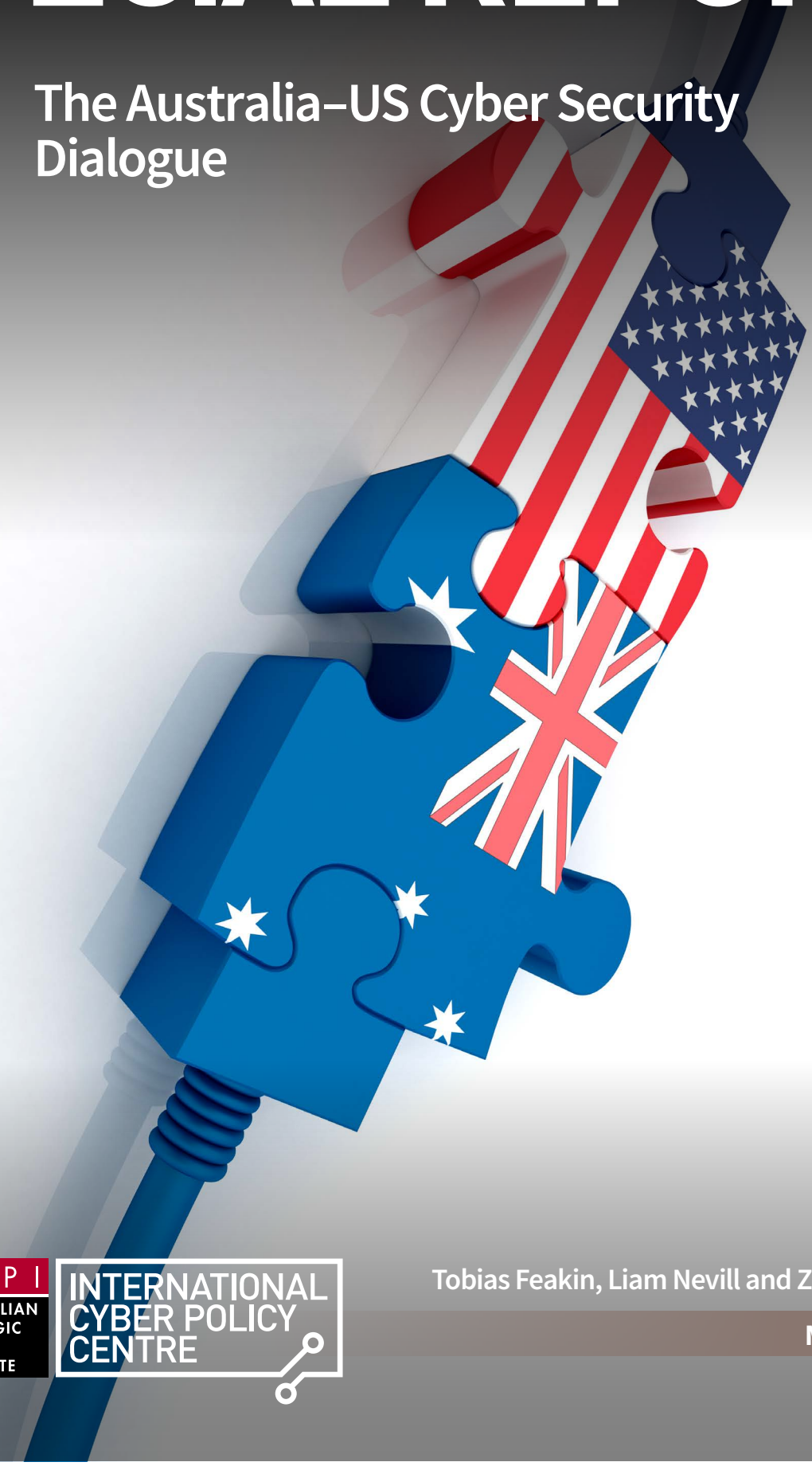
SPECIAL REPORT

The Australia–US Cyber Security Dialogue



Tobias Feakin, Liam Nevill and Zoe Hawkins

March 2017

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

Tobias Feakin

Toby was Director of ASPI's International Cyber Policy Centre at the time of the dialogue. He is now Australia's Ambassador for Cyber Affairs.

Liam Nevill

Liam is the Principal Analyst in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber policy issues.

Zoe Hawkins

Zoe is an Analyst in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber policy issues.

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: Australia and USA flags on computer cables © alxpin / iStock

The Australia–US Cyber Security Dialogue

Tobias Feakin, Liam Nevill and Zoe Hawkins

March 2017

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

First published March 2017

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

FOREWORD

The inaugural Track 1.5 Australia–US Cyber Security Dialogue, held in Washington DC in September 2016, added to the continual strengthening of the Australian–US cyber relationship. Jointly facilitated by ASPI and CSIS, it brought together government officials, business leaders and academics from both countries. Given the existing strong bonds between our nations, in government, business and academia, the dialogue was able to dive straight into frank and free-flowing discussions on matters affecting Australia, the US and the region more broadly. Perhaps most importantly, a practical forward work plan was agreed for ASPI and CSIS to pursue before the next dialogue, to be held in Australia later in 2017. I certainly welcome the efforts by both ASPI and CSIS to broaden and deepen such a critical bilateral relationship—one that will only become more important in coming years.

Alastair MacGibbon,
Special Adviser to the Prime Minister on Cyber Security

Participants at the dialogue in Washington DC, September 2016

INTRODUCTION

Unlike other traditional security issues, cybersecurity can't remain purely the purview of states. The multifaceted nature of the threat requires a multifaceted response. Australia and the US face an environment in which our understanding of 'the rules' is being challenged by states that push the envelope of acceptable behaviour online through disruption and disinformation. But governments aren't the exclusive targets. States pursue competitive economic advantage through the theft of intellectual property from foreign corporations, cybercriminals siphon money from banks, and hacktivists compromise the data of organisations. So working with allies, bringing together the public and private sectors and pooling information and resources will be essential elements of tackling this threat effectively.

The inaugural Australia–US Cyber Security Dialogue held in Washington DC in September 2016 examined all these issues and how best to manage them in a cooperative manner. The dialogue was facilitated by the Australian Strategic Policy Institute (ASPI) and the Center for Strategic and International Studies (CSIS). The robust bilateral and cross-sectoral discussion sessions, summarised below, traversed issues of cooperation in the Asia–Pacific, combating cybercrime and advancing the digital economy. The dialogue identified focus areas and a corresponding ASPI–CSIS joint work plan designed to further advance bilateral collaboration in this critical policy area. The three initiatives, outlined in the final section of this report, will sustain the momentum of Australia–US cyber cooperation, laying the groundwork for the agenda and driving discussion at the 2017 dialogue.

Today's cybersecurity landscape

Cybersecurity is now a daily concern for world leaders and business professionals. From state-led cyber espionage and information operations to financially motivated cybercriminals exploiting regional safe havens, mature cyber policy is now a critical requirement for national security and economic prosperity. Our vulnerability to these threats only continues to increase as the connectivity of our civil society, infrastructure, governments and militaries grows exponentially, so we must take coordinated steps to mitigate these risks. However, the proliferation of cyberspace isn't just a security concern; it also offers great opportunities for advances in governance and the digital economy, so we must develop a nuanced approach to cyberspace that balances security and openness.

Cybersecurity is a frequent point of contention among leaders of the major powers. President Obama regularly exchanged strong views with his Chinese counterpart, President Xi, over state-led economic espionage and explicitly accused Russia's President Putin of undertaking strategic information operations to influence the 2016 US Presidential Election.

The cyber discussion is equally important among close allies in order to shore up economic and national security wellbeing. The partnership between Australia and the US is longstanding and deeply embedded in our national consciousness, but the relationship's ability to adapt to a changing international environment is sometimes overlooked. It's this bilateral capacity to embrace new forms of exchange and business that has enabled it to endure.

Cognisant of this and the growing importance of cybersecurity discussions, Prime Minister Malcolm Turnbull travelled to Washington DC for bilateral meetings with President Obama in January 2016, ready to talk cybersecurity

on multiple fronts. He was said to be impressed by how central it was in all of his meetings, from President to Secretary: they all wanted to address aspects of cybersecurity with a tech-savvy alliance partner's Prime Minister.

During that trip, the Prime Minister announced the new Australia–US Cyber Security Dialogue to be convened by ASPI and CSIS.[1] The idea was a simple one: while the two countries are strong alliance partners that have excellent government relationships, there was more that could be done.

> There's never been a more important time to invest in deepening the Australia–US partnership.

There's never been a more important time to invest in deepening the Australia–US partnership in this regard. Our neighbourhood, the Asia–Pacific, is undergoing significant change, including rapid economic growth, increasing connectivity, insufficient cyber policy or legislation development and rampant cybercrime in some areas. The release of Australia's Cyber Security Strategy and the election of Donald Trump mean that 2017 is an important time to reaffirm cybersecurity as a priority international issue and reassert the value of bilateral cooperation towards that effort.

SESSION 1: CYBER COOPERATION IN THE ASIA–PACIFIC

The Asia–Pacific's increasing importance to the economic and strategic interests of Australia and the US meant that examining the region's cybersecurity was an obvious choice for the first in-depth session at the Australia–US Cyber Security Dialogue. The digital potential of the entire region offers enormous development and trade opportunities that, if effectively harnessed, will benefit the economies of both countries.

Connectivity rates in the Asia–Pacific are soaring, growing at 12% during 2015.[2] But about half the region is still not connected to the internet, providing a huge reservoir of people yet to take advantage of the benefits of digital commerce and development. The region's economies continue to grow, and GDP growth rates of 5.4% in 2016 are driving the increasing importance of the region to broader international economic security.[3] However, this economic growth hasn't been evenly distributed across the Asia–Pacific, and there are significant regional disparities. In some cases, the rapid proliferation of networks isn't being matched by the necessary regulatory frameworks, governance structures or individual and corporate savviness towards cybersecurity threats. Digital tigers such as South Korea, Japan and Singapore are leading the way, but less developed states such as Laos and Bangladesh are struggling to establish cyber maturity. These disparities have created cybercrime hotspots in permissive regulatory environments, such as the Philippines, and protectionist barriers to trade in over-regulated economies, such as China. So, while regional connectivity promises prosperity, it can also complicate security and trade flows.

This unevenness also reflects the geopolitical realities of the Asia–Pacific. The region's geostrategic power struggles are being replicated in cyberspace, as major powers compete to exploit digital benefits and jostle to influence emerging countries as they come online. China is making waves in cyberspace. Its government is heavily investing in baseline ICT infrastructure across the region, condoning or overlooking cybercrime operations from within its borders, and leveraging cyberspace as a tool for information operations such as those conducted in July 2016 at Vietnamese airports in relation to the South China Sea disputes.

As China pursues its strategic interests through cyberspace, so too does the US. At the ASEAN Summit in Laos during September 2016, President Obama and Secretary of Defense Ash Carter reinforced the US commitment to rebalance towards Asia and its central security role in the Asia–Pacific. The US views cyberspace as an important mechanism by which to maintain its regional influence, and President Trump has outlined plans to prioritise investment in both its defensive and offensive cyber capabilities. The US and China have demonstrated some promising moves towards compromise, such as their September 2015 agreement on state-sponsored intellectual property theft.[4] However, their visions for the future of cyberspace remain at odds.

With the US as its central security partner and China as its top two-way trading partner, Australia has a vested interest in stabilising the region's digital landscape. Australia and the US's historic bilateral relationship, shared values and mutual interest in Asia–Pacific stability make them natural partners in ensuring that the current rules-based global order is recreated online.

In this complex strategic environment, Australia and the US must develop a nuanced and coordinated approach to regional cybersecurity. There's value in taking strong collective stands to defend the future of an open, free, secure and reliable cyberspace and advocating for principles of free trade and civil liberties, such as privacy

and freedom of speech. However, the inherently instable nature of contemporary cybersecurity means that unnecessary confrontation is best avoided in favour of strategic nudges and moves to collectively establish norms of online behaviour.

While military cooperation between Australia and the US is an important element of the bilateral relationship, cybersecurity is a whole-of-government issue. To facilitate more preventive and proactive cyber diplomacy, Australia and the US should move beyond incident response measures and work together to build capacity, develop international norms of online behaviour and establish confidence building methods in the Asia–Pacific. At the same time, Australia and the US should strive to be cyber role models for the region, exemplifying best practice in cybersecurity policy, practice and awareness at home.

The private sector must be a partner in the development and implementation of norms to ensure that there's consent among the various communities within the multistakeholder environment.

All of these collaborative efforts must involve partnering and potential co-ownership with the private sector, which operates much of the world's internet infrastructure. In many cases, private-sector companies have established links to government-owned enterprises in the region that can be used to help increase local cyber maturity. There's scope to improve the intelligence-sharing capacity of companies and to modernise international and cross-sectoral threat sharing mechanisms, creating a more detailed and real-time dialogue. Companies also have an important role to play in cyber norm development and implementation, and some US companies are already well engaged on this issue. The private sector must be a partner in the development and implementation of norms to ensure that there's consent among the various communities within the multistakeholder environment.[5]

The first session of the dialogue discussion cemented the importance of bilateral cyber cooperation in the Asia–Pacific. Delegates agreed there are significant benefits and risks at stake in the pursuit of regional cyber stability and underscored the role for private-sector partnership in this effort. As the fast-changing neighbourhood of two mature allies, the Asia–Pacific will remain a focus of the Australia–US Cyber Security Dialogue in coming years.

SESSION 2: FIGHTING CYBERCRIME IN THE ASIA–PACIFIC

Across the globe, financial losses due to cybercrime continue to mount. Estimates of the cost of cybercrime to the Asia–Pacific vary, but a suggested cost to Asian business of about US$81 billion in 2015 implies that it's a bigger problem than any one country can address on its own.[6] For the participants at the Australia–US Cyber Security Dialogue, discussing growing cybercrime threats and current cooperation between governments, law enforcers and the private sector highlighted some of the hurdles that must be overcome to elevate the fight against cybercrime.

The cross-jurisdictional nature of cyberspace means that multi-layered cooperation between both countries' government and law-enforcement agencies is required for cybercrime prevention and prosecution. At the government-to-government level, information sharing between the US and Australia is growing. In fact, Australia was the first country to enter into a sharing framework with the US Department of Homeland Security.[7] That's a promising step for bilateral cooperation on cybercrime and should encourage other countries to contribute as well.

However, the quality of the public–private partnership to fight cybercrime is not as high as it needs to be in either Australia or the US. In both countries, the government approach to the private sector is seen as paternalistic and, as a result, has both offended industry and disincentivised its full participation. Improving this perception through a more respectful government approach in pursuit of sincere, productive partnership will be a key requirement for improving cooperation on cybercrime.

Doing so is important, as the private sector has a crucial role to play in cybercrime information sharing. There's far more intelligence about the cybersecurity threat landscape available than is currently being shared between the private and public sectors in both countries. Issues of classification can stifle governments' ability to divulge data, while private-sector entities may withhold information from the government and other companies because they are worried about losing industry advantage, suffering damage to their reputation or facing legal issues. As a result, some companies prefer to passively benefit from others' information sharing before showing their own hand. Information sharing is only of value when the right information is exchanged consistently, building both goodwill and trust between parties and reinforcing the value of the agreement. More forthcoming attitudes from all stakeholders will be necessary to address the growing cybercrime challenge.

To that end, governments in Australia and the US must take seriously the task of communicating to the private sector the business case for information sharing. Sharing relevant intelligence with trusted partners can make cybercriminals' operations more difficult and improve the rate at which they are apprehended across the board, probably lowering the net cost to the average company. Sectoral information sharing and analysis centres and programs in which members must submit a minimum number of malware samples every day to retain their membership have been suggested as mechanisms by which to halt this race to the bottom.[8] Likewise, governments in Australia and the US must work to overcome unnecessary bureaucratic red tape and make useful threat trend information available to the private sector, where appropriate.

Ultimately, this problem can't be viewed in simplistic bilateral terms. Cyberspace is a dynamic and complex ecosystem of connections, and our response must reflect that. Effectively addressing cybercrime requires trusting relationships between both countries' governments and private sectors in order to create a multipolar collaborative

network between all four parties, rather than just a selection of two-dimensional connections. Doing so will allow for greater threat information sharing across multiple divides, and is an important goal to work towards.

Beyond information sharing, building cyber capacity in the Asia–Pacific is a significant area for Australia and the US's bilateral government-to-government and public–private cooperation. Cybercriminals are able to act with impunity within certain countries that don't have the resources, capability or legal framework to address cybercrime. Coordinated efforts to shut down those safe havens will increase the cost of business for cybercrime groups and decrease the rate of harm. So helping regional countries to engage in cyberspace more securely, by providing law enforcement training or policy development assistance, will promote online stability in the Asia–Pacific in line with US and Australian security interests. The growth of stable, trusted digital markets in the region will also assist Australian and American businesses to engage the region digitally with the confidence that they won't fall victim to cybercriminals or to regulations that impede their ability to compete. So, fortunately, the business case for this method of fighting cybercrime is a lot easier to make.

The private sector is particularly well positioned to tackle this task, as many companies possess the necessary investigative capabilities and local knowledge to help regional countries raise the difficulty of criminal operations. Therefore, bringing the private sector in at the design phase of projects is vital for executing effective capacity building around the region.

There's much that the US and Australia can do together to reduce the volume and seriousness of cybercrime. More robust threat information sharing and the active removal of cybercrime safe havens should be central focus areas for bilateral partnerships between both countries' government and private sectors. Further maturing US–Australian cooperation on cybercrime in the Asia–Pacific will provide increased security and economic prosperity for both countries.

SESSION 3: ADVANCING A SECURE DIGITAL ECONOMY

Digital communications have bridged the enormous physical distance between the US and Australia, enabling people on both sides of the Pacific to take advantage of innovative technologies and services. The growing opportunities for trans-Pacific digital trade prompted the Australia–US Cyber Security Dialogue to consider how best to securely expand the digital economy. McKinsey & Company estimated transnational data flows to be worth US$2.8 trillion in 2014, highlighting the increasingly important role of digital trade in the economies of both Australia and the US, as well as the broader Asia–Pacific region.[9] The dialogue discussion traversed the connection between cybersecurity and consumer confidence in digital commerce, corporate understanding of the threats and risks of cyberspace, the role of innovation and the effects of government regulation and free trade agreements on the digital economy.

Public trust in cybersecurity measures that protect personal and financial information underpins the stability and growth of digital commerce. Therefore, it's in companies' direct interests to effectively protect their customers' personal information from cyber threats. Discussions at the dialogue indicated that private-sector threat awareness is comparatively greater and deeper in the US than in Australia. In Australia, only the top group of the large ASX-listed firms seem to have a good grasp of the issue, with a significant drop-off below that level. The new Australian Cyber Security Strategy includes several measures designed to address the issue, including education and awareness raising for senior executives.[10]

However, raising the awareness of the C-suite is only one part of the solution. Cybersecurity product vendors need to reflect upon the limited success of their messaging, which has only penetrated a select number of corporate entities in Australia. The onus is on the cybersecurity industry to not only translate its products in a relatable way, but to also ensure that they're scaled to meet the needs of small to medium-sized enterprises, not just the top end of town.

Innovation in digital goods and services is a key theme of the economic policies of both the US and Australian governments, and these developments must be integrated within broader cybersecurity considerations. Innovative services and products promise to unlock new markets and increase productivity at home and abroad. The US remains a hotbed of innovative digital businesses, attracted to communities such as Silicon Valley where capital and technical expertise are concentrated. Australia recognised this when the first of several Australian international innovation hubs was established in San Francisco in 2015. Innovation requires a strong commitment to a digital-first policy, an alignment with cybersecurity policy and cybersecurity capability development, 'baked-in' awareness of cybersecurity, and encouragement of other regional partners to follow suit. Cooperation between the public and private sectors to implement innovation and cybersecurity policies is critical to ensure that investment and regulation are aligned with each other.

Inconsistent and contradictory trade regulations in the Asia–Pacific were also a key topic of discussion for Australian and American business at the dialogue. Trade agreements are one way to encourage regional countries to enact common policy and regulatory frameworks. The World Trade Organization agreement laid the foundation for digital trade as it exists now, but it didn't consider complex issues such as data storage. Building on the World Trade Organization arrangement, the rules of the Trans-Pacific Partnership's (TPP's) 'Digital Two Dozen' included

measures to prevent the balkanisation of the internet by limiting data localisation, and provisions on government cooperation on cybersecurity.[11] However, the US withdrawal from the TPP during the first week of Donald Trump's Presidency indicates that a different approach to trade agreements and regional regulations between the US and the Asia–Pacific more broadly will be necessary.[12]

In particular, data-localisation regulations requiring foreign companies to store citizens' data within a country's borders is a trend of concern for Australia and the US. It's a worrying indicator that security concerns are overshadowing the economic benefits of the current distributed network model. There are legitimate reasons for governments to access data that is stored remotely, and there should be an effective way for them to do so when reasonably necessary. But the complexity of providing such access highlights the difficulties of operating across multiple regulatory regimes. So the rationale for regulatory harmonisation is not only to reduce compliance costs for business. It's also based on the need to give governments confidence that they can access the data they need for security and law enforcement purposes. This imperative then has to be balanced against concerns about privacy and the protection of human rights.

It's reasonable to worry about foreign governments inappropriately exploiting data stored overseas, but there are ways for states to protect the privacy and security of their citizens while guaranteeing access to data that they require without inhibiting trade. For example, the recent European Union–US Privacy Shield agreement recognises that transatlantic data flows are an important part of the relationship and necessary for digital economic activity.[13] The agreement was made to resolve the uncertainty brought about by the European Court of Justice's overturning of the previous agreement due to concerns about US surveillance of EU citizen information stored in the US.[14] The new Privacy Shield agreement provides clarity for businesses in the US and the EU and assures the EU that the personal information of Europeans still benefits from a high level of privacy protection if it's transferred to the US.

There are significant opportunities to deepen digital trade between the US and Australia and to enable the continued economic growth of the Asia–Pacific.

There are significant opportunities to deepen digital trade between the US and Australia and to enable the continued economic growth of the Asia–Pacific. Cooperation to harmonise trade regulations in the region and investment in cybersecurity as an enabler of the digital economy will be the keys to unlocking the future potential of digital trade. Short-term bilateral actions can be taken to remove unnecessary impediments to the growth of digital trade between Australia and the US, and other regional partners can follow later. Identifying the policy and regulatory changes our respective governments can take now to enable this growth will be a key task for the Australia–US Cyber Security Dialogue before its next meeting in 2017.

AUSTRALIA–US CYBER COOPERATION: NEXT STEPS

The dialogue discussions on bilateral cooperation to combat cybercrime and support digital trade in the region are invaluable but, ultimately, actions speak louder than words. That's why it's important to translate the dialogue's productive conversations into an action plan that addresses short-, medium- and long-term issues. ASPI and CSIS have identified three joint projects to be pursued in the lead-up to the 2017 dialogue. This joint forward work plan will facilitate improved bilateral public–private cooperation on cybersecurity issues, increase the strength of Asia–Pacific cybersecurity, and identify ways to reduce the barriers to deeper business engagement.

First, effectively coordinating capacity-building efforts in the Asia–Pacific will strengthen the scope and reach of bilateral efforts and better engage private sector skills and capacity. Capacity building is the key to enhancing the region's security, facilitating new business opportunities and shaping the region's perspectives on key international cyber policy issues. ASPI's annual report, *Cyber maturity in the Asia–Pacific region*, has consistently identified countries in the Southwest Pacific and Southeast Asia as having a weak political and legal approach to cybersecurity and a severe lack of cyber incident response capability. As discussed, both Australia and the US have significant strategic, law enforcement and economic interests in improving the cybersecurity capacity of Asia–Pacific countries, particularly among ASEAN countries. Additionally, the private sectors in both countries also have an interest in improving Asia–Pacific cybersecurity. Stable online environments and trust in digital transactions are crucial for expanding business opportunities in this economically thriving region.

Funding for capacity building is obviously finite, so it's important to ensure that projects are as efficient as possible. Consultation with government and the private sector in Australia and the US will help projects to be devised in a manner that reduces the duplication of effort, pools resources and ensures that projects work towards the achievement of mutual strategic goals. ASPI and CSIS will work with dialogue partners to identify priority areas of focus for cybersecurity capacity-building, either geographical or thematic. Through this consultation and associated research, the cybersecurity capacity-building projects of dialogue stakeholders will be made as efficient as possible, and will better engage private-sector skills and capacity in the process. Increasing communication and transparency among capable governments and companies may help to establish novel partnerships that will benefit the region.

Second, a bilateral public–private cybersecurity incident response exercise would elevate cross-sectoral cooperation and improve cyber resilience in both countries. Exercises that test national responses to cybersecurity incidents are valuable ways to evaluate cyber incident and crisis response capacity. Such simulations challenge the ability of states and organisations to identify the issue, contain the effects and recover from the consequences as quickly and efficiently as possible. They are useful tools for revealing the strengths of current policy frameworks and highlighting areas of weakness that need addressing. Importantly, it's not only governments that must prepare for such incidents. Private-sector organisations, as the heartbeat of national economies, are also significant targets and accordingly must prepare themselves by improving their resilience through such exercises.

ASPI and CSIS will connect interested private sector and government dialogue partners and offer consultative support to the design of an exercise that's relevant and realistic and meets corporate, agency and national-level exercise goals. Best practice and big mistakes identified during the simulation will help to inform subsequent dialogues and highlight areas for further cooperation and incident response improvement.

Lastly, ASPI and CSIS will develop a research paper that identifies bilateral and regional barriers to digital trade and proposes solutions to overcome them. As technologically advanced countries with active and innovative business sectors, Australia and the US are well placed to take advantage of growing connectivity in the region. Gaining a deeper understanding of the roadblocks and their causes will help both countries capitalise on the significant growth opportunity presented by digital trade. This project will examine aspects of bilateral trade and investment regulations, information transfer restrictions and national policy approaches to digital trade and investment, and identify solutions to establish a deeper complementary economic relationship between the US and Australia. The outcomes of this paper will be a starting block for the next dialogue's agenda and aim to influence the development of policy and regulation in both countries.

Australia and the US possess a wealth of shared values, strategic interests and regional opportunity when it comes to deepening their cybersecurity relationship.

Australia and the US possess a wealth of shared values, strategic interests and regional opportunity when it comes to deepening their cybersecurity relationship. Putting the above plan into action will ensure that the next 12 months is full of progress, and that the second Australia–US Cyber Security Dialogue has a solid foundation of cyber partnership and understanding on which to build. Continuing to mature the bilateral cooperation between longstanding partners in this way will advance our mutual strategic interests and provide better security outcomes for Australia, the US and the Asia–Pacific.

NOTES

1 ‘ASPI and CSIS to bring together new Australia–US Cyber Security Dialogue’, ASPI, Canberra, 20 January 2017, online.

2 Simon Kemp, ‘Digital landscape of Southeast Asia in Q4 2015’, *TechInAsia*, 23 November 2015, online.

3 International Monetary Fund, ‘Asia: maintaining robust growth amid heightened uncertainty’, media release, 6 October 2016, online.

4 ‘Fact sheet: President Xi Jinping’s state visit to the United States’, media release, The White House, Washington DC, 25 September 2015, online.

5 Jessica Woodall, *Cyber norms and the Australian private sector*, ASPI, November 2016, online.

6 Leo Lewis, Don Weinland, Michael Peel, ‘Asia hacking: cashing in on cyber crime’, *Financial Times*, online.

7 Department of Homeland Security, *Enhancing cybersecurity collaboration with Australia*, Washington DC, 16 May 2012, online.

8 Financial Services Information Sharing and Analysis Center, online; Cyber Threat Alliance, online.

9 James Manyika, Michael Chui, Diana Farrell, Steve Van Kuiken, Peter Groves, Elizabeth Almasi Doshi, *Open data: unlocking innovation and performance with liquid information*, McKinsey & Company, October 2013, online.

10 Department of the Prime Minister and Cabinet, *Australia’s Cyber Security Strategy: enabling innovation, growth and prosperity*, 2016, online.

11 Office of the US Trade Representative, *The digital 2 dozen*, 2016, online.

12 The White House Office of the Press Secretary, *Presidential Memorandum Regarding Withdrawal of the United States from the Trans-Pacific Partnership Negotiations and Agreement*, 23 January 2017, online.

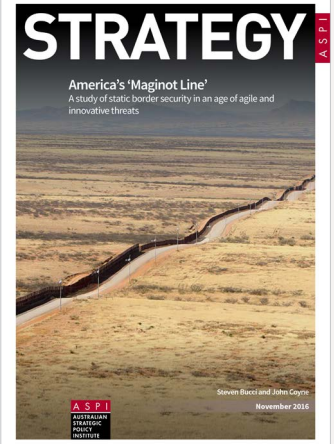
13 European Commission, *The EU–US Privacy Shield*, 24 November 2016, online.

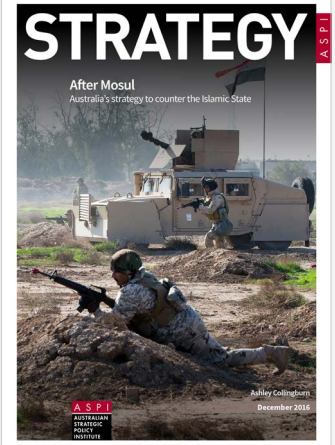
14 Penningtons Manches, ‘EU–US Privacy Shield update’, *Lexology*, 25 October 2016, online.

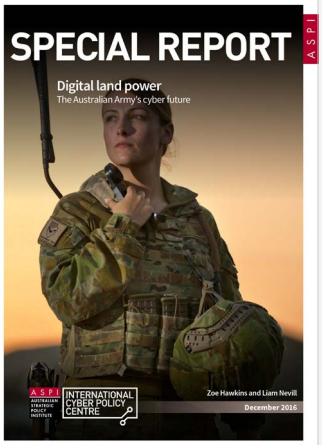
ACRONYMS AND ABBREVIATIONS

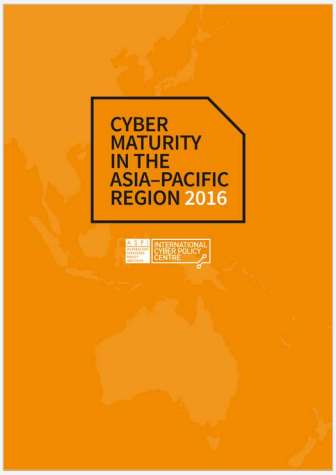
ASEAN	Association of Southeast Asian Nations
ASPI	Australian Strategic Policy Institute
CSIS	Center for Strategic and International Studies
EU	European Union
GDP	gross domestic product
TPP	Trans-Pacific Partnership

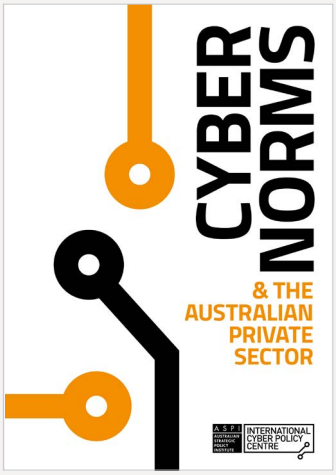
Some previous ASPI publications











The Australia–US Cyber Security Dialogue

ISSN 2200-6648