RAND CORPORATION

Australian National University

NATIONAL SECURITY COLLEGE

Exploring Cyber Security Policy Options in Australia

Igor Mikolic-Torreira, Don Snyder, Michelle Price, David Shlapak, Sina Beaghley, Megan Bishop, Sarah Harting, Jenny Oberholtzer, Stacie Pettyjohn, Cortney Weinbaum, and Emma Westerman

Key findings

- An interdisciplinary exercise generated three overarching policy recommendations to improve cyber security in Australia: Create and enforce technology security standards, craft international agreements to address cyber security challenges, and improve risk awareness to keep users safe online.
- There was broad consensus that the policy domain will continue to struggle to keep pace with technological change. Therefore, ideas and solutions deemed most desirable allowed innovation to flourish while setting standards for security and creating mechanisms for responding to attacks.
- Debate among exercise participants indicated an underlying tension between risk-based approaches and compliance-based interventions to improve cyber security.
- The solutions identified are not immediately executable. Future exercises could consider their secondary and tertiary effects, and this type of analysis is essential before solutions can be implemented.
- Future exercises could consider how policy development, including the Australian Government's next Cyber Security Strategy, should challenge assumptions about government roles, responsibilities, and authorities and incentivise a broader range of government and non-governmental stakeholders to participate in building and implementing cyber security solutions.

SUMMARY ■ In December 2016, RAND and the National Security College at The Australian National University partnered to facilitate a cyber security–focused 360º Discovery Exercise in Canberra.

The exercise used plausible scenarios to explore the challenges Australia faces in securing cyberspace by placing pressure on government authorities, industry capabilities, users' tolerance for malicious cyber activity, and the ability to develop interdisciplinary solutions to pressing cyber security challenges. The scenarios considered the security of the Internet of Things and intellectual property theft against a backdrop of evolving international norms of behaviour in cyberspace.

This was the third in a series of cyber security exercises developed by RAND. The two prior exercises were conducted in the United States—in Washington, D.C., and at the University of California, Berkeley, near Silicon Valley.[1] Like these prior events, the Australian exercise provided a rich set of observations and options to strengthen cyber security and enforcement while protecting the benefits afforded by a free and open Internet. However, the solutions proposed by exercise participants and discussed in this report need further development. For example, the solutions do not yet assign clear roles and responsibilities, may require new authorities for government agencies, and have not been subject to a detailed analysis of their effects and challenges to implementation.

Participants represented the public and private sectors, academia and think tanks, industry associations, and the media. The exercise was conducted under the Chatham House Rule, allowing us to quote participants without attributing quotes to individuals or their organisations.

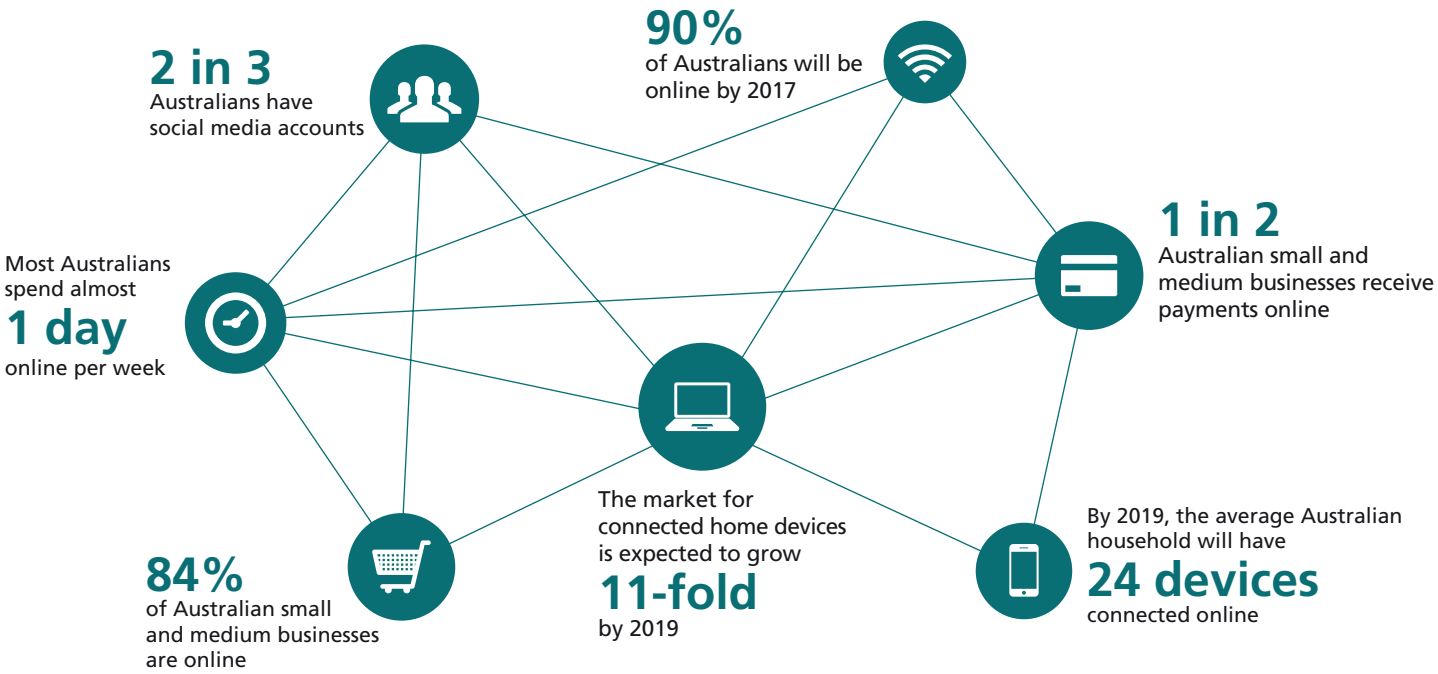
The exercise provided specific insights for Australian cyber security policy—specifically, how to build on Australia's

Australia's Cyber Security Strategy was designed to address cyber threats affecting national security, including criminal activity, espionage, sabotage, and unfair economic competition.

current Cyber Security Strategy released by Prime Minister Malcolm Turnbull in April 2016. The strategy was designed to address cyber threats affecting national security, including criminal activity, espionage, sabotage, and unfair economic competition. It calls for Australia to work with allies to promote international norms of behaviour consistent with a free, open, and secure Internet and to foster public-private partnerships. Figure 1 shows how the Cyber Security Strategy presents the current state of cyber connectedness and reliance in Australia. The strategy also issued a call to action for developing and strengthening partnerships and cyber defences, asserting Australia's position as a champion for responsible activity in cyberspace, promoting growth and innovation, and building the country's cyber expertise.

In his opening remarks at the exercise, the Hon. Dan Tehan, MP, Minister Assisting the Prime Minister for Cyber Security, stated that malicious cyber activity costs Australia's economy AU$1 billion per year, with additional non-financial costs associated with active cyber espionage against the Australian Government and economy. He challenged exercise participants to think not in terms of a whole-of-government approach but a much wider whole-of-community approach.

Figure 1. Australians are becoming increasingly connected online



SOURCE: Commonwealth of Australia, Department of the Prime Minister and Cabinet, A*ustralia's Cyber Security Strategy*, Canberra, 2016, p. 14, https://cybersecuritystrategy.dpmc.gov.au (CC BY 4.0).

INSIGHTS FROM THE EXERCISE

Participants from outside the Australian Government expressed a general desire for the government to take responsibility for the challenges of cyber security on behalf of users and industry. Questions of whether the government could actually carry out these responsibilities effectively and what the unintended consequences might be were generally not discussed.

The scenarios presented during the exercise involved existing technologies, but participants were unable to identify a single solution—a silver bullet—to resolve all the challenges presented. While this result is not surprising to those who work in the security domain, it made participants realise that multiple solutions would be needed, and that those solutions would involve multiple stakeholders and connections between them that do not currently exist.

Of the solutions that were proposed during the exercise, all required multipronged approaches with participation from across sectors and could not be achieved through government action alone. Exercise participants believed that the policy domain would continue to struggle to keep pace with technological change, despite an increasing focus on cyber security across the Australian economy and society as a whole. Future exercises could consider how to reduce this lag.

Some proposed solutions required coordination across multiple sectors or among multiple participants in one sector; many of these partnerships do not exist but could be developed. The exercise highlighted the importance of continuous interplay between policy-oriented people (in the public and private sectors) and technologists. Future exercises could focus on these aspects as key objectives in the exercise scenarios.

Distinguishing this exercise from the two previous events conducted in the United States was a sense that Australia is heavily reliant on other countries for its economic vitality and, to some extent, its national security. Participants discussed this contrast, emphasising the Australian economy's higher degree of dependence on trade with Pacific and Southeast Asian partner nations to meet demand domestically. Particularly relevant to the exercise is that Australia depends on imported goods to support its technology infrastructure. Participants also noted that the nation's defences require international alliances and an ability to work effectively with partners, perhaps more so than is required in the U.S. defence sector. As a result, participants hesitated to recommend actions that might lead to a direct confrontation with an important economic partner. This perspective influenced the types of solutions that participants did and did not find appealing during the exercise.

In scenarios involving state-sponsored cyber events or individuals launching attacks from other jurisdictions, participants favored solutions that prioritised benefits for Australia over solutions that punished the actors and could lead to an international confrontation. In general, participants were wary of actions that might prompt sophisticated malicious cyber activity or spark a trade war in the region.

Multiple participant breakout groups suggested that raising awareness of the risks of lax cyber practices would be key to ensuring that cyber security is a whole-of-nation priority, and they suggested imposing cyber security standards on connected devices sold in Australia. There was a sense throughout discussions that uninformed or lax security decisions could harm the entire society. One participant made a comparison to vaccines, noting that people can opt out to a point, but such choices eventually affect other people's safety.

The groups also compared the concept of cyber security standards to how the Australian Government regulates children's toys: It requires importers and manufacturers to meet minimum safety standards before a toy may be sold in Australia and issues penalties for noncompliance. Participants suggested similar government standards to establish a baseline for the security of technologies. In addition to pass-fail standards, they recommended certifications paired with a method to help consumers understand the security level of a given device and compare the security certification of various devices, thus informing purchasing decisions.

> Cyber security is like vaccines: You can opt out to a point, but eventually you jeopardise other people's safety.
> —Exercise participant

One critical question that this solution raised was whether such standards would be counterproductive or able keep pace as technology evolves. Participants were concerned about the risk of ill-conceived standards or standards that do not adequately take account of the global environment.

There is a need for further discussion to explore whether traditional conceptions of 'standards' befit cyber challenges. Equally, there is a need to navigate the complexities of who would set standards, whether standards might upset market competition, whether they could be written and enacted rapidly enough to keep pace with technology developments, and how to resolve disputes if a certified product or service or its underlying system were subsequently attacked.

On the topic of education, when pressed as to why cyber security education is not already part of Australian school curricula, participants offered few definitive reasons. This suggests a lack of awareness of efforts within Australia's education sector to address this aspect of prevention, as well as a lack of awareness of the education initiatives in Australia's Cyber Security Strategy. Thus, there is an opportunity for political and business leaders to better link their education-related messaging to efforts related to cyber security, e-safety, and science, technology, engineering, and mathematics career development.

OPPORTUNITIES FOR AUSTRALIA

Throughout the exercise, participants raised ideas that deserve further consideration than was possible during a single day of discussions. Several of these topics warrant a more in-depth analysis.

Attribution Challenges of Cyber Attacks

Even if perfect attribution of malicious actors can never be attained, a future exercise could determine what level of confidence in attributing an incident is good enough, as well as how laws, regulations, investigations, and behavioural norms should be designed around such a framework.

In non-cyber criminal investigations, perfect attribution is never the minimum requirement. Instead, courts determine whether attribution, or guilt, has been proven. Participants in the exercise asserted that malicious cyber actors should not be held to a higher burden of proof than those accused of other crimes, yet they also acknowledged that attribution is complex in the cyber domain and that the burden of attribution feels greater when there is a potential for war, such as when state-sponsored actors are involved.

International Agreements for Investigation and Prosecution

Participants proposed that Australia enter into international agreements to create avenues for criminal investigations and prosecutions—without limiting the Australian Government's options to provide for its own defence, security, and law enforcement. Participants agreed that the government could be more open about how it contributes to and engages in international agreements to enable other stakeholders in the Australian economy to help shape and support desired outcomes. Representatives from various government agencies, law enforcement agencies, and industry sectors could build on the government's existing approach to design a framework reflecting multi-stakeholder interests for Australia's involvement in future international agreements.

Careful Consideration of Response Options

Retaliation was often perceived as counterproductive to Australia's economic interests, yet participants recognised that some values are worth protecting and defending, even if doing so comes at significant cost. One participant raised the question, 'When do we consider [a cyber attack] an act of war?' Answering that question requires further discussion about how to draw such a line, what options are available before that line is crossed, and what actions Australia would be prepared to take if the line were crossed.

Consumer Protection Protocols

Participants considered the decision to be offline an individual right, yet, increasingly, citizens are unable to opt out of digital connectivity, even for devices that should (by today's conventions) be operable without Internet access. Future exercises could determine whether certain types of devices—such as vehicles or medical devices—should be operable offline (to help protect privacy and manage security risks), as well as how categories of devices and standards should be written and whether users should be allowed to opt out of data sharing. A discussion of the ethics issues surrounding these questions would be

timely, given the developing role of artificial intelligence and machine learning in making devices 'smarter' while collecting even more information about users.

A Quality Assurance System for Connected Devices

One proposed solution was to create a check-mark system for quality assurance of cyber devices that is both visible on device packaging and understandable to consumers. Exercise participants colloquially described this as a 'cyber kangaroo' logo. Local governments, together with industry, have an opportunity to develop a framework for the cyber kangaroo, including the design of the measurement criteria and enforcement and monitoring mechanisms. This group could also consider how to respond the first time a product with the cyber kangaroo logo is hacked and who would be responsible for responding to such an attack.

Building Cyber Security Instruction into School Curricula

Participants felt that school curricula with age-appropriate lessons in cyber security, paired with increased adult awareness and education, is urgently needed, along with a dramatic increase in stakeholder and public communication to raise awareness of privacy rights, the need to protect private data when connected to the Internet, and what various organisations are doing to improve outcomes.

Each of these opportunities fits within the themes of Australia's Cyber Security Strategy. Future study for each of these ideas should address the following questions:

- How would the proposed solution be implemented?
- Who should be responsible, and does that individual or agency have the necessary authority to implement the proposed change?
- Who determines when standards are needed, how standards will be set, and how they will be updated as technologies evolve?
- How should leaders across government, industry, and the research community—in Australia and throughout the region—be prepared to respond when a malicious cyber incident occurs?
- What precedents, analogous examples, and lessons learned could be applied to these topics?

This report provides context for how the solutions were imagined and how they might fit into Australia's cyber environment.

EXERCISE DESIGN

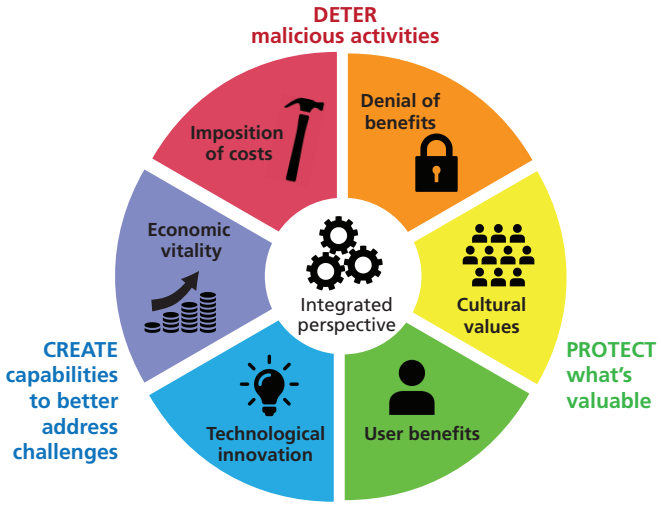
During the one-day exercise, participants were presented with two scenarios set in the year 2022, each crafted to present specific cyber security challenges and stimulate discussion on topics relevant to Australia's Cyber Security Strategy.

During each scenario, all 60 participants were divided into six teams. Two teams were responsible for designing solutions to deter malicious actors from achieving their goals, either by imposing so many costs on the actors that the ends were not worth the means or by denying the benefits of the action, such as removing value from the desired information or access.

Another two teams were responsible for protecting that which is valued by society, to make sure that solutions did not infringe on cultural values or deny legitimate users the benefits of technology.

The final two teams were responsible for maintaining an environment that fostered technological innovation and promoted economic vitality. These six teams and their goals are shown in Figure 2.

Figure 2. Participants were assigned to six themed breakout groups for the scenario discussions



The event began with an Internet of Things (IoT) scenario, after which participants were divided into different groups to address an intellectual property (IP) violation scenario. Both scenarios are described in the following sections. The scenario details were designed to provoke discussion and are not meant to be predictive of specific future events.

Exercise participants represented the public and private sectors, academia and think tanks, industry associations, and the media, as shown in Figure 3. Australian Government participants included officials from national security and non–national security agencies, as well as officials from state and territory governments. There was also participation from two foreign embassies. Private-sector participants included representatives from the software and hardware technology, cyber security, telecommunications, defence, consulting, accounting, and mining industries, as well as industry associations and media outlets. Participants from the research community came from four universities and two think tanks.

Internet of Things Scenario

It is the year 2022, and Internet-connected devices have become integral to all facets of business and society. Wireless cars notify owners when they need maintenance, factory machines detect when supplies need to be reordered and place the orders themselves, and health devices provide doctors and medical practitioners real-time access to patients' vital measurements, insulin levels, and heart rates. Figure 4 shows examples of the types of devices connected to the Internet.

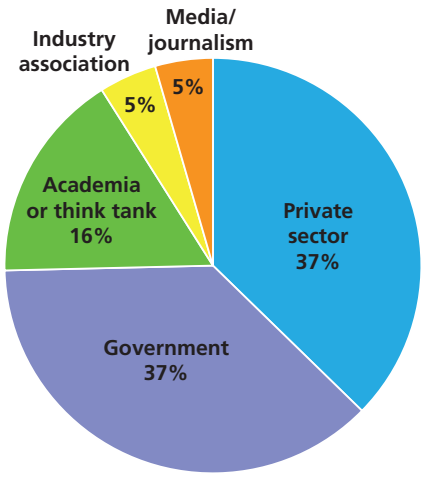
Yet the security of IoT devices is often an afterthought. Security patches are rolled out slowly and do not always reach the devices in circulation. As a result, Australian society suffers as criminals find ways to exploit IoT vulnerabilities.

In the scenario, an entire criminal enterprise evolves around extorting businesses, government agencies, and community organisations by disabling or slowing the IoT-enabled devices that are essential to operations (e.g., factory machinery, restaurant refrigerators) and holding them for ransom. These attacks eventually escalate, affecting implanted medical devices, such as pacemakers, and causing the deaths of 12 elderly Australian patients. Meanwhile, thousands of vulnerable devices remain embedded in Australian citizens who demand government action.

A hack against a driverless automobile goes awry, causing it to veer onto a crowded sidewalk and kill three pedestrians. An investigation identifies a vulnerability common to a majority of driverless cars, leading authorities to ban them from roads until the problem is corrected. Concern about the safety and security of IoT devices has reached the point that citizens are demanding action from the government.

Exercise participants were asked to identify solutions that would create a more secure IoT without negating the benefits these technologies provide society.

Figure 3. Participants represented a range of industries and sectors

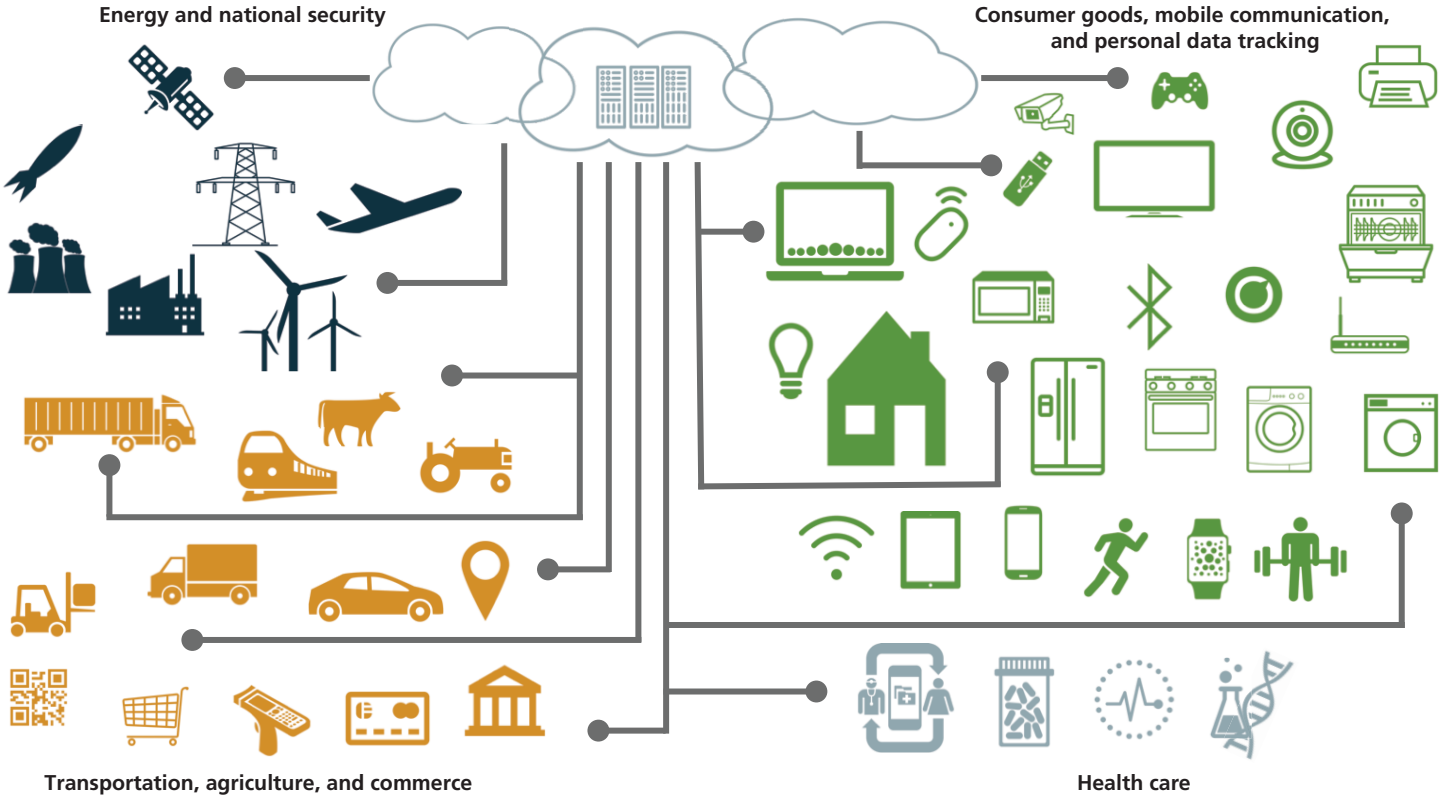


Intellectual Property Scenario

By 2022, Australia has entered bilateral cyber agreements with 13 countries, including South Korea, Vietnam, China, and Indonesia, in addition to its long-standing security relationships with Five Eyes partners: Canada, New Zealand, the United Kingdom, and the United States. These arrangements have resulted in successful investigations and prosecutions of criminal networks targeting Australian citizens' finances and credit cards.

Mining and resources remains a key sector of the Australian economy. Over the previous two years, a large Australian mining company lost one bid after another for major contracts to other international bidders. The firm was recently forced into bankruptcy, and its assets were purchased by competitors. One such acquirer has begun merging information technology systems when it finds evidence of extensive network intrusions on the company's computer systems. The intruders had full access

Figure 4. The global economic value of the IoT is estimated at AU$2.7 trillion



to the mining company's internal systems, including contract data, bidding histories, and all corporate communications.

Meanwhile, an Australian green energy innovator reveals that the design for its next-generation solar panel, reputed to be the most advanced panel in the world, has been stolen. The firm has state-of-the-art cyber defences and has tracked the theft to a foreign government's military cyber unit.

With the future of two Australian sectors in jeopardy, insurance companies are unable—or claim they are not obligated—to pay the costs of the breaches, and company executives and investors demand action by the Australian Government.

Exercise participants must devise solutions that protect the future viability of Australia's economy while protecting the IP that allows companies to thrive.

After being presented with each of these scenarios, participants were divided into the six groups shown in Figure 2, each diverse in terms of members' organisational affiliations.

DETER MALICIOUS ACTIVITY

Two groups of participants worked independently from each other to deter malicious actors—state and nonstate. One team's goal was to impose costs on malicious actors to disincentivise attacks. Such costs could include harm to reputation, loss of freedom, or any other cost the team could conceive. The second team was responsible for denying actors the benefits of their actions, perhaps by preventing them from succeeding or reducing the value of their gain such that the ends were not worth the means.

Four groups of participants in total addressed these topics: two teams in the IoT scenario and another two teams in the IP scenario. This same approach was repeated for each of the topics shown in Figure 2 (cultural values, user benefits, technological innovation, and economic vitality).

Across all groups working in this topic area, none gave serious consideration to legalising 'hacking back' in the aftermath of a malicious cyber incident—or hacking the suspected perpetrator in an effort to prevent similar attacks, recover or delete

> If perfect attribution can never be attained, then what level of confidence is good enough, and how should laws, regulations, and international norms be designed around such a standard? —Exercise participant

stolen IP, or expose the perpetrator's identity. Hacking back is currently illegal in Australia (and in the United States), and no team suggested changing the law. Instead, discussion focused on whether hacking back actually protects anyone or is simply a form of retaliation.

Report, Investigate, and Prosecute

A participant in the exercise noted that if criminals physically broke into an organisation, the owners would not hesitate to report the crime to law enforcement, yet cyber crime seems to be different. The participant added that refusing to report a serious crime is, itself, a crime, but corporate attorneys regularly advise their clients to do just that when it comes to cyber breaches and compromises, especially when corporate or customer data are involved.

No team recommended punishing Australian organisations that refuse to report crimes, which itself was noteworthy. However, participants wanted to see a much higher rate of prosecution for cyber criminals, including as a means to deter malicious activity. One team suggested implementing an anonymous reporting mechanism, whereby organisations can anonymously report cyber incidents to the government without facing financial repercussions from shareholders and consumers' loss of trust. (The team did not explore the question of what level of government would be responsible for taking these reports.) The same team also asked how Australia could respond to a failure of duty of care from a manufacturer without stifling innovation.

This desire to regulate manufacturers without stifling innovation led to ideas focused on the suppliers who make devices available to Australian consumers. Although manufacturers may be overseas, suppliers are likely to be local and can therefore be held responsible for the security of the technologies they sell in Australia. As previously mentioned, participants compared this solution to how children's toys are regulated in Australia: The federal government sets safety standards for toys, and importers and suppliers are held accountable for adhering to them.

A significant challenge raised in all discussions about prosecution was the need for better attribution of malicious actors. Yet participants remained sceptical that perfect attribution would ever be attainable, and they questioned whether the challenges of attribution would get better or worse over time. A senior government official in the room asked, 'In six years, how will we be doing with attribution: better or worse?' This was followed by a long pause.

As a result of this concern, participants rejected many law enforcement approaches as not possible without attribution sufficient for a court of law, not useful when criminals live in countries without extradition agreements with Australia, or irrelevant if these cases still remained too difficult to prosecute for other reasons. Debate ended with a participant asking the question, 'If perfect attribution can never be attained, then what level of confidence is good enough, and how should laws, regulations, and international norms be designed around such a standard?'

Some participants suggested a 'name and shame' approach, naming the attackers to publicly shame them as retribution when prosecution is not possible. However, other participants did not think this approach would be effective or politically palatable when used against attackers overseas.

Create New International Relationships

Participants wanted the Australian Government to create new international relationships to combat cybercrime across international borders. They acknowledged the strength of Australia's existing Five Eyes relationships while advocating extending and developing relationships in the Asia-Pacific region.

Despite discussion of civil and criminal legal options to pursue individual and state-sponsored attackers, participants expressed concern about other countries trying to impose the same penalties on the Australian Government and private sector. For these reasons, participants wanted government to establish new international agreements with avenues for criminal investigations and prosecutions, without limiting the country's options to provide for its own defence, security, and cyber investigations. Participants believed that these agreements would allow Australia to protect its own interests without risking disproportionate retaliation. Future discussions with government and industry stakeholders could shape the terms of such agreements and identify priority countries for negotiation.

PROTECT WHAT'S VALUABLE

Another two teams were responsible for identifying and protecting Australia's essential cultural values and protecting the benefits users receive from cyber technologies. For example, a solution that denies Australians access to the Internet—providing maximum security with no benefits to users—would have been unacceptable. Participants highlighted egalitarianism as a core value among Australians and a practical concern for policy development. They quickly identified that cyber security protections are nearly entirely the discretion of manufacturers and service providers, who may not always have end users' best interests at heart.

One group presented this challenge as a three-pronged problem: Security is not designed into products, consumers are insufficiently informed about security, and there are incentives for malicious actors to exploit security vulnerabilities.

At one point, a participant described security as a feature the marketplace will regulate: People will buy the devices that are more secure. Other participants pointed out that this is not happening now: Consumers are buying products because of features, not security, so manufacturers, importers, and retailers are not incentivised to build and sell more secure devices. Nor do manufacturers generally pay a significant price when security flaws are exploited.

Protect National Interests

A consistent theme throughout the exercise was the desire for government to protect the industries and organisations that provide jobs to maintain a thriving economy. Therefore, participants found any suggestions that could result in international retaliation or a refusal by international markets to do business in Australia to be undesirable or a clear nonstarter.

Yet, there was also a question of when an actor has gone too far. The question was not answered, but it prompted the realisation that some values are worth protecting and defending at significant cost. However, participants declined to identify this threshold.

Celebrate Corporate Solutions

A few times during the event, participants returned to the idea of rating and ranking the cyber security of organisations and products—and celebrating the most secure and innovative. This was seen as a solution that could incentivise good corporate governance and leadership and create an incentive for more secure products.

Participants suggested providing users the option to register their new devices with the manufacturer, which could activate insurance coverage for the device and allow manufacturers to push software and security updates and issue product recalls more easily.

However, accompanying this discussion was an acknowledgement that not all devices are created equal: A pedometer is not a car, and different devices have different limitations for encryption and software standards. The requirement must fit the device. The discussion did not venture beyond products to explore the role of security in the various services that citizens depend on; payment processing and other data-dependent services are equally vulnerable to cyber attack and worthy of further analysis.

> Users are the ones who lose out when there's a problem. Security can't be an afterthought.
> —Exercise participant

Secure Individual Rights

'Where do we sit in the balance between freedom and security?' asked a senior exercise official. Participants replied that the Australian public would certainly be outraged by a major IP theft, but, without an immediate threat, they saw little justification for an invasion of privacy that may come with increased security.

Participants raised the topic of individual rights in a discussion of the choice to be 'offline.' Participants felt that users should be able to opt out of digital connectedness, but they acknowledged the challenge of doing so today, let alone in 2022. They cited online banking as an example in that consumers can choose not to bank online, but their financial information is still accessible via the Internet and stored in networked databases, regardless of their personal choice. The assumption was that in five years there would be even fewer opportunities for citizens to live offline.

In the U.S. exercises—particularly in the Silicon Valley exercise—this topic led to a discussion about informed consent: How should consumers be informed about the technologies they are buying and how their personal data will be used. While Australian exercise participants did not use the phrase *informed consent*, they did raise the concept in discussions of user-controlled connectivity.

Unplug Yourself

Participants wanted devices to be able to disconnect from the Internet and still perform their primary function, when that primary function is not connectedness. Participants cited entire classes of devices that have been made 'smart,' sometimes with questionable value to the user. They raised the example of a tractor with built-in sensors to measure soil salinity, moisture, and crop yields. It is not unusual for end-user agreements to specify that the manufacturer owns the data collected, and the manufacturer could sell these data to third and fourth parties for purposes that do not benefit the tractor's owner. Participants wanted users to have the choice to opt out of such data sharing.

Even more concerning to participants was the risk to the farmer, whose tractor could be hacked and, possibly, held for ransom during a harvest.

Participants cited entire classes of devices that have been made 'smart,' sometimes with questionable value to the user.

CREATE CAPABILITIES TO BETTER ADDRESS CHALLENGES

The final two teams were responsible for maintaining an environment that fostered technological innovation and maintained the long-term economic vitality of Australia.

Australia as an Enabler

In the United States, discussions about economic vitality were highly focused on protecting the domestic technology sector. However, Australia imports much of its technology, so the focus for participants in this exercise was ensuring the availability of jobs for Australians. The result was a reluctance to impose excessive regulation on technology imports, with the fear that that manufacturers would simply sell their goods elsewhere and Australian consumers would miss out. This would also cost the Australian economy opportunities to evolve and compete in the increasingly technology-driven global economy.

Participants did not want to risk starting a trade war by putting too many requirements on imports or punishing other countries for malicious acts; they felt Australia had too much to lose by doing so.

One solution was the creation of the previously mentioned cyber kangaroo logo, a seal of quality assurance for cyber-connected devices. Participants were enthused about a symbol that consumers could see on products and easily recognise as a stamp of approval. They described the cyber kangaroo as a tool for building trust with consumers, but they also acknowledged the practical and complex challenges of setting standards, determining which organisations would be responsible for

assigning the label to products and ensuring its effectiveness in the marketplace, and planning how to respond the first time an approved product is targeted by malicious cyber actors.

How to Protect IP

While trying to think of novel approaches, some participants suggested that when IP is stolen by a foreign actor, Australia should encourage compromised firms to bring the product to market as quickly as possible, reducing the financial value of the IP to the thief and protecting Australian businesses. But other participants pointed out that foreign companies would likely stop doing business in Australia if they were required to publicly reveal their own IP too, if hacked.

One group suggested the model in Singapore, which requires critical information infrastructure 'owners and operators to take responsibility for securing their systems and networks' and 'facilitate the sharing of cyber security information with and by' the Cyber Security Agency of Singapore.[2]

Participants suggested a tax that pays for research in critical cyber security areas, but they did not want to discourage international investment in the economy with excessive taxes that lead companies to do business elsewhere. They felt strongly that the Australian Government should show strength by responding in some way, especially when another country is involved, but they were unsure about what actions should be taken. Suggestions included sanctions or and publicising the bad behaviour, perhaps to hurt the reputation of the attacker. White- and blacklists were suggested, but participants were not able to sufficiently explore how to implement and manage them in the time available for discussion.

CONCLUSIONS

The participants found that no single solution could solve any of the issues raised in the scenarios. All plausible solutions required multiple actors: government, the private sector, and consumers. Often, as anticipated in Australia's Cyber Security Strategy, these actors would need to coordinate their efforts. However, the exercise revealed areas in which collaboration between sectors occurs solely through informal relationships rather than being mandated through official duties and authorities, clearly defined roles and responsibilities, or formally agreed-upon processes and procedures for handling crisis events.

This introductory exercise provided an opportunity for stakeholders from varying industries and government disciplines to begin identifying challenges to the status quo and propose solutions. Future exercises could develop ideas about how to implement the proposed solutions or how to avoid unintended consequences. The types of consequences that could be explored in future events include the solutions' impact on Australian industries, innovation, trade (imports and exports), procedures for criminal investigations and prosecutions (domestically and across international borders), and Australia's ability to keep multiple options open when responding to national security events.

One key lesson was that finding satisfactory resolution to the scenarios in the exercise is difficult after a crisis has occurred. Proactive measures need to be implemented in advance to avoid attacks or dampen their effects, and such responses require establishing mechanisms to prevent or mitigate a crisis, communication and relationships across sectors that can be leveraged during a crisis, and contingency plans when attacks happen despite all efforts to prevent them. Australia's Cyber Security Strategy acknowledges that more effort is needed in this area.

Exercise participants often suggested creating cyber security standards, such as product safety standards, minimum security requirements for product importers, and mechanisms to measure, modify, and enforce standards. This topic was discussed more frequently than many other solutions and could serve as an initial area for the government to pursue changes. Pursuit of this topic could have the secondary impact of facilitating stronger relationships and lines of communication between government and industry, establishing new government authorities for cyber security, and laying the foundations for future policy advances in law enforcement, diplomacy, and national security.

Discussions about cyber security standards and enforcement included three goals that should be explored collectively to develop cohesive solutions. First, exercise participants believed that standards would need to be more stringent for medical devices, vehicles, and other product groups that could jeopardise public safety. Thresholds could be lower for pedometers, household appliances, and other products that could be hacked but pose a lower risk to user health and safety. Second,

standards would need to differ based on the technical capabilities of the devices. For example, a Bluetooth pedometer should not be held to the same security standard as an autonomous vehicle. And third, government needs the ability to revise cyber security standards as quickly as technologies change so that standards neither lag behind the state of the art or developing threats nor discourage innovation and new developments that would benefit users.

Discussions around achieving all of these policy goals should include identifying mechanisms to foster cooperation between government and other sectors, what buy-in is needed from consumers, and how to educate users about operating safely in cyberspace. The research community should also have a role in supporting the development and implementation of these policies.

Notes

[1] For more information about the two U.S.-based exercises, see Igor Mikolic-Torreira, Ryan Henry, Don Snyder, Sina Beaghley, Stacie L. Pettyjohn, Sarah Harting, Emma Westerman, David A. Shlapak, Megan Bishop, Jenny Oberholtzer, Lauren Skrabala, and Cortney Weinbaum, *A Framework for Exploring Cybersecurity Policy Options*, Santa Monica, Calif.: RAND Corporation, RR-1700-WFHF, 2016, www.rand.org/t/RR1700.

[2] Cyber Security Agency of Singapore, Singapore's Cybersecurity Strategy, 2016, https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy.

Acknowledgements

We are grateful to Rory Medcalf for hosting RAND and this exercise and to the ANU faculty and students who participated as facilitators and rapporteurs, including Roger Bradbury, Rajeev Goré, Matthew Sussex, Adam Henschke, Brett McDonald, James Mortensen, Tom Chen, Ana Stuparu, Wayne McLean, Andrea Soriano, and Bruce Luckham. We also thank Jennifer Moroney and the RAND Australia team for helping to ensure the success of the exercise and for their assistance and guidance with the planning.

Special thanks to the Hon. Dan Tehan, MP, and Gai Brodtmann, MP, for their support for the event. The exercise also benefited from the contributions of Air Chief Marshal Sir Angus Houston AK, AFC (Ret'd), Alastair MacGibbon, and Samantha Yorke, who played the role of senior officials. We also express our appreciation to our reviewers, Michael Sulmeyer and Karl Mueller, as well as to Christopher Mouton, who provided feedback that greatly improved this report. The Australia exercise was sponsored by KPMG, Macquarie Telecom Group, ISACA, Cisco, Omni Executive, CBR Innovation Network, and Stone & Chalk.

Finally, we owe an enormous debt to our participants, who took a full day from their work to share their perspectives and expertise. We hope that they have come away inspired to continue discussing these important issues and navigating the complex challenges of enhancing cyber security.

About This Report

Today's cyber environment presents unlimited opportunities for innovation, interaction, commerce, and creativity, but these benefits bring serious security challenges for governments, private organisations, and individual users. The cyber domain has evolved so swiftly that legal, economic, and societal mechanisms for maintaining security have struggled to keep up. Satisfactory solutions that balance the priorities of stakeholders will require building partnerships among public and private organisations, establishing mechanisms and incentives to foster routine information sharing and collective defence, and educating users about their role in thwarting increasingly sophisticated attacks.

The goal of this project was to develop an initial framework for cyber security that considers the roles of a range of stakeholders and how their concerns relate to each other. In support of this objective, the RAND Corporation developed and conducted a cyber security–focused 360° exercise in Washington, D.C., California's Silicon Valley, and Canberra, Australia, with participants from government agencies, the technology sector, advocacy organisations, and academic institutions. The games' objective was to foster improved understanding of the positions of other cyber security stakeholders and to illuminate areas of agreement and disagreement. The outcomes are intended to support debate and decisionmaking on future cyber security policies and practices.

The exercise in Canberra was developed by the RAND Corporation and planned and facilitated jointly with the National Security College at Australian National University (ANU) and RAND Australia. This research was funded by a grant from the William and Flora Hewlett Foundation as part of its Cyber Initiative, which seeks to address a broad range of topics that affect the security, stability, and resilience of a free and open Internet and connected devices. The research was conducted within the Acquisition and Technology Policy Center of the RAND National Security Research Division (NSRD) and the Science, Technology, and Policy program of RAND Justice, Infrastructure, and Environment (JIE). NSRD conducts research and analysis on defence and national security topics for the U.S. and allied defence, foreign policy, and intelligence communities and foundations and other non-governmental organisations that support defence and national security analysis. JIE is dedicated to improving policy and decision making in a wide range of policy domains, including civil and criminal justice, infrastructure protection, transportation and energy policy, and environmental and natural resource policy.

Questions or comments about this report should be sent to the principal investigator, Igor Mikolic-Torreira (Igor_Mikolic-Torreira@rand.org). For more information on the Acquisition and Technology Policy Center, see www.rand.org/nsrd/ndri/centers/atp or contact the director (contact information is provided on the web page). For more information about RAND Science, Technology, and Policy, see www.rand.org/jie/stp or contact the director at stp@rand.org.

Limited Print and Electronic Distribution Rights

For more information on this publication, visit www.rand.org/t/RR2008.

Australian National University

NATIONAL SECURITY COLLEGE

www.rand.org

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RR-2008-WFHF