouraged.
- By promoting the formation of 'cyber free trade agreements' that foster open and equitable e-commerce, Australian business will benefit.
- Including minimum network security standards in those agreements would strengthen cybersecurity standards across the region.

Session Two: Social and Cultural Benefits

Aim of session

- To identify the social and cultural benefits of cyberspace as well as the basic principles that can promote such benefits as freedom and confidence.

Overarching assessment

The power of networks challenges the power of hierarchy. The use of cyberspace leads to greatly increased social and cultural benefits for individuals and communities. A multi-stakeholder model that's open and transparent enables freedom of expression, access to information online and economic growth. It also allows access to services and education and grants opportunities to engage in the policy process that weren't previously available to most of the population.

Social and cultural benefits of cyberspace

- *Access to information*: The internet allows access to a wide range of opinions on a vast range of topics. It creates new non-traditional avenues for education and training, overcoming the tyranny of distance.
- *Freedom of expression*: Cyberspace provides a means for individuals to have their opinions heard and to influence others on a large scale.
- *Collective social organisation*: By bringing people with shared interests together, cyberspace can enable the formation of new social groupings or movements. Once they're established, their longevity and activities can be positively influenced by online coordination and communication.

- *Economic development*: e-business and e-trade use new ways of doing business. They grant the consumer access to new overseas markets, lowering the cost of traditional products through competitive advantage. The internet also improves access to a wider range of goods and services that might not have been available in certain regions. It also creates an expanded consumer market for products, encouraging domestic innovation and entrepreneurship.
- *Cultural understanding*: The internet's lack of borders allows cross-cultural interaction between people with diverse backgrounds.

Best practice

- *eHealth.gov.au*: An eHealth record is a secure online health summary of an individual's medical information. It allows doctors, hospitals and other healthcare providers to view and share that information when granted access by patients.
- *Data.gov.au*: The internet provides a means to access and reuse public datasets from the Australian Government.
- *Open Government Partnership*: This multilateral organisation promotes transparency in government, encourages citizen participation and tackles corruption. The partnership provides an international forum for governments, the private sector and the public to address the challenges of governance in the 21st century.

Challenges to social and cultural benefits in cyberspace

- *Damaging information*: Cyberspace facilitates the spread of radical ideologies, extremism, child exploitation material and the sharing of knowledge on how to construct weapons, such as explosive devices.
- *Damaging speech*: Radical and inflammatory opinions can lead to violent repercussions domestically and internationally. The internet isn't regulated to the same extent as traditional forms of media. Potential audiences are also much larger and impacts much wider.
- *Privacy*: What privacy should look like in the online environment hasn't yet been settled. Complicating the issue is uncertainty about public–private boundaries in cyberspace.

Session Three: Cybersecurity

Aims of session

- To evaluate the current trend of cyber threats, identify major challenges and problems, and find practical measures for prevention and response.
- To improve practical cross-border cooperation among all stakeholders, including the private sector.
- To prioritise cybersecurity domestically and internationally with national and regional strategies, legislation, organisational institutes and technical expertise, such as computer emergency response teams and computer security incident response teams (CERTs and CSIRTs).

Overarching assessment

As internet penetration grows, the need to prioritise cybersecurity is becoming increasingly pressing. Most at risk are countries experiencing an exponential rise in the number of citizens moving online but with minimal legal and policy frameworks or the technical capability to apprehend and punish malicious actors in cyberspace. Cross-border coordination and cooperation are essential to help avoid misunderstandings and build best practice.

Security challenges, threats and trends

- Cyberspace lowers the barriers to malicious actors, both state and non-state, so the pool of actors that may collide is much larger than is the case for traditional security issues.
- Attribution following cyberattacks is difficult. This creates problems when monitoring compliance with international laws or adherence to established norms of behaviour.
- There are many differing norms for dealing with intellectual property (IP). Modern democratic states have a tacit agreement not to use espionage tools to steal IP, but such norms are not developed in other states.
- Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems are facing increasing attacks from malicious actors. Private industry owns most critical infrastructure, so collaboration is essential to combat these threats.

International cooperation and practical actions

- Following the consensus report of the United Nations Group of Governmental Experts (UNGGE) on the applicability of international law, including the UN Charter, to cyberspace, there's a need to address the subject of peacetime norms below conflict level. Those norms will be associated with a range of activities (sabotage, subversion, espionage) for which there's little or no international law, but this shouldn't prevent the initiation of dialogue, either bilaterally or in multilateral forums.
- Negative media coverage of cybersecurity problems should be countered by actively sharing government successes and collaborations within the region.
- Publishing cyber policy documents such as white papers that outline government policy, forward planning and organisational structure can compel governments to think more deeply about cybersecurity. It can also help to establish international norms and can contribute to building trust in the international community.
- Providing a local context for cybersecurity can be greatly beneficial. For example, creating drop-in centres where small local businesses can get malware fixed improves end-user awareness and builds overall resilience.

Session Four: International Security

Aim of session

- To identify strategies to ensure international stability in cyberspace, prevent the unintended escalation of future conflicts regionally and internationally, and resolve cyber conflicts through reliable and peaceful methods.

Overarching assessment

Confidence building measures (CBMs) are designed to strengthen the predictability of behaviour, avoid escalations in conflict and avert misunderstandings between states. In the cyber setting, CBMs are designed to avoid mishaps between states in the context of cyber operations at both the conflict and subconflict levels.

While the development of norms is a long-term process, CBMs address problems between states in the short term. Transparency measures and de-escalation measures should either be established or adapted for the cyber context. The international community should work to create and implement such measures as a matter of urgency.

Practical transparency measures and CBMs

- Publicly express national strategic cyber intent through policy documents such as white papers, international strategies and public statements. Clear indicators of intent can prevent misunderstandings on various issues and neutralise incorrect perceptions of what might, on the outside, appear to be threatening behaviour.
- Initiate or expand military cyber-officer exchanges and civilian cyber-staff secondment programs.
- Declare what action government would take after certain cyber actions by other states or non-state actors. Crucial to this process is establishing and releasing a threat threshold. This would make clear what governments would see as a threat to national security.
- Establish meaningful and updated cyber points of contact across civilian policy areas, policing and military branches, in addition to the contact information of the designated cyber leader (where the position exists).
- Promote transparency around military and civilian cyber platforms, including clearer delineation and identification.
- Establish proportionality of response in cyber actions.
- Engage the private sector in forming CBMs. A potential starting point is an affirmation of a shared regional approach to strengthen economic growth with broadly similar business environments and legal frameworks. All actors have a shared interest in building this environment.

Private sector contributions

- Operating system and application vendors can work to create more secure consumer products and improve end-user education on their products.
- Private industry can pledge not to undertake disruptive actions that will damage the internet infrastructure of countries.
- The sector should participate in international centres such as the new Interpol centre in Singapore and the European Cyber Crime Centre (EC3).

- Some industry associations have well-established information-sharing and cooperation agreements. These could be expanded and used as best practice on the international level.

Barriers

- There's a need to overcome resistance to simple measures such as hotlines and desktop exercises.
- CBMs apply to state actors, but many cyberthreats originate from non-state actors.
- Proportionality of response in cyberspace needs to be established.

Session Five: Cybercrime

Aim of session

- To identify measures to effectively counter cybercrime through multilateral and transnational cooperation, including public and private partnerships.

Overarching assessment

The internet has created tremendous opportunities for criminals. Because businesses are the main target of cybercrime and most of the internet's infrastructure lies in the private sector's hands, strong public–private collaborative approaches are needed. These relationships should include technical level actors such as law enforcement and CERT/CSIRT teams who share threat data in both directions, but also grow to include the private sector in formulating policy.

The sources of cybercrime are often offshore. Governments and industry must work together to identify and minimise barriers to effective international cooperation in response to cybercrime.

The Budapest Convention on Cybercrime provides an effective means to facilitate international cybercrime cooperation between signatory states at a practical level. It promotes harmonised legal frameworks that will help to deny safe haven to cybercriminals. It's an effective model that should be promoted over regional, disaggregated approaches to cybercrime, which can allow online crime to prosper.

Existing international cooperation

- There are effective ongoing bilateral partnerships between international law enforcement organisations. Recent successes in this area include the involvement of the Australian Federal Police (AFP) in the disruption of a Romanian credit card hacking group in late 2012.
- In 2011, the Pacific Cybercrime Legislation Workshop was held in Tonga by the Secretariat of the Pacific Community, in partnership with the Australian Attorney-General's Department and the Council of Europe. In line with the Budapest Convention, the workshop presented best practice in the development of domestic cybercrime legislation.
- The US National Cyber-Forensics and Training Alliance (NCFTA) brings law enforcement, private industry and academia together to share information to stop current and emerging cyberthreats. The NCFTA is a non-profit organisation that works as an intermediary between the private sector and law enforcement. Its industry members include banks, internet service providers (ISPs), telecommunications firms and credit card companies. They can pass threat and malicious software data to the NCFTA, which can then pass the information on to government.
- Strong policing partnerships exist across Southeast Asia. They could be leveraged to include cybercrime prevention capacity-building elements.
- Nations can collaborate with partner countries to overcome barriers to lawful access to telecommunications data and content held in overseas jurisdictions.

Australian best practice models

- Australia has recently released the National Plan to Combat Cybercrime to better align the efforts of agencies in all Australian jurisdictions. The plan identifies strengthening international cooperation as a key priority.
- As gatekeepers to the internet, ISPs have a key role to play in ensuring that we're able to combat online criminal activity effectively. The icode, a voluntary industry code used by service providers to help fight cybercrime, defines integrated steps of early identification and notification and directs end-users to remediation tools for devices infected by malicious software.

- The Australian Cybercrime Online Reporting Network (ACORN) will provide a centralised point for the reporting of cybercrime in Australia. It will then refer cases to the appropriate government or law enforcement agency. It will also provide up-to-date advice to the community on cybercrime and aggregate data on the cost and scope of cybercrime.
- CERTs cooperate directly with the private sector and through the Trusted Information Sharing Network for Critical Infrastructure Protection.
- Individual end-user and SME education programs include staysmartonline.gov.au, cybersmart.gov.au, scamwatch.gov.au and the thinkuknow.org.au cyber safety program.
- The Australian Crime Commission (ACC) prepares the National Cybercrime Intelligence Assessment, a classified document for law enforcement and government that attempts to quantify the impact of cybercrime on individuals, business and government.
- An effective way to boost end-user alertness is through cybersecurity awareness weeks, which can be tailored to fit domestic circumstances and levels of ICT development.
- The National Cybercrime Working Group is chaired by the Secretary of the Attorney-General's Department and comprises police and justice agencies from each Australian jurisdiction. The group oversees the national response to cybercrime as a whole, including the policy dimensions.

Building on best practice

- Ensure that robust frameworks exist for the effective investigation and prosecution of cybercrime. Criminalising online malicious activity underpins wider confidence in the internet economy on the part of businesses and end-users.
- ISPs are uniquely positioned as gatekeepers to the internet and should be more accountable for bots on their networks.
- Collect cybercrime arrest and conviction numbers from each jurisdiction and gather them into one national database. Aim to lead internationally in publishing data about arrests.

Barriers

- The tension between privacy and the needs of data retention for enforcement purposes needs to be balanced.
- We need to establish the extent to which the private sector is affected by cybercrime. It's estimated that 90% of cybercrime damage affects business, but it often goes undetected or unreported.
- Businesses, which may be concerned about damaging their reputations, need to overcome their reluctance to cooperate with law enforcement on near-miss cyber incidents.
- We need better ways to engage with SMEs.
- Governments need to be flexible enough to realise that success can take different forms. Because there are limits to traditional forms of law enforcement in cyberspace, a focus on disruption and target hardening, as opposed to prosecution, can be beneficial.

Session Six: Capacity Building

Aims of session

- To define the key features of capacity building in cyberspace, particularly in the cybersecurity area.
- To listen to the needs of all relevant stakeholders.
- To identify strategic gaps in capacity-building support practices.
- To share case studies, best practices or lessons learned on capacity building in cyberspace, including how the private sector has been engaged effectively.
- To propose sustainable capacity-building models that all developing countries and developed countries can participate in.

Overarching assessment

It is in Australia's interest that all countries in our region have strong, robust cybersecurity policies and mechanisms in place. Capacity building plays an integral role in this area and can help countries identify threats and then reach minimum technical and policy standards for a baseline level of cybersecurity.

International cooperation and practical actions

- Public statements supporting the view that Australia supports the raising of cybersecurity standards across the region would be beneficial.
- Non-military organisations, such as AusAID in partnership with private industry, or NGOs such as the International Telecommunication Union (ITU), could assist with audits of cyber capabilities in the region.

Collaborating for a stronger region

- Collaborate to establish what a baseline cybersecurity regime would look like for developing nations.
- After identifying where capacity is lacking, engage the private sector to help build it, particularly to protect critical infrastructure.
- After technical baselines are met, establish effective policy frameworks and develop means for implementation and assessment.
- Providing a local context for cybersecurity can be greatly beneficial. Creating centres where SMEs can get malware fixed improves end-user awareness and builds overall resilience.
- Build on technical knowledge by encouraging international CERT/CSIRT cooperation, including practical exercises and the sharing of information on malicious activity and threats.
- Encourage existing industry-based groups that share threat data and information to further expand their networks internationally.

Barriers

- We need to find domestic funding sources for capacity building. Budget cuts and efficiency dividends are obstacles. There's potential to use the development budget and engage AusAID and the wider private sector.
- We need to ensure consistency and avoid duplication of effort with partner countries.
- There's a need to define a baseline cybersecurity regime for developing nations.

What is ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. We are responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

Why is cybersecurity of strategic importance?

The twenty-first century is going to be defined by the cyber domain. There will be a great responsibility to ensure that those that wish to exploit cyberspace for negative purposes are denied as much operating space as possible. This must be achieved without reducing the openness and freedom that the cyber domain has enabled. Understanding these challenges and creating innovate solutions will be essential for government and private sector alike, and in response to this need ASPI has established its International Cyber Policy Centre (ICPC).

ASPI International Cyber Policy Centre

The ICPC brings together the various Australian Government departments with a responsibility for cyber issues, along with a range of private sector partners and creative thinkers to assist Australia in creating constructive cyber policies both at home and abroad. We aim to facilitate conversations between government, private sector and academia across the Asia–Pacific region to increase constructive dialogue on cyber issues, and do our part to create a common understanding of the issues and possible solutions in cyberspace.

Australia has an increasingly prominent international diplomatic role with respect to cyberspace. Australia's non-permanent seat on the UN Security Council in

2013 and 2014 creates an opportunity for Australia to demonstrate international leadership on cyber matters.

Australia has committed to working cooperatively on cyber issues within the Asian region by engaging key stakeholders in the public and private sectors. During the 2013–14 ASEAN Regional Forum cycle Australia will co-chair a session on cyber confidence building measures. The International Cyber Policy Centre will work closely with government partners to provide subject-area input into this and other processes.

The Centre has four key aims:

- Lift the level of Australian and Indo-Pacific public understanding and debate on cybersecurity.
- Provide a focus for developing innovative and high-quality public policy on cyber issues.
- Provide a means to hold Track 1.5 and Track 2 dialogue on cyber issues in the Indo-Pacific region.
- Link different levels of government, business and the public in a sustained dialogue on cybersecurity.

Contact

Dr Tobias Feakin

Director, ASPI International Cyber Policy Centre

Email: tobiasfeakin@aspi.org.au

Phone: +61 2 6270 5107

Ms Jessica Woodall

Analyst, ASPI International Cyber Policy Centre

Email: jessicawoodall@aspi.org.au

Phone: +61 2 6270 5106

Web: http://cyberpolicy.aspi.org.au

twitter.com/ASPI_ICPC

Mr Peter Jennings

Executive Director, ASPI

Email: peterjennings@aspi.org.au

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
ASPI-ICPC http://cyberpolicy.aspi.org.au

RRP $5.00 ISSN 2200-6648