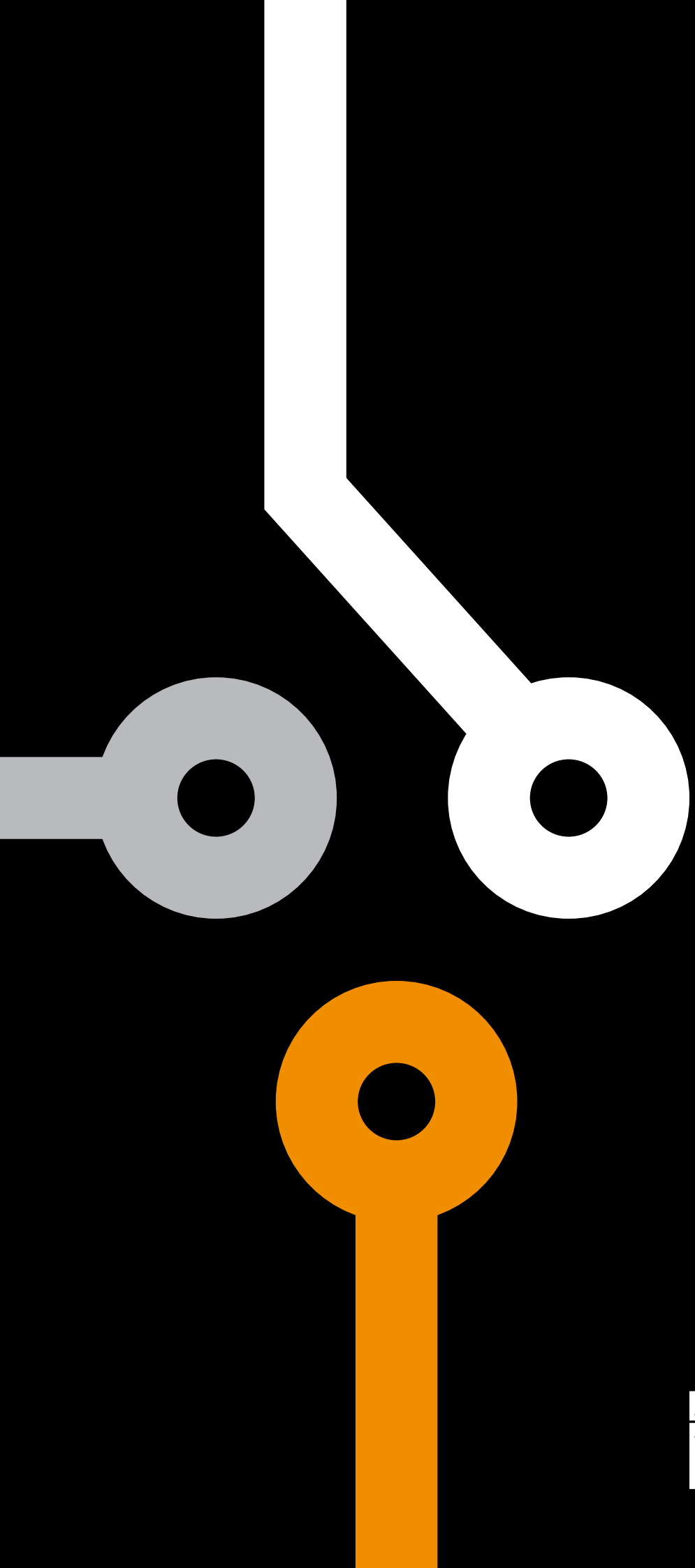
ISSUES PAPER:

THE INTERNET OF INSECURE THINGS



ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

ABOUT THE AUTHORS

Eliza Chapman
Eliza is a research intern at ASPI and the International Cyber Policy Centre, and assisted with research for the 2017 Cyber Maturity Report. Eliza has a Bachelor of Science degree in Biology from Emmanuel College, Georgia, USA and a Graduate Certificate in International Relations from Flinders University, Adelaide. While spending time abroad, she became particularly interested in Australia–US relations and the implications for current and future security arrangements. Eliza will finish her Masters in International Relations next year.

Tom Uren
Tom is a Visiting Fellow in the International Cyber Policy Centre. He has worked in various analytical and operational areas in Defence and has diverse expertise across internet and cyber issues. Tom researches and writes on international and domestic cyber issues. He has a BSc(Hons) in Molecular Biology and previously worked for CSIRO in research on forest tree molecular genetics.

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's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

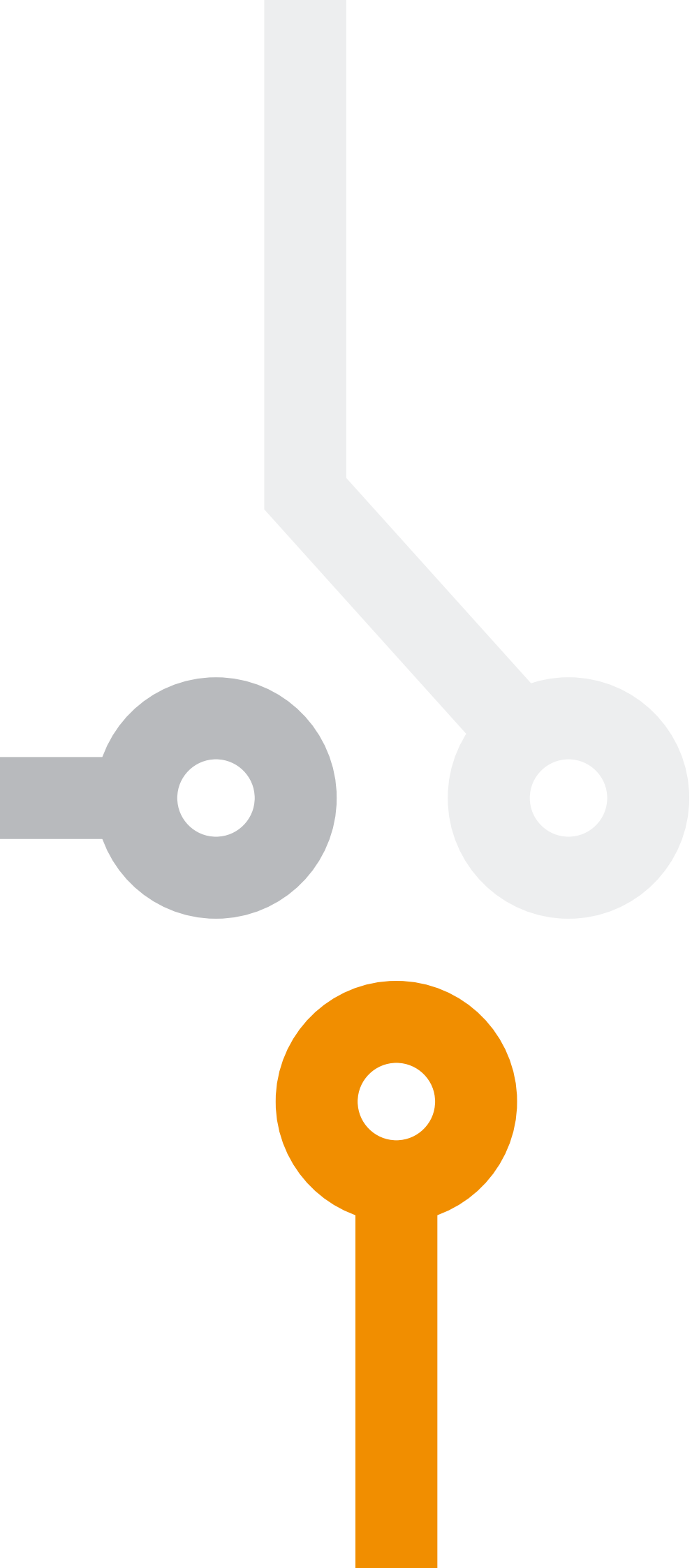
It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia–Pacific.

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 sponsors but special mention in this case should go to JACOBS, which has supported this research.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

JACOBS®



ISSUES PAPER:

THE INTERNET OF INSECURE THINGS

ELIZA CHAPMAN AND
TOM UREN

CONTENTS

INTRODUCTION

The Internet of Things (IoT) is the term used to describe the growing number of devices being connected to the internet. Some of the more common IoT devices include home appliances such as Google Home, wearable devices, security cameras and smart meters. It's been predicted that the number of connected devices was close to 8.4 billion in 2017 and that there will be over 20 billion devices connected by 2020.[1] Even though the IoT has been developing since the rise of the internet in the early 1990s, there's no universally accepted definition. Kevin Ashton, who coined the phrase in 1999, says the IoT is much more than just connected appliances and describes it as a 'ubiquitous sensor network' in which automation leads to innovation.[2] While there are some justifiable cybersecurity concerns about the IoT, there are also many notable advantages to living in a connected world. The IoT is saving lives through advanced healthcare technology, manufacturers are saving time and money through automation and tracking, and a plethora of home devices are adding value to people's lives by providing a range of different services.

There are many different ways to categorise IoT devices, which makes safeguarding the technology challenging. The IoT can be dissected by industry, such as healthcare, transport, manufacturing and consumer electronics. One major subcategory of the IoT has earned its own acronym: the IIoT (industrial internet of things), to which control systems belong. Another way of categorising devices is by looking at their individual capabilities. Devices that can take action pose a different threat from devices that simply collect data to report back to the user.

The IoT offers benefits to all industries, but the connectivity of these once isolated things also introduces new vulnerabilities that can affect our homes and industries. As well as promising convenience and efficiency, the IoT is a problem because a vast number of internet connected devices with poor default security create a large attack surface that bad actors could take advantage of for malicious ends. A variety of international organisations and government groups are working on issues pertaining to the IoT, but at present there's no coordinated vision to implement standards for the IoT on a global scale. Similarly, in Australia, a host of different cyber agencies and industrial groups are working to overcome some of the cybersecurity issues that the IoT presents, but a coordinated strategy detailing how government and industry can collaborate on the IoT is needed.

This issues paper aims to give a broad overview of IoT issues to increase awareness and public discussion on the IoT. In December 2017, ASPI's International Cyber Policy Centre produced a discussion draft asking stakeholders key questions about IoT regulation, governance, market incentives and security standards to help inform this issues paper. We received responses from government, industry representatives, technical experts and academics. While those stakeholders were consulted in the research phase of this paper, the views here are those of the authors.

KEY ISSUES IN IOT

1. THREAT TO CRITICAL INFRASTRUCTURE

In 2016, a severe storm disrupted crucial services in South Australia, resulting in a loss of power for 850,000 customers.[3] Trains and trams stopped working, as did many traffic lights, creating gridlock on flooded roads. The storm, together with the failure of backup processes, resulted in the death of a number of embryos at a fertility clinic in Flinders Hospital.[4] The total cost for South Australian businesses as a result of the blackout was estimated to be $367 million.[5] Some have noted that, due to the interconnectedness of infrastructure, this event mirrored the potential effects of a large-scale cyberattack.[6]

Disrupting utilities that power an entire city could cause more damage than traditional terror tactics and can be done externally and with more anonymity. Again, severe storms demonstrate that a loss of power can cause more deaths than the physical destruction of infrastructure. When Hurricane Irma caused the air conditioning at a Florida nursing home to fail, 12 residents died of suspected heat-related causes.[7]

Digital weapons are being used intentionally by nation-states to inflict physical destruction or compromise essential services. The now infamous attack on Iran's nuclear program, known as Stuxnet, used infected USB drives to contaminate computer systems with malware,[8] which caused physical damage to a number of uranium centrifuges.[9] In 2015, hackers used stolen user credentials to attack a Ukrainian power grid, which resulted in loss of power for more than 230,000 people.[10] In 2016, the attackers used malware specifically designed to attack Ukraine's power grid to disrupt the power supply to Kyiv. This indicates that malicious actors have both the resources and the intent to develop cyberattack capabilities targeted at essential services.[11]

The IoT overlaps with critical infrastructure because many control systems are also now connected to the internet. Kaspersky researchers found more than 3,000 industrial control systems in Australia by using Shodan and Censys IoT search engines.[12] Studies have also revealed vulnerabilities in control systems made by major vendors, such as Schneider Electric and Siemens.[13]

In the discussion version of this paper, several respondents expressed the view that a separate cyber organisation focusing specifically on the security of critical assets and services would be unhelpful. However, many acknowledged a need for greater collaboration between those responsible for protecting these assets to help mitigate IoT-related threats. The Australian Cyber Security Centre (ACSC) could seek to increase coordination between owners and operators of critical assets, helping with the technical aspects of adopting voluntary industry standards for the IoT. The ACSC has the technical expertise to participate in the formation of international standards and could work with policy experts in the Department of Home Affairs to encourage national adoption.

2. THE CYBER LANDSCAPE IN AUSTRALIA

The cyber landscape in Australia is complex. Government cybersecurity responsibilities have recently been reorganised through the establishment of the Department of Home Affairs and structural changes to the Australian Signals Directorate and ACSC. Getting a clear picture of roles and responsibilities was difficult, and it would be beneficial to identify any gaps in roles and responsibilities after these recent organisational changes have been properly implemented. Industry roles could be identified in an IoT road map that helps industry and government bodies work together to more effectively mitigate IoT threats. Consumers should be educated on cybersecurity and responsible ownership of IoT devices, including patching and updating, building on initiatives such as Stay Safe Online.

The IoT has exacerbated an already confronting problem: the lack of skilled cybersecurity professionals both nationally and globally. The Australian Cyber Security Growth Network estimates that a further 11,000 skilled experts will be needed in the next decade.[14] In January 2018, the network announced that cybersecurity qualifications will be offered at TAFE institutions around Australia, which is a significant step forward.[15] However, cybersecurity is a broad domain that requires not only workers with technical skills but also experts in risk management and policymaking, among other areas. Advances in automation and data analytics could help to address the skills shortage, as those technologies will increase the availability of cybersecurity experts, by replacing technical jobs in other areas.

We need to think about IoT security as a holistic system that combines practical skills-based training with industry best practise. The under-representation of women in cybersecurity has been widely noted and overcoming it was listed as a priority in Australia's Cyber Security Strategy.[16] The government has conducted research to better understand the issue and is running workshops to help increase participation.[17]

3. SECURITY RATINGS AND CERTIFICATIONS

A number of countries, including Australia, are considering the value of security ratings for IoT devices. In October 2017, Dan Tehan, the then Minister Assisting the Prime Minister on Cybersecurity, suggested in a media interview that such ratings should be created by the private sector, not by the Australian Government.[18] The UK Government is also exploring 'how to encourage the market by providing security ratings for new products', as outlined in its National Security Strategy.[19] Introducing a product security rating for consumer electronics has the potential to improve awareness of cybersecurity issues and to encourage industry to adhere to minimum security standards. But whether the ratings should be initiated by government or industry is only the beginning of the issue, as there are several problems with cybersecurity ratings that need to be addressed.

First, the vulnerability of an IoT device could potentially vary over its lifetime as weaknesses are discovered and then patched. The energy efficiency of a refrigerator or washing machine, by contrast, is relatively fixed, and so energy-efficiency ratings can be trusted over the device's lifetime. With IoT devices, new vulnerabilities are constantly being exposed. At best, a security rating would reflect the security of a device based on the information available at the time of the security assessment. It would need to be adapted as security standards evolve and new vulnerabilities are discovered.

Second, it's worth investigating whether a cyber rating could lull consumers into a false sense of security by negating their own role in protecting themselves from attack. Before implementing a security rating system, we need to research whether purchasing a device that claims to be secure could make consumers less likely to install updates or change default passwords.

Third, as mentioned in the introduction of this report, there's considerable variation in IoT products. A Jeep Cherokee and a baby monitor (both of which have been compromised) present vastly different dangers, but the compromise of either can have serious consequences. While all IoT devices should include baseline security features in the design phase, devices deemed to be high risk should also require commensurately robust security features. Burdening otherwise cheap, low-risk devices with expensive certifications or strict security regulations, however, could make them commercially unviable in Australia. It's important to recognise that it will be challenging and expensive to come up with a rating that appropriately addresses all the different categories of IoT devices.

In 2018, the IoT Alliance Australia (IoTAA) is prioritising the introduction of an 'IoT product security certification program' as a part of its strategic plan.[20] Exactly what this will look like remains unknown, but it's likely to be performed by accredited independent bodies that evaluate products based on security claims. The Australian Information Industry Association recommends an accreditation scheme that would also certify organisations making IoT devices. The authors' view is that some manufacturers (for example, Samsung) make so many products that this would be ineffective as a stand-alone tactic, but this idea could be used in collaboration with an individual product rating.

4. REGULATION AND STANDARDS

Regulation and standardisation are at the forefront of the IoT debate, and positions tend to be polarised, as reflected in the responses to our discussion draft. The respondents acknowledged that regulation isn't always effective and can impose a significant cost, but some also said that there's potentially room for government to play a more direct role if a device is deemed to provide a critical service to the community. Some industries, such as transport and healthcare, already have safety standards addressing a wide range of security concerns; those standards need to prioritise current and emerging cybersecurity threats.

Multiple IoT-related bills introduced into the US Congress last year exemplified some of the legislative attempts to enforce IoT security by way of law. The Internet of Things (IoT) Cybersecurity Improvement Act of 2017 stresses the importance of built-in security and the provision of security patches,[21] while the Cyber Shield Act of 2017 seeks to introduce a voluntary certification process for IoT devices.[22]

While US lawmakers have proposed some government regulation, some in Australia believe that IoT security would be more effectively regulated by industry. Legislation takes time to introduce and often struggles to keep pace with the quickly evolving technology it seeks to control. Taking a market-driven approach to IoT security may mean that imposed standards will more rapidly adapt to the changing security climate.

Some classes of IoT devices, however, present little threat to their owners, but their poor security allows them to be co-opted in ways that can be used to harm other internet users or internet infrastructure. This is similar to a widget-making factory that causes air pollution; the factory owner and widget buyer both benefit from lower costs of production and neither has a strong incentive to do the work needed to reduce air pollution, as that would raise costs. In economics, this is described as a negative externality, and negative externalities can be effectively dealt with through regulation. The authors' view is that incentives do not exist for effective industry-led standards to develop, especially for consumer IoT devices.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are the two major global providers of standards. The ISO and IEC have a joint technical committee focusing on information technology and a subcommittee focusing on the IoT and related technologies. Australia is a member of the subcommittee through Standards Australia. ISO/IEC also has the 27000 series, which is a series of standards that addresses the security of information security management systems.[23] The European Union Agency for Network and Information Security released baseline security recommendations for the IoT in late 2017.[24] Standards have also been developed in Asia, including a draft policy on the IoT by India[25] and a general framework by Japan.[26] Other organisations working on IoT standards include the IEEE (Institute of Electrical and Electronics Engineers), The Open Group, and SAE International. While a considerable amount of work on IoT standards has been completed, a draft report on the status of global IoT standards by the National Institute of Standards Technology in the US indicates that there's a long way to go. The report reveals several gaps in current standards development and implementation, including network security, IT system security evaluation and system security engineering.[27] It also highlights the variety of SDOs (standards development organisations) working in this space. There's currently a need for international consensus on IoT standards and a clear pathway to implementation.

Locally, the IoTAA has drafted multiple versions of IoT security guidelines to help promote secure designs for manufacturers and to support industry in understanding security and privacy issues. The IoTAA has also outlined key focus areas for 2018 in its Strategic Plan to Strengthen IoT Security. Australia also has iotsec, a non-profit start-up that promotes security in IoT devices to help industry and consumers.

While regulation and standardisation are often thought of in a binary way (enforced by either government or industry), the feedback from the discussion draft highlighted the importance of approaching IoT security in a holistic manner, in which government, industry and consumers all play a role. Furthermore, IoT cybersecurity is a problem of global, not national, proportions. Devices sold in Australia are manufactured all over the world. Being only a small proportion of the IoT market, Australia risks becoming a dead-end market if device makers' security costs outweigh their income from sales. For this reason, any attempt to introduce standards for IoT devices in Australia must be done with a global mindset. The challenge now is to reach international consensus and to encourage manufacturers to adopt the standards. An IoT definition would help to focus global efforts both to secure and to develop the technology and help to articulate its scope.

CONCLUSION

The IoT offers Australia many economic and social advantages and should be embraced and used to benefit all Australians. However, it also introduces new risks and vulnerabilities that our current regulatory systems aren't necessarily mitigating effectively. It's the authors' view that our current policy and regulatory settings are almost certainly suboptimal, but effective management of the IoT from a government policymaking perspective requires many difficult trade-offs, and easy answers aren't immediately apparent. Corruption of traditional ICT devices such as phones and laptops has resulted in the theft of both personal and corporate data. Connecting more devices, such as watches, whitegoods, automobiles and industrial equipment, has intensified this problem and introduced new types of threats. Other incidences of organised crime and terrorism have shown that malicious actors exploit seams in systems, regulation and security. For this reason, it is imperative that we continue to address gaps in these areas to limit opportunities for the exploitation of IoT devices. This paper is intended to illuminate some of the issues involved in managing IoT risk so that industry and government can have a robust discussion and work collaboratively to improve the security of IoT devices.

NOTES

1 Gartner, 'Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016', 2017, *Gartner.com*, online.

2 Rain RFID Alliance, 'RAIN Q&A with Kevin Ashton RFID and the internet of things', 2015, pp. 1–4, online.

3 Australian Energy Market Operator, Black System, 2017, p. 5, online.

4 'SA weather: human error to blame for embryo-destroying hospital blackout during wild storms', ABC News, 23 January 2017, online.

5 Business SA, Blackout Survey Results, 2016, online.

6 Roger Bradbury, 'South Australian power shutdown "just a taste of cyber attack"', The Australian, 2016.

7 '12 of 14 nursing home deaths after Irma ruled homicides', *VOA News*, online.

8 European Union Agency for Network and Information Security, *Stuxnet analysis*, online.

9 Council on Foreign Relations Cyber Operations Tracker, *Stuxnet*, online.

10 Council on Foreign Relations, *Compromise of a power grid in eastern Ukraine*, online.

11 'CRASHOVERRIDE: analysis of the threat to electric grid operations', *Dragos.com*, pp. 10–11, online.

12 Oxana Andreeva, Sergey Gordeychik, Gleb Britsai, Olga Kochetova, Evgeniya Potseluevskaya, Sergey I Sidorov, Alexander A Timorin, *Industrial control systems and their online availability*, p. 8, online.

13 Sagar Samtani, Shuo Yu, Hongyi Zhu, Mark Patton, Hsinchun Chen, *Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques*, University of Arizona, 2016, online.

14 Australian Cyber Security Growth Network, *Cyber security sector competitiveness plan*, 2017, online.

15 Australian Cyber Security Growth Network, *Australian TAFEs join forces to tackle the cyber security skills gap*, 2018, online.

16 Australian Government, *Australia's Cyber Security Strategy*, p. 53, online.

17 Australian Government, *Women in cyber security*, online

18 Denham Sadler, *Security ratings for IoT devices?*, 2017, online.

19 UK Government, *National Cyber Security Strategy 2016–2021*, 2016, pp. 36–37, online.

20 IoT Alliance Australia, 'Strategic plan to strengthen IoT security in Australia', 2017 (unpublished material).

21 Mark Warner, Cory Gardner, *Internet of Things Cybersecurity Improvement Act of 2017*, 2017, online.

22 *Cyber Shield Act of 2017*, 2017, online.

23 ISO, *ISO/IEC 27000 family— Information security management systems*, online.

24 European Union Agency for Network and Information Security, *Baseline security recommendations for IoT*, 2017, online.

25 Department of Electronics and Information Technology, *Draft policy on internet of things*, Indian Government, 2015, online.

26 National Center of Incident Readiness and Strategy for Cybersecurity, *General framework for secure IoT systems*, Japanese Government, 2016, online.

27 National Institute Standards Technology, *Interagency report on status of international cybersecurity standardization for the internet of things (IoT)*, 2018, pp. 54–55, online.

ACRONYMS AND ABBREVIATIONS

ACSC	Australian Cyber Security Centre
IEC	the International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	internet of things
IoTAA	IoT Alliance Australia
ISO	International Organization for Standardization
USB	universal serial bus

Some previous ASPI publications

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC
www.aspi.org.au/icpc/home


ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
INTERNATIONAL
CYBER POLICY
CENTRE