POLICY BRIEF

CYBER INFORMATION SHARING:

LESSONS FOR AUSTRALIA

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

ABOUT THE AUTHOR

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

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. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI INTERNATIONAL CYBER POLICY CENTRE

The ASPI International Cyber Policy Centre (ICPC) brings together the various Australian Government departments with responsibilities 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. The centre aims to facilitate conversations between government, the private sector and academia across the Asia–Pacific region to increase constructive dialogue on cyber issues and do its part to create a common understanding of the issues and possible solutions in cyberspace.

The ICPC has four key aims:

- Lift the level of Australian and Asia–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 Asia–Pacific region.
- Link different levels of government, business and the public in a sustained dialogue on cybersecurity.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various funders.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE INTERNATIONAL CYBER POLICY CENTRE

CommonwealthBank

THALES

.auDA .au DOMAIN ADMINISTRATION LTD

POLICY BRIEF

CYBER INFORMATION SHARING:

LESSONS FOR AUSTRALIA

LIAM NEVILL

MAY 2017

CONTENTS

INTRODUCTION

Sharing information on the cyber landscape is a necessary and efficient way to benefit from mutual exposure to cyber threats and boost collective defensive capacity. For this reason, effective processes for sharing cyber information among industry sectors, government and academic cybersecurity analysts and researchers are being pursued.

In 2016, Australia's Cyber Security Strategy noted that 'Organisations, public and private, must work together to build a collective understanding of cyber threats.' It went on to say, 'By securely sharing sensitive information and working together—in real time where possible—we can build a stronger collective understanding and ability to analyse and predict cyber threats.'[1] While not explicitly stated in the strategy, this requires a trusted national network to share critical cybersecurity information between the public, private and research sectors.

The US has been pursuing cyber information sharing since the late 1990s, when the federal government directed the creation of public–private partnerships for critical infrastructure protection.[2] The now decades-long development of a variety of information sharing models in the US, and the greater complexity of its industrial and commercial sectors, provide a healthy catalogue of case studies and lessons for the Australian cybersecurity community as it pursues deeper information sharing mechanisms.

This paper draws on the examples, issues and recommendations discussed in the MITRE Corporation report *Building a national cyber information sharing ecosystem*, by Bruce J Bakis and Edward D Wang. Informed by those insights, this paper offers recommendations for the development of Australia's national cyber information sharing system.

1 Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy: enabling innovation, growth & prosperity*, Australian Government, Canberra, April 2016, online, 30.

2 Bruce J Bakis, Edward D Wang, *Building a national cyber information sharing ecosystem*, MITRE Corporation, May 2017, 7.

THE US EXPERIENCE: RECOMMENDATIONS AND GUIDELINES

The US has been pursuing sectoral and public–private cyber information sharing organisations since the late 1990s. As a result, the US has a more diverse ecosystem of cyber information sharing organisations that have been operating for several years with different levels of success. The MITRE Corporation has recently completed a review of several case studies in the US to identify recommendations for the establishment of a national unclassified cyber information sharing network.

The conclusions of this research are equally applicable to Australia, and the opportunity to learn from the successes and mistakes of a more mature system shouldn't be overlooked.

MITRE has identified nine questions, dubbed the 'Gnarly 9', that express the key challenges in building and operating a cyber information sharing organisation (see box).[3] These nine points should be considered carefully by Australia for each part of a national cyber information sharing network as efforts to establish a national system build steam.

The Gnarly 9

1. What is the essence of the consortium?

Identify the consortium's short-term, mid-term and long-term missions.

2. What are the implementation milestones?

Develop a high-level plan (strategy and roadmap) that matches up with the missions and that includes specific milestones at each phase.

3. What information will be shared by members, and how will it be shared?

Determine what information will be shared by whom, for whom, and for what purposes. Other considerations include defining the appropriate level of sensitivity, whether the information will be attributed or anonymous, and whether it will be used for tactical defence or strategic decision-making.

3 Bruce Bakis, 'The gnarly nine: how to make sure your ISAO is a success', MITRE, 20 April 2016, online.

4. What is the consortium's value proposition?

Establish a value proposition that sets the consortium apart to encourage potential members to commit resources, time and effort. Determine what services the consortium will provide for its members.

5. What are the membership criteria and composition?

Decide whether membership will be based on location, sector, event, or type of threat. For example, will it be capped or unlimited? Is there a vetting process for membership? What are the roles of law enforcement and the government?

6. How can members trust the consortium to safeguard their sensitive information?

Look for a trusted, independent third party to manage operations. Determine the appropriate controls. Create platforms and mechanisms for building trust among members, such as institutional and individual non-disclosure agreements.

7. How does the consortium fit into the local, regional and global cyber ecosystems? What are the roles of the government and law enforcement?

Determine who has access and under what circumstances information can be shared or used outside the consortium, and define the consequential obligations.

8. What is the consortium's leadership and governance?

Identify key stakeholders and their roles. Consider the benefits of organising as a non-profit, trusted, independent third-party. Develop a plan for selecting a board of directors, for creating steering and subcommittees, and for staffing.

9. What is the consortium's financial plan?

How you address the other eight questions will drive your financial plan, and your financial plan will affect how you address those questions. Explore seed funding and grants to get started; without it, you must start small, lean heavily on member in-kind contributions, or boost membership fees. Determine the fee structure for founding members and other membership categories, including sponsors.

Source: Adapted from Bruce Bakis, 'The gnarly nine: how to make sure your ISAO is a success', *MITRE*, 20 April 2016, online.

These questions, born out of the American experience, should inform the development of the strategy and roadmap, and the conduct of the pilot phase, of new cyber information sharing organisations in Australia.

This strategy should address information sharing organisations' goals and objectives. The organisations should reach agreement on participation, the organisational structure, membership structure, products and services, operations plans, engagement and marketing plans, and physical and technical infrastructure. This should be underpinned by an implementation roadmap for the establishment of the organisation to guide pre-launch, launch, pilot and transition to full operations.[4]

Regional and sectoral organisations are the building blocks of a larger, national cyber information sharing ecosystem. Currently, the hub of this system in the US, as in Australia, is the federal government. However, MITRE notes that achieving the development of a national cyber information sharing system may require the development of a trusted, independent, third-party clearing house, integrator and analysis centre.[5] Alternatively, a 'federation of federations' model could be adopted, but may be too complex for the Australian ecosystem.[6] Low trust among participants hampers the establishment of cyber information sharing networks, and a trusted intermediary as the hub of a larger national network has the potential to enhance trust among all parties.

4 B Bakis, I Lachow, E Wang, *MITRE cyber information sharing services*, public release 15-1704, July 2015.

5 Bakis & Wang, *Building a national cyber information sharing ecosystem*, 59.

6 MITRE Corporation, *Cyber Information-Sharing Models: An Overview*, October 2012, 4

THE EXISTING AUSTRALIAN CYBER INFORMATION SHARING ECOSYSTEM

Before making plans to widen and deepen Australia's cyber information sharing network, it's important to understand Australia's existing cyber threat information sharing arrangements. The current set-up consists of several government-led initiatives and informal industry-led and sector-based sharing arrangements.

The **Australian Cyber Security Centre (ACSC)** is a fusion of Australian government agencies, co-locating cybersecurity capabilities from Defence, the Attorney-General's Department, the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police and the Australian Criminal Intelligence Commission. When the ACSC was established, it was intended to become a 'hub' for information sharing with the private sector, state and territory governments, academic researchers and international partners. However, as noted in the Cyber Security Strategy, the ACSC's location in ASIO's secured headquarters has made collaboration difficult, and the centre will move to a new location in Canberra later in 2017 to overcome this obstacle.[7]

Joint cyber security centres (JCSCs), initiated by the Cyber Security Strategy, will be established in capital cities to allow greater engagement between the Australian Government, state governments and the private sector. The first centre opened in Brisbane in February 2017, and the government has stated that it plans to have established the Sydney, Melbourne and Perth JCSCs by the end of 2017 and the Adelaide centre by mid-2018.[8] The associated **Online Threat Sharing Portal** proposed in the strategy hasn't yet been delivered.

The Cyber Security Strategy directed **CERT Australia** to increase the scale of its engagement with the private sector, particularly critical infrastructure providers, to provide them with the information necessary to protect themselves. The not-for-profit **AusCERT** continues to provide security information and services to members.

7 S Jeffery, 'Green light for Cyber Security Centre move from ASIO headquarters', *Sydney Morning Herald*, 23 April 2017, online.

8 Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy: 2017 Update*, Australian Government, Canberra, April 2017, online, 15

The **Australian Cybercrime Online Reporting Network (ACORN)** is a national system established under the National Plan to Combat Cybercrime that allows members of the Australian public to report cybercrime and obtain advice on recognising and managing cybercrime. Quarterly statistics on cybercrime are published on its website.[9]

The **Trusted Information Sharing Network (TISN)** for Critical Infrastructure Resilience was created by the Australian Government in 2003. The TISN is separated into several key areas of focus built around 'sector groups'. The groups include banking and finance, health, transport, energy and communications, among others, and focus on promoting mechanisms for information sharing within those sectors on a broad range of issues, not just cybersecurity. The TISN originally included an IT Security Expert Advisory Group (ITSEAG), but the group has not been active since 2011–12.[10]

The government undertook to enhance cross-sectoral information flows, including on cybersecurity, in the 2015 Critical Infrastructure Resilience Strategy.[11] It's unclear how this has been incorporated into the **Critical Infrastructure Centre** within the Attorney-General's Department, announced in early 2017.

ASIO's **Business Liaison Unit** communicates on a broad range of security issues, and it's likely that this includes cyber information where relevant. **Industry Consultation on National Security (ICONS)** is a CEO-level forum chaired by the Attorney-General to share and discuss information on national security with business leaders.

9 ACORN statistical reports: online.

10 Last report released in March 2012: *Risk management for industrial control systems (ICS) and supervisory control systems (SCADA) information for senior executives*, TISN for Critical Infrastructure Resilience, online. There is no mention of ITSEAG in the 2013 TISN report.

11 Attorney-General's Department, *Critical Infrastructure Resilience Strategy: Policy Statement*, Australian Government, May 2015, online, 9

THE FUTURE OF THE AUSTRALIAN CYBER INFORMATION SHARING ECOSYSTEM

As noted above, the Australian Government intends to create a multilayered cyber information sharing network, and the Australian Cyber Security Centre's (ACSC) *2016 Cyber Security Survey* noted that ACSC agencies, led by CERT Australia, are increasing their information sharing capabilities. However, despite the ACSC's conviction that sharing cybersecurity information increases the cost in time and money for malicious cyber actors, and limits their effectiveness, the Survey's results show that information, intelligence sharing and collaboration was viewed by respondents as the least important factor in mitigating cyber risks.[12] The Survey went on to say 'Sharing sensitive information requires an existing relationship and degree of trust', making it vital to build partnerships before an incident occurs. The Survey's poor results for perception of the value of information sharing indicate that the foundations of trusted information sharing networks in Australia remains weak.

As Australia embarks on a process to develop a deeper and wider national cyber information sharing network, careful consideration of the lessons learned by the US and other international partners is necessary to ensure early success and long-term sustainability.

The ultimate shape of the Australian cyber information sharing system will be differentiated from that of the US system by Australia's own unique requirements and size. The current JCSC approach is focused on cross-sectoral organisations in state capitals, which will become the 'vital growth engine of an ecosystem'.[13] This suggests that the Australian cyber information sharing network will evolve into a hub-and-spokes model. The nature of the 'hub' will therefore be critical to the success of the overall network.

As the cross-sectoral JCSC system is established, a parallel development of a formal network of sectoral organisations should also be considered. The physical nature of the JCSC system means that a virtual platform for sectoral organisations would probably be more cost- and time-effective, drawing on JCSC infrastructure and resources where necessary. Alternatively, the JCSCs may evolve to have a sectoral specialisation based on their geographical location (for example, Sydney, Melbourne, or both, for the financial sector, Perth for the resources sector and Adelaide for the defence industry sector).

Regardless of the nature of the national network, it will be necessary to carefully ensure diversity among participating members so that information sharing delivers robust value.

12 Australian Cyber Security Centre, *2016 Cyber Security Survey*, Australian Government, Canberra, April 2017, online, 26-27

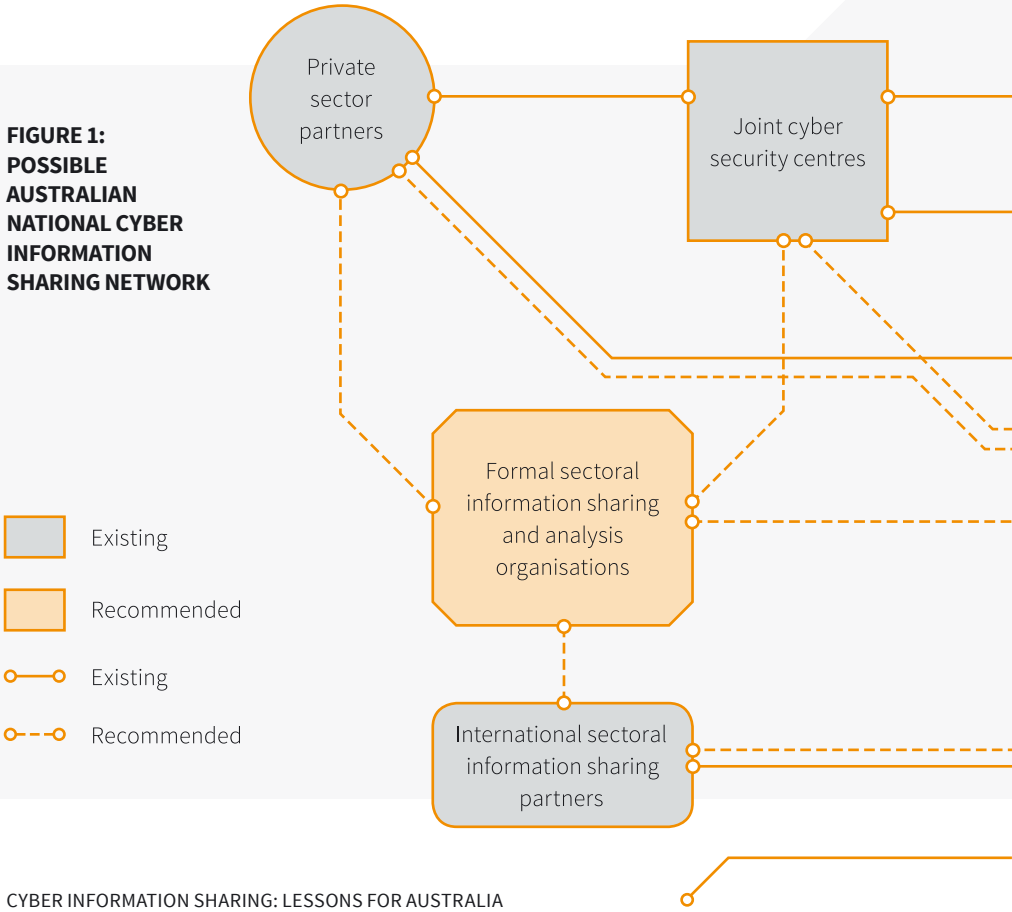
13 Bakis & Wang, *Building a national cyber information sharing ecosystem*, 75.

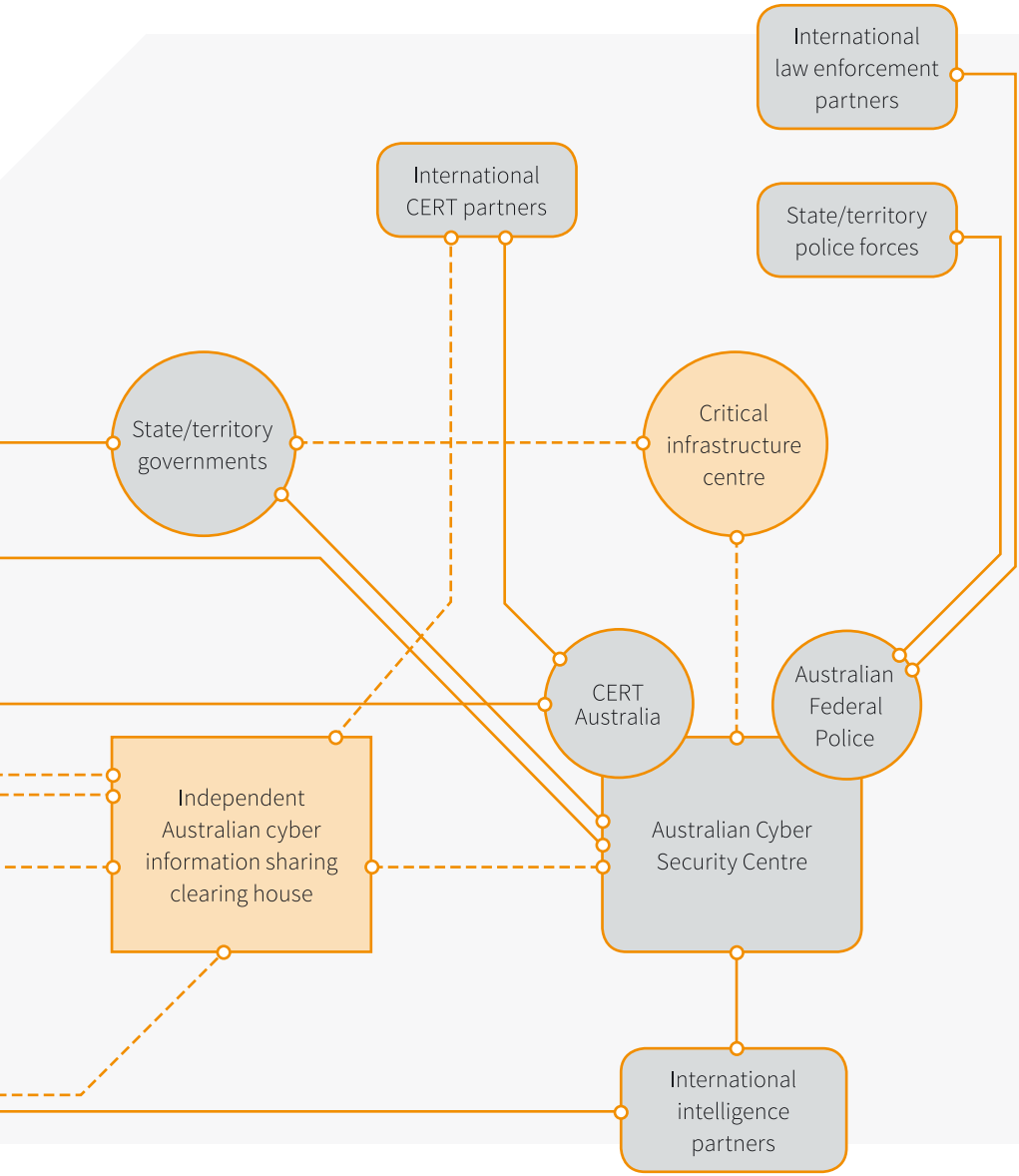
Concerns about the capacity of partners to handle information securely, and resentment towards those who take more than they give, need to be managed to preserve the value proposition of cyber information sharing.

Figure 1 shows a possible model for an Australian national cyber information sharing network. This model would meet the Australian Cyber Security Strategy's call for a multilayered public–private information sharing network, building comprehensive sharing of information between partners.

Following the recommendations of MITRE, this information could be provided to an independent clearing house that integrates and analyses multiple information feeds, making it easier to ensure that information is appropriately managed and ensuring a level of anonymity for information providers. This is needed to build the trust necessary for participant buy-in and sustained information sharing. This model builds on the existing information sharing organisations, but significant investment in automated, secure, standards-based information sharing will be necessary in order to successfully provide actionable information in real time.

FIGURE 1: POSSIBLE AUSTRALIAN NATIONAL CYBER INFORMATION SHARING NETWORK




International law enforcement partners
International CERT partners
State/territory police forces
State/territory governments
Critical infrastructure centre
CERT Australia
Australian Federal Police
Independent Australian cyber information sharing clearing house
Australian Cyber Security Centre
International intelligence partners

RECOMMENDATIONS

A national cyber information sharing network will be an important mechanism to enable the achievement of stronger national cyber defences and resilient networks. The development of this network will be an evolutionary process, but Australia should take heed of the lessons learned by partners in the US and elsewhere.

Therefore, Australian governments at the federal, state and local levels, and private sector and academic partners, should take the following actions to achieve a multilayered, national cyber information sharing network.

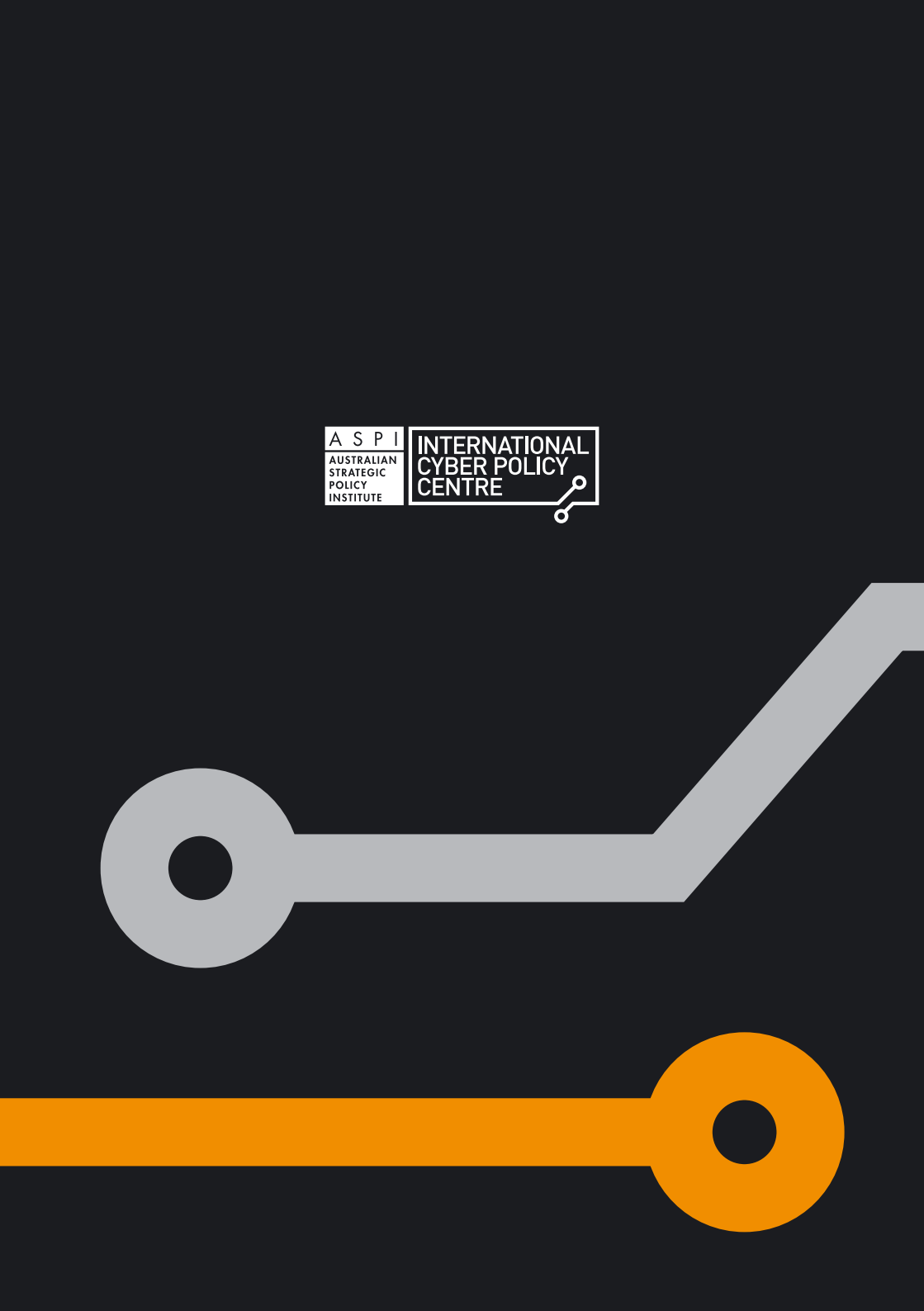
1. Develop a collaborative strategic plan and roadmap for the national ecosystem overall, and tailored plans for each JCSC and sectoral information sharing organisations to meet their specific needs and environment.
    - The national information sharing network is complex, so staging development is necessary to ensure that it's built sustainably. Pilot programs will be critical to evolving organisations 'on the go' to meet the urgent need for stronger information sharing networks.
2. Focus on building a trusted network.
    - Consider the establishment of a not-for-profit, trusted and independent third-party cyber information clearing house to be the hub of the national network. This encourages trust and reduces government dominance of the network, facilitating multistakeholder buy-in and cooperation.
3. Government should participate fully in a national system, but not seek overall leadership. Rather, it should provide necessary seed funding and policy and regulatory changes to support private-sector engagement.
    - Prioritise private-sector leadership of the JCSCs and sectoral organisations to ensure that they are an active and vital part of a national information sharing system.
    - This will help generate a stronger sense of private-sector ownership and commitment.
4. The national information sharing network needs to adapt to threats and share information that is actionable by all parties. Government should continue to optimise its processes to ensure that classified, high-value and actionable information is efficiently fed into the national unclassified sharing network.
    - Automated, secure, standards-based sharing will be critical to achieving this objective.
5. Have a realistic financial plan for each JCSC and sectoral organisation.
    - Start-up costs are likely to be too high to be covered by membership fees alone.

ACRONYMS AND ABBREVIATIONS

ACORN	Australian Cybercrime Online Reporting Network
ACSC	Australian Cyber Security Centre
ASIO	Australian Security Intelligence Organisation
ICONS	Industry Consultation on National Security
ITSEAG	IT Security Expert Advisory Group
JCSCs	joint cyber security centres
TISN	Trusted Information Sharing Network

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.aspistrategist.org.au
facebook.com/ASPI.com
@ASPI_ICPC
https://www.aspi.org.au/icpc/home


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