SPECIAL REPORT

Australia–China cyber relations in the next internet era

Simon Hansen

December 2015

Simon Hansen

Simon Hansen was a research intern in ASPI's International Cyber Policy Centre during which time he worked as a Visiting Fellow at the China Institute of International Studies (CIIS). This paper is the outcome of research at CIIS.

About CIIS

China Institute of International Studies (CIIS) is the think tank of China's Ministry of Foreign Affairs. It conducts research and analysis on a wide range of foreign policy issues. Research at the Institute is focused on medium and long-term policy issues of strategic importance, particularly international politics and world economy. The Institute hosts various seminars and conferences to discuss international developments and has constructed a world-wide scholarly and second-track exchange network.

About ASPI

ASPI's aim is to promote Australia's security by contributing fresh ideas to strategic decision-making, and by helping to inform public discussion of strategic and defence issues. ASPI was established, and is partially funded, by the Australian Government as an independent, non-partisan policy institute. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Cover image: Binary numbers and Australian and Chinese flags © ASPI

Australia–China cyber relations in the next internet era

Simon Hansen

December 2015

First published December 2015

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

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

 Facebook.com/ASPI.org

 @ASPI_org

CONTENTS

Chinese President Xi Jinping (C) delivers a keynote speech during the opening ceremony of the Second World Internet Conference in Wuzhen Town, east China's Zhejiang Province, 16 December 2015. © Li Tao/Xinhua Press/amanaimages

EXECUTIVE SUMMARY

Competition for influence in cyberspace has increased. States are pressing their diplomatic footprint in regional and international forums in an attempt to sway the future of the internet and advance their interests in cyberspace debates. Equally, states are developing military capabilities to protect and exploit interconnected networks.

Over the past five years, Australia has been building formal cyber policy partnerships and information-sharing arrangements with the US, New Zealand, Japan, Korea, India and China. Recent regional dialogues fulfilled a commitment Foreign Minister Julie Bishop made at the 2013 Seoul Cyberspace Conference 'to initiate bilateral cyber policy talks'.[1] The most important and challenging of those partnerships is with China.

Cybersecurity is a first-order national security issue, and ICT networks are critical for Australia's digital future and economic prosperity. Closer dialogue with China—our largest trading partner and biggest perceived cyber threat—is needed.

Common ground between Australia and China on cyber policy is thin, and there's disagreement on many issues. But closer dialogue is needed to find opportunities to cooperate on shared threats and to limit the likelihood for misadventure. This special report is a building block for that discussion.

Dialogue should focus on confidence building measures and practical initiatives in the short term to improve mutual understanding and foster communication. In the long term, as confidence improves, we should broach sensitive issues, manage areas that we disagree on, and establish rules and norms to limit the likelihood of a crisis.

Four key policy objectives are outlined in this report:

Reach mutual understanding on key terms, national policy and organisational structure to promote certainty and stability in the relationship.

Explore practical initiatives to deal with cybersecurity threats, including policing and law enforcement; regional capacity building; and an industry forum.

Discuss ideological differences in attitudes to the internet, presenting opinions and respecting them even if they are fundamentally opposed.

Finally, and most importantly, broach strategic issues and establish robust mechanisms and limits to prevent the rise of conflict.

ASPI has worked closely with the China Institute of International Studies to advance discussion on cyber policy, and several viable policy initiatives are proposed in this report. The author completed research for the report as a visiting fellow at the institute's headquarters in Dongcheng, Beijing.

AUSTRALIA, CHINA AND CYBERSPACE

Over the past five years, Australia has been building formal cyber policy partnerships and information-sharing arrangements to advance its interests (Figure 1). In 2011, the Australia–US Ministerial Consultations released a Joint Statement on Cyberspace. And in 2012, Australia and New Zealand held their first cyber dialogue to address common concerns.

Figure 1: Australia's emerging cyber policy architecture

More recently, in 2014 and 2015, Australia added inaugural cyber dialogues with Japan, Korea, China and India to its calendar. Those dialogues fulfilled a commitment Foreign Minister Julie Bishop made at the 2013 Seoul Cyberspace Conference 'to initiate bilateral cyber policy talks'.[2] The most important and challenging of those partnerships is with China.

Australia and China have both raised cybersecurity as a first-order political issue. The Department of the Prime Minister and Cabinet reported to the Australian Government in mid-2015 on the recommendations of its cybersecurity review and intends to release a new cybersecurity strategy. In China, President Xi Jinping established the Central Leading Group for Cyberspace Affairs in February 2014 to provide strategic guidance to China's cyber policy approaches.

Both nations have also supported the development of a stable and secure internet. At the 2014 World Internet Conference in Wuzhen, President Xi stated in a letter to the participants—presented by Vice Premier Ma Kai—that China intends to work with the 'international community to promote the building of a peaceful, secure, open, and cooperative cyberspace'.[3] In April 2015, at the Cyberspace Conference in The Hague, Foreign Minister Julie Bishop stated that the Australian Government is committed to an 'open, secure and peaceful internet'.[4]

But there are clear ideological differences between Australia and China. It's unsurprising that states with different values and political traditions have reached different conclusions about the internet. President Xi himself stated at a landmark address to the Australian Parliament in November 2014 that 'it is natural for us to have disagreements on some issues'.[5]

Also, a strategic trust deficit in the Australia–China relationship will affect the extent of dialogue. One major view in China is that Australia and our allies are exploiting a dominant position in cyberspace to undermine other states. This view has gained acceptance in China following the Snowden revelations and reveals a genuine perception of vulnerability. In Australia, public discussion has largely positioned China as a cybersecurity threat rather than an enabler of security—as shown by media attention to the alleged theft of F-35 design plans and the Ben Chifley Building blueprint.[6]

In the next internet age, as nations continue to set the rules of the road, cybersecurity dialogue needs policy engagement, clear views, good—even robust—dialogue and an optimistic sense of partnership. Between Australia and China there are political readiness, strengthening trade and investment ties, and a growing urgency to identify areas of cyberspace that are critical to the interests of both nations.

Why cyber cooperation?

Recent years have seen promising developments in the Australia–China economic relationship. In 2013, Australia and China commenced direct currency trading and opened annual leadership talks. According to the Department of Foreign Affairs and Trade's *Composition of trade 2013–2014*, China–Australia two-way trade was valued at $159.7 billion and outstripped our trade with our next two major trade partners combined, Japan and the US.[7] The Australia–China High-Level Dialogue and the Strategic Economic Dialogue were inaugurated in 2014, and the China–Australia Free Trade Agreement was signed in June 2015.

Cyber policy dialogue that focuses on tackling shared threats and promoting economic growth while managing areas of concern is the way forward. Indeed, mutual economic development is a hallmark of both the now-defunct 'Team Australia' and Xi's 'China Dream'. States need to protect ICT systems that sustain shared prosperity and find common cause to combat threats that undermine security. The Turnbull government will further push Australia's digital transformation agenda and encourage dependence on networks that drive productivity.

Indeed, at the 2015 Global Cyberspace Conference, Foreign Minister Bishop stated that 'today's diplomatic efforts should focus on ensuring the internet continues to flourish as a central institution of economic activity.'[8] For Australia and China, there's an increased need to provide clarity and reassurance about cyber policy concerns that affect the gold-bearing veins of our relationship.

There are measures that states are willing to address readily, such as cooperative mechanisms to combat cybercrime. And there are other measures that will take longer to agree on, such as red lines on state-based cyberattacks that could damage critical economic infrastructure, or stopping the corrosive effects of economic cyber theft.

Past cyber policy discussion

Australia and China cyber policy engagement suggests an ad hoc and limited approach. Nevertheless, there has been some success as part of the computer emergency response team (CERT) relationship, the ASEAN Regional Forum (ARF) and the UN. A brief overview of this foundation is needed before a future agenda can be outlined.

Computer emergency response teams

CERT Australia and China CERT have established information-sharing and incident response mechanisms. In 2013, both sides signed a memorandum of understanding to build contact mechanisms, enhance information sharing, streamline priority incident handling and leave open opportunities for joint projects, such as capacity building.

Regionally, both national CERTs lead the Asia–Pacific CERT (APCERT) steering committee responsible for general operating policies, procedures and guidelines for regional internet security. APCERT has been conducting joint exercises, including cyber exercise drills to prepare for international cooperation following potential cyber incidents. CERTs from each country interact during the drills to enhance communication protocols, technical capabilities and incident responses.

ASEAN Regional Forum

China and Australia have also led discussions at the ARF workshop series on measures to enhance cybersecurity. In 2013, China and Malaysia co-chaired a workshop that focused on legal and cultural differences between states in cyberspace. In 2014, Australia and Malaysia co-chaired a workshop on cyber confidence building measures, one of the aims of which was to establish a network of contacts within ASEAN states that could be activated in times of cyber crisis. And in 2015, at the ARF Workshop on Cyber Security Capacity Building in Beijing, Chinese Assistant Foreign Minister Zheng Zeguang set the direction for a 'consensus-driven, pragmatic, and prosperity-focussed approach to capacity building'.[9]

There's also been progress in other regional discussions, such as the APEC Telecommunications and Information Working Group and its three steering groups (on liberalisation, ICT development, and security and prosperity). Recent issues have included cybercrime, the internet economy, mobile security, Domain Name System Security Extensions, and Internet Protocol version 6.

United Nations

At the UN, Australia and China worked together in the 2012–13 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Information Security (GGE), a group that met previously in 2004–05 and 2009–10.

In 2013, the GGE reached consensus in its report A/68/98 that international law, in particular the UN Charter, applies to the state use of ICT. The group also made recommendations on responsible state behaviour, confidence building measures and capacity building measures. On 2 December 2014, the General Assembly welcomed the work of the GGE and took note of its recommendations in Resolution A/RES/69/28.

In June 2015, the GGE—in which Australia is no longer a member—agreed to a consensus document that enshrines a number of norms that guide state activity in cyberspace. One important recommendation is that a state shouldn't conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure.[10]

But how states define terms such as 'critical infrastructure' remains ambiguous, along with other issues such as the applicability of humanitarian law. And this is the fail point of the GGE: while the small group agreed on certain norms, the real test is *how* each state will interpret and apply those norms. It remains to be seen whether the consensus recommendations suggest complete agreement and understanding between the GGE members. As the mandate of the GGE continues to develop into a specific agenda, it'll be hard to find ground on which to base a meaningful consensus.

One issue is particularly divisive—the application of existing law versus the establishment of new international law. As the 2012–13 GGE chair, Australia stressed the application of existing international law, partly in response to earlier calls by China and Russia that new laws may be needed. China's previous views were expressed in the 2011 International Code of Conduct and at the World Conference on International Telecommunications in 2012.

China's cyber discussions

Australia is relatively late in establishing its own cyber dialogues in the region. It's worth looking at existing cyber discussions that China has to gauge how those experiences can inform our approach.

- In October 2015—six years on from an agreement to enhance cooperation in the Action Plan for Promoting Trilateral Cooperation—South Korea, Japan and China held their second trilateral cybersecurity dialogue. Shield Security Research Center has attributed slow progress to strained diplomatic ties and the difficulty in sharing sensitive information on cyber threats with non-allied countries.[11]
- The US and China have an official cyber working group that began in 2013 under the Strategic and Economic Dialogue. Since the US Department of Justice indicted five People's Liberation Army officers for theft in May 2014, dialogue has stalled, although a new cybersecurity commitment to limit attacks was made in September 2015, including a public agreement that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, trade secrets or other confidential business information.[12]
- In October 2015, the UK and China agreed to a joint statement on building a global comprehensive strategic partnership, including the establishment of a high-level security dialogue and a commitment to not conduct cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage.
- The emerging economies of Brazil, Russia, India, China and South Africa have also established a working group on cybersecurity. Early discussion has focused on best practice and capacity building to combat terrorism; controversial US global surveillance networks have also been a topic.
- The Shanghai Cooperation Organisation had early success when it signed the 'Cooperation in the Field of Information Security' agreement in 2008, setting the agenda on the concept of state sovereignty in cyberspace and combating terrorism.
- In May 2015, Russia and China inked an extensive cybersecurity pact, 'agreeing to not conduct cyber attacks against each other, as well as counteract technology that may destabilise the internal political and socio-economic atmosphere or interfere with the internal affairs of the state'.[13]

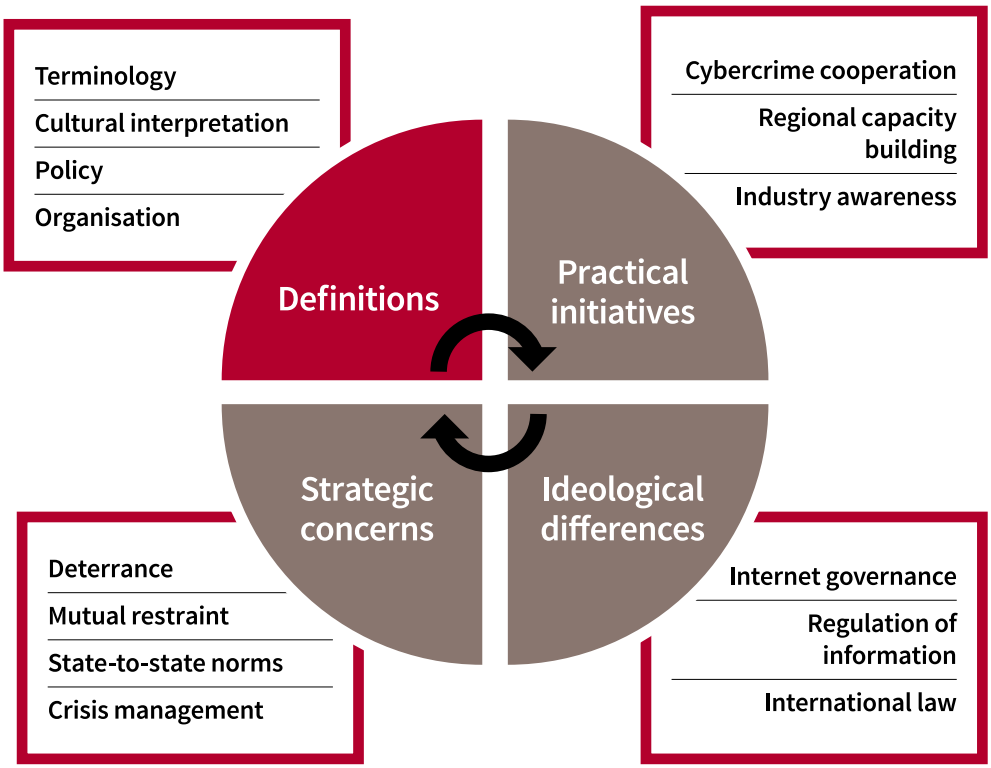
Even though these experiences reveal opportunities for the development of cyber relations, progress will be slow. The effort will be more successful with nations that share similar values towards the internet and aren't entirely straightjacketed by strategic rivalry and the need to cast blame.

An agenda for cyber cooperation

This report recommends four key areas to develop Australia–China cyber relations (Figure 2):

- Reach mutual understanding on key terms, national policy and organisational structure to promote certainty and stability in the relationship.
- Explore practical initiatives to deal with cybersecurity threats, including policing and law enforcement; regional capacity building; and an industry forum.
- Discuss ideological differences in attitudes to the internet, presenting opinions and respecting them even if they are fundamentally opposed.
- Finally, and most importantly, broach strategic issues and establish robust mechanisms and limits to prevent the rise of conflict.

Figure 2: Areas for cyber cooperation



SHARING DEFINITIONS, POLICIES & ORGANISATIONAL STRUCTURES

Clarifying terms is a baseline confidence building measure that leads to transparency and understanding while ensuring that each side isn't talking past the other.

Terms, concepts, cultural interpretations

Across cultures and languages, it's difficult to find and agree on shared definitions. In China, concepts of 'network security' (*wangluo anquan*) and particularly 'information security' (*xinxi anquan*) aren't just technical issues; they're also a content and regulation matter. In Australia, notions of cybersecurity more narrowly relate to the security of the systems, as opposed to their content.

'Informationisation' (*xinxihua*) and 'information security' (*xinxi anquan*)—two key terms in China—are strongly linked with domestic development and political stability. Concepts such as 'cyber sovereignty' (*wangluo zhuquan*) and 'positive energy' (*zhengnengliang*) reveal a managed approach to information and a concern about interference in China's internal affairs.

There's a need to discuss concepts such as 'cyberattack' (*wangluo gongji*), 'cyberwar' (*wangluo zhanzheng*), 'cyberterrorism' (*wangluo kongbu zhuyi*) and 'privacy' (*yinsi*). International debates haven't led to any concrete definitions, but even identifying differences can be an objective worth exploring.

However, there's an interest in limiting discussion on particular issues. For instance, the idea of 'cyber weapon' isn't well defined, and it may be in Australia's interest to remain circumspect. Defining terms too finely would draw us into discussion about arms control and limitations on cyber offensive capabilities.

This may be a preferable option in the long term, to limit the 'proliferation' of cyber weapons, but it's currently not a strong position when Australia has, presumably, a technological advantage over competitors. Importantly, there are no rules or means to ensure that states are taking their responsibilities for cyber 'arms control' seriously and not free-riding on other states' goodwill. In short, cyber arms control discussions will need to be reconciled with states' covert cyber activities and interests in promoting them.

Organisational structure, policy and strategy

Australia and China should explore the policy and organisational structure of each other's major cyber policy actors. It's a good place to start, as there's a lack of publicly available information. Australia's cybersecurity strategy was last released in 2009. China is expected to release its first national cybersecurity strategy—at least internally—this year.

Both governments are grappling with their cyber policy coordination. In China, the Cyberspace Administration of China (formerly the State Internet Information Office) has taken on a coordinating role. The high-profile Central Leading Group is chaired by President Xi Jinping and includes Premier Li Keqiang and Liu Yunshan. Established departments such as the Ministry of Industry and Information Technology and the Ministry of Public Security are

traditional stakeholders. In Australia, cyber policy is in the hands of the Department of the Prime Minister and Cabinet, while the Cyber Security Operations Board and the Australian Signals Directorate oversee the operation and coordination of capabilities.

At a minimum, discussion would need to explore organisation and coordination frameworks, policy leadership, cyber policy, national cybersecurity strategy, and the major departments and their roles. Transparency about cyber policy organisation is a good confidence building measure, especially when responsibilities are changing quickly—promoting suspicion abroad.

PRACTICAL INITIATIVES

There are at least three areas for further practical cooperation that builds on existing information-sharing arrangements: law enforcement cooperation on cybercrime, regional capacity building, and an industry forum.

Law enforcement cooperation on cybercrime

Previous experience with other international partners suggests that Australia could develop closer cooperation with China on information sharing, threat assessments, transnational investigations and domestic legislation development.

The transnational Cyber Crime Investigation Centre in Indonesia opened in 2011, and Australia delivered significant contributions in training and technical assistance. We're also a founding partner of the Global Forum on Cyber Expertise, announced in 2015, and will participate in the Preventing and Combating Cybercrime in Southeast Asia initiative with Japan and the US.

Opportunities to share experiences about domestic legislation on cybercrime and build enforcement capacity would be valuable to both sides. In principle, cooperation between the Australian Federal Police and the Ministry of Public Security on corruption and economic fugitives—as part of Operation Fox Hunt and Operation Skynet—is encouraging.

But there are limits to law enforcement cooperation. Australia and China have different views on how to coordinate international approaches to cybercrime. We've acceded to the Budapest Convention on Cybercrime, while China has advocated for a separate UN treaty. Australia holds that existing conventions harmonise international cooperation well, while China has suggested that a UN treaty on cybercrime would better address the needs of developing countries. There are also political differences in the balance between security, freedom and privacy. In any case, broader differences in multilateral cybercrime approaches shouldn't impede bilateral cooperation, as operations could be assessed on a case-by-case basis.

Regional capacity building

In regional forums, particularly the ARF, there's been consistent signalling by Australia and China on the need to bolster regional states' cyber capacity. The ASEAN region is a priority, as there's haphazard adoption of cybersecurity policy in the region. One suggestion that deserves further analysis comes from Caitríona Heinl at the S. Rajaratnam School of International Studies. Heinl advocates for a permanent mechanism for regional coordination and information sharing.[14] This could be achieved by way of collaboration with states that are at different levels of cyber maturity, with more mature nations providing training and expertise—a point argued in ASPI's most recent cyber maturity assessment.[15]

This idea would resonate with China. In a statement to the inaugural ASEAN–China cyberspace forum, Cyberspace Minister Lu Wei suggested the establishment of a regional information harbour to build capacity and report cyber intrusions. This mechanism could operate within the ARF, a new ASEAN CERT or the existing APCERT. Australia should consider its own contribution to such a proposal, particularly industry-led expertise and training. Our role

in the MH370 search and rescue mission and the Joint Agency Coordination Centre stands as a good example of regional information sharing, policy coordination and leadership.

Industry meeting on the digital economy

In the US–China economic relationship, there have been signs of declining enthusiasm for bilateral trade and investment in the high-tech sector. Concern reached a new high in early 2015, when China called for a 'cybersecurity review regime' to assess all IT products across its economy, and particularly in the banking sector.

This has raised concern among international companies that China is forcing them to comply with contentious policies, allowing authorities to install backdoors to enable third-party access. If companies don't comply, they risk being cut out of China, the largest and fastest-growing technology and telecommunications market—with more than 600 million internet users and worth an estimated US$466 billion.

China has begun to flex its tech muscles over the past few years, as *The New York Times*' Paul Mozur and Jane Perlez explain:

> Beijing is developing its own operating system and has placed government procurement bans on Microsoft's Windows 8. Other companies, like Qualcomm, have faced antitrust investigations in China. Several American business groups also lashed out this year at a Chinese law they said would prevent tech companies based in the United States from selling hardware and software to China's banking industry.[16]

China's digital policies and security laws have been seen as discriminatory and anticompetitive, and the Obama administration has previously taken its concerns to the World Trade Organization, asking China to clarify its intent.

All nations have an interest in developing transparent standards for inspecting and sourcing technology products. And, while Australia has less of a stake in the global high-tech industry, it's foreseeable that alleged discriminatory policy could jeopardise business support for Australia's own China trade policy, especially if those review processes continue to move into the finance and banking sectors.

An open investment regime and an attractive investment environment are essential to increase employment and maintain living standards. They are the engine room of Australia's economic progress. There should be greater political attention to how cybersecurity policy affects industry and how governments can create a strong business and innovation environment, particularly in the IT and banking sectors.

This paper proposes a joint Australia–China industry forum on the digital economy, to be organised by an interdepartmental group and to work with business and industry. The forum is proposed as a platform to discuss joint research and development projects; transparent global standards; education and training on information security; cybersecurity mitigation strategies and public awareness; and confidence building through sharing information and best practice.

BROACH IDEOLOGICAL DIFFERENCES

Australia and China have different ideological approaches to the internet (Table 1). It's important that those differences are drawn out in official discussions. There are many areas of debate, but three critical differences can be drawn out.

Table 1: Key ideological debates

Australia	China	Issues
Multi-stakeholder internet governance	UN-led internet body	Governing the internet, internet architecture distribution, IANA* transition, internet sovereignty
Freedom of information	Regulation of information	Economic benefits versus increased political security, supply chain concerns
Apply existing international law	New international law	UN Charter and the use of force (Chapter VII), international humanitarian law, human rights under international humanitarian law, state responsibility, Tallinn Manual, Budapest Convention on Cybercrime

* IANA: Internet Assigned Numbers Authority.

Governing the net

A predominant international view supported by Australia is that nation-states have an important but secondary role in the internet and should ensure that the internet is free, open and secure. This view proposes that internet governance isn't a state-led hierarchy, but a multi-stakeholder arrangement between civil society, industry and government. The model is worth pursuing, as it would better support economic growth and the flow of ideas.

A view China and others have supported is that nation-states should take the lead in a UN-led internet body that takes over from existing key internet institutions. Because national borders exist, the internet isn't entirely an open commons. And, when borders exist, state sovereignty applies, so states are best placed to govern the net. China's cyber chief, Lu Wei, has advocated this view in international forums, such as Internet Corporation for Assigned Names and Numbers and the London process.

In the end, neither view is entirely practical. A true multi-stakeholder approach is unworkable, given the influence of developing nations' views and their interest in regulating information, but the state-centric model threatens the very interconnectedness of open, global networks. Political imagination is needed to reconcile state sovereignty over networks with broader state obligations to an open, safe and peaceful global internet.

Information in cyberspace

One concern for China is that the internet could potentially undermine political and social stability. A perceived vulnerability about the allocation of internet resources and the risk of political interference and subversion—

from state and non-state actors—have led China's leaders to develop a more regulated internet: the legendary 'Great Firewall'.

Therefore, the notion that information should be free and open isn't globally accepted. Australia is a proponent of internet freedom, and outlining how strict regulation of the internet can erode investment, trade and other productive activity is a key diplomatic message. But this might not prove convincing in the long term as China continues to develop its own autocratic command of networks.

International law

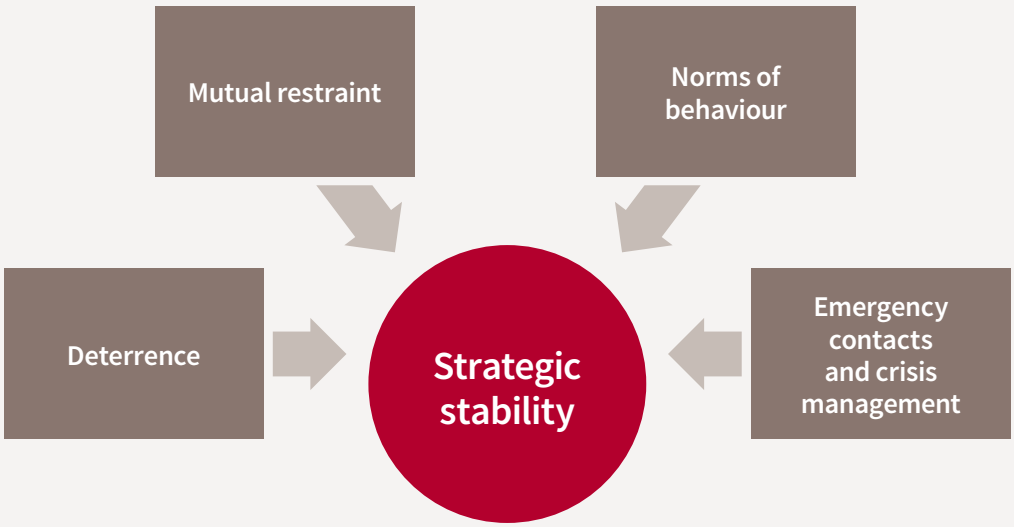
Australia acknowledges the application of international law to state conduct in cyberspace. However, as Foreign Minister Bishop has stated, 'it is not easy—it requires a careful analysis of exactly *how* the rules of international law apply in a cyber setting.' Certain applications of law are still the subject of interpretation, laws meant to constrain behaviour will continue to be unclear and, for the most part, definitions are implicit and aren't formalised.

While there's been apparent consensus in the GGE report, the conversation about the application of international law has only just started. The simplest distinction is that Australia takes the view that the scope of international law should be expanded to cyberspace, while China and other emerging nations argue that new treaties and laws are needed. Outlining further distinctions will require robust dialogue.

STRATEGIC ISSUES

In Australia–China relations, there needs to be a sustainable way to promote certainty and stability in cyberspace. The best way to ensure stability is deterrence, mutual restraint and established norms of behaviour, mixed with measures to prevent a crisis arising from misinterpretation or miscommunication. There are four critical areas of dialogue in that regard (Figure 3).

Figure 3: Stability in cyber relations



Deterrence

Deterrence is a contested concept in cybersecurity debates, as a cyberattack is fundamentally different from other attacks. Identifying the source of the attack and attributing it is problematic, along with effectively signalling offensive cyber capabilities. Still, a clear policy, strong cybersecurity defence and a mature cyber offensive capability are key elements for cyber deterrence and allow each side to act confidently and rationally.

The rapid development of offensive cyber capabilities continues to concern world leaders, and early openness to cooperation has given way to more forbidding tones. In mid-September 2015, President Obama warned that 'the US is prepared to take some countervailing actions in order to get China's attention'—a message backed up by a sanctions program established by executive order in April.[17]

Mutual restraint

What measures of self-restraint should states implement to promote international stability in cyberspace? Red lines are clearly needed to avoid an unnecessary crisis, as there's no clear idea about what states shouldn't do. Should

civilian critical infrastructure be exempt from targeting, as well as dual-use civilian–government infrastructure? And are CERTs, as the primary tool for incident response, acceptable targets in a network attack?

These questions will fuel an evolving conversation. The GGE has provided a useful guideline for states, as has the recent deal between the US and China on cyberattacks. It's now time to find a platform for practical discussion. The ARF is a working model and is well poised to develop a framework to limit the potential for cyber conflict and build a network to activate during a crisis.

Norms of state behaviour

Cyberespionage

Espionage remains an effective and acceptable instrument of the state, but there's been contention recently—especially between China and the US—on the intent of cyber espionage. Whether there's a clear distinction between politically motivated espionage (such as the alleged hack of the US Office of Personnel Management) and economically motivated espionage (such as the highly publicised hack of US companies) is debated. Recent pacts that the UK and US have made with China to not conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information will no doubt be tested.

Computer network attack

There are a number of issues to discuss about the prospect of cyberwarfare and computer network attacks. Key questions include: What's a cyberattack and what's the threshold for war? Is there a distinction between defensive and offensive 'cyberweapons' and postures in cyberspace? Is pre-emptive strike or a no-first-use policy applicable to cyberattacks? What are the rules of 'cyber conflict', and is the Tallinn Manual on the law applicable to cyber warfare[18] a useful tool for analysis? How do offensive capabilities shape other states' capability choices? These issues represent a small slice of potential discussion, but reveal how much dialogue is needed over the long term.

Emergency lines of communication and crisis management

One recommendation of the 2015 GGE document is the development of and support for bilateral consultations to enhance interstate confidence building and reduce the risks of misperception, escalation and conflict that stem from ICT incidents. Australia and China should improve existing channels of communication for crisis management and develop early warning mechanisms.

CONCLUSION

Dialogue reduces mistrust through transparency and predictability. This paper outlines four key areas for Australia–China cybersecurity discussion, each more challenging than the last: definitions and communication; practical cooperation; ideological differences; and strategic issues.

Along with the suggestions made in the paper, an institutionalised Track 2 dialogue should be established. ASPI has already convened cybersecurity dialogues with Chinese think tanks, including the China Institute of International Studies and the China Institute for Contemporary International Relations. Discussion has been robust, and there's scope to develop a joint statement and engage in creative policy activities such as cyber war games and crisis coordination exercises as part of Track 1.5 activities.

In the next internet age, Australia–China cybersecurity discussion needs policy engagement, good dialogue and an optimistic sense of partnership. A substantive cyber dialogue will promote certainty and stability in the relationship and create policy settings conducive to economic prosperity.

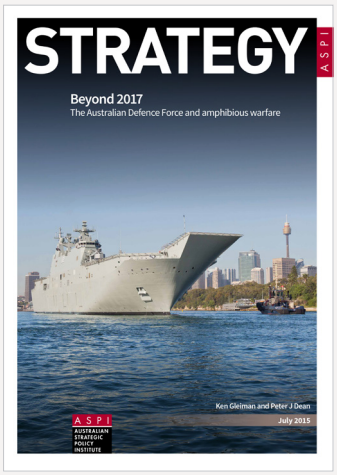
NOTES & ACRONYMS

1 Department of Foreign Affairs and Trade, *Annual report 2013–2014*, 19 September 2014, online.
2 Department of Foreign Affairs and Trade, *Annual report 2013–2014*, 19 September 2014, online.
3 State Council, 'World Internet Conference open in E China's Wuzhen', 19 November 2014, online.
4 Minister for Foreign Affairs, 'Statement for Plenary Session on International Peace and Security', 17 April 2015, online.
5 Xu Haijing, 'Chinese President Xi Jinping wins hearts, minds in Australia', *Xinhua, 25 November 2014,* online.
6 Lisa Millar, Ben Knight, 'Chinese spies hacked secret US weapons systems including F-35 Joint Strike Fighter: reports', *ABC News*, 29 May 2013, online.
7 Department of Foreign Affairs and Trade, *Composition of trade 2013–2014*, online.
8 Minister for Foreign Affairs, 'Statement for Plenary Session on International Peace and Security'.
9 Tobias Feakin, 'Cyber capacity building through the lens of techno nationalism', *ASPI Strategist*, 17 August 2015, online.
10 Report of the GGE (A/70/174), 22 July 2015, online.
11 SHIELD Security Research Center, Hitachi Systems, 3 September 2013, online.
12 Reuters, 'US and China in urgent talks on cybersecurity deal', *The Guardian*, 20 September 2015, online.
13 Olga Razumovskaya, 'Russia and China pledge not to hack each other', *Wall Street Journal*, 8 May 2015, online.
14 Caitríona Heinl, 'Regional cybersecurity: moving toward a resilient ASEAN cybersecurity regime', *Asia Policy*, July 2014, online.
15 Tobias Feakin, Jessica Woodall, Liam Nevill, *Cyber maturity in the Asia–Pacific*, ASPI, 26 October 2015, online.
16 Paul Mozur, Jane Perlez, 'China flexes tech muscles before a state visit', *New York Times*, 8 September 2015, online.
17 Executive Order: Blocking the property of certain persons engaging in significant malicious cyber-related activities, 1 April 2015, online.
18 Originally titled the *Tallin manual on the international law applicable to cyber warfare; published in 2013 by Cambridge University Press.*

Acronyms and abbreviations

APCERT	Asia–Pacific CERT
APEC	Asia–Pacific Economic Cooperation
ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
CERT	computer emergency response team
ICT	information and communications technology
IT	information technology
UN	United Nations

Some previous ASPI publications



Australia–China cyber relations in the next internet era

$5.00 ISSN 2200-6648