Policy Quick takes

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

Tom Uren

Clean pipes: Should ISPs provide a more secure internet?

Introduction

One of the largest online challenges facing Australia is to provide effective cybersecurity to the majority of internet users who don't have the skills or resources to defend themselves. This paper explores the concept of 'Clean Pipes', which is the idea that internet service providers (ISPs) could provide security services to their customers to deliver a level of default security. The Australian Government looks to be implementing a version of Clean Pipes: on 30 June 2020 the Prime Minister announced a funding commitment to 'prevent malicious cyber activity from ever reaching millions of Australians across the country by blocking known malicious websites and computer viruses at speed'.[1] This paper examines arguments for Clean Pipes and possible implementation roadblocks.

Background

Australia's 2016 Cyber Security Strategy recognised the opportunities and risks that come with cyberspace and committed to 'enabling growth, innovation and prosperity for all Australians through strong cyber security'.[2]

Despite that strategy, however, the online security environment has continued to deteriorate.

There have already been several significant and newsworthy attacks[3] so far this year:

- Toll Group was affected by ransomware in both February and May.[4]
- BlueScope Steel's operations were affected by ransomware in May.[5]
- MyBudget, a money management company, had outages caused by ransomware in May.[6]
- Lion Australia, a beverage giant, was crippled by ransomware in June.[7]

However, most attacks aren't publicly reported, so these incidents are undoubtedly just the tip of the iceberg. A 2018 estimate that included broader direct costs calculated the potential loss to the Australian economy at $29 billion per year.[8]

During the Covid-19 crisis, there's also been significant domestic and international concern about the vulnerability of critical infrastructure such as hospitals and the health sector to cyberattacks. Interpol warned that cybercriminals were targeting critical healthcare institutions with ransomware, and the Cyber Peace Institute issued a call for all governments to 'work together now to stop cyberattacks on the healthcare sector'.[9] This also rose to the highest levels of international diplomacy—the Department of Foreign Affairs and the Australian Cyber Security Centre (ACSC) issued a joint statement on 'unacceptable malicious cyber activity', and US Secretary of State Mike Pompeo warned of consequences for malicious cyber activity affecting hospitals and healthcare systems.[10]

This high-level diplomatic concern emphasises not only that cybersecurity is critically important, but that our current approaches to protecting Australia have failed to adequately protect all of our critical infrastructure.

The problem

Providing resilient cybersecurity isn't an inherently intractable task—for those who have the necessary skills and resources. Individual organisations can and do make significant improvements in their cybersecurity posture when they're motivated to prioritise security and invest the resources required, but when cybersecurity is viewed as an economy-wide challenge, there are significant sectors of the economy that do not, and probably never will, have the ability to successfully defend themselves.

Unfortunately, the motivation, capability and resources to provide robust cybersecurity are not aligned within the Australian internet ecosystem. Currently, too few businesses in Australia are motivated and capable of providing for their own security. These are businesses that understand the risk to their operations that arise from failing to address security. Their business model demands that this risk be addressed, and, accordingly, they'll pay to mitigate it. Some parts of the Australian business community *could* provide for their own cybersecurity but don't give the task sufficient priority. Government should employ strategies that encourage them to invest in their own security. However, the bulk of Australian people and businesses fall into a third category: they would *like* to defend themselves online but don't have the expertise or the resources to do so.

Large parts of the Australian economy and community can't protect themselves online because they don't have the skills or resources to do so.

Criminals, meanwhile, are agnostic about their targets and will attack whoever it is profitable to attack. As weaknesses in security in one area of the economy get shored up, other avenues are explored. If the top end of town is too tough, criminals will ransack those with relatively poor security—individuals and small and medium-sized enterprises.

They also take a 'belt and braces' approach to extracting money from their victims. In the May 2020 Toll Group ransomware attack, for example, the criminals first attempted to extract money with 'traditional' ransomware—encrypting IT systems to disrupt operations. When Toll refused to pay the ransom, the criminals changed to the exact opposite tactic and threatened to publicly release corporate data unless they were paid.[11]

Given that malicious actors seek out weakness and vulnerability wherever it exists in the economy, and that some parts of the economy will never have the sophistication and ability to protect themselves, we need to develop initiatives that provide 'default security' and bring resources and skills to those who don't have them—who are generally small and medium-sized enterprises and consumers.

There are already initiatives that bring default security to groups that don't have the skills or resources to protect themselves. They occur at different 'layers' of the architecture of the internet: at the hardware level, in operating systems, in some of the services that underpin the operation of the internet, and in the software applications that people use to access the internet (see Table 1).

Table 1: Current default security protections occur at different layers

Internet communications layer	Examples of default security initiatives
Browser based	Google Safebrowsing and Microsoft SmartScreen.
Domain Name System (DNS)	Some providers filter domain names to stop malware and phishing (Quad9, OpenDNS etc.)
Operating systems	Automatic updates, in-built anti-malware protections, architectural improvements such as address space layout randomisation and data execution prevention.
Computing hardware	Hardware security (trusted platform modules, Apple's Secure Enclave etc.)

At the most fundamental level, chip manufacturers have invested in the development of more secure computing architectures.[12] Building upon those hardware improvements, operating system manufacturers have also baked default security into their products. This includes features such as automatic updates that make it easier to patch vulnerabilities, built-in anti-malware features such as Windows Defender and architectural features that make it more difficult for hackers to seize control, such as address space layout randomisation and data execution prevention.[13]

At the internet services layer, a number of Domain Name System (DNS; the system that converts human-readable internet addresses into internet protocol addresses) providers also include default security protection: Quad9, OpenDNS,[14] Comodo Secure DNS[15] and CleanBrowsing,[16] among others. For example, Quad9 states in its FAQ that it 'uses threat intelligence from a variety of public and private sources and blocks access to those malicious domains when your system attempts to contact them'.[17]

Google's Safebrowsing[18] and Microsoft's SmartScreen,[19] for example, are web-scanning, anti-phishing and anti-malware systems built into their respective browsers and operating systems to prevent users from visiting potentially dangerous web pages. As users browse the web, the pages they visit are compared to a list of 'known-bad sites' that have been confirmed to be hosting phishing or malware. If a user tries to visit one of those sites, instead of taking them directly there the user is shown a warning. These protections are imperfect, as the user can ignore the warning and click through to the site, and criminals and hackers are constantly trying new techniques to evade them, but they have very broad reach. Safebrowsing is used in Google's Chrome, Mozilla's Firefox and Apple's Safari browsers, and together with SmartScreen in Microsoft Edge these systems protect billions of users by default. Google's *Transparency report* statistics show that the SmartBrowsing system issued in the order of 5–10 million warnings per week so far this year up to late May 2020.[20]

These security improvements have occurred at different 'layers' of the internet—in browsers, in operating systems and in the underlying plumbing of the internet. They are also 'high-leverage' initiatives, in that these investments can improve security for millions to billions of internet users.

There have been improvements in default security in some aspects of online security over the past two decades, but there's still a very long tail of vulnerability that we must cope with for the foreseeable future. Additionally, other developments threaten to undermine those improvements. The proliferation of the 'internet of things' (IoT)—internet-connected but poorly secured and increasingly ubiquitous consumer devices—threatens to introduce a large vector of insecurity that could drastically affect overall cybersecurity.[21]

Given the success of previous default-security initiatives, what other initiatives could have a widespread positive impact on the cybersecurity of millions of users?

Clean Pipes

One proposal that could help provide advanced capabilities to internet users is that ISPs be required or encouraged to perform 'due diligence' to protect their users from malicious traffic. This concept has been called 'Clean Pipes', drawing an analogy to water utilities providing clean drinking water.

Clean Pipes could involve ISPs using a variety of technologies to provide default security to their clients. At the conceptual level, this would involve:

1. positively identifying threats, which could be, for example
    - internet locations that host malware or phishing
    - malware command and control
    - bogus traffic that can be used in attacks that try to overwhelm a service
    - 'spoofed' traffic that claims to originate from somewhere it doesn't
2. having some capability to proactively protect from different threats, such as
    - blocking and warning users who are attempting to navigate to dangerous locations, such as ones that host malware or phishing
    - removing bogus or spoofed traffic
3. being able to adjust this blacklist dynamically and alter it through customer feedback if a location is inadvertently blacklisted.

These kinds of capabilities are already deployed around the world, in corporate networks, by British Telecom[22] and recently by Telstra.

The advantages

The key advantage of Clean Pipes is that it brings *advanced scalable protection* to an ISP's entire customer base, which is particularly important to that majority of customers who don't have the skills and resources to provide for their own security. It's also highly leveraged—although in a well-organised protection system the entire workforce involved in identifying malicious internet sites may be thousands of people, the knowledge they generate can be used to provide protection to potentially millions of ISP customers.

There are other advantages. ISPs also have a unique position in the network and are able to see *all* of the internet protocols that are being used, not just the very few that are used in web browsing. This means that ISPs can see different indicators of malicious behaviour than can, say, operating systems manufacturers, browser manufacturers, DNS providers, or even the anti-malware systems that work on individual computers. Each of these different vantage points into the internet has a different view and can be used to detect or even interrupt different kinds of activity. Browser-based protection, for example, can warn users of malicious websites but can do nothing to stop malware command and control once a computer is compromised.

Not only do ISPs get different views, they also get to *act* on those other protocols, blocking or redirecting them if need be. This is already standard practice where ISPs need to protect their networks from activity that could degrade or disrupt the network[23] or where there's already an established mechanism to block illegal content.[24] ISPs could protect users from threats that can't be tackled by the other default security providers previously mentioned.

There's no legal impediment to ISPs providing some level of protection to their customers (excepting techniques that would be privacy-invading). Telstra has already implemented some customer protection under a Cleaner Pipes initiative and has blocked the 'command and control communications of botnets and malware and [stopped] the downloading of remote access trojans, backdoors and banking trojans'.[25] These initiatives can be written into terms-of-service contracts, although perhaps an ideal position would be to provide users with the ability to opt out if they don't want default protection. For example, Google Safebrowsing and Microsoft SmartScreen both provide warnings that users are still able to navigate past.

ISPs already operate security operations centres and have security teams to protect their own networks' integrity, so there are already skills and expertise resident within their organisations, although skill levels can vary significantly between ISPs. Providing default security to customers may require additional investment in resources, but it requires that an existing capability be grown rather than a new one created from scratch.

Additionally, ISP-level protections could be particularly useful in mitigating the risk from poorly secured IoT devices. Those devices can't take advantage of some of the other default security advances that have taken place over recent years, such as improvements in browsers or operating systems, but they still communicate over the internet and do so in relatively standard ways, such that anomalous behaviour can be detected and at least some malicious behaviour blocked. That is, ISPs providing Clean Pipes could help mitigate one of our potential looming security threats.

Although ISPs providing default security protection has many benefits and could significantly reduce the damage caused by malicious traffic, it isn't a panacea for all the ills of the internet. As with protections built into operating systems and browsers, malware, phishing and other threats will break through and cause harm to internet users.

ISP-level concerns and blockers

In Australia, ISPs, other than Telstra, don't provide extensive default security protections to their customers. There are several reasons for this that fall into four categories:

1. costs and ISP security expectations
2. capability to detect and act
3. understanding harms
4. reputational risk.

Costs and security expectations

Possibly the underlying reason that most ISPs don't invest significantly in Clean Pipes is that enhanced security costs more money and neither customers nor ISPs expect that an ISP should provide increased levels of default security.

Related to this, ISPs don't believe that their customers value a more secure service, so there's no potential profit available to justify a business case to provide these security services; therefore, no resources are allocated.

Additionally, there's been no legal or regulatory obligation that has pushed ISPs to provide enhanced default security services.

Capability to detect and act

All ISPs have some level of security capability, which they need to protect their own networks. However, providing increased levels of default security to customers requires more extensive and more advanced capability to both *detect* malign behaviour and to *act* on it.

All ISP security operations must prioritise self-protection and they might not have additional capacity to detect malicious activity that doesn't directly threaten their own operations. Without a clear view of malicious activity that affects their customers (or even third parties), ISPs are unable to act on it.

Any individual ISP would be able to identify *some* threats on its network, but a collaboration with multiple partners provides a more comprehensive and effective picture of both the threats and effective mitigations. Holistically understanding threats requires collaboration with multiple partners in the security ecosystem, including providers of threat intelligence, other industry verticals and competitor ISPs. Each organisation provides a different slice of the view so that the overall picture is far more complete than any individual organisation can develop on its own.

This industry collaboration would require two separate forms of trust:

- Competitors would have to trust that companies within the same industry would not seek to gain competitive advantage through security collaboration. This is relatively straightforward within the information security community, as competitive advantage is seen to lie outside security, and effective security is generally perceived as a precondition for competition rather than as a basis for it.[26]
- Companies need to trust the technical competence of collaborators. This is currently based on reputation and past performance, and there's no formal process for technical trust to be built or certified.

The two forms of trust affect both the *ability* and *willingness* to share reliable information and to act effectively on information received. Discussions with stakeholders have indicated that significant skill and capacity differences exist between the security operations within different ISPs, and that those differences may make it difficult to engage in effective widespread information sharing across Australian ISPs.

Beyond merely detecting malicious activity, ISPs also need to have the ability to act on it. Acting on malicious behaviour requires additional financial investment beyond detecting it, so, even if ISPs see damaging activity, they may have decided that the costs of implementing default security for customers are simply too high. At the ISP level, most customers don't pay extra for security services, so investment in providing improved security might not be seen as an economically viable return on investment.

Understanding harms

Beyond merely detecting malicious activity is understanding the harm that it causes. What malicious activity that ISPs see on their networks causes the most harm to customers? For activity that damages their own networks, that harm is easy for ISPs to understand, but quantifying damage caused to customers is very difficult.

Understanding the harms to customers could be improved by information sharing about the costs of cybercrime from government mechanisms such as ReportCyber, from NGOs such as IDCARE,[27] or even from other industry verticals that collate information about the most damaging cybercrimes affecting their customer bases.

Some ISPs, particularly smaller ones, might not be able to detect malicious activity and don't understand the harms it causes their customers. In such cases, ignorance is bliss—once an ISP sees malicious activity and understands that it causes harm to its customers, it faces its own version of the 'trolley problem'. Do they intervene to protect their customers from dangerous activity on the internet, even though that may come at some financial cost?

Reputational risk

ISPs could also be concerned about the reputational risks involved in attempting to provide default security.

A key reputational concern is that ISPs may inadvertently block legitimate traffic. Although terms and conditions can mitigate legal concerns, ISPs still have to strike a balance between providing enhanced security and the risk that false positives will affect service quality. Importantly, there are harms to customers that occur when ISPs accidentally block non-malicious traffic *and* when ISPs allow customers to be harmed by malicious traffic. An ideal balance would minimise both harms while preserving online freedom, but this balance is inconsistently applied across different ISPs and is therefore probably suboptimal.

ISPs may also be concerned about the perception that default security requires them to compromise customer privacy. Certainly, government internet initiatives have focused on law enforcement and intelligence requirements, and Australia's metadata retention laws[28] and the *Assistance and Access Act 2018*[29] have been controversial.[30] Telstra's recent announcement regarding Cleaner Pipes, however, hasn't so far been the subject of any significant level of controversy about privacy.

In any case, whether through lack of obligation, understanding, capability or a business case, there's no broad-based, ISP-led effort to provide default security to Australian internet users.

Government challenges

The challenges facing government mirror those facing ISPs.

The Australian Government hasn't tried to lead a broader effort to provide default security to Australian internet users through a Clean Pipes initiative involving ISPs. In some sense, it hasn't accepted that leading this kind of initiative is its job. In the absence of an industry consensus that ISPs should be providing some level of default security, the absence of government leadership or direction probably means that this *status quo* will continue.

A significant concern may be the controversies over privacy, censorship and surveillance that have accompanied previous internet initiatives, such as an internet filter proposed in 2012[31] and the previously mentioned metadata retention legislation and Access and Assistance Act. Those former initiatives have been focused on supporting law enforcement or preventing access to harmful content, rather than on providing secure internet access to consumers.

Concerns about privacy, censorship and surveillance could be mitigated by government initiatives having:

1. a clear focus on threat filtering, with a clear and explicit goal of protecting internet users
2. government leadership that doesn't necessarily include government implementation
3. actions focusing exclusively on cybersecurity threats rather than falling into mission creep and including other online harms (such as child exploitation) that are being tackled through other avenues (such as the e-Safety Commissioner)[32]
4. transparency about how default security provisions are enacted and what they achieve
5. a default system with an opt-out for those who don't want to participate.

The cost of cybercrime isn't well understood, and that makes it difficult to appropriately allocate resources. One of the most quoted estimates for cybercrime (a Microsoft-commissioned report from Frost and Sullivan) estimated in 2018 that cybercrime could cost Australia $29 billion per year,[33] whereas a 2019 ACSC report estimated $328 million in annual losses.[34] The ACSC report was based mostly on incidents self-reported to the ReportCyber platform and so is likely to be an underestimate of the cost, but the 100-fold difference between the estimated and measured values shows that the level of uncertainty is high. More comprehensive data would be helpful, and a granular understanding of the cyber threats that are causing the most harm would provide an economic justification for security investments that would be required to mitigate that harm.

Conclusion

This paper has documented some of the arguments for Clean Pipes initiatives in which ISPs deploy their security capabilities to provide default cybersecurity for their customers, and the potential difficulties in implementing such initiatives.

Large portions of the Australian economy and community aren't capable of effectively providing for their own cybersecurity, and there are significant opportunities for wide-ranging and effective improvements in the security environment for *all* internet users. Those approaches would be additional to other broad-based security improvements that have occurred in recent years and could go some way to mitigating the threat from the proliferation of poorly secured IoT devices.

Road map

Currently, these opportunities aren't being taken up because the Australian Government has yet to set a clear policy direction and because industry doesn't see this as a business obligation. Recently announced government funding, including over $35 million to develop a 'new cyber threat-sharing platform' and over $12 million towards 'strategic mitigations and active disruption options' is an opportunity to change this *status quo*.[35]

The Australian Government should:

- clearly articulate its position on ISPs providing default security services in its 2020 Cyber Security Strategy (Home Affairs)
- raise the baseline of ISP security operational expertise by facilitating technical workshops (funding is available to support technical tools, but skilled cybersecurity personnel are also needed to both provide validated information and to make effective use of threat information) (ACSC)
- investigate providing incentives to ISPs to implement improved default security (this could include technical training to improve capacity, funding for new capabilities, or even regulation or legislation to encourage adoption) (Home Affairs)
- convene closed-door consultations with ISPs to discuss how the government could support and encourage the delivery of default security to customers (Home Affairs)
- require transparency reports in which ISPs report on their efforts to provide safe and secure networks (Australian Communications and Media Authority)
- more comprehensively quantify the cost of cybercrime in Australia through surveys and by engaging directly with Australian industry (Home Affairs).

ISPs should:

- work with government to centralise and expand upon existing industry-wide efforts in collaboration, intelligence sharing and coordinated action.

Australian industry, beyond ISPs, should:

- increase the sharing of technical indicators of compromises that are affecting its customers (a government-supported centralised clearing house for information would support this)
- measure the cost of cybercrime and share information, within intelligence-sharing bodies, about the most damaging cybercrime techniques
- factor in consideration of the cost and risk of failing to manage security issues in supplying their services.

Notes

1 Scott Morrison, 'Nation's largest ever investment in cyber security', media release, 30 June 2020, online.
2 Department of Home Affairs (DHA), *Australia's Cyber Security Strategy*, Australian Government, May 2016, online.
3 The underlying cause of these attacks is not public, so it isn't possible to say whether ISPs providing Clean Pipes would have prevented them.
4 Ry Crozier, 'Toll Group "returns to normal" after Mailto ransomware attack', *iTnews*, 18 March 2020, online; Ry Crozier, 'Toll Group suffers second ransomware attack this year', *iTnews*, 5 May 2020, online.
5 Ry Crozier, 'BlueScope confirms a "cyber incident" is disrupting its operations', *iTnews*, 15 May 2020, online.
6 Bension Siebert, Shuba Krishnan, 'MyBudget blames hack for outage affecting thousands of customers', *ABC News*, 15 May 2020, online.
7 Ben Grubb, 'Drinks giant Lion hit by cyber attack as hackers target corporate Australia', *Sydney Morning Herald*, 9 June 2020, online.
8 Swetha Das, 'Direct costs associated with cybersecurity incidents costs Australian businesses $29 billion per annum', *Microsoft News Centre Australia*, 26 June 2018, online.
9 Interpol, 'Cybercriminals targeting critical healthcare institutions with ransomware', news release, 4 April 2020, online; 'CyberPeace Institute—call for government', CyberPeace Institute, 26 May 2020, online.
10 Michael Pompeo, 'The United States concerned by threat of cyber attack against the Czech Republic's healthcare sector', press statement, US Department of State, 17 April 2020, online; Department of Foreign Affairs and Trade, Australian Cyber Security Centre (ACSC), 'Unacceptable malicious cyber activity', news release, Australian Government, 20 May 2020, online.
11 Toll Group, 'Toll IT systems update', 29 May 2020, online.
12 For example, investment in trusted platform modules, Apple's Secure Enclave in iOS devices.
13 Microsoft, 'The most secure Windows ever', no date, online.
14 OpenDNS, 'Why users love OpenDNS', 2020, online.
15 Comodo Cybersecurity, 'Secure internet gateway', 2020, online.
16 CleanBrowsing, 'Browse the web without surprises', no date, online.
17 Interestingly, when customers use these optional DNS services their ISP loses visibility and can no longer detect malware and assist them; 'FAQ: DNS need to know info', *Quad 9*, 2019, online.
18 Google, 'Google safe browsing', 2019, online.
19 Microsoft, 'Microsoft Defender SmartScreen', 27 November 2019, online.
20 Google, 'Google safe browsing', 2019, online.
21 Eliza Chapman, Tom Uren, *The Internet of Insecure Things*, ASPI, Canberra, 19 March 2018, online.
22 Dave Harcourt, 'BT's proactive protection: supporting the NCSC to make our customers safer', National Cyber Security Centre, UK Government, 25 October 2018, online.
23 Such as, for example distributed denial of service (DDoS) attacks that attempt to overwhelm networks or websites.
24 For example, Interpol's 'Worst of' provides a list of domains carrying child abuse material; Interpol, 'Blocking and categorizing content', 2020, online.
25 Andrew Penn, 'Safer online and the new normal', *Telstra Exchange*, 6 May 2020, online.
26 Even within the cybersecurity industry competitors collaborate, and the Cyber Threat Alliance serves as a model for competitors sharing information about threats. There are also many effective information-sharing initiatives overseas and in Australia (for example, see 'Member ISACs', National Council of Information Sharing and Analysis Centers, 2020, online).
27 'National identity and cyber support', *IDCARE*, 2020, online; ACSC, 'ReportCyber', Australian Signals Directorate, Australian Government, 2020, online.
28 DHA, 'Data retention', Australian Government, March 2020, online.
29 DHA, 'The Assistance and Access Act 2018', Australian Government, September 2019, online.
30 For example, see Elise Scott, 'Senate passes controversial metadata laws', *Sydney Morning Herald*, 27 March 2015, online; Damien Manuel, 'Think your metadata is only visible to national security agencies? Think again', *The Conversation*, 5 August 2019, online; Stilgherrian, 'Home Affairs report reveals deeper problems with Australia's encryption laws', *ZDNet*, 29 January 2020, online.
31 Ry Crozier, 'Conroy abandons mandatory ISP filtering', *iTnews*, 8 November 2012, online.
32 There are already mechanisms to block objectionable material, such as the *Sharing of Abhorrent and Violent Material Act 2019*, and those mechanisms should remain separate from security provisions. See Attorney-General's Department, 'Abhorrent violent material', Australian Government, no date, online.
33 Frost and Sullivan, *Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World*, 2018.
34 ACSC, *Cybercrime in Australia—July to September 2019*, Australian Signals Directorate, Australian Government, 2019, online.
35 Morrison, 'Nation's largest ever investment in cyber security'.

Acronyms and abbreviations

ACSC	Australian Cyber Security Centre
DNS	Domain Name System
IoT	internet of things
ISP	internet service provider
NGO	non-government organisation

About the author

Tom Uren is a Senior Analyst in ASPI's International Cyber Policy Centre.

Acknowledgements

ASPI's International Cyber Policy Center receives funding from a variety of sources including sponsorship, research and project support from across governments, industry and civil society. There is no sole funding source for this paper.

What is ASPI?

The Australian Strategic Policy Institute 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's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber and emerging technologies and their impact on broader strategic policy. The ICPC informs public debate and supports sound public policy by producing original empirical research, bringing together researchers with diverse expertise, often working together in teams. To develop capability in Australia and our region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises both in Australia and overseas for both the public and private sectors. The ICPC enriches the national debate on cyber and strategic policy by running an international visits program that brings leading experts to Australia.

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.

ASPI

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

© The Australian Strategic Policy Institute Limited 2020

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers. Notwithstanding the above, educational institutions (including schools, independent colleges, universities and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.

First published July 2020.

ISSN 2209-9689 (online),
ISSN 2209-9670 (print)

There is no sole funding source for this paper.


ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
INTERNATIONAL
CYBER POLICY
CENTRE