

Australia's cybersecurity future(s)

It's January 2024. Does Australia still have the internet?

Frank Smith, Aim Sinpeng, Ralph Holz, Sarah Logan,
Jonathon Hutchinson and Hui Xue



About the authors

Frank Smith is a Senior Lecturer in the Department of Government and International Relations at the University of Sydney and co-founder of the Sydney Cyber Security Network.

Aim Sinpeng is a Lecturer in the Department of Government and International Relations at the University of Sydney and co-founder of the Sydney Cyber Security Network.

Ralph Holz is a Lecturer in Networks and Security in the School of Information Technology at the University of Sydney.


Sara Logan is a Lecturer in International Relations at the Australian National University.

Jonathon Hutchinson is a Lecturer in Online Media in the Department of Media and Communications at the University of Sydney.

Hui Xue is a Research Associate in the School of Social and Political Sciences at the University of Sydney.

Acknowledgements

This report was produced in collaboration between the Sydney Cyber Security Network and ASPI's International Cyber Policy Centre. It was made possible thanks to a research grant provided by the Sydney Policy Lab. We also thank our research assistant Bryce Pereira, as well as the other experts and visionaries who provided helpful comments and feedback.

 @SydneyCyber

<https://sydney.edu.au/arts/our-research/centres-institutes-and-groups/sydney-cybersecurity-network.html>

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.

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

© The Australian Strategic Policy Institute Limited 2018

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 December 2018

Cover image: Cyber security graphic: iStockphoto/kutubQ



THE UNIVERSITY OF
SYDNEY

Australia's cybersecurity future(s)

It's January 2024. Does Australia still have the internet?

Frank Smith, Aim Sinpeng, Ralph Holz, Sarah Logan,
Jonathon Hutchinson and Hui Xue

Issues Paper
Report No. 13/2018

Contents

Introduction	03
Scenario analysis	04
Drivers of change	05
Asia online	05
Tech giants	05
Great-power conflict	06
2024: Fragmented world, fragmented internet	06
Enter the dragon	07
The Western Front	08
Fault lines	08
Moving forward: strategic choices and challenges for Australia	10
Australia will be caught in the fray	10
Internet fragmentation isn't all bad everywhere	12
Australia lives in a dangerous neighbourhood	13
Tough choices	13
Notes	14
Acronyms and abbreviations	15

Introduction

Australia wants to create a future for cyberspace that's open, free and secure, but that future is not assured. According to Dr Tobias Feakin, the Ambassador for Cyber Affairs, 'Australia's vision ... and our ambitions across the broad spectrum of cyber affairs are impossible to achieve alone.'¹ Key drivers are outside of the country's control. The government can—and should—advance a positive vision, but Australia might not get its way.

What if the future of cybersecurity looks different from what we hope or expect? This is a hard question to answer. Day-to-day concerns demand our immediate attention, and, when we think about the future, we tend to extrapolate from current trends. As a result, we're shocked or surprised by discontinuous change, and woefully unprepared to face new realities. The risk is particularly acute in cybersecurity, in which rapidly changing technologies combine with diverse social and political forces to create unexpected consequences. Therefore, as difficult as it is to rethink our assumptions about the future, failing to do so could be dangerous.

This report uses scenario analysis to examine one such future: a world where cyberspace is fragmented in the year 2024. Contrary to the ambition of Australia's International Cyber Engagement Strategy, cyberspace is neither open nor free in this scenario. We analyse what that implies for cybersecurity. In particular, we examine the challenges and opportunities that Australian policymakers may face in the future and wish they had planned for in our present.

We conclude that Australia will be caught in the fray if the internet breaks apart. While this scenario isn't all bad, Australia could be forced to fend for itself in an increasingly dangerous neighbourhood. The scenario isn't a forecast or prediction. It's a compelling narrative to provoke new thinking and critical discussion about what Australia must do now to prepare for different cybersecurity futures.

Our approach is as follows. First, we explain the methodology. Second, we identify the forces of change that drive this scenario. Third, we interact these drivers to describe one possible world in 2024. Finally, we highlight the strategic choices and challenges that this scenario raises for Australia.

Scenario analysis

Scenario analysis is a methodology for critical thinking about alternative futures. It was pioneered at RAND in the 1950s by Herman Kahn in his attempt to ‘think the unthinkable’ about thermonuclear war. The method was further developed by Pierre Wack and Ted Newland at Royal Dutch Shell, where scenario analysis was credited with anticipating the possibility of oil shocks during the 1970s.² It’s now commonly used in industry and government. For instance, scenario analysis informs the US National Intelligence Council’s quadrennial *Global trends* report.³ It’s also applied by the Center for Long-Term Cybersecurity at the University of California, Berkeley, in reports on *Cybersecurity futures 2020* and *Asian cybersecurity futures*.⁴

The goal of scenario analysis is to ask and, ideally, answer ‘what if’ questions about how different drivers of change—social, political, economic, technological—could combine to produce discontinuities and thus different possible worlds. This approach is forward looking. We apply it to imagine Australia’s cybersecurity environment circa 2024. It may be unsettling. Following best practice, we sought to simplify and then exaggerate the drivers of change in order to throw an alternative and perhaps undesirable future into sharp relief. Nevertheless, scenario analysis is still rooted in reality. The propositions behind this qualitative analysis are plausible, the narrative is internally consistent, and the results reflect expert consultation.

This report breaks from the norm of scenario analysis by focusing on one of many possible futures. Our focus is not predictive, however. We do not argue that internet fragmentation is probable or likely to play out as per this scenario. We do suggest that this kind of future is significant because it challenges Australia’s preferred vision for an open, free and secure cyberspace. Fragmentation is also a significant concern in internet policy.⁵ Furthermore, while it may be a single scenario, a fragmented world contains different environments or ecosystems, and analysing that diversity helps compensate for our focus on only one potential future. The challenges and opportunities of such a future therefore warrant special consideration (just as other scenarios warrant further research). Rather than fight the scenario, we encourage you to ask: *What would Australia need to decide and do differently for cybersecurity if it confronts this world in 2024?*

Drivers of change

Our scenario depicts the interplay or interaction effects of three hypothetical drivers for change: Asia online, tech giants, and great-power conflict. While none is certain, each premise is plausible. More importantly, the resulting scenario is not a linear extrapolation or forecast based on any single trend. It's the combination of drivers that could contribute to internet fragmentation and result in a cybersecurity environment markedly different from today's.

Asia online

First, the number of users, devices and applications in Asia grows substantially over the next five years. We imagine that internet penetration in the region grows faster than expected, jumping from less than 50% today to more than 80%, so that more than 3.5 billion people are online in Asia. As a result, there are as many people online in this region come 2024 as the total number of internet users around the world in 2019. By 2024, Asia is also home to more than 15 billion connected devices.

We assume that this rapid expansion of connectivity is unrivalled in other regions. It roughly correlates to Asia's youthful and growing population, as well as its economic power as the new centre of the global economy. However, economic and political opportunities remain unevenly distributed over the next five years, as is the region's digital transformation. Most web traffic in Asia is mobile, but connection speeds vary greatly across the urban-rural divide, and economic growth hasn't reduced economic inequality.

Tech giants

Second, we posit large and locked-in technology platforms as another driver for change.

Although new applications flourish over the next five years, we assume that the underlying technology stacks, layers or platforms upon which those applications are built resemble a few large tectonic plates. And those platforms are increasingly dominated by a handful of huge corporations.

Tech giants dominate the user experience, software development and hardware. For most people in 2024, 'cyberspace' is difficult to distinguish from megabrands such as Google, Apple, Facebook, Amazon and Microsoft, or, similarly, Alibaba, Tencent, Baidu, Sina Weibo and Huawei. These companies also dominate the marketplace for talent. Regardless of where they work, most software developers work with toolkits and application program interfaces that plug into a dominant platform. Proprietary software developed by tech giants enjoys a home-field advantage over apps built by third-party providers. Industry concentration shapes hardware and telecommunications infrastructure as well, including the 'internet of things' (IoT). On the one hand, we imagine that connected devices are ubiquitous and produced by a plethora of manufacturers in 2024. On the other hand, in many markets, many of these connections are mediated by platforms, hubs and bridges dominated by the 'Big 10' tech giants.

Great-power conflict

The third driver is strategic competition and conflict between great powers. We posit a multipolar world in 2024. No great-power concert has emerged to manage territorial conflicts or the myriad state and non-state cyber operations. The US remains the only superpower with global reach, but that reach is rivalled by China's, especially in the Pacific and Indian oceans. US power projection into the region is further limited by budget constraints (accentuated by an ongoing recession), as well as costly commitments to fighting in the Middle East and deterring a weak but assertive Russia. While NATO endures, nationalism and populism have fuelled extreme swings in American and European politics, fraying the alliance. ANZUS endures as well, but the US lacks a coherent strategy towards Asia in 2024. As a result, the US military posture isn't supported by consistent political and economic policies.

Meanwhile, China has continued to rise. The Middle Kingdom is a middle-income country in 2024, with a nearly \$15 trillion economy. Its One Belt, One Road and Digital Silk Road initiatives have established Chinese infrastructure, standards and platforms in several neighbouring economies. However, this economic and strategic agenda is resisted by India in the south and Russia in the north, along with European and American interests in Africa and Oceania. We posit that the Chinese economy has not dipped into recession, although its officially reported growth rate of 3% in the last quarter of 2023 is viewed with considerable scepticism. In China, as elsewhere, economic angst and nationalism have increased variability in foreign policy and contributed to competition and conflict in the region.

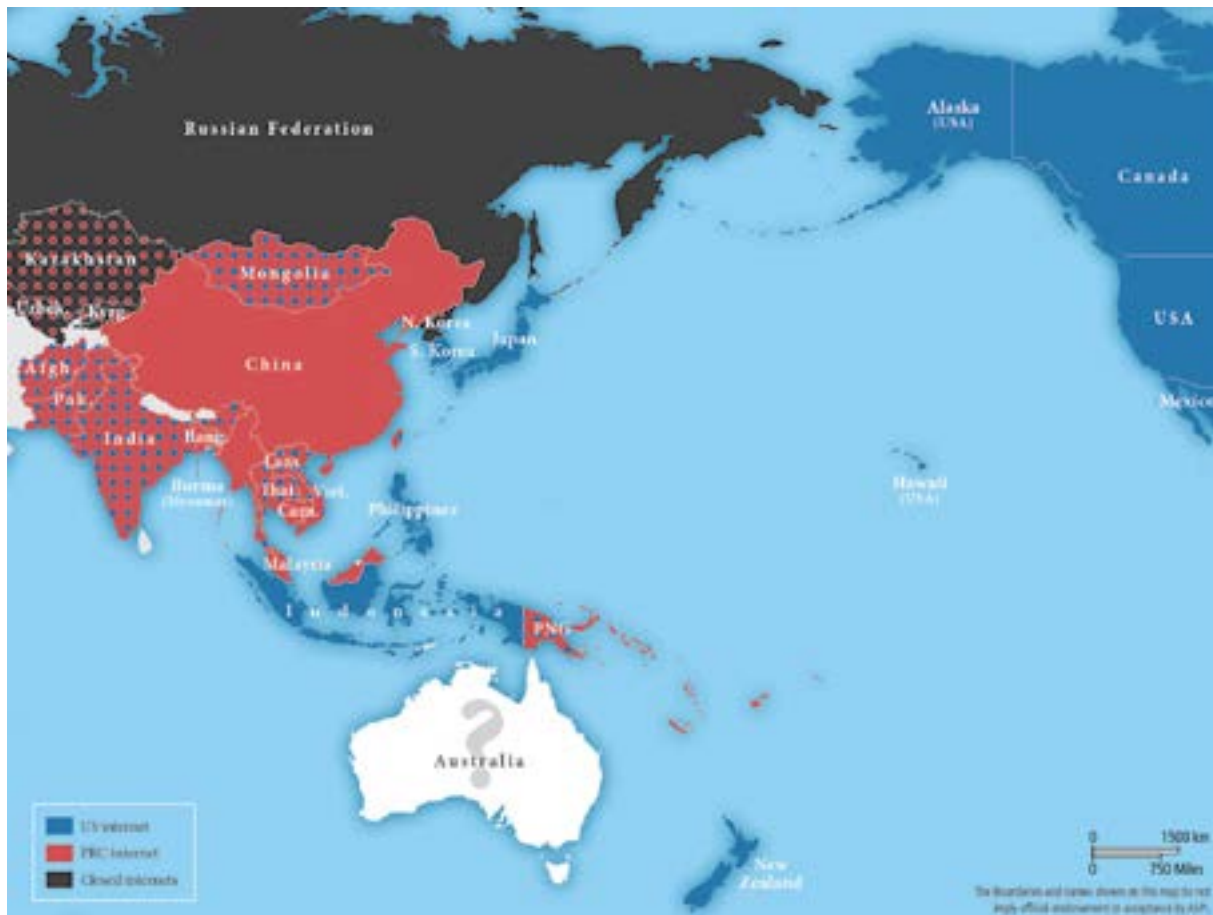
2024: Fragmented world, fragmented internet

In this scenario, Asia comes online but cyberspace fragments by 2024. Years of mounting tensions between the US, China, Russia and Western Europe have combined with entrenched platform technologies to result in a world where the internet—singular—is a thing of the past. The 'World Wide Web' is anachronistic. Instead, there are several weakly connected internets, each of which contains content and services that are largely inaccessible from outside the same country, region or bloc. There are tunnels through these walled gardens, but few users beyond specialists, spies and criminals have the skill or inclination to use them. Most users' online access and experience is mediated and monitored by whichever tech giants enjoy official sanction in their local market. In most places, 'social media' are just media, and the IoT is just things.

The world's largest internets are American and Chinese. Access to each correlates with physical proximity to the US or China, coupled with the broader user base of their respective tech giants. In particular, the American internet is accessible in most of the Western Hemisphere (corresponding to the American and Latin American regional internet registries). It's also accessible in Western Europe, but tensions across the Atlantic have combined with divergent data protection and antitrust regulations, fuelling the emergence of a continental internet in the remnants of the European Union. Russia's national internet is effectively cordoned off by internal information controls (heightened following the death of Vladimir Putin), combined with external blocking of untrusted traffic (Russian IP addresses being equated with criminal or intelligence operations and rejected by most border

routers). National networks have also emerged in North Korea, Saudi Arabia and Venezuela. In addition to indigenous applications, the governments that regulate these and similar shards of cyberspace typically contract with Chinese or American firms to build platforms that are closed and customised for local censorship and surveillance.

Figure 1: Internets of the region, 2024



Enter the dragon

Like the Belt and Road Initiative, or the Nine-Dash Line, geography is a notable feature of the Chinese internet in 2024, which is portrayed as several concentric circles. Domestic services and content sit at the centre, behind the Great Firewall. China's 'Social Credit' system hasn't proved particularly effective in regulating behaviour offline; a goth-like fashion trend dubbed 'false negative' has even emerged to frustrate facial recognition. Nevertheless, China has become a nearly cashless society, and both big data and artificial intelligence are used to effectively monitor most online activity. The incidence of malware has decreased dramatically, and domestic cyber incident response is well coordinated. Some cybersecurity experts worry that foreign intelligence services are exploiting the backdoor access required by China's regulation of commercial encryption, yet the government denies any such allegation.

Outside the Great Firewall, similar services and content are available to those individuals, organisations and countries that use the platforms provided by China's tech giants (or their local affiliates). Many do, particularly in Asia. By default, users in this second ring give their data to Chinese service providers.

Most of that information is stored on servers inside China. The outermost ring consists of custom networks that China has built but for which—purportedly—it has handed information controls over to the client, such as for the heavily restricted mobile apps recently launched in North Korea.

The Western Front

For many users in the US, the American internet in 2024 appears similar to the World Wide Web in 2019. A similar set of tech giants from Silicon Valley and Seattle dominate the market. Their proprietary platforms seem to seamlessly integrate users' digital lives. Toddlers are frequently reported to perceive voices such as Google Home and Amazon Echo as disembodied members of their families. Data breaches of personally identifiable information are so common as to rarely make news; occasionally, car fleets and wired housing developments that have been bricked by cyberattacks make headlines. Net neutrality remains contentious and partisan. Demands from law enforcement for data collected by bystanders' wearable tech during the Denver bombing in 2022 have ignited another round of debate over encryption (a debate joined by lobbyists for fintech and cryptocurrencies).

Lobbying by tech giants, fractious domestic politics and anti-statist ideology limit US federal regulations on cybersecurity. One exception is wireless broadband. A government-sponsored, industry-led consortium has rolled out a mobile network called *US5G*. Chinese companies are banned from building this infrastructure. Likewise, Chinese and Russian cybersecurity software is banned from use on US Government computers. The Security and Exchange Commission has also imposed reporting requirements on cryptocurrencies and initial coin offerings. Domestic information sharing has improved modestly after years of concerted attacks against critical infrastructure, but individual users still have little recourse, and the quality of cyber insurance is variable. US diplomats pay lip service to ideas such as 'internet freedom' and 'cyber norms' when they criticise authoritarian regimes, but the promotion and practice of the American internet abroad is largely determined by the commercial strategies of its tech giants.

Figure 2: The US5G logo



Fault lines

Asia is a contested zone in 2024. The US and China vie for power in the region while Chinese and American firms compete for market share. Unfortunately, the US and China appear caught in the 'Thucydides trap', as the rising and ruling powers jostle near the brink of armed conflict.⁶ War was narrowly averted in 2022 following a naval skirmish in the South China Sea that killed 65 sailors and marines aboard American and Chinese warships. Patriotic hacking—both state-sanctioned and

self-radicalised—during this incident was intense and occasionally destructive. Since then, submarines have been reported patrolling undersea cables in the Pacific. In addition, real and imagined instances of Chinese and American firms facilitating offensive cyber operations by military and intelligence agencies have driven yet another wedge between their rival internets.

On the one hand, countries in the Indo-Pacific enjoy more choice than those in the Western Hemisphere, since the American and Chinese internets are both viable options in this region. Some countries are choosing to bandwagon with China. In 2024, Alibaba, Tencent, Baidu, Sina Weibo and Huawei are providing a bundle of telecommunication, media, IoT and financial services called *WeConnect*. This bundle has proved remarkably popular in Malaysia, for instance, and among the Chinese diaspora across Asia. *WeConnect* has also increased internet access in Myanmar and Cambodia by an order of magnitude: millions of their people have leapfrogged from having no phones to using Chinese smartphones overnight. In contrast, Japan uses the American internet as a matter of policy, and most users in Indonesia and the Philippines remain locked into Facebook and Google. India is non-aligned (despite the prevalence of American platforms), and Pakistan is hedging its bets (despite widespread adoption of *WeConnect*). Competition and choice between American and Chinese internets are fuelling digital innovation across the region.

On the other hand, innovation in this scenario is not improving global integration. Choosing one internet increasingly means forgoing access to others. Chinese and American cybersecurity standards are not compatible. Nor is compatibility of much interest to the tech giants. Years of national tariffs, investment restrictions, divergent regulations and export controls have limited their sales in the others' domestic markets. Combined with the *US5G* network, these policies have forced American firms to shift away from Chinese suppliers. Similarly, the 'Made in China 2025' initiative has made Chinese tech giants more self-sufficient. The US–China skirmish in 2022 accelerated the disintegration of once highly integrated supply lines and manufacturing. When competing for customers in Asia, the tech giants are incentivised to collude within their own internet and exclude foreign rivals.

Moreover, the range of choice in this region comes at considerable cost. While some aspects of cybersecurity have improved inside Chinese and American internets, those improvements are lost in the mixing zones between them. Cheap, outdated and counterfeit technologies are most vulnerable, enabling cybercrime in 2024 to cost Asia as much as \$3 trillion per year. Ransomware, DDoS by IoT botnets, cryptocurrency fraud, industrial espionage, election interference—all are common, especially at the local level. Diverse technology limits the spread or scale of most attacks, but it also provides criminals with many smaller targets of opportunity outside the Great Firewall. Jumbled laws across different jurisdictions also provide safe haven for state and non-state actors to launch attacks and hide ill-gotten gains. In this scenario, data protection isn't imagined to be a top priority for hundreds of millions of people who are coming online for the first time. Even more than the American internet, the Chinese internet in 2024 owes its success to users willing to forgo privacy in exchange for access and convenience. The appetite for adopting digital technologies in this contested environment is a recipe for legal and illegal innovation alike.

Moving forward: strategic choices and challenges for Australia

The world that we describe would have serious implications for Australian cybersecurity. At least three lessons stand out in our analysis.

Australia will be caught in the fray

In this scenario, China remains the primary pillar of the Australian economy and the US remains Australia's security guarantor. Australia won't want to take sides, and with good reason. But the digital economy may prove more sensitive to geopolitical tension than other markets, in which case Australia could face tough choices in cyberspace sooner rather than later.

The costs of choosing either an American or a Chinese internet could be significant, though not equal. Not choosing could be costly as well. While a mediating, brokering or hedging strategy may prove the lesser evil, it may also make Australia the target of intense pressure. Domestic affairs could become a microcosm of fierce regional competition. Potential outcomes include foreign surveillance, censorship and the manipulation of Australian markets, networks and politics. Chinese platforms are particularly suspect, but American technologies aren't above reproach. How will federal, state and local governments respond in March 2024, for example, if mass student protests in Melbourne are manipulated through *WeConnect*? How much more difficult will whole-of-government policies and operations be, even at the federal level, if the tensions between cybersecurity and economics become increasingly pronounced?

29 November 2023

Australian Fintech Firm Shuttered: US Alleges Data Manipulated by China

The Sydney-based cryptocurrency exchange TransPacific Ledger (TPL) was forced to shut down last night, less than a day after the discovery of data irregularities in trading worth more than \$1.5 billion.

TPL suspended operations after the firm was implicated in the crash of blockchain backed indexes in the United States. Trading data brokered by TPL may have been manipulated in high-speed transactions between the US and China.

A darling of the Sydney start-up scene, TPL had been seen as a trusted and profitable intermediary between American and Chinese financial markets. 'We have a sales office in Hong Kong, we're fully licensed in Australia, and we comply with all US regulations,' said TransPacific CEO Ed Jones in an interview last month.

However, US cryptocurrency exchanges crashed on Monday when irreconcilable discrepancies were reported across several ledgers. 'TPL appears to be the common link,' according to the White House press secretary, 'but China is behind the bad data.' US intelligence officials point to recent advancements in Chinese quantum computing, claiming that these computers could hack the authentication protocols behind blockchain. 'Maybe this was an experiment that got out of hand,' said one anonymous source.

Beijing brusquely rejected these claims. 'False accusations accomplish nothing,' according to one government spokeswoman. Prominent voices in Chinese media are now blaming unnamed criminals in Australia and demanded their immediate extradition.

The Australian Securities and Investments Commission is working with the Australian Signals Directorate in its investigation. Neither agency was available for comment. The ASX lost 5% after news about TPL broke on Tuesday.

Please note: the above is a fictional article created by the authors for the purpose of this report.

By straddling both internets, both networks could be used to push and pull divisions in Australian government and society. Moreover, even if Australia tries to straddle the US and China, other countries in Oceania may decide differently. For instance, how will Canberra respond if Papua New Guinea, Bougainville and Solomon Islands bargain to adopt the Chinese internet in 2024 unless Australia increases development assistance to expand and maintain their undersea cables? In this scenario, Australia will have to decide how much it's willing to pay for its preferred strategy, both at home and around the neighbourhood.

Internet fragmentation isn't all bad everywhere

As costly as straddling or choosing between American and Chinese internets would be for Australia, this isn't a doomsday scenario. Some aspects of cybersecurity stand to improve inside each network. Harmonised standards and coordination across like-minded jurisdictions could improve incident response, information sharing (including vulnerability disclosure), patching and attribution. Technological diversity may increase at the regional and global levels, limiting the scale of any given platform and thus the extent to which attacks spread beyond any given country, region or bloc. Trust inside these networks may improve as well. For example, this scenario imagines that the average American in 2024 is relatively confident about US5G (despite expert debate about whether this network is demonstrably more secure than the Chinese alternative). Real or imagined, these security gains may make joining one club or another an attractive prospect for Australia.

Granted, the security gains inside each network are offset by friction between them. Australian policymakers will also bristle at claims by China, Russia and other authoritarian regimes that strict censorship and surveillance improve the security of their respective internets. Nevertheless, fragmentation or disintegration need be neither chaotic nor absolute. For better or worse, cross-fertilisation and ideological hypocrisy will occur as well, with American companies mirroring some of the practices used by their Chinese counterparts and vice versa.

The New York Times

Thursday, January 4, 2024

Mastercard and Walmart introduce a Social Credit System

Dismissing comparison to China, Walmart claims new system will help its consumers "live better" and "save money" during the US recession.

Please note: the above is a fictional article created by the authors for the purpose of this report.

Australia lives in a dangerous neighbourhood

The concurrent great-power transition and digital transformation of the region could be more turbulent than in any period in recent history. Tech giants will shape this transformation, but their commercial interests diverge from the public interest in Australian cybersecurity. In contrast to powerful corporations, international organisations such as the International Telecommunication Union appear even less impactful than usual in this scenario. Even multi-stakeholder organisations such as ICANN could be coopted or captured by commercial and geopolitical interests.

Tough choices

Australia isn't helpless in this environment, but it should prepare to help itself. Looking back, policymakers in 2024 may wish that preparation had started in 2019. Options include redoubling Australian efforts to champion an open, free and secure cyberspace in order to avoid the future imagined here. Advancing regional leadership, investing in capacity building and taking assertive action on shared interests may prove helpful. At the same time, however, policymakers should consider tough choices about cybersecurity in a less benign environment:

- Is Australia prepared to play hardball, not only with the US and China, but also with commercial tech giants, in order to advance its national interest?
- If forced to take sides or straddle the great powers, how should Australia choose, and how can it mitigate the costs of doing so?
- Even if there's no defining moment (for example, President Trump or President Xi declaring 'You're either with us, or against us'), is muddling through on issues such as encryption in Australia's national interest, especially if incremental decisions aggregate into a decisive choice?
- What, if anything, can Australia do to help the next billion users in Asia come online in ways that improve rather than undermine critical aspects of cybersecurity?
- And will a *laissez-faire* or, alternatively, compliance-driven approach to domestic cybersecurity suffice or prove lamentable in the years ahead?

These are important questions to answer, regardless of whether or not the scenario that we describe comes to pass. Scenario analysis doesn't need to provide accurate predictions in order to provoke strategic thinking about the future of Australian cybersecurity.

Notes

- 1 Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy*, Australian Government, October 2017, 7.
- 2 For background, see Pierre Wack, 'Scenarios: Shooting the Rapids – How Medium-Term Analysis Illuminated the Power of Scenarios for Shell Management,' *Harvard Business Review* (1985), 139-150; Peter Schwartz, *The Art of the Long View: Planning for the Future in an Uncertain World*, Doubleday, New York 1991; Naazneen H. Barma, Brent Durbin, Eric Lorber, and Rachel E. Whitlark, "'Imagine a World in Which': Using Scenarios in Political Science', *International Studies Perspectives* 17 (2016), 117-135.
- 3 For example, see National Intelligence Council, *Global trends: paradox of progress*, January 2017, [online](#).
- 4 Center for Long-Term Cybersecurity, *Cybersecurity futures 2020*, online; Jonathan Reiber, Arun M Sukumar, *Asian cybersecurity futures: opportunities and risk in the rising digital world*, Center for Long-term Cybersecurity, [online](#).
- 5 Among others, see William J Drake, Vinton G Cerf, Wolfgang Kleinwachter, *Internet fragmentation: an overview*, Future of the Internet Initiative White Paper, World Economic Forum, January 2016, [online](#); Scott Malcomson, *Splinternet: how geopolitics and commerce are fragmenting the World Wide Web*, OR Books, New York, 2016; Davey Alba, 'The world may be heading for a fragmented "splinternet"', *WIRED*, 7 June 2017, [online](#).
- 6 Graham Allison, 'The Thucydides trap: are the US and China headed for war?', *The Atlantic*, 24 September 2015, [online](#).

Acronyms and abbreviations

DDoS distributed denial of service

ICANN Internet Corporation for Assigned Names and Numbers

IoT internet of things

NATO North Atlantic Treaty Organization

Some previous ICPC publications



ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE



THE UNIVERSITY OF
SYDNEY

