What do Australia's parliamentarians think about cybersecurity and critical technology?

Gai Brodtmann, Dr Alexandra Caples, Danielle Cave and Jacinta Keast

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Policy Brief
Report No. 76/2023

About the authors

Gai Brodtmann is Chair of ASPI Council, former Member for Canberra and former Shadow Assistant Minister for Cyber Security and Defence.

Dr Alexandra Caples is Director, Cyber Technology and Security at the Australian Strategic Policy Institute.

Danielle Cave is Director, Executive, Strategy and Research at the Australian Strategic Policy Institute.

Jacinta Keast is an Analyst at the Australian Strategic Policy Institute.

Acknowledgements

Thank you to those who reviewed this research and provided input into the questions that were created for this study. Thank you also to current and former ASPI coordinators, interns and researchers Emilia Currey, Hillary Mansour, Joshua Dunne and Emily Williams for their energy, enthusiasm and drive that made this study a reality. Our future is in good hands with these exceptional young national security and public policy thinkers and leaders.

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 Cyber, Technology and Security

ASPI's Cyber, Technology and Security (CTS) analysts aim to inform and influence policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS remains a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and Internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity building team that conducts workshops, training programs and large-scale exercises for the public, private and civil society sectors. Current projects are focusing on capacity building in Southeast Asia and the Pacific Islands region, across a wide range of topics. CTS enriches regional debate by collaborating with civil society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on. If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Important disclaimer

ASPI

Tel Canberra: +61 2 6270 5100
Tel Washington DC: +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_CTS

First published November 2023.

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

No specific sponsorship was received to fund production of this report.

What do Australia's parliamentarians think about cybersecurity and critical technology?

Gai Brodtmann, Dr Alexandra Caples, Danielle Cave and Jacinta Keast

Policy Brief
Report No. 76/2023

Contents

Preface

In 2020, the then Director of ASPI's International Cyber Policy Centre, Fergus Hanson, approached me to research the views of the 46th Parliament on a range of cybersecurity and critical technology issues. The resulting data collection was then conducted in two parts across 2021 and 2022, with the results analysed and written up in 2022 and 2023. Those parliamentarians who 'opted in' completed and provided an initial quantitative study, which I then followed up on with an interview that explored an additional set of qualitative questions. The results, collated and analysed, form the basis of this report.

This research aims to provide a snapshot of what our nation's policy shapers and policymakers are thinking when it comes to cybersecurity and critical technologies. What are they worried about? Where are their knowledge gaps and interests? What technologies do they think are important to Australia and where do they believe policy attention and investment should focus in the next five years?

This initial study establishes a baseline for future longitudinal assessments that could capture changes or shifts in parliamentarians' thinking. Australia's ongoing cybersecurity challenges, the fast-moving pace of artificial intelligence (AI), the creation of AUKUS and the ongoing development of AUKUS Pillar 2—with its focus on advanced capabilities and emerging technologies (including cybertechnologies)—are just a few reasons among many which highlight why it's more important than ever that the Australian Parliament be both informed and active when engaging with cybersecurity and critical technologies.

We understand that this in-depth study may be a world first and extend our deep and heartfelt thanks to the 24 parliamentarians who took part in it. Parliamentarians are very busy people, and yet many devoted significant time to considering and completing this study.

This was a non-partisan study. Parliamentarians were speaking on condition of strict anonymity, without any identifiers apart from their gender, chamber, electorate profile and backbench or frontbench status. Because of that, the conversations were candid, upfront and insightful and, as a result, this study provides a rich and honest assessment of their views.

Gai Brodtmann

Executive summary

Some key conclusions can be drawn from the participating parliamentarians' attitudes towards critical technology and cybersecurity.

1. **Parliamentarians share common concerns about Australia's vulnerabilities and the capabilities and intentions of other state actors.**

In the cybersecurity domain, parliamentarians were primarily concerned about state-backed cyberattacks against critical infrastructure. They were next most concerned about the threat of state-backed cyber-enabled foreign interference. They ranked such attacks well ahead of other types of state-backed activity, including cyber espionage and intellectual property (IP) theft. State-backed cyber threats also caused them more concern than either non-state cyber threats or data breaches from poorly designed systems:

> '[I] have a lack of understanding of adversary capabilities—resources, time and personnel—on cybersecurity, particularly China. If there were a broader appreciation it would be easier to counter this area.'

Parliamentarians generally saw Australia's defence and intelligence organisations, defence industry and financial markets as cyber resilient. Conversely, many saw politicians' offices, political parties, state and territory governments and local councils as most vulnerable to malicious cyber actors—but still did not prioritise cybersecurity investment in those areas. Instead, parliamentarians prioritised cybersecurity investment into the water and sewerage sector, democracy and national identity institutions, and the energy sector, which were seen as currently having average levels of cyber resilience.

On risk mitigation, all participants agreed that the federal government should have a data management strategy for the public sector, and a majority supported a significant overhaul of the legacy ICT systems that support Australia's critical national infrastructure.

In the critical technology domain, participants largely agreed on the need for Australian sovereign capacity in specified critical technology sectors—including cybersecurity technology, quantum computing and AI—to secure Australia's national security and economic interests in a less certain geostrategic environment. Almost all participants also indicated that, where Australian sovereign capacity in critical technologies is lacking or unattainable, it's important for Australia to have access to reliable supplies from other nations.

Some parliamentarians either did not know what Australia was doing to shape international critical technology standards or did not think that it's doing enough. Opinions varied on how Australia could best shape global technology standards, from involvement in multilateral forums to having Australia focus its efforts on standards for biotechnology and AI. Some participants indicated that governments had limited influence on technology development and that Australia, in particular, was not a centre of global technology production.

2. **Parliamentarians need more education to understand and keep up with the pace of cyber developments and technological advancement.**

The study revealed a common concern that parliamentarians and policymakers are not educated on the nature, nomenclature and nuances of critical technology and cybersecurity:

> 'Everyone kind of knows about technology but they just accept it in the form that it comes to them. Policymakers need to know more about it, but that's the difficulty. We have got to find ways to explain it better.'

> 'Parliamentarians have a responsibility to lead the debate on this. There's a reluctance to engage in attribution, but we have to do more of it because we have to make it real for constituents. [We] need to raise [our] literacy levels and awareness about cyber.'

Parliamentarians noted both the importance and challenge of keeping pace with developments in the cybersecurity domain, and how important it is to guiding Australia's response to these challenges.

They openly admitted to being struck by how little they know about the opportunities and threats in those domains and how quickly those evolving fields are moving beyond their understanding. As one parliamentarian put it, Australian policymakers interested in deepening their understanding of cyber and critical infrastructure security 'don't know what they don't know' and rely almost completely on experts to provide digestible information and guidance:

> 'The best way of understanding is through connecting [us] with examples and showing how Australia is placed to handle it … [This is] an important area for parliament.'

> '[I] want to know more about all of it, and about what we know and what we don't know. Politicians should know more about this stuff.'

> 'It will be a generational change [among parliamentarians]. I think it's very difficult to get people to go 'back to school'. You see this in the very large discrepancy in knowledge and technological literacy. Some people have made an effort; some people just throw their hands in the air.'

3. **Parliamentarians see a need for an integrated national response.**

Parliamentarians agreed that state-backed backed cyberattacks on Australia's critical infrastructure are a priority threat. However, their views on priority sectors for investing in cybersecurity resilience varied greatly.

Nonetheless, they broadly recognised the need for Australia to keep pace with technological developments to ensure future national security and prosperity. They outlined broad approaches—aside from policy and regulation—required to underpin a national response to the challenges, including:

- developing an overarching integrated strategy to guide Australia's response, including a coherent approach to data management
- working with allies to set cyber and critical infrastructure standards and ensure ongoing access to critical technologies
- building sovereign capacity

- becoming more active in multinational forums through 'shaping' discussion and debate, not necessarily 'leading'
- reviewing our approach to foreign investment and free trade agreements to protect our sovereignty
- adopting greater flexibility and agility in legislative and regulatory approaches to cope with a rapidly changing environment
- improving the level of cyber awareness and literacy among the Australian public and parliamentarians.

This report sets out our research methodology and key findings, including 'deep dives' into thematic areas of most interest to parliamentarians and case studies on cybersecurity and critical technology investment priorities. It concludes with a detailed set of policy recommendations. The recommendations cover two key areas:

- creating an education program on critical technologies and cybersecurity for parliamentarians, drawing on government agencies, civil society and research institutes
- identifying and developing appropriate parliamentary mechanisms to actively engage on critical and emerging technologies, particularly on AI and AUKUS Pillar 2.

Methodology

This study used qualitative and quantitative data collection to gain insight into the participating parliamentarians' attitudes to two areas that are key to Australia's future: cyber security and critical technology.

Data collection for the study was conducted during a six-month window between October 2021 and March 2022. In October 2021, the then Director of ASPI's International Cyber Policy Centre contacted all 227 parliamentarians serving in both houses of the 46th Australian Parliament via email to request their participation in the study. ASPI sent out further rounds of invitations over the following six months, into 2022, to maximise participation.

The study was divided into three parts:

1. Quantitative component: a standardised set of questions completed by the participating parliamentarians independently in their own time (2021–22). Participants were asked multiple-choice questions, ranked preference questions and questions for which they were required to indicate their responses on a standard Likert scale, choosing between five sentiments from 'strongly agree' to 'strongly disagree'.
2. Qualitative component: a series of open-ended questions via one-on-one interviews with lead author Gai Brodtmann (2022).
3. Collation, analysis and write-up of the quantitative and qualitative data collected (2022–23).

The questions in the study were developed in consultation with cybersecurity and critical technology experts from the private and public sectors, academia and parliament. They were also designed to support longitudinal studies (for example, to conduct the same study for each parliament, noting that we're now in the 47th parliament).

The study posed 25 cybersecurity questions grouped around the following topics:

1. Investment in cybersecurity
2. Online threats and cyber resilience
3. Data management, ownership and storage
4. Cybersecurity policies and infrastructure
5. Public engagement on cybersecurity
6. Future challenges and responses
7. Areas of interest in cybersecurity.

The study then posed 21 critical technologies questions grouped around the following topics:

1. Investment in critical technology
2. Sovereign capacity in critical technology
3. Critical technology values and standards
4. Future challenges and responses
5. Areas of interest in critical technology.

In each case, participants were first asked to provide answers to each question based on a consideration of Australia's national security interests, and then to revisit the question based on a consideration of Australia's economic prosperity interests.

An ASPI research assistant or intern attended all interviews to scribe the participants' responses. Participants were provided with the qualitative questions in advance of the interview to assist with their preparation. Note that, while the study questions contain hyphenated terms including 'cyber-attacks' and 'cyber-security', this report and its graphs follow ASPI's style guide in not hyphenating compound 'cyber' words.

A full list of the study questions is in Appendix 3. Where participants did not answer the question, we have taken that as an indication of lack of knowledge, rather than lack of interest.

During the data-collection period:

- 24 parliamentarians—10.6% of the 46th Australian Parliament—took part in the qualitative study
- 18 of those 24 parliamentarians—7.9% of the 46th Australian Parliament—took part in the quantitative study.

On review, we're pleased with this participation rate, particularly given that the study was conducted against the backdrop of a looming federal election and the Covid-19 pandemic. However, we acknowledge that the sample size and demographics impose some limitations on this research, as outlined below.

Research limitations

'Opt in' studies frequently attract those individuals most interested in the particular subject matter. Parliamentarians who opted into this study were likely to have been those with more knowledge or experience of or interest in cyber and critical technology than their contemporaries. Future studies should seek to increase the sample size to increase confidence in the data.

Despite the small size of the sample, we find it to be sufficiently representative of the demographics of the 46th Australian Parliament. ASPI's sample includes representatives from across the political spectrum, and representatives from both the Senate and the House of Representatives.

ASPI's sample group reflected most of the demographic metrics of the 46th parliament (to within five percentage points). Seventy-one per cent of participants were from the House of Representatives and 29% were from the Senate—a sample close to the 46th parliament, in which 67% of parliamentarians served in the House of Representatives and 33% served in the Senate. Of those participants, 58% were backbenchers and 42% were frontbenchers or shadow frontbenchers. This is similar to that of the 46th parliament, where 62% were backbenchers and 38% were frontbenchers or shadow frontbenchers.

In terms of electorate classification, the ASPI sample contained a similar number of participants from 'inner metropolitan', 'outer metropolitan' and 'rural' electorates as the 46th parliament.

However, the ASPI sample had 12 percentage points more male parliamentarians (75% vs 63%), and parliamentarians from 'provincial' electorates were 10 percentage points higher relative to the 46th parliament. Further iterations of this study will seek to improve representativeness to better reflect the demographics of the parliament, particularly on gender and electorate classification. For further details on the demographics of the ASPI sample versus the 46th parliament, see Appendix 1.

Definitions and topics of focus

Cybersecurity

The Australian Cyber Security Centre (ACSC) defines cybersecurity as measures used to protect the confidentiality, integrity and availability of systems and devices and the information residing on them.[1] Where this report refers to cybersecurity, we're referring to issues including data protection, cyber resilience, cyber espionage and privacy.

The study questions addressed a range of issues but focused on cyber resilience in different sectors and where investment was needed to address vulnerabilities in Australia's infrastructure. Our definition of cyber resilience, guided by the Australian National Audit Office, was described as a measure of how well an organisation or individual can manage a cyberattack or data breach while continuing to operate effectively. We noted also that cyber resilience reduces the likelihood of successful cyberattacks.[2]

Critical technology

Critical technology is defined as technology that can significantly enhance, or pose risks to, Australia's national interests (including our national security, economic prosperity and social cohesion).

The critical technologies mentioned in the study were guided by the Australian Government's 2021 'List of critical technologies in the national interest' (later updated in 2023).[3] When this report refers to critical technology, we're referring to technologies including fifth-generation mobile technology (5G), quantum computing, AI, synthetic biology and the internet of things (IoT).

The study sought parliamentarians' views on how different critical technologies relate to Australia's national security and economic prosperity, and on our sovereign capacity in those areas. It also explored what critical technology investment should look like. Finally, parliamentarians were also asked for their views on future challenges in critical technology and the regulatory and policy responses required to address them.

Research findings: cybersecurity summary

Identified challenges

The parliamentarians listed a wide range of cybersecurity challenges facing Australia within the next five years. For most, the dominant challenges were:

- the lack of a 'whole of government' approach
- protecting Australia's democracy, society and critical infrastructure against cyberattacks and cyber-enabled political interference
- the need to increase cybersecurity investment and engagement with industry and the Australian public
- ransomware attacks
- Australia's lack of sovereign skills and workforce
- the need to educate and support the community to stay safe online.

Knowledge gaps

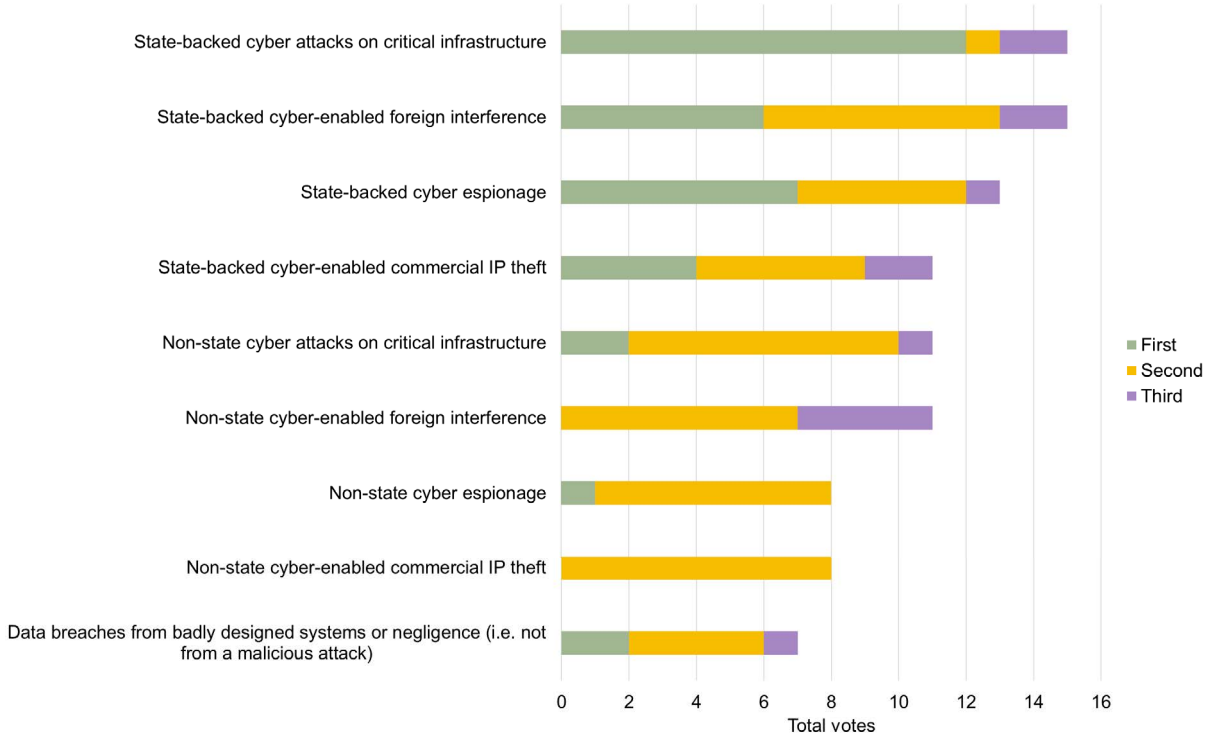
Parliamentarians were in strong agreement on the need for a national strategy, improved ICT systems and data management, but were mindful of their own lack of awareness in key areas, such as how cyber threats might manifest, current levels of cyber resilience across Australian government and industry sectors, and cyber governance arrangements.

Online threats and cyber resilience

Key finding 1: Parliamentarians saw state-backed cyberattacks on critical infrastructure as the most concerning cyber threat for Australia.

The study presented clear findings on parliamentarians' views of key threats in the cyber domain. Participants saw state-backed threats (attacks against critical infrastructure, espionage, foreign interference and IP theft) as being of greater concern than malicious cyber activity conducted by non-state actors (Figure 1).

Figure 1: On a scale of 1–3, please rank the top three threats you personally are most concerned about for Australia



Across the board—taking into account all state-backed and non-state-backed cyber threats—participants saw state-backed attacks on critical infrastructure as the most pressing threat:

> 'The world of "The Bourne Identity" [is] not as far away as we'd like to think.'
>
> 'I am not saying that there aren't non-state actors, but they are insignificant compared to the amount of effort being put in by states. China and Russia …'
>
> 'State by a mile. Simply because of the resources that a hostile state is able to bring to bear to the task.'
>
> 'I am more concerned about state-backed actors because of the scale of destruction that they can cause, but that shouldn't be confused with that I am not concerned about non-state.'

Participants also ranked state-backed cyber-enabled foreign interference as a prominent threat and common source of concern, followed by state-backed cyber espionage and then, slightly behind, state-backed commercial IP theft (perhaps regarded as a subset of espionage more broadly).

They ranked non-state-backed espionage and non-state-backed IP theft equally, and as less of a threat overall than state-backed activity:

> '[The main difference is] that organised crime is predominantly after money whilst foreign state actors are more after intelligence and the ability to cause massive disruption to their political enemies.'
>
> 'I think we're very exposed on industrial espionage and theft of IP. There's a constant attack on IP and we can't afford to lose control of it. We need to keep control of it and profit from it.'

However, some participants explicitly rejected this idea due to the capabilities of non-state actors as well as the increasingly blurred lines between categories of malicious actors within the cyber domain. Some parliamentarians were aware of the extensive role that contracted cybercriminal groups frequently play in state-backed cyberattacks.

‘It’s kind of one and the same now. [The] criminal organised crime element of cybersecurity I think is so intertwined with foreign state actors like China and Russia that you can’t draw a distinction anymore.’

‘[Some] governments are turning a blind eye or tacitly approving [illicit cyber] behaviour … Countries like Syria or North Korea … some eastern bloc countries … China and Russia.’

Interestingly, opinion varied greatly on data breaches as a security (note that the study’s data collection had concluded prior to recent and prominent data breaches, such as those at Medibank, Optus and Latitude). Data breaches garnered the lowest number of total allocations, but two participants ranked them as the greatest threat of all—equal to the first-place rankings allocated to non-state-backed attacks on critical infrastructure, and greater than the first-place rankings allocated to any other non-state-sponsored threat.

Key finding 2: Parliamentarians saw political parties, state and territory governments, local councils and individuals as the least cyber resilient sectors.

Participants were asked to provide views on the cyber resilience of the Australian government, business and public sectors (Figure 2), using the following definition of cyber resilience: ‘Cyber resilience is a measure of how well an organisation or individual can manage a cyberattack or data breach while continuing to operate effectively. Cyber resilience also reduces the likelihood of successful cyberattacks. Cyber resilience is measured on a spectrum and is achieved by having effective arrangements in place for managing cyber risks, by monitoring and reporting against cybersecurity deliverables and having a culture of cyber resilience.’

Figure 2: On a scale of 1–10, how ‘cyber resilient’ do you consider the following to be (1 being not at all cyber resilient and 10 being very cyber resilient)

In general, those participants who felt able to comment had more positive perceptions of the cyber resilience of Australian sectors less closely affiliated with the federal government. Within government, participants broadly regarded cyber resilience as weaker at the state and local levels of government than at the federal level.

The majority of parliamentarians saw defence and intelligence and defence industry as Australia's most cyber-resilient sectors. However, participants awarded those sectors average scores of 8.3 and 7.7 (respectively) out of 10, and less than 25% awarded a score greater than 8 to either sector. These results suggest a view that there's still some room to improve cyber resilience across defence and intelligence agencies and defence industry. Other federal government agencies received an average score of 6.0, just slightly above the aggregated mean score of 5.4:

> 'I'm not totally confident that the systems [in government] are secure. Are our networks that we're connected to fully secure? I'm not confident of that.'

Parliamentarians viewed the cyber resilience of other Australian government sectors less favourably. State and territory governments, political parties and politicians' offices all scored relatively poorly, between 4.2 and 4.3. Local councils' cyber resilience score of 2.7 was particularly dismal, over 32% lower than that awarded to any other sector (other than individuals). Over 25% of participants gave local councils the minimum score of 1.

Views on non-government sectors were more mixed. Participants viewed the financial services and markets sector as relatively cyber resilient, with an average score of 7.3, higher than any non-defence related sector. The space technology and data storage and processing sectors also performed relatively well, scoring 6.8 and 6.5, respectively.

However, participants assessed that the core utilities and services that underpin basic social and economic functioning were significantly less cyber resilient. Water and sewerage, health and medical services, transport and food all scored comparatively poorly. The transport and food sectors scored 4.9 and 3.9, respectively—among the lowest cyber resilience scores of any sector:

> 'Uplift across so many critical sectors in the private sector that haven't invested to protect themselves, their shareholders, customers, staff. They don't have cybersecurity [staff], they haven't resourced appropriately.'
>
> 'It's hard to justify [investing in cybersecurity infrastructure] until they're victim to a ransomware attack—and this is inevitable. They're naive and haven't prepared.'

Participants also indicated an awareness of cybersecurity risks associated with third-party providers to government and key sectors.

> '[Advanced persistent threat operators] are looking at service providers who are using immature servers, security. [It's] easy to find holes in it. The acceleration of increased attack … we're not keeping up with our defences. The more it's exposed, the more we're vulnerable for additional state, non-state penetration.'

Finally, participants were also asked to provide a cyber resilience score for 'democracy and national identity' institutions. Examples were included as a general point of comparison, including the Australian Electoral Commission (AEC) and the National Archives of Australia (NAA). Participants

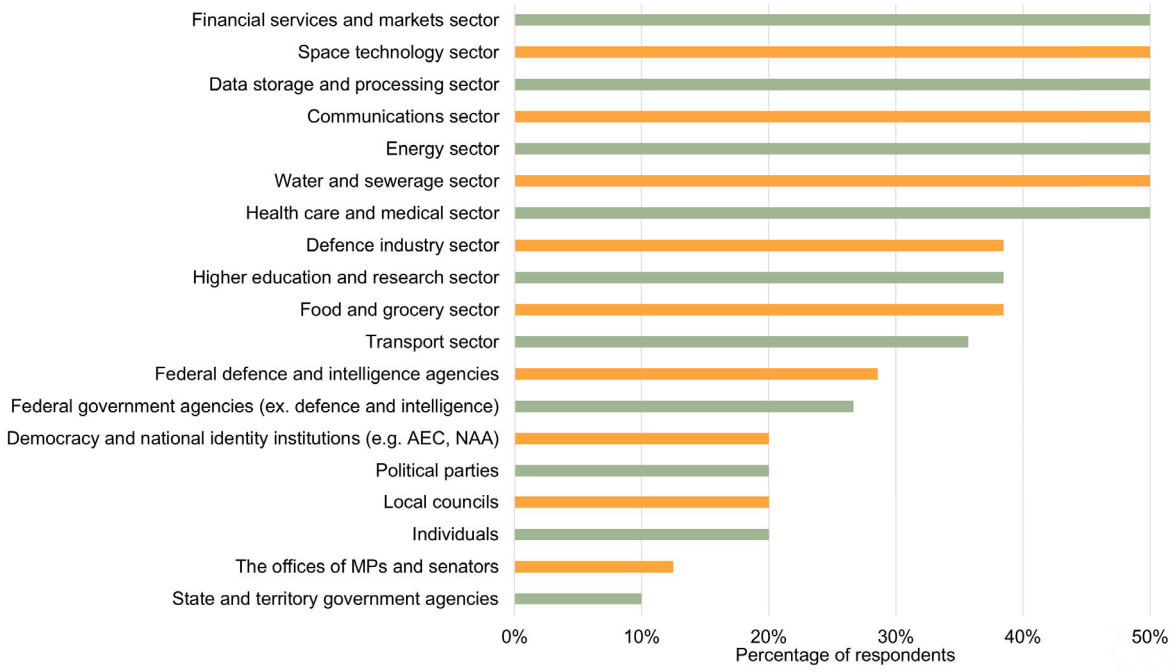
scored the cyber resilience of democracy and national identity at 5.7, which was broadly in the middle of the group. This suggests an awareness that cyberattacks can undermine democratic institutions and social cohesion; for example, through online disinformation campaigns.

> 'Electoral interference. This has been seen in other areas. In Australia it could influence a close election. That would be [a] massive threat to democracy.'

Key finding 3: A significant number of parliamentarians did not understand key sectors' resilience to cyberattack.

Several participants indicated that they lacked an understanding of cyber resilience across key sectors, in line with earlier comments about their inability to keep pace with cybersecurity threats and opportunities. Half of the participants indicated that they were 'not sure' of the cyber resilience of critical infrastructure sectors such as communications and energy, water and sewerage, or health care—and almost 40% were not sure of the level of cyber resilience of the defence industry sector (Figure 3).

Figure 3: Percentage of parliamentarians who answered 'not sure' for each sector in q. 14: On a scale of 1–10, how 'cyber resilient' do you consider the following to be (1 being not at all cyber resilient and 10 being very cyber resilient)



These clear results in an opt-in study suggest that such knowledge gaps extend to a much broader group of parliamentarians, many of whom will be asked to make policy decisions that inform or depend on one or more of those sectors. Fifty per cent of participants also indicated that they were 'not sure' about cyber resilience in the data storage and processing sector—a knowledge gap that has significant implications for live policy questions on data security.

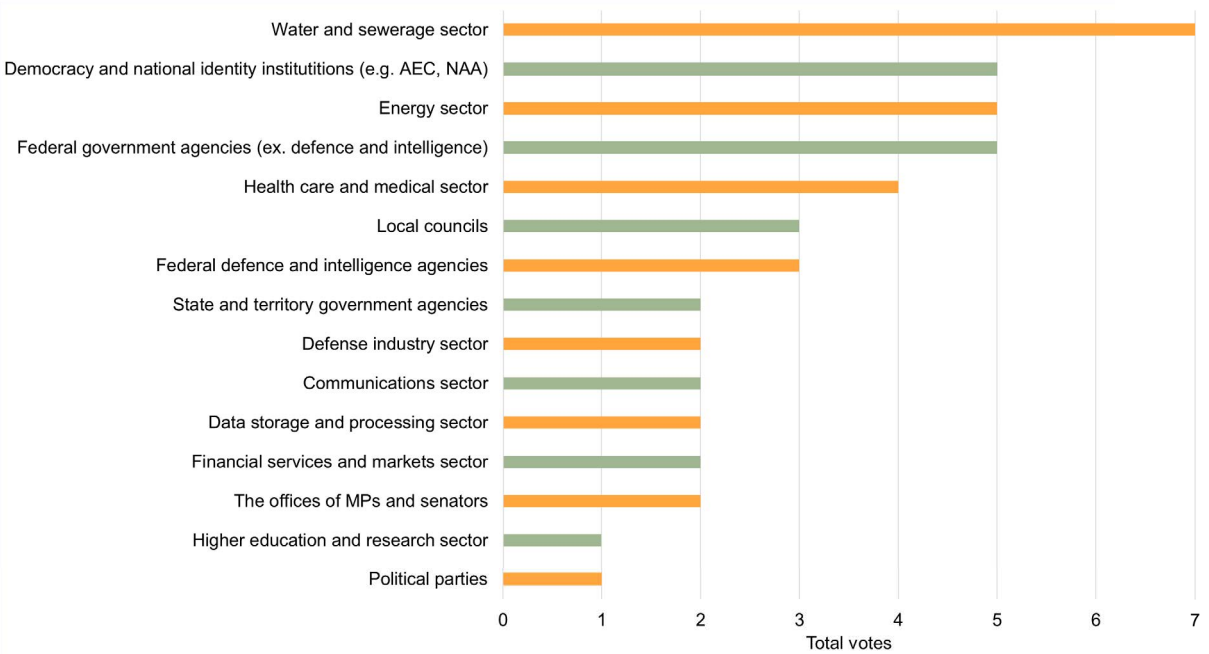
The study also revealed the wide range of views on cyber resilience among participants. For example, views on financial services and markets were mixed: 50% of participants were 'not sure' while the remainder considered the same sector to be among the most resilient.

Case study 1: Prioritising cyber resilience investment

Key finding 4: Parliamentarians saw critical infrastructure sectors, federal government agencies and 'democracy and national identity' institutions as priority areas for cyber resilience investment.

Participants were then asked to nominate three priority sectors for cyber resilience funding, selecting from those identified in Figure 3. Fifteen per cent of participants either did not address this question or answered 'not sure' or 'don't know' (Figure 4).

Figure 4: From the previous list, which three sectors should receive prioritised investment in the next 12 months to assist with improving their cyber resilience?



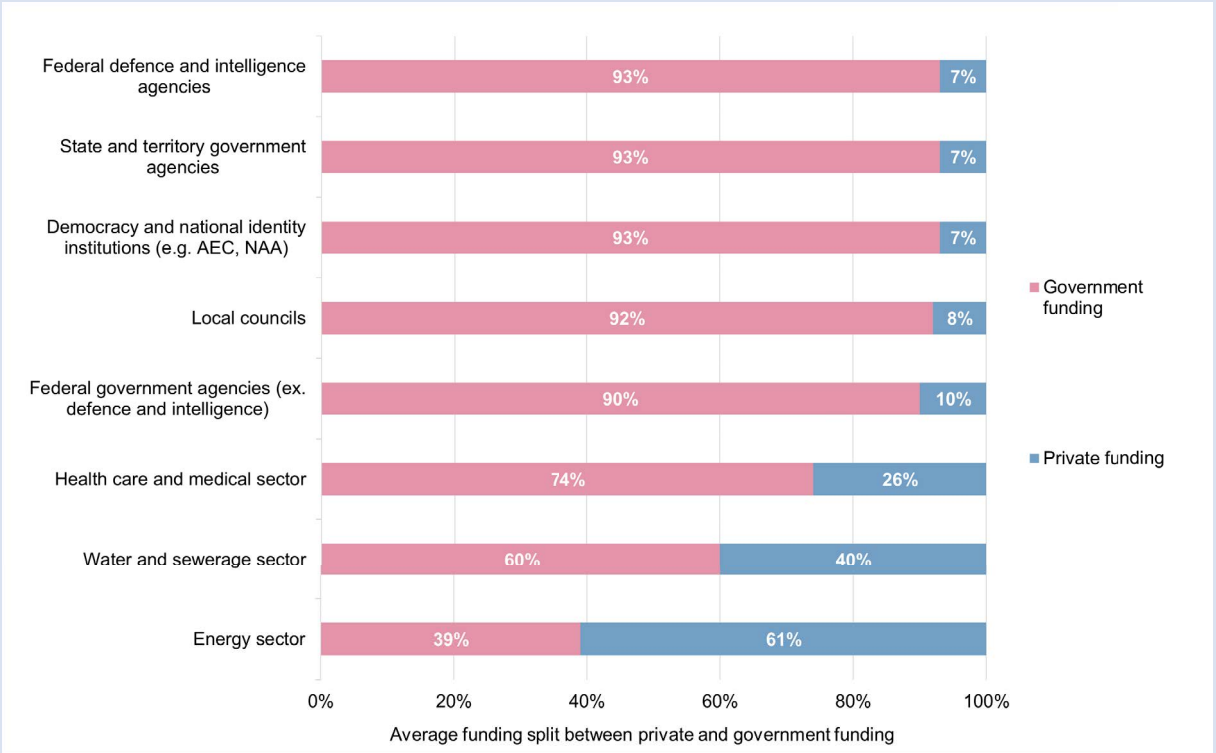
The top five sectors in which to invest in cyber resilience all fell below the average cyber resilience score in Figure 2.

The study suggests that participants place less importance on cyber resilience for state and territory governments, political parties and politicians' offices, and local councils. Despite poor or very poor cyber resilience ratings, none of those sectors was an immediate investment priority.

Key finding 5: Parliamentarians saw a need for public funding for cyber resilience in every (identified) sector (with the exception of the financial services sector).

Participants were asked to provide views on how to invest in cyber resilience in the three priority sectors they had individually identified. They allocated investment on a continuous scale—from 100% private investment to 100% government investment—in each of their three priority sectors. Figure 5 displays only those sectors that received at least three nominations in the previous question (see Figure 4), to ensure an adequate sample size for analysis.

Figure 5: Of the three sectors you selected above, please indicate on the scale below where you believe this investment should come from



Broadly, participants' funding allocations reflected traditionally accepted views of the government's role in a deregulated economy. Public funding was allocated to sectors historically seen as being the responsibility of government, and private funding to those sectors in which government often takes a more 'light touch' regulatory role.

Unsurprisingly, participants allocated majority public funding (over 90%) to federal government agencies and the defence and intelligence sectors. Participants who allocated a percentage of private sector funding to those public-sector entities may have had industry contributions in mind. Reflecting a sense of shared industry and government responsibility in those sectors, utilities (water and sewerage, and energy) and the health care and medical sector received a greater investment allocation towards private funding (note that this study was conducted before the 2022 Medibank data breach).[4]

Key finding 6: A third of parliamentarians never feel personally safe online against scams or cyberthreats.

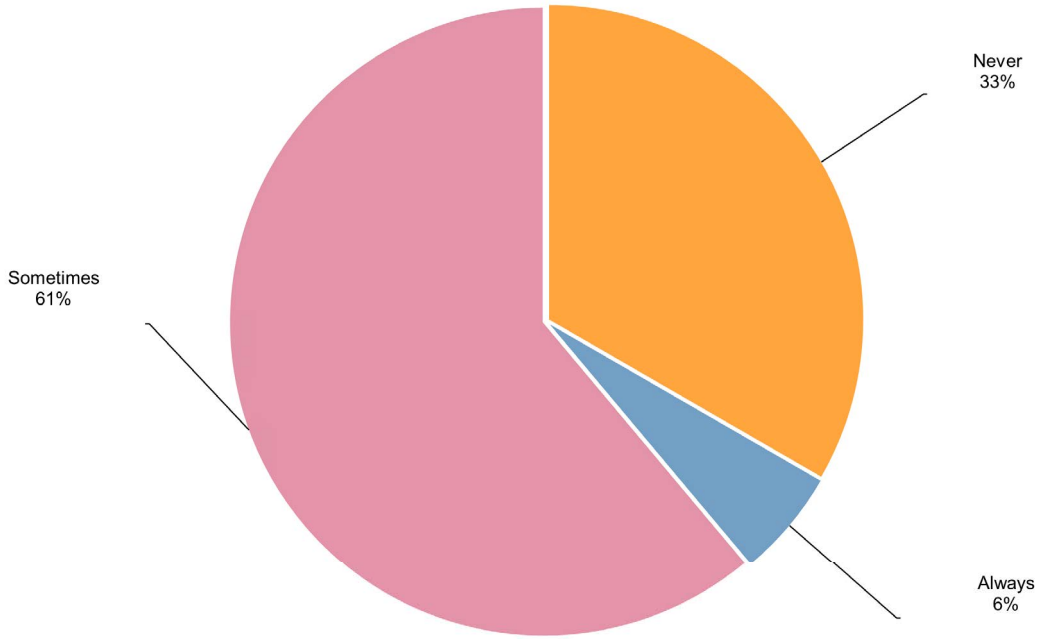
Participants were asked whether they personally felt safe online. More than a third of participants suggested that they never felt safe online against scams and/or cyber threats (Figure 6). When asked about the kinds of scams and cyber threats they worried about, participants named a range of possibilities, including cyber espionage:

> 'I treat my mobile phone as if it's an open line of communication to the CCP, because that's basically what it is.'
>
> 'I assume I'm bugged, so I won't say anything on text to give away a national secret. I use encrypted apps. I know what we do. I'm aware of what can be done, and assume it's being done to me.'

Some parliamentarians were concerned about their personal data being accessed:

> '[I'm] worried about my personal information … a lot of data has been sitting on Facebook or Insta or WhatsApp. I worry that that information is held by overseas companies. I worry about this a lot. I don't feel safe much at all when I'm online. It's something I think a lot about at the moment.'
>
> '[I] feel reasonably safe at work, but not 100% sure what's going on at home. Accessing our systems, privacy, two different schools. Not sure how secure things are at home.'

Figure 6: Do you personally feel safe online against scams / cyber threats?



Data management, ownership and storage

Key finding 7: Parliamentarians unanimously agreed that the Australian federal government should have a public sector data management strategy.

Despite a 100% agreement on the need for a national public-sector data management strategy, (noting there is now a draft strategy under consideration)[5] participants offered a range of justifications that ultimately came down to consistency, privacy and security.

Ensuring data is managed consistently:

> '[We] need central government articulating what [data management] is, [to] make it clear. There are many departments that don't understand it and don't prioritise it and don't realise how vulnerable they are.'
>
> 'We need a single standard that provides clarity and consistency and reduces the gaps that [malicious] actors can exploit. The more gaps, the more vulnerabilities we have, the more opportunities there are for us to get it wrong.'
>
> 'It just seems to be a matter of common sense. Why wouldn't you have a strategy? It's changing so fast, so volatile, it's complicated. You must have a strategy. In an area that's changing so fast and so volatile, hoping for the best just seems daft.'

Federal government standard setting:

> ‘How else are we going to keep on top of the regulations? Someone’s got to lead with it. And it’s definitely up to the federal government to show the public sector how they should do it.’
>
> ‘[Currently], the [private] tech sector is driving what should be there, and it’s just really fractured, and they’re not really addressing real needs—it’s fragmented. Fragility means there’s more opportunity to stay involved … There’s atrophy here. It’s a really big issue.’

Protecting Australians’ digital privacy and identities:

> ‘I’d feel much better about our data and sensitive data being stored and controlled locally and covered by our own data-protection law and not at the whim of a foreign actor that can access and change that data. If [data] is not controlled, you’re opened up to vulnerability.’
>
> ‘… the identifiable citizen-related data that is gold for people who want to make a profit and do us harm … [The] citizen ID parts are what we’re most concerned about.’
>
> ‘Privacy laws being impacted by overseas actors … Privacy law is being enforced by contract.’

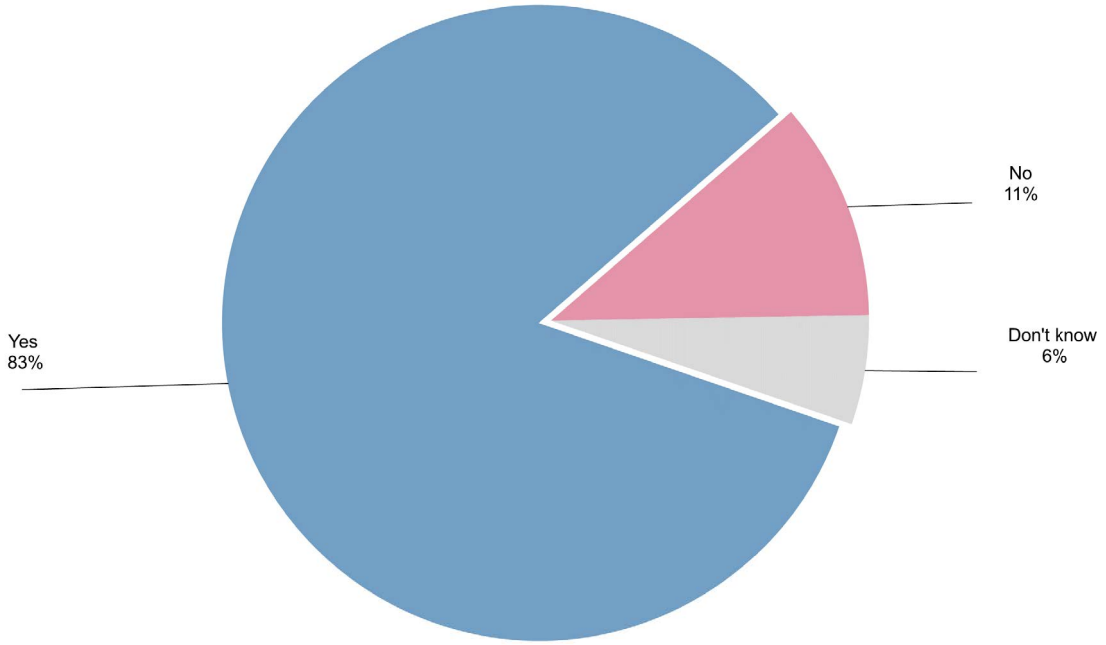
Protecting Australia’s national interests:

> ‘If you can’t control your data, you’re not really sovereign.’
>
> ‘[There are] too many exposure points. [A data management strategy] won’t remove them, but it will minimise them.’
>
> ‘Data that could have an impact on our prosperity and national security. There does need to be clear guidelines of what classifies valuable data. We need to weigh up the risk and benefit—how we define “valuable data” is subjective.’
>
> ‘Yes, the high-security material [must] be regulated very closely … Things that could be attacked and affect wider society should be more protected.’

Key finding 8: The majority of parliamentarians indicated that a federal data management strategy should include both the public and the private sectors.

The majority (83%) of participants indicated that the federal government data management strategy should be comprehensive, including both the public and private sectors (Figure 7).

Figure 7: Should the federal government have a data management strategy for the private sector (i.e. critical infrastructure operators)?



Participants generally echoed many of the same priorities for a comprehensive data management strategy as were offered for a stand-alone public-sector strategy. They noted the value of large datasets and disparities in the way data is handled across government, the private sector and the community:

> '[The] private sector actually has more data on citizens than the government. We go to big lengths to protect citizens with the COVID safe app [because of] concerns that government shouldn't know things about citizens, yet citizens share [similar] things on Facebook … There's so much data held privately so they should be under some sort of regime as well.'

They also acknowledged interdependencies between government and the private sector on cybersecurity:

> 'If [a private entity] contract[s] or provide[s] services to the government, then [it] should be signing up to a degree of cybersecurity.'
>
> 'Non-state criminal actors weaponise these systems—critical infrastructure, utilities, banking—and they bring them down and can still cripple a nation.'
>
> 'Yes, [we need] a framework and guidelines, and standards. Because [private entities] are more susceptible, and the last resort in countermeasures comes back to government anyway. They're the safety net; they should operate on regulations.'

Key finding 9: Parliamentarians held a range of different views on the role of government in developing and implementing federal data standards.

Those participants who supported a comprehensive data management strategy generally agreed that the government should play a role in setting standards but held a range of views on whether and how the government should provide practical support:

> 'The private sector is actively looking for guidance in this space. I do think that they want guidance in this space and the federal government should be clear in what industries they want to host data in Australia.'
>
> 'The private sector should do this for its own benefit, and banks, finance do, but it's so important that the government should have a role and help in making sure that there is one. It will also support the small to medium enterprise sector who may not have the wherewithal to do it.'
>
> 'I think there's an obligation of the government to say "this is the level we think you should be", because some people just don't understand how vulnerable their businesses are.'

Those participants who argued against a comprehensive data management strategy questioned the need to impose the same or similar data management standards and responsibilities on the private sector:

> 'The question is, should the same [data management] impositions be made on businesses that don't have anything to do with the federal government?'
>
> 'I think that [I] probably wouldn't go far as to say that businesses ought to be required to have [the same] level of security [as government].'

Data storage

Key finding 10: The majority of parliamentarians indicated that classified government data and identifiable citizen-related data should be stored on servers located in Australia.

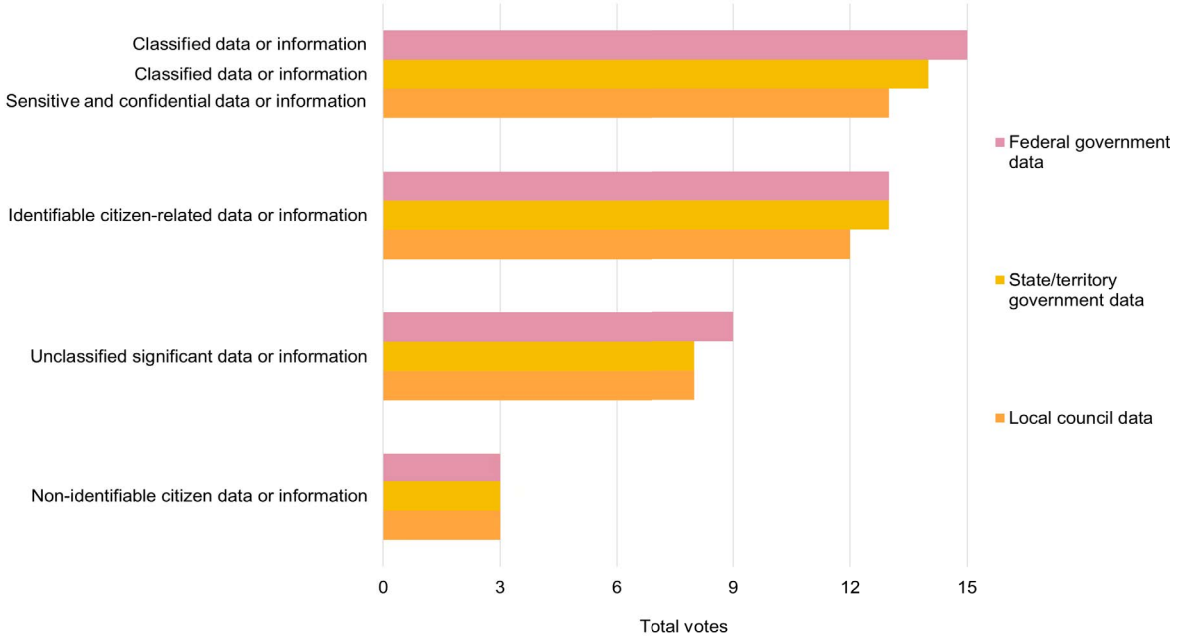
Participants were asked to consider 'jurisdictional risk'—the idea that offshore servers under the sovereign jurisdiction of another country are subject to the law of that country. They were not specifically asked about, for example, the risk of remote access to servers located in Australia, insider threats, or secure cloud alternatives.

On that basis, participants' views on the types of data that required mandatory storage were consistent across all levels of government (Figure 8).

Most participants agreed that it should be mandatory to store classified or sensitive government data on Australian servers—83% for federal government data, 78% for state and territory government data and 72% for local council data.

Identifiability appears to be a key factor in determining data-security priorities. Participants also put a strong emphasis on storing identifiable citizen-related data on servers located in Australia. In contrast, only 17% of participants thought it should be mandatory for federal non-identifiable citizen-related data to be stored on Australian servers.

Figure 8: What types of [federal government / state/territory government / local council] data should it be mandatory to store on Australian servers?



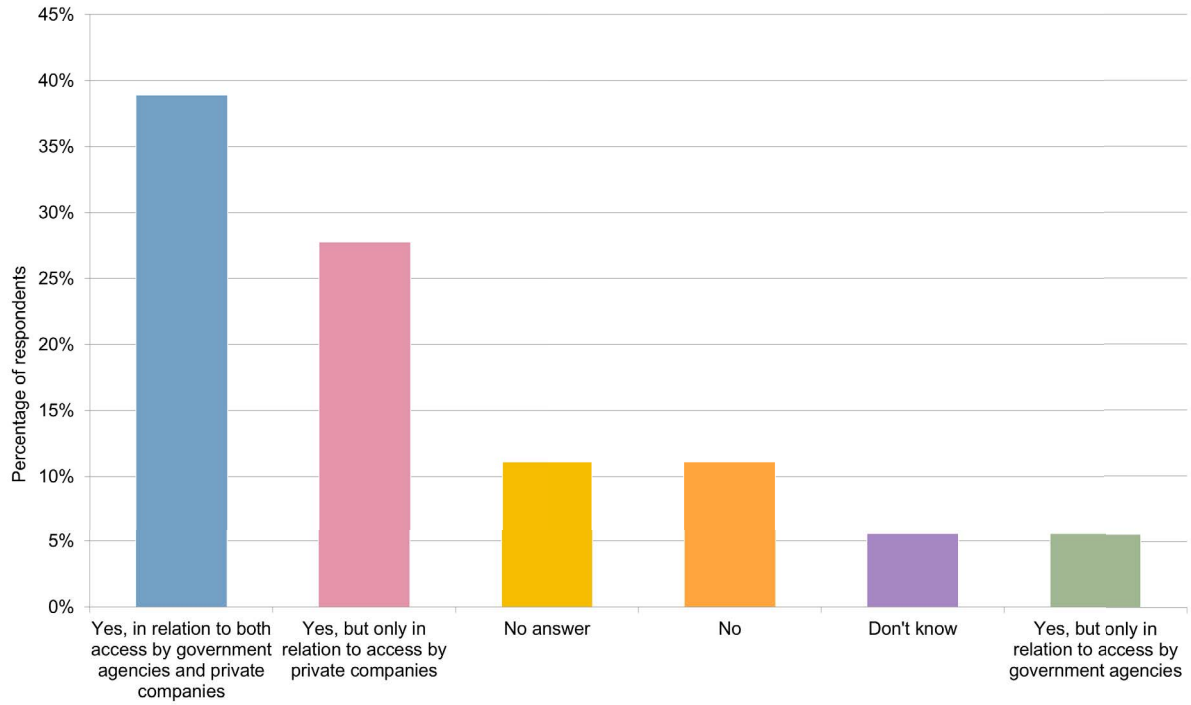
Note: Only the federal government and state and territory governments use and store 'classified data or information'. The highest data category for local governments is 'sensitive and confidential data or information'. Those two categories are amalgamated here on the basis of equivalence, and intended to provide a basis for comparison across three tiers of Australian government.

Data ownership

Key finding 11: Parliamentarians were divided on who should 'own' Australians' personal data.

The question of data ownership split those participants who indicated a preference (11% of participants did not respond). Thirty-nine per cent agreed that Australians should own and manage access to their personal data in both private and government contexts, while a further 28% supported Australians' right to approve the information that private companies can access (Figure 9). This suggests that more than a third of participants believe that the government should not be able to access personal data without an individual's authorisation, but also that the government has a greater role as a data regulator or 'watchdog' than private corporations.

Figure 9: In Estonia, citizens own their personal data and approve the information that can be used by government agencies. It is a criminal offence for government agencies to access unauthorised personal data. Should Australians own their personal data?



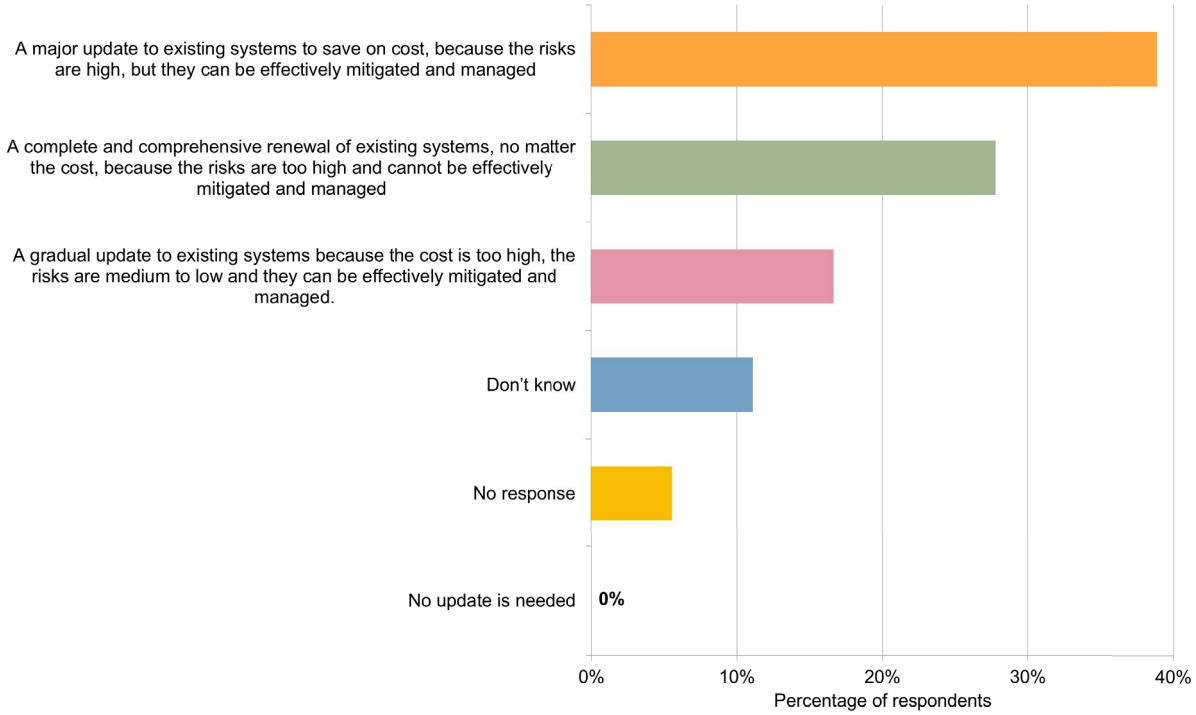
Cybersecurity policies and infrastructure

We've noted that parliamentarians viewed attacks on critical infrastructure as a significant threat. This section of the report explores participants' views on the vulnerability of critical infrastructure sector systems—and on responding to ransomware attacks, which are commonly aimed at critical infrastructure sectors.

Key finding 12: Every participant agreed that legacy ICT systems supporting critical infrastructure should be updated.

Eighty four percent agreed that existing critical infrastructure sector ICT systems need some sort of upgrade, although they held different views on the scale and speed required (Figure 10). More than a quarter of participants (28%) indicated the need for a complete upgrade to legacy ICT systems supporting critical national infrastructure, no matter the cost. A slightly larger group (39%) agreed that major updates should be undertaken, provided such updates were 'cost-effective', which may reflect their views on the relative risk posed by legacy ICT systems, the importance of fiscal responsibility, or both. Only a small number of participants preferred the most conservative of the available options—a gradual update of existing systems (16%—less than the percentage of those who did not answer the question). These results suggest that parliamentarians from across the political spectrum are broadly aware of potential critical infrastructure vulnerabilities.

Figure 10: In your opinion, when it comes to legacy ICT systems that support critical national infrastructure, what is the best way to manage these from a cybersecurity perspective?

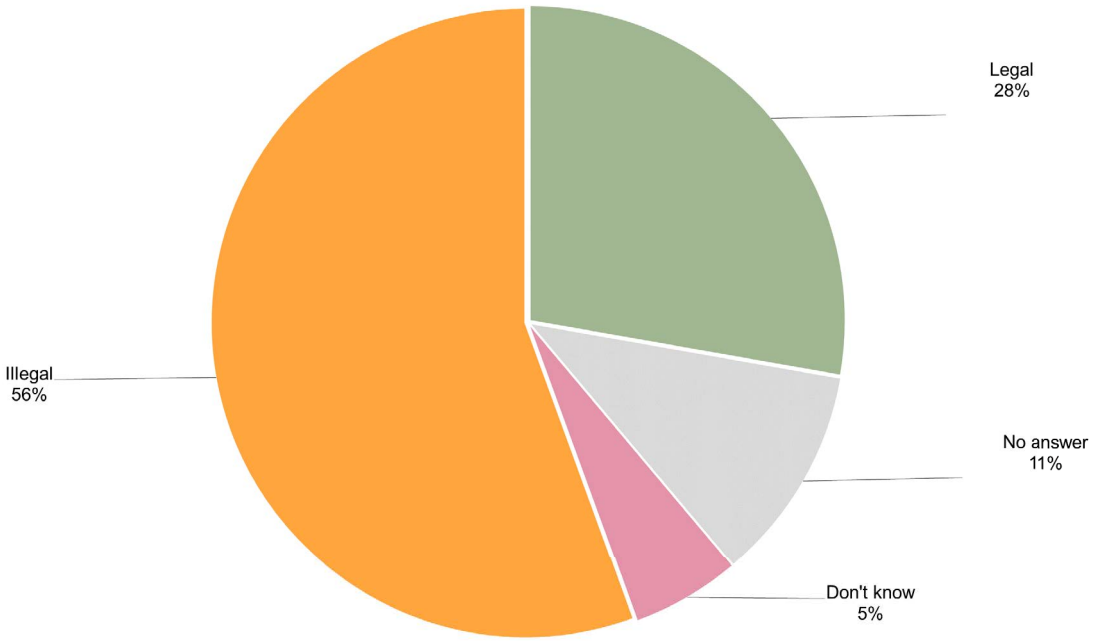


Ransomware and response

Key finding 13: Parliamentarians were polarised on how to respond to ransomware attacks.

Participants were divided on whether ransomware payments should be legal or illegal. A slim majority of participants (56%) indicated that paying ransomware demands ought to be illegal (Figure 11).

Figure 11: Should it be legal or illegal in Australia to pay ransomware demands?



Their justifications for prohibiting the payment of ransomware demands in Australia were primarily philosophical, rather than based on the consideration of individual cases:

> 'We don't pay ransoms to terrorists—[it] should be the same in the physical as the virtual world. [We] don't pay ransoms or [else] it turns it into an industry, a lucrative crime. It's the same in the physical as in the virtual world.'
>
> 'There are expectations on industry. There is a prevention strategy we can use to minimise opportunities for ransomware. The onus is on us.'
>
> 'If our technology and defence is good enough, we should be able to withstand it … Intelligence and countermeasures should be good enough to prevent ransomware attacks.'

Some argued that a total ban on the payment of ransomware demands in Australia was complex and premature, and could in fact undermine Australians' interests:

> 'If we [enacted] an outright ban, people would die. There are lives on the line.'
>
> 'We will eventually illegalise [paying ransomware demands], but we can't do that yet—a gradual shift into illegal in the next five years. We need to give people warnings and get the message before we make it illegal.'
>
> 'As a legislator and a policymaker—the long-term implication would be to stop a market for that by making it illegal. But this means serious implications for the people who are caught out first.'

These participants made the case for regulation and visibility:

> '[There] should be mandatory reporting though, even if confidentially to an agency on the demand, data, resolution.'
>
> 'I think you can discourage [ransomware]. I am much more interested in managing it. What we do want is to know about it, [then] put in precautions and defences. If private corporations and private citizens are attacked and paying it without telling anyone, then we don't know the scale of the problem.'
>
> '[The] US has a sophisticated strategy on [ransomware] payments made by crypto, then law enforcement can get involved … We need to regularise it and structure it, but not ban it. We can have a coordinated response.'

Regardless of their views on ransomware, participants generally acknowledged the complexity of this issue and the need for expert attention and consideration:

> 'It's a very tough policy question … if you pay someone that is holding you to ransom for money, you're only encouraging them to do it further to you or to another person. There's nothing to say that if you pay the ransom that you'll get control back of your data.'
>
> 'It's an incredibly difficult policy to land on but people who have been impacted upon just want it back. It's a very difficult policy decision for the government to say that if you do pay that you're breaking the law. [It's a] vexed question.'
>
> 'I'm not 100% confident in this because it could be so bad for someone, but [the] principle of paying extortionists is the road to hell … [I feel] bad for the companies that would be taken to court [and] protective of the victims, but [I feel] like [the federal government] should send a clear message.'

Some drew a distinction between ransomware attacks against government entities and those against the private sector:

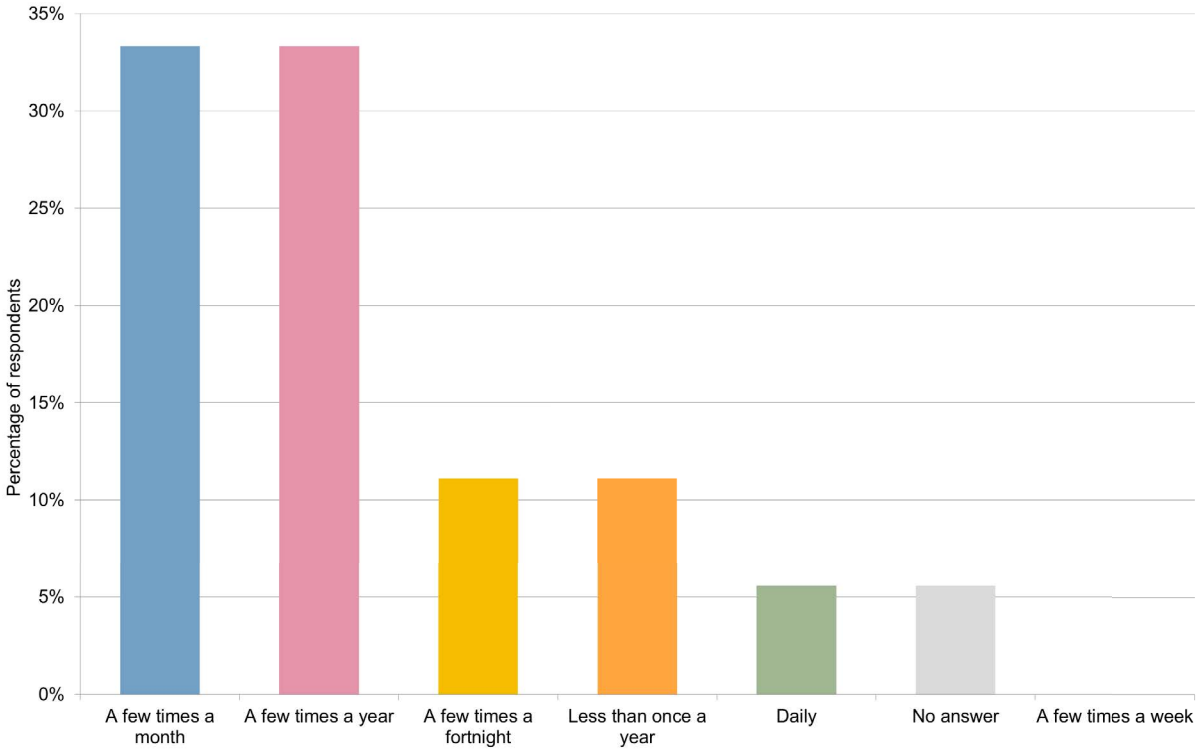
‘It [could] be harmful if you made [paying ransomware demands] illegal. Company directors would ruin their fiduciary responsibility to their companies. Company law is the number one priority. And keeping [them] solvent.

‘I’ve got a problem with ransomware demands. Our protections are not adequate … If you protect yourself sufficiently you won’t be in that circumstance … If it’s just the government, the real problem is private companies, it’s like “go away” money, and that’s the end of it.’

Public engagement on cybersecurity

Participants displayed a wide variety of different responses regarding how often they are engaged by the public on issues relating to cybersecurity (Figure 12). Two-thirds (67%) of participants indicated they were engaged a ‘moderate amount’, either a few times a month (33%) or a few times a year (67%). A much smaller number of parliamentarians (17%) reported being engaged more frequently than a few times a month, while 11% are engaged less than once a year.

Figure 12: Which one of the below comes closest to describing how often you are engaged by constituents and industry on issues relating to cybersecurity?



Participants reported that, although they’re sometimes contacted about ‘cyber interference [and] concerns about China’s foreign interference’, concerns about scamming and personal privacy online typically dominate constituents’ engagement with their federal representatives:

‘… Individuals being scammed. Romance scams. People who have given money even after being told not to.’

‘Scams: they’ve heard of them, come across them. Rarely, they’ve been scammed, but usually it’s just that they’ve been contacted by a fake thing. [They] wonder what the government is doing about these issues.’

‘Constituents worry about their data and are concerned about who has their private information.’

In contrast, industry engagement focuses on business opportunities, legislation and workforce challenges:

> 'Industry stakeholders approach [parliamentarians] for one of three [reasons]: [First,] to sell a product—tech, chip, black box, etc … these are irregular. [Second,] people who don't like the form of legislation [because] it's too intrusive, it'll cost them too much. [Third,] people who want to work in defence.'
>
> 'Businesses want to get a share of cyber. [Industry representatives] usually want information … [or] financial support from government.'
>
> '[Business representatives] talk about workforce issues and what they want to do as private industry to help.'

The need for a national response: cybersecurity governance

Participants were asked to outline those agencies or departments they believed are responsible for cybersecurity issues. Study results likely reflect respondents' own exposure and experience, and reflect a degree of uncertainty about cybersecurity governance. Half of the participants indicated that they see one federal government department or agency as having lead responsibility for cybersecurity issues (Figure 13). A third of participants indicated that there is no lead department. The remaining 17% of participants either didn't know or didn't answer the question. In a follow up question (Figure 14) views varied on which agency—or agencies, noting many participants wrote down multiple answers—has the lead responsibility for cybersecurity issues.

Figure 13: From your perspective, is there a federal government department/agency that has the lead responsibility for cybersecurity issues?

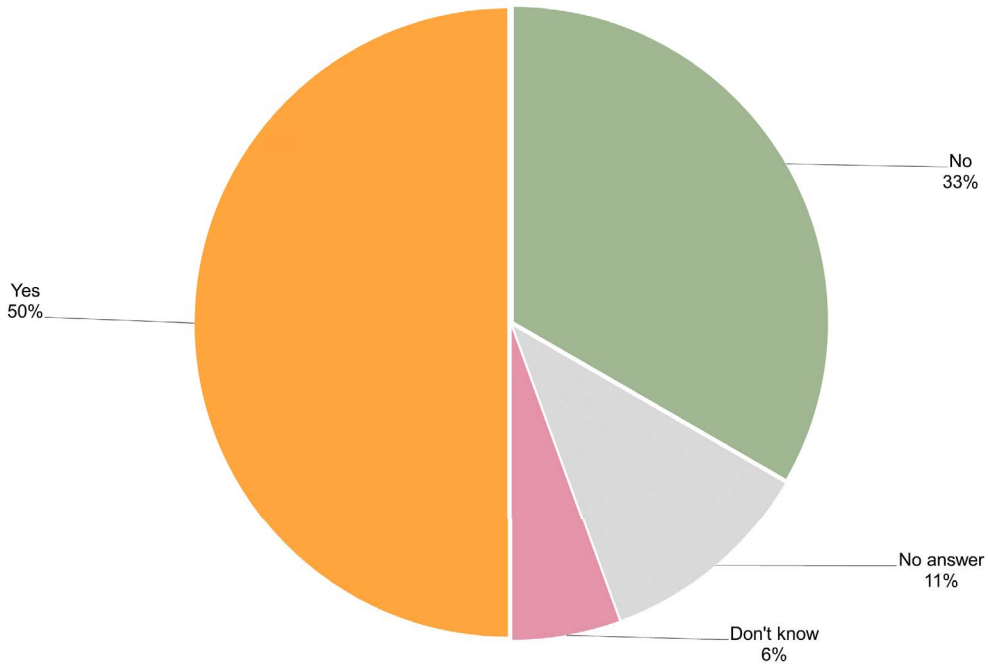
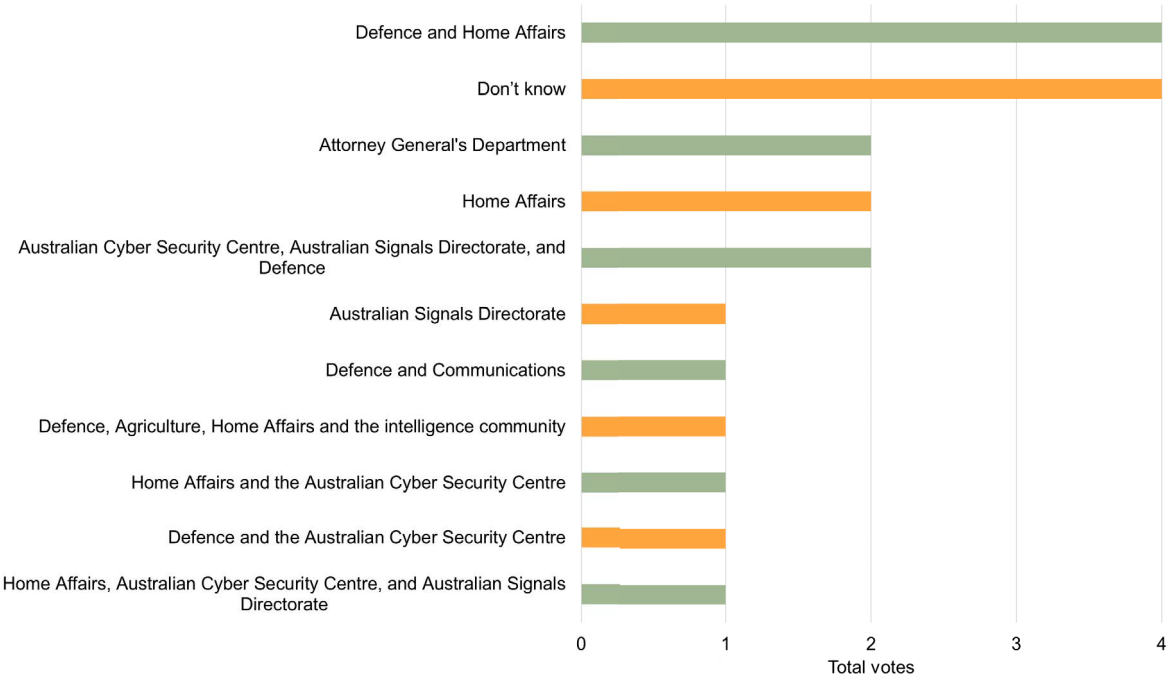


Figure 14: If you answered 'yes' to 'Is there a federal government department/agency that has the lead responsibility for cybersecurity issues?', please state which government department that is



Participants who provided views on the current lead federal government agency and completed a follow-up interview were then asked to provide views on which agency they thought should take the lead (Figure 15). Most participants were unsure, which might indicate uncertainty on either the scope of cybersecurity issues that need to be managed or the capacities of different departments and agencies. Equally, it may be an acknowledgement of the real complexities of cybersecurity governance. In each case, participants selected an agency, or combination of agencies, with existing national security responsibilities.

Figure 15: From your perspective, which federal government department should have the lead responsibility for cybersecurity issues?

Research findings: critical technology summary

Identified challenges

Participants were asked what they saw as the biggest challenge facing Australia regarding critical technologies in the next five years, and why. According to participants, the major critical technology challenges facing Australia are:

- our ability to become self-sufficient and develop sovereign capabilities
- Australia's ability to keep up with the competition
- the need to better educate parliamentarians on the changes and challenges
- the need to develop a cross-sectoral, strategic approach to responding to these challenges
- ensuring that Australia's critical technology sectors reflect our values
- foreign interference in Australia's democratic process and the resilience of our democracy to assault by adversaries equipped with emerging technologies

Participating parliamentarians also identified challenges in developing and harnessing specific technologies, such as space and hypersonic technologies, AI and robotics.

Knowledge gaps

Parliamentarians openly noted that they lacked sufficient education in most, if not all, critical technologies addressed in the study:

> 'Nearly all of them. This is not something that gets talked about among parliamentarians … It's not in submissions.'
>
> 'Critical technology isn't put before parliamentarians. It's not discussed. I think building a definition of what these technologies are and what they mean, and then talking specifics on Australia's capabilities, should itself be the objective.'
>
> '(I) want to know more about all of it, and about what we know and what we don't know. Politicians should know more about this stuff.'
>
> '[These are] globally significant issue[s], and politicians should know what Australia's capabilities and knowledge base are.'

Four critical technology sectors stood out in the study responses due to the parliamentarians' particular and persistent reference to them:

1. Quantum technology, computing and engineering

   'I read and see that it's something that there is a lot of Australian interest and activity in, but I couldn't explain it to you.'
2. Artificial intelligence

   'The role that AI will play across our economy, [both] opportunities and risks.'
3. Cybersecurity technology

   'We [parliamentarians] are probably getting most of [our] cybersecurity information [from] Hollywood.'
4. Critical infrastructure, particularly energy infrastructure

   '(The) energy space is *du jour* and I'm interested in it … We've got a long way to go.'

Critical technology standards and sovereignty

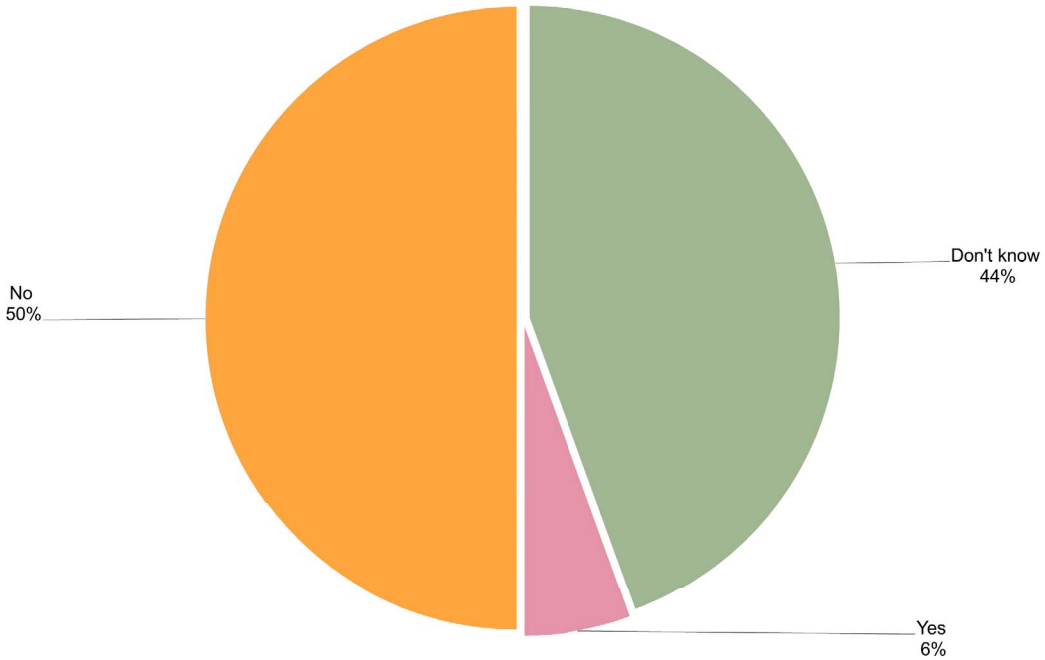
This section looks at parliamentarians' attitudes towards priority critical technologies—Australia's role in setting international standards, whether technology is value free, foreign investment and sovereignty.

International standards

Key finding 14: Parliamentarians either don't know what Australia is doing to shape international critical technology standards or don't think it is doing enough.

While participants' levels of engagement with the other questions concerning values and standards were relatively high, Figure 16 indicates that nearly half (44%) of participants don't know whether Australia is doing enough to shape international critical technology standards. Among the remaining 56% of participants who responded either 'yes' or 'no', participants demonstrated a very strong consensus. Only one participant indicated that Australia is doing enough to shape international standards, representing a mere 6% of the total sample of parliamentarians. The remaining 50% of participants (and the overwhelming majority of those who answered the question) indicated that Australia isn't doing enough. Those participants who answered 'don't know' may care about international standards but lack regular exposure to those negotiations. Those who answered 'no' may have done so for a range of reasons, but Australia's lack of influence in this space emerged as a key theme.

Figure 16: Do you personally believe Australia is doing enough to shape international standards on critical technologies?



Key finding 15: Parliamentarians believe there are limits to Australia's influence over international technology standards.

Several parliamentarians noted their belief that there are limits to Australia's influence in setting international technology standards, both because governments play a limited role in technology development generally and because Australia is not a global technology producer. Perhaps as a consequence, some study participants, when questioned further, viewed the government's role as establishing expectations and governance arrangements for international standard setting, to shape specific outcomes. Even if Australia did not take the lead, multilateral forums were considered appropriate mechanisms either for shaping standards:

> 'We're improving at getting involved in the multilateral forums that set these standards, from the International Maritime Organization to critical technology.'

or to prevent other actors setting standards that might disadvantage Australia:

> 'Telco standards and bodies are well attended by strategic rivals. But there are no Australians at the industry standards forums for telco and IT. Telco and IT—we need more Australians in those areas.'
>
> 'Participating and engaging in contested elections for those forums, organising like-minded democracies to ensure candidates for positions in multilateral forums aren't going to bend things to their interests.'

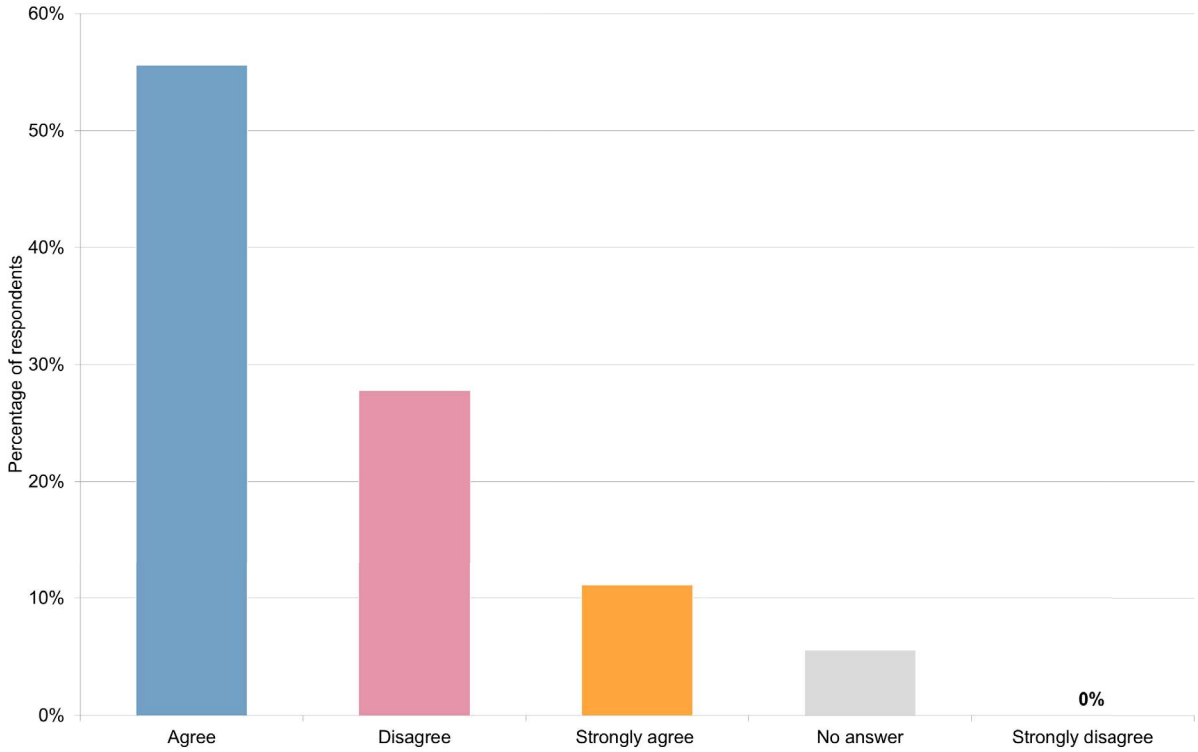
When asked where Australia should focus its efforts on international critical technology standards, participants named a range of technologies, including biotechnology, foreign ownership of critical infrastructure, AI, and chemical, biological, nuclear and lethal autonomous weapons. Some participants noted that 'we can never do enough' and that some countries aren't playing by the rules:

> 'There's legacy debt to make up for when we were naive. We invited states to be narrative setters in setting standards, thinking that they'll agree to be bound by them. Other countries are not adhering to these standards, but we do.'

'Values' in critical technologies

Parliamentarians were clearly divided when asked whether technology reflects the values of the countries in which it is designed and produced. More than two-thirds of participants suggested that technology reflects the values of the countries in which it is designed and produced (56% agreed and 11% strongly agreed). Nearly a third (28%) of participants disagreed, indicating that technology does not reflect the values of its origin country (Figure 17).

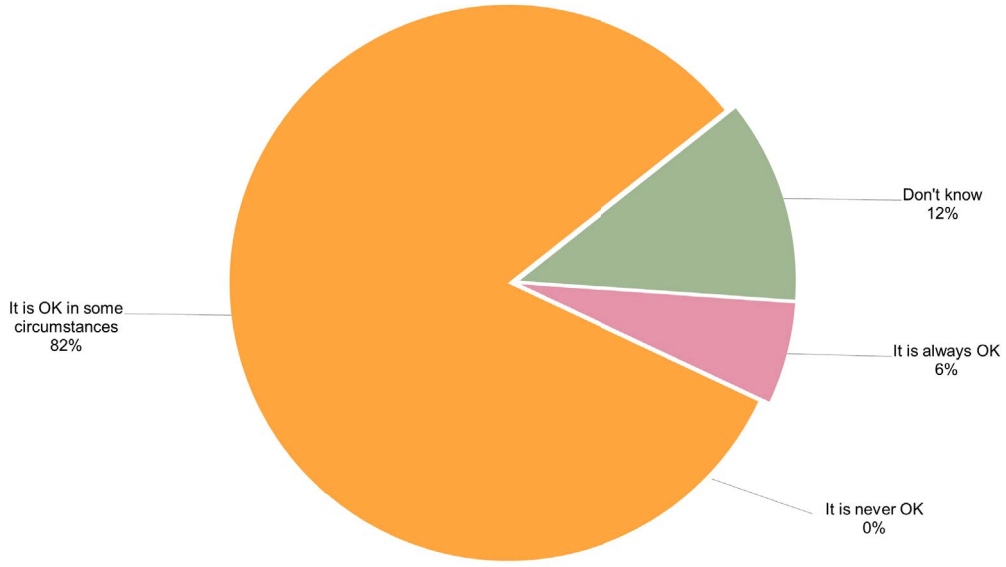
Figure 17: Do you personally agree or disagree that technology reflects the values of the countries it is designed and produced in?



Key finding 16: The majority of parliamentarians were comfortable to deploy technologies designed and manufactured in authoritarian countries in Australia, 'in some circumstances'.

In a follow-up question about whether it is 'OK' to deploy technologies designed and produced in an authoritarian country, the majority thought it was OK in some circumstances (82%), while only 6% thought it was 'always OK' (Figure 18). This suggests that parliamentarians adopt a risk-based approach to technologies from authoritarian countries, even if they apply different risk thresholds. Different perceptions of risk may be based on differences in threat awareness.

Figure 18: Do you personally believe it is OK or not OK to deploy technologies designed and produced in authoritarian states in Australia?



Case study 2: Critical technologies: investment priorities

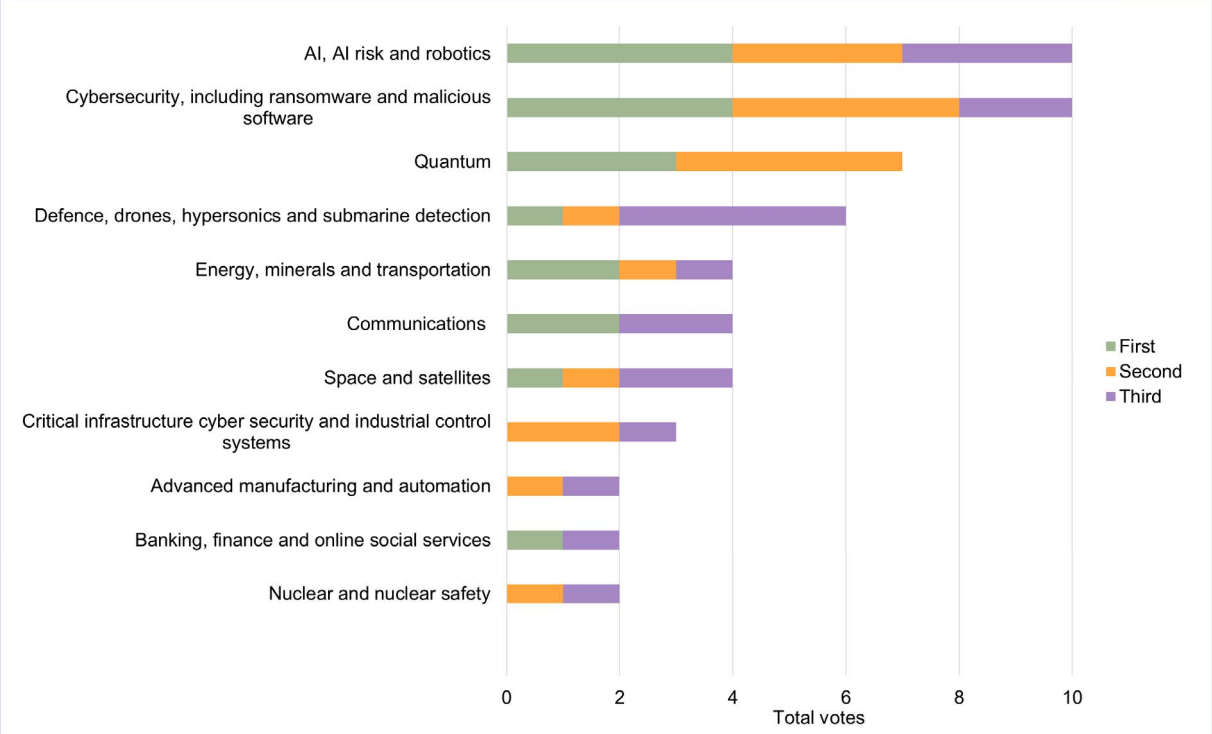
Investment in critical technologies

Key finding 17: Parliamentarians prioritised investment in quantum and AI technologies to advance Australia's national security and economic interests.

Participants were asked about investment into the research, development and manufacture of critical technologies in Australia—initially they were asked to prioritise national security interests and then they were asked to prioritise economic prosperity. Investment in this context was deemed to include all activity in the sector, including workforce and skills and research, manufacturing and production processes.

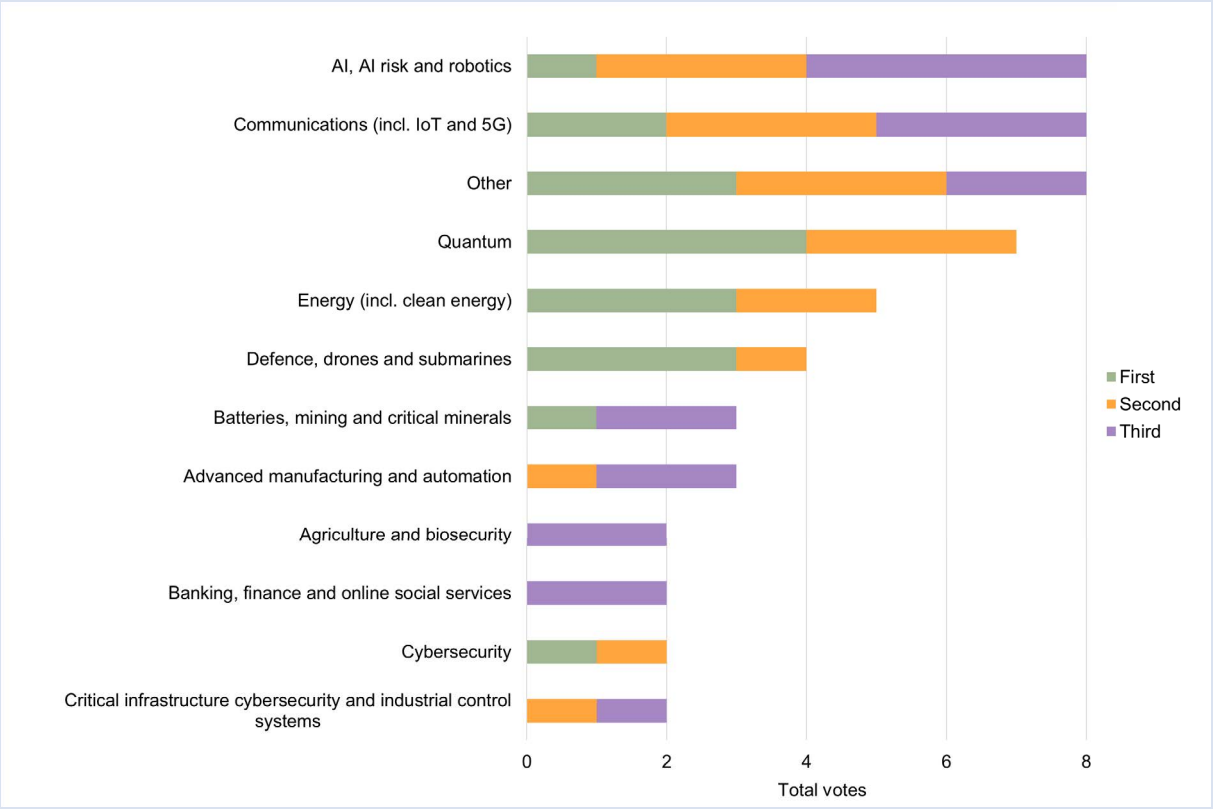
Participants were asked to self-identify their top three critical technologies, rather than to choose from any list. Figure 19 shows the 'rankings' cast in favour of all 11 categories of critical technologies that received at least two rankings. Rankings are separated according to the priority (first, second or third) that was allocated to them.

Figure 19: Please rank the top three critical technologies where you personally believe Australian investment should be prioritised to advance Australia's national security interests



When asked to prioritise national security, parliamentarians identified cybersecurity (which included ransomware), in addition to AI and robotics, as their highest priorities for Australian investment (Figure 19). Whereas their views on where to invest for economic prosperity included a wider range of critical technologies (Figure 20). When economic prosperity was the priority, they identified energy and communications technology rather than cybersecurity as the highest priorities, although quantum computing and AI featured as high priorities on both lists.

Figure 20: Please rank the top three critical technologies where you personally believe Australian investment should be prioritised to advance Australia's economic prosperity



Note: The category 'Other' refers to a range of identified critical technologies that do not fall into any of the categories listed, such as neuromorphic computing and two-factor authentication.

This section focuses on parliamentarians' views on how critical technologies should be funded and the appropriate split of government and private investment. Participants were asked to allocate investment against the critical technologies captured in this study on a continuous scale from 100% private investment to 100% government investment.

Figure 21 shows participants' average investment allocations. On average, participants suggested that private and government investment be split evenly between the technologies collectively ranked as the top three national security investment priorities: AI, AI risk and robotics; cybersecurity; and quantum computing. Participants slightly preferred government investment (<10%) for cybersecurity and AI, while the allocations to quantum computing slightly preferred private investment (<10%).[6]

Unsurprisingly, participants allocated majority government investment into defence, drones, hypersonics, submarine detection, space and satellites, which are all areas that require long-term, large-scale investment and remain, for the most part, public goods.

Figure 21: Of the three critical technologies you selected above as technologies where you personally believe Australian investment should be prioritised to advance Australia's [national security / economic prosperity], please circle on the scale below where you believe this investment should come from

Note: The national security or economic prosperity category 'bar' is missing for some technologies. In these cases, fewer than two participants identified those technologies as a top 3 priority in the missing category.

Far from competing, security and economic interests were broadly aligned on investment across nearly all the identified critical technologies. Energy and transportation were the exception—participants allocated investment quite differently when asked to consider energy and transport technologies from a national security perspective than when asked to allocate investment through an economic prosperity lens. Participants clearly emphasised a greater percentage (more than 30 percentage points) of public funding to these technologies when asked to consciously consider national security.

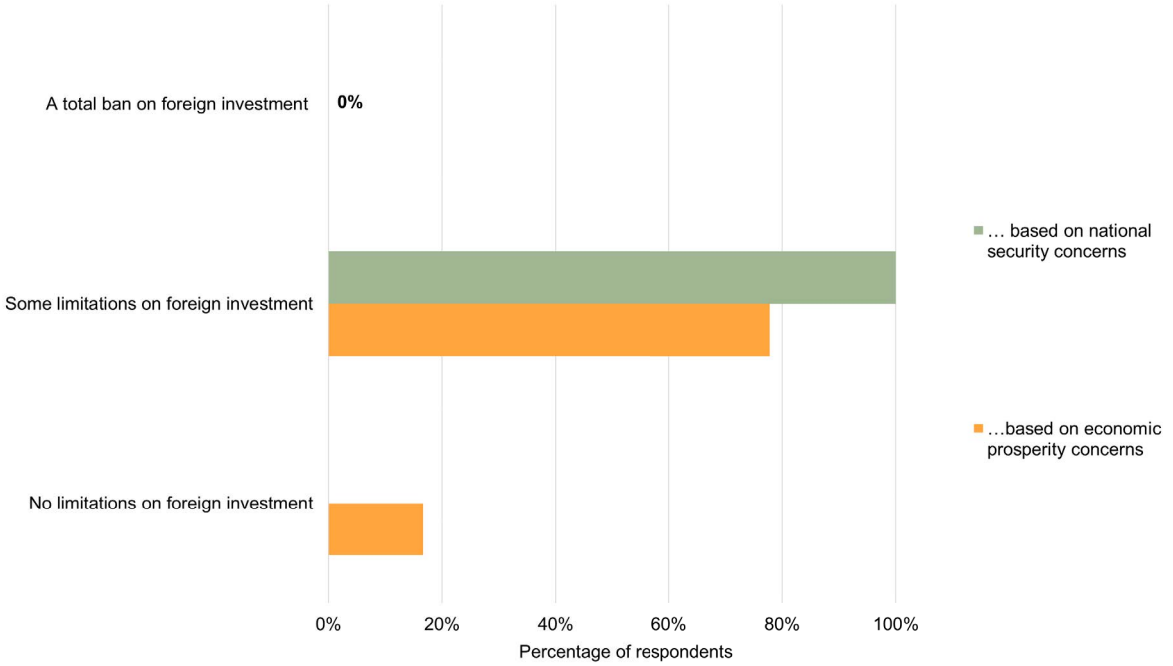
Foreign investment

Key finding 18: Most parliamentarians advocated limiting foreign investment to some degree—and economic considerations were as strong a driver as national security interests.

Key finding 19: Parliamentarians' views on limiting foreign investment were influenced by the country of investment origin, as well as by the proposed critical technology sector for investment.

Parliamentarians were broadly aware that certain types of foreign investment might carry economic or national security risk. No participant indicated the need for a total ban on foreign investment into Australian critical technologies firms, although most advocated limiting foreign investment in critical technology manufacturers and developers to some degree, on either national security and economic interest grounds, and often both (Figure 22). This suggests that parliamentarians value Australian or sovereign control over critical technology capabilities and supply chains.

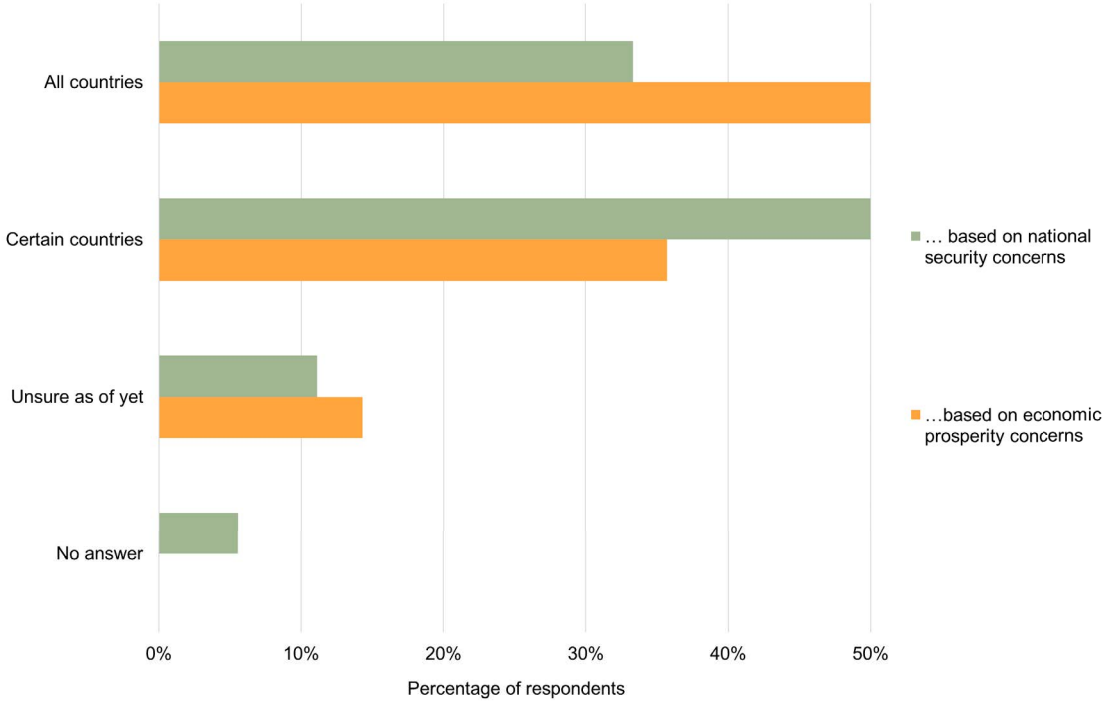
Figure 22: Should there be limitations on foreign investment in Australian businesses that develop or manufacture critical technologies based on [national security / economic prosperity] concerns?



Country of investment origin was also a clear influence on parliamentarians' views across the full spectrum of Australia's interests (Figure 23). Interestingly, more parliamentarians appeared to favour a flat limitation on foreign investment 'from any country' when asked to consider economic prosperity, which further suggests a focus on a strong domestic economy and sovereign industry.

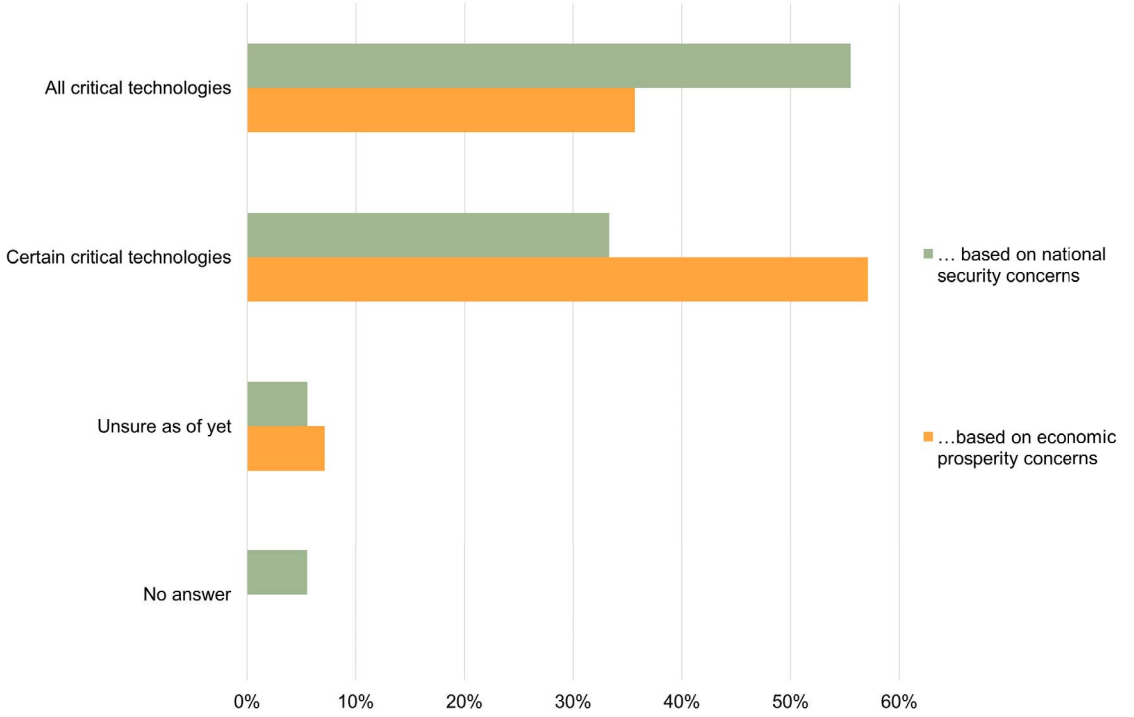
A national security lens reflected a more conservative stance on foreign investment overall but also a more nuanced view. Of those participants in favour of limiting foreign investment, one-third indicated that foreign investment from all countries should be limited (which would include countries with which Australia shares security agreements, such as the US, the UK, Canada and New Zealand). Fifty per cent of participants indicated that foreign investment from certain countries should be limited for reasons of national security.

Figure 23: If you answered 'some limitations on foreign investment', should there be some limitations on foreign investment from …



Parliamentarians who had already indicated the need to limit foreign direct investment were then asked whether that foreign investment should be limited based on the type of critical technology—for national security or economic prosperity reasons (Figure 24).

Figure 24: If you answered 'some limitations on foreign investment', should there be some limitations on foreign investment for …



The majority of participants agreed that foreign investment into 'certain' or 'all' critical technologies should be limited, with little variation in the total numbers between the national security and the economic lens. However, national security considerations tended towards a 'blanket' approach: 89% indicated that foreign investment into 'certain' or 'all' critical technologies (33% and 56%, respectively) should be restricted on national security grounds. Participants took a more selective approach when considering economic factors: a higher percentage sought to limit foreign investment in certain technologies only (57%) than sought to ban foreign critical technology investment completely (36%).

Sovereign capacity

Key finding 20: The majority of parliamentarians indicated a need for greater sovereign capacity in some or all critical technologies.

Key finding 21: The majority of parliamentarians agreed that access to reliable, secure critical technology supplies is important where sovereign capacity does not exist.

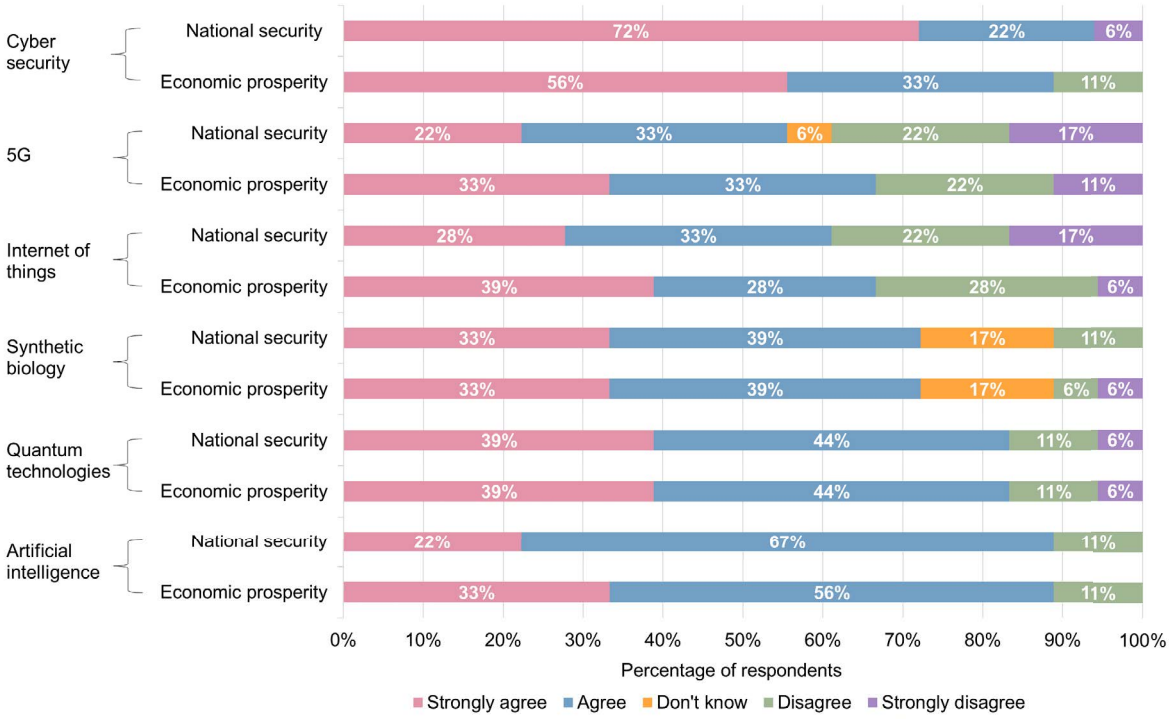
In line with the findings on limiting foreign investment, most participants indicated that Australia needed to build greater sovereign capacity in some or all critical technologies (Figure 25). There was little difference between responses based on national security or economic considerations.

Irrespective of a security or an economic focus, at least half of the participants supported developing sovereign capacity in all six identified critical technologies.

The majority supported developing Australian sovereign capacity in three key areas: cybersecurity technology, AI and quantum computing:

> 'We could be economically developing these capabilities [to process data here], but instead we're sending them overseas.'
>
> 'We should be doing more to lead internationally in security, modern manufacturing, developing technology for both security and economic reasons.'

Figure 25: Please circle the degree to which you agree or disagree with the following statement in respect to each area of technology listed below: 'It is important for Australia's [national security / economic prosperity] that it develops a sovereign capacity to produce in the following areas of critical technology'



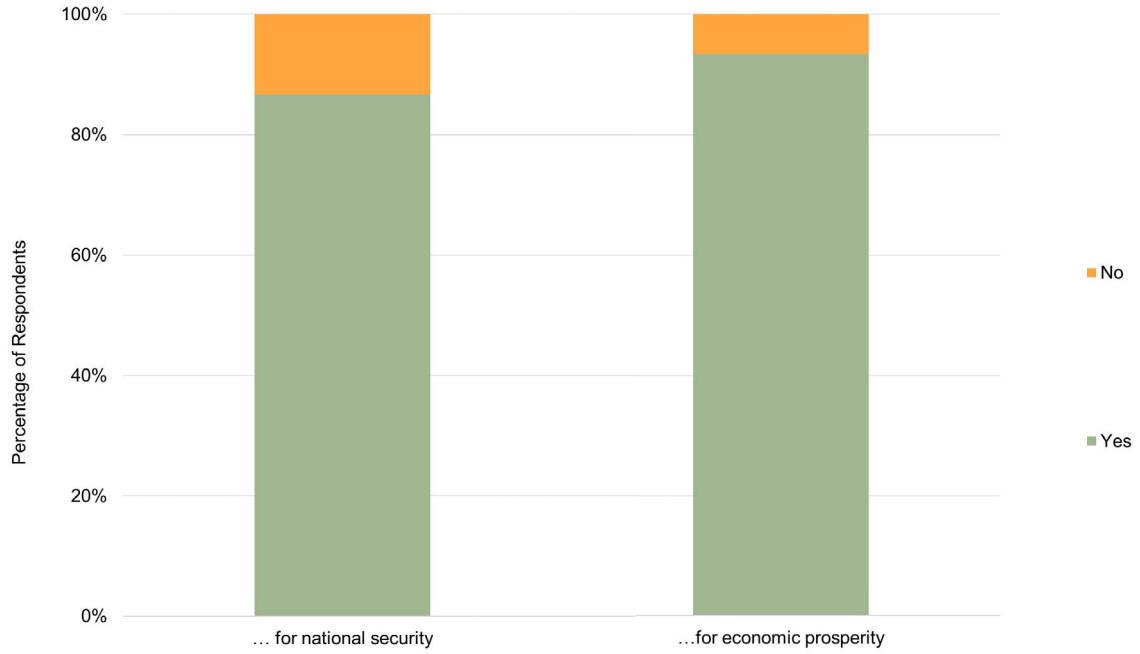
Although there are some marginal differences between national security and economic prosperity weightings, particularly for 5G and the IoT, participants appeared to highly value ready access to cybersecurity, AI and quantum computing for national security and economic prosperity reasons. This is understandable, as those technologies underpin a range of others and are perhaps those to which parliamentarians have been most often exposed.

However, parliamentarians also recognised that Australia is not a major technology provider and might not develop or maintain sovereign capacity in all or any critical technologies:

> 'It's the big sovereignty question. A lot of the technology is being developed by private multinational large companies. How much a nation like Australia [which relies on corporations] is able to [observe] the integrity of those systems—it's hard to be sure. It's unclear. It's opaque.'
>
> 'I don't think we can have a fully self-sufficient or sovereign supply chain on these issues as some of them are beyond our individual resources.'

Those parliamentarians who did not consider sovereign capacity to be important in critical technologies were nonetheless overwhelmingly (over 80%) of the view that access to reliable, secure critical technology supplies from other nations remained important (Figure 26).

Figure 26: If it's not important for Australia to have a sovereign capacity in these areas, is it important to have access to a reliable, secure supply from other nations for [national security / economic prosperity]?



Policy recommendations

This research offers some early but key insights on parliamentarians' views on various cybersecurity and critical technology issues, including areas they have themselves identified as knowledge gaps, priority areas and issues of concern. Based on our key findings (collated in Appendix 2), we propose the following policy recommendations.

1. **Create an education program for parliamentarians on critical technologies and cybersecurity.**

   Parliamentarians and advisers urgently need better access to education and high-quality information about critical technologies and cybersecurity. Despite being extremely time poor, they have expressed their hunger for such information. Such an education program is vital in light of rapid, ground-breaking technological developments such as generative AI and long-term, whole-of-economy commitments to advanced capabilities through AUKUS Pillar 2. This program should start immediately and could occur via numerous overlapping mechanisms:

   1.1. Identifying or establishing a clear source of objective, accessible advice for parliamentarians on key and emerging technologies and their likely impacts. If established a non-partisan Technology Assessment Office could provide an education and coordination function.[7]

   1.2. Briefings and round tables with civil society, think tanks, research institutes and peak institutions, particularly in non-sitting weeks. Parliamentarians have made it clear that they do not lack access to the private sector but would strongly welcome access to objective and independent experts. In sitting weeks, relevant parliamentary groups—including relevant committees and friendship groups—should host regular expert briefings and round tables in which civil society, think tank and research institute experts can brief parliamentarians on current and emerging trends affecting Australia and its place in the world.

   1.3. Briefings from key government actors. Federal departments and agencies, including agencies in the national intelligence community, should increase their offering of private briefings to parliamentarians on cyber security and critical technology topics, to ensure a steady stream of policy and operationally relevant information. This should include outreach during non-sitting weeks, when parliamentarians may have more time to engage on such issues. At a minimum, regular briefings should be provided by: the Department of Home Affairs, the Australian Cyber Security Centre, the Office of National Intelligence's new Cyber and Critical Technology Intelligence Centre, the Department of Foreign Affairs and Trade (DFAT), the Department of Industry, Science and Resources, the Commonwealth Scientific and Industrial Research Organisation, Defence (including the Defence Science and Technology Group and the Australian Strategic Capabilities Accelerator), the Department of Finance, and the Attorney-General's Department. When appropriate, agencies such as the Australian Signals Directorate and Australian Security Intelligence Organisation should also provide input. One agency—probably the Department of Home Affairs—should coordinate that program to ensure that briefs are relevant, timely and structured.

2. Parliament should build mechanisms to take a more active role in AUKUS Pillar 2.

AUKUS Pillar 2 capabilities, if developed and implemented successfully over the coming decade, could fundamentally enhance not just Australian defence capability but Australia's entire economy. But delivery will be difficult. In addition to the financial investment, Australia also has to align resourcing, expectations and research with both the US and UK. That type of alignment is unprecedented and will require both political capability and investment. As the smallest member in this trilateral partnership, Australia must get government, parliament, industry and civil society working more closely and collaboratively on the critical technologies that underpin AUKUS capabilities. To prepare for this, parliamentarians should:

2.1. build and invest in the new Parliamentary Friends of AUKUS group, using this mechanism as an opportunity to actively develop deep and ongoing relationships with US and UK counterparts, and to reguarly engage with them on specific challenges and issues;

2.2 establish a US–UK–Australia Parliamentary AUKUS Pillar 2 working group.

Establishing such Pillar 2 connections between parliamentarians will be essential in the years to come.

3. Parliamentarians should support a renewed commitment to Australian government engagement with key international standards development organisations.

Parliamentarians may have different views on specific cyber security threats and critical technologies but most agree on the need to work with partners and allies to shape international standards that ensure best practice on information security, cyber security (including AI), data and privacy protection controls. A non-partisan commitment to funding Standards Australia, boosting DFAT's capacity in this space and supporting other relevant standards agencies to consistently engage Standards Development Organisations would support future Australian access to technologies and systems that are secure by design.

Appendix 1: Participant profile

This appendix outlines a demographic analysis of the study's 24 participants. All 24 participants were members of the 46th Australian Parliament during the research study collection period (2021–2022). We note that the ASPI study included participants from across the political spectrum. Future studies will seek to improve ASPI's representative sample, relative to the demographics of parliament at the time.

Overall, we consider that the demographic analysis reveals a diverse range of study participants, who demonstrated a heterogeneity of experience and attitudes that is well reflected in the research findings.

The 24 participants represented 10.6% of the total federal Australian parliamentarian population—a sample we feel is sufficiently large and representative of the 46th parliament's inherent diversity to serve the purposes of the study. Our sample was compared against the demographics of the 46th parliament, as at 7 February 2019.[8]

Gender

Eighteen of the study's participants identified themselves as male (75%). The remaining six participants identified themselves as female (25%). The percentage of male participants in the ASPI sample was 12 percentage points higher than the percentage of males in the 46th parliament (Figures 27 and 28).

Figure 27: Gender representation in ASPI sample

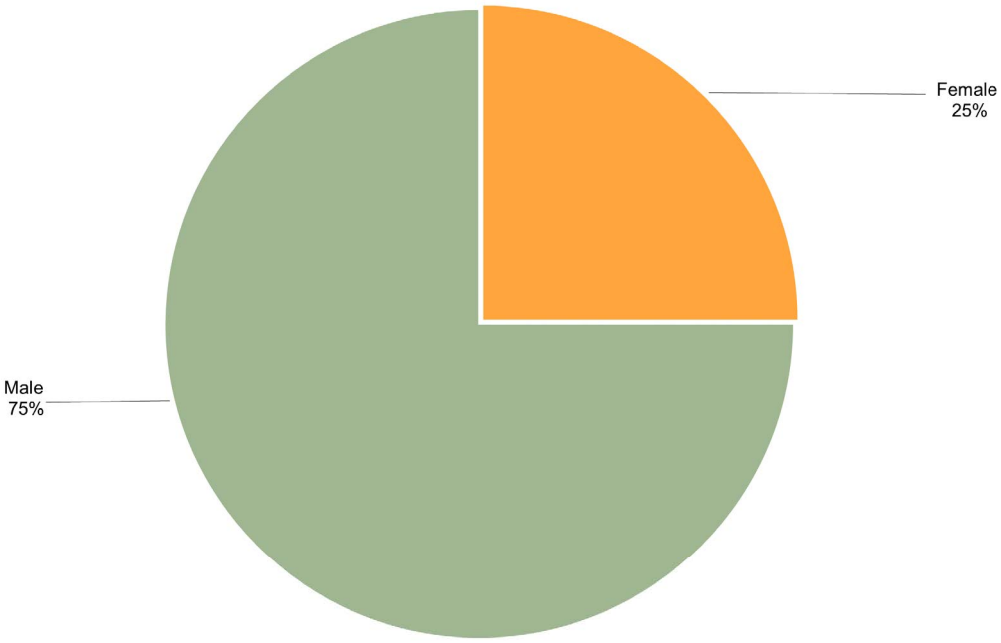
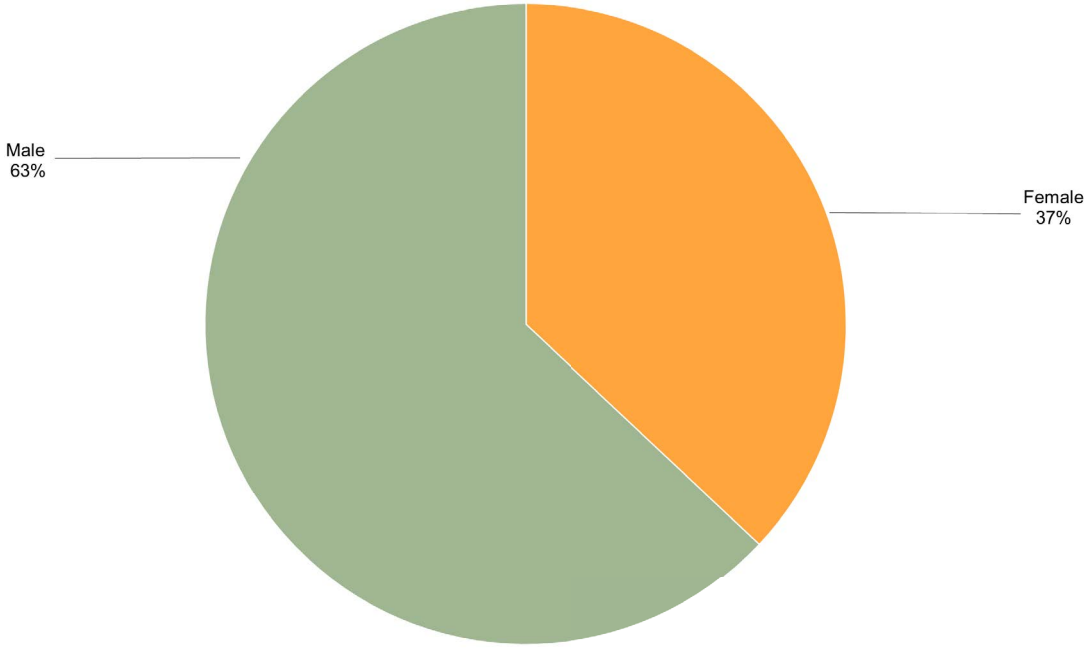


Figure 28: Gender representation in the 46th parliament



Chamber

Seventeen of the study's participants identified themselves as serving in the House of Representatives (71%). The remaining seven participants identified themselves as Senators (29%). This is similar to the demographics of the 46th parliament, in which 67% of parliamentarians served in the House of Representatives and 33% served in the Senate (Figures 29 and 30).

Figure 29: Chamber representation in ASPI sample

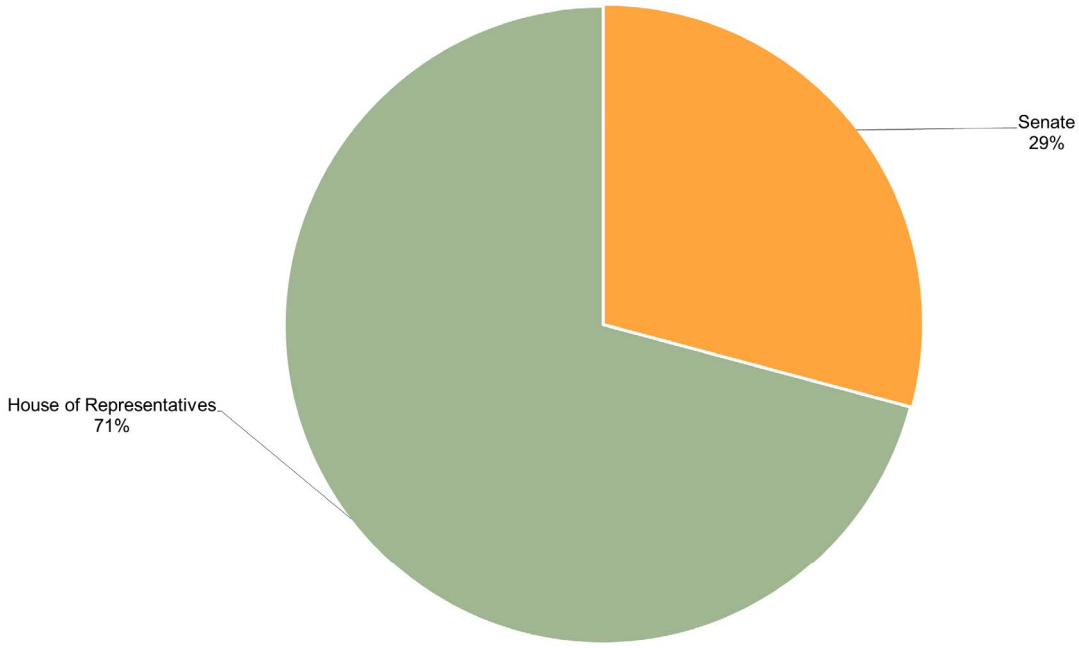
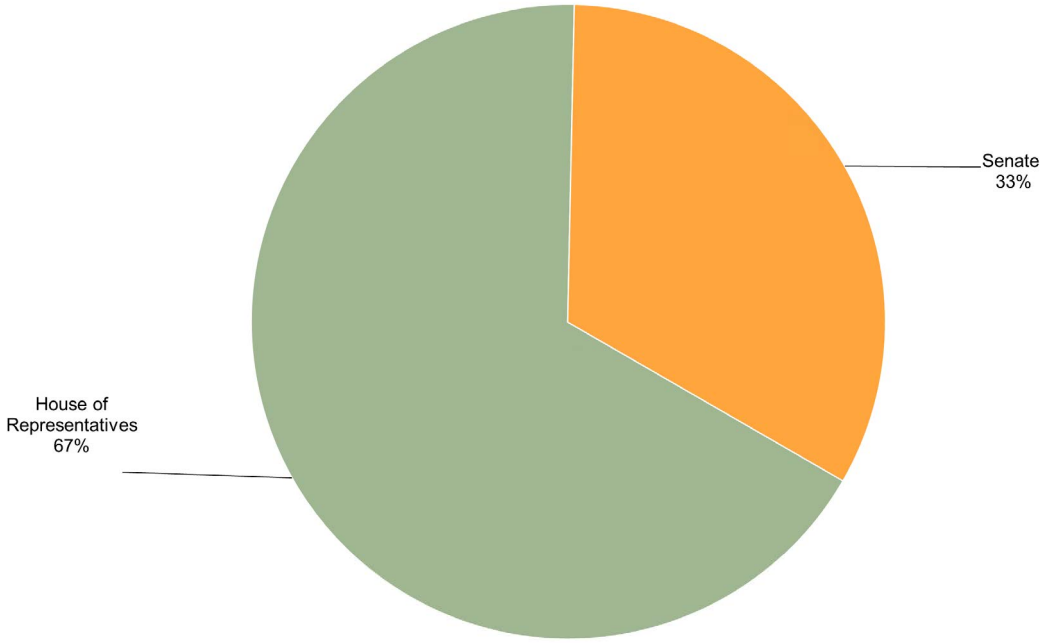


Figure 30: Chamber representation in 46th parliament



Status

Fourteen of the study's participants were backbenchers (58%). The remaining 10 participants were frontbenchers or shadow frontbenchers (42%). ASPI's sample was close to the demographics of the 46th parliament, in which 62% of parliamentarians were backbenchers and 38% were frontbenchers or shadow frontbenchers (Figures 31 and 32).

Figure 31: Status representation in ASPI sample

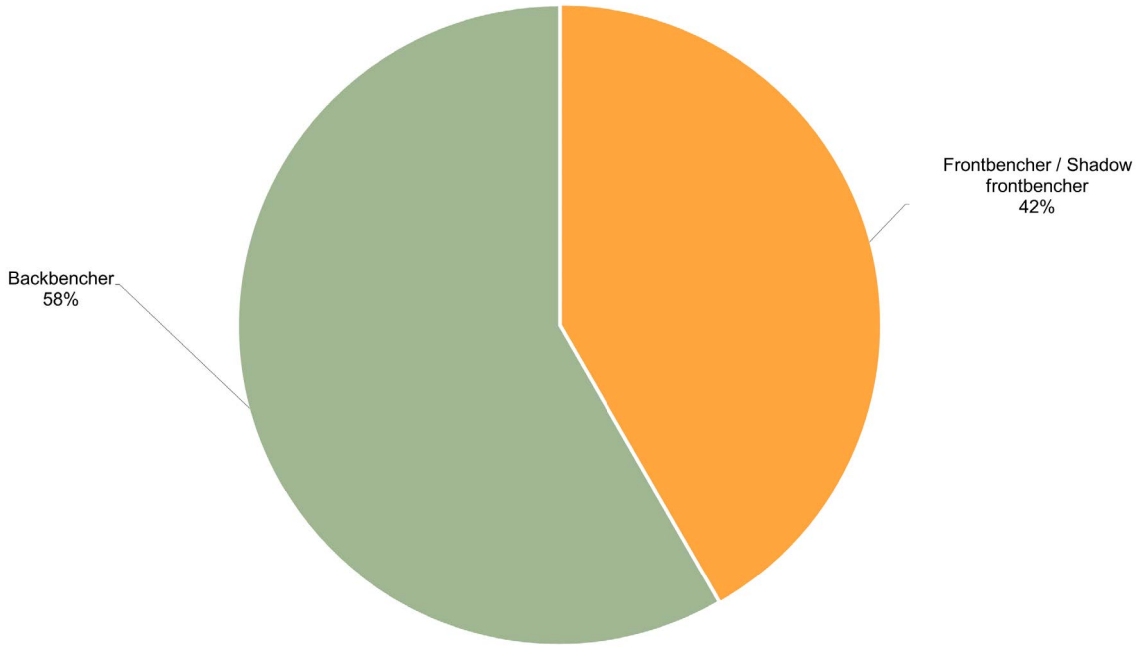
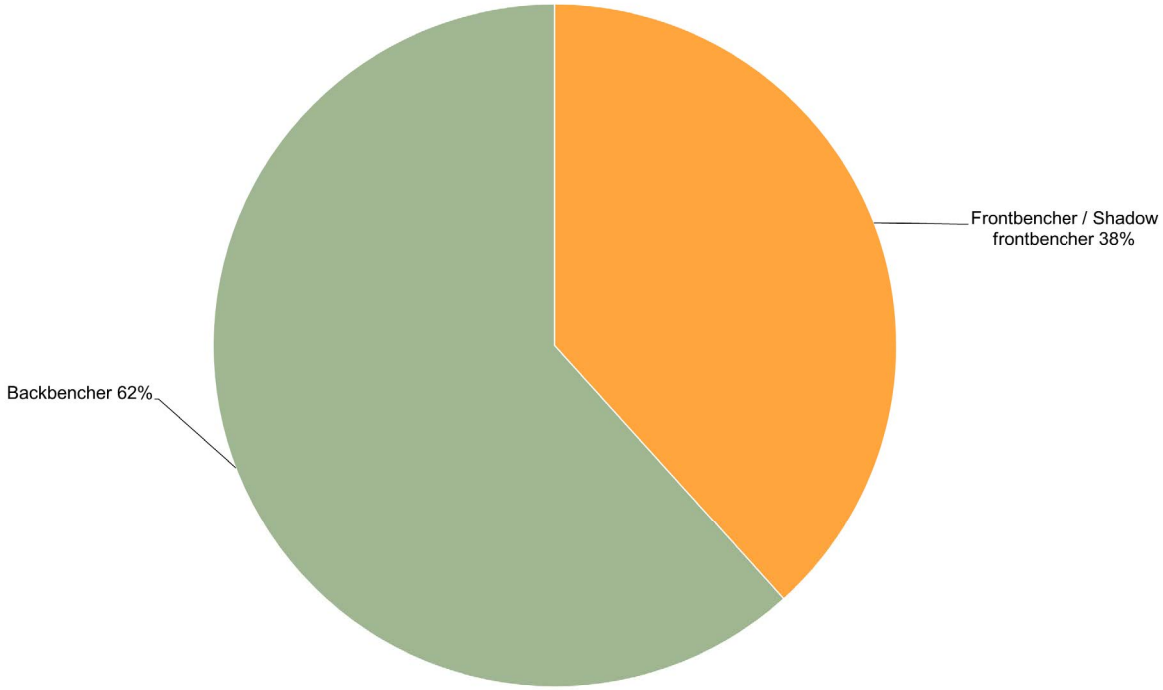


Figure 32: Status representation in 46th parliament



Electorate classification (House of Representatives)

Note: Details of the seven participating senators were not included in this section in order to preserve participants' anonymity.

This demographic section includes only the 17 participants serving as members of parliament in the House of Representatives. All electorate classifications are as defined by the Australian Electoral Commission.

Six of the study's participants represented electorates classified as 'inner metropolitan' (35%) (Figure 33). Five participants represented electorates classified as 'outer metropolitan' (30%). One participant represented an electorate classified as 'provincial' (6%). The remaining five participants represented electorates classified as 'rural' (29%). ASPI's sample was close to the demographics of the 46th parliament, in which 30% of parliamentarians were from 'inner metropolitan' electorates, 28% were from 'outer metropolitan' electorates, and 25% were from 'rural' electorates (Figure 34). However, the 46th parliament counted 16% of parliamentarians from provincial electorates, which is more than double the percentage of such parliamentarians represented in ASPI's sample.

Figure 33: Electorate representation in ASPI sample (House of Representatives only)

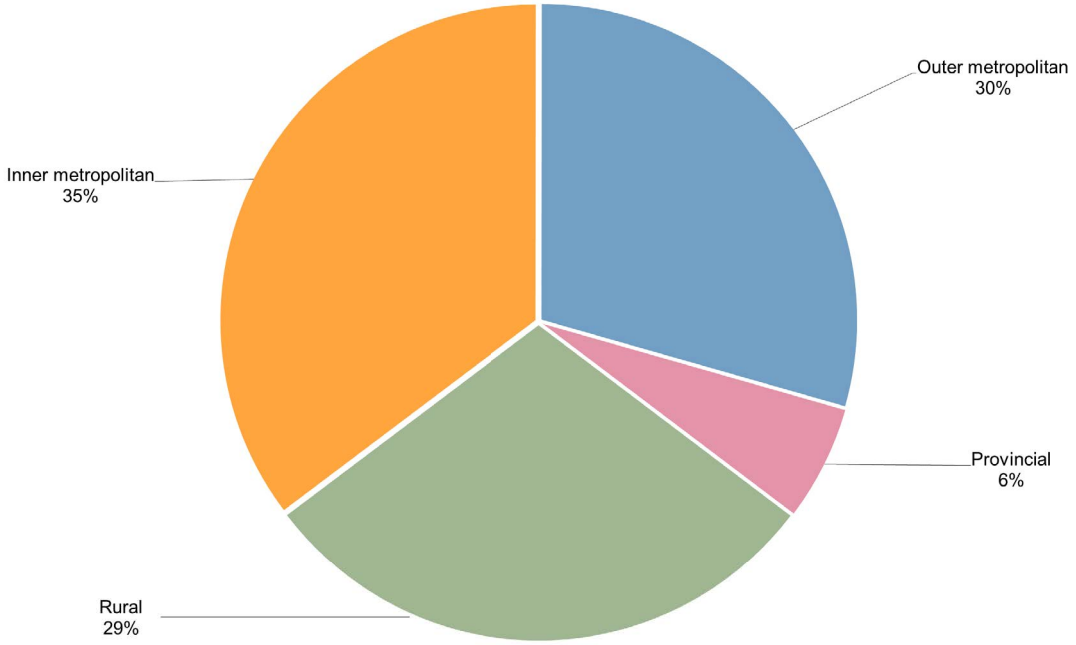
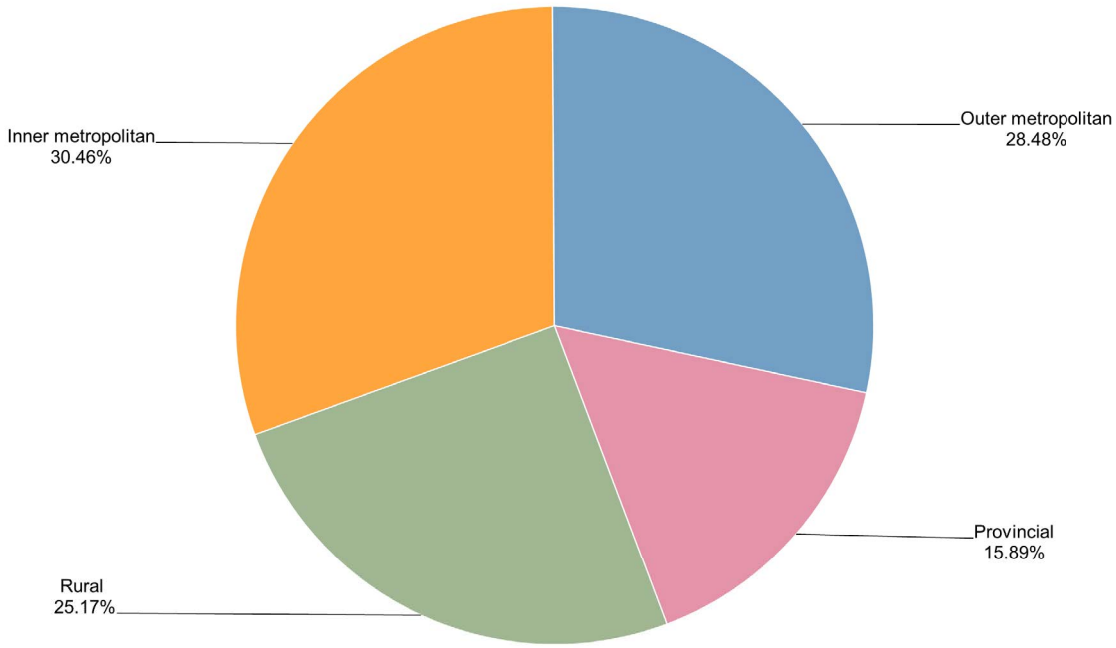


Figure 34: Electorate representation in 46th parliament (House of Representatives only)



Appendix 2: List of key findings

Appendix 3: List of study questions

ASPI Cybersecurity and Critical Technology Study

NB: *As discussed in 'Methodology', this study contained both a quantitative and a qualitative component. All parliamentarians involved in this study participated in a one-on-one interview where they answered qualitative questions. Seventy five percent of those parliamentarians also answered initial quantitative study questions.*

For ease of reading, this appendix combines both the quantitative and qualitative components of the study, which appear as follows in this study:

Quantitative: Q1, Q1A, Q1B, Q1C, Q2, Q2A, Q2B, Q2C, Q3, Q3A, Q4, Q4A, Q5, Q6, Q7, Q11, Q13, Q14, Q15, Q16, Q17, Q18, Q19, Q20, Q21, Q22, Q23, Q24, Q25, Q26

Qualitative: Q7A, Q8, Q9, Q10, Q11A, Q12, Q17A, Q18A, Q24A, Q25A, Q25B, Q26A, Q27, Q28, Q29

Section 1: Critical technology

Critical technology is defined in this study as technology that can significantly enhance, or pose risks to, Australia's national interests (influencing our national security, economic prosperity and social cohesion).

This section asks how different critical technologies relate to Australia's national security and economic prosperity, as well as Australia's sovereign capacity in these areas, and what investment in this space should look like. These are followed by open-ended questions regarding future challenges and an assessment of the current regulatory/policy responses to these challenges.

1. Please rank the top three critical technologies where you personally believe Australian investment should be prioritised to advance Australia's national security interests:

1. _____
2. _____
3. _____

1A. Of the three critical technologies you selected above, please circle on the scale below where you believe this investment should come from *(please note: investment holistically covers this area of technology, from research right through to skills and manufacturing/production)*

1) Private funding |___|___|___|___|___|___|___|___|___|___|___| Australian Government funding

100% 50/50 100%

2) Private funding |___|___|___|___|___|___|___|___|___|___|___| Australian Government funding

100% 50/50 100%

3) Private funding |___|___|___|___|___|___|___|___|___|___|___| Australian Government funding

100% 50/50 100%

1B. Should there be any limitations on foreign investment in Australian businesses that develop or manufacture critical technologies based on national security concerns?

a No limitations on foreign investment

b Some limitations on foreign investment

c A total ban on foreign investment.

1C. If you answered 'some limitations on foreign investment', should there be:

a Some limitations on foreign investment

i from certain countries

ii or all countries

iii unsure as of yet

b Some limitations on foreign investment

i from certain critical technologies

ii or all critical technologies

iii unsure as of yet

2. Please rank the top three critical technologies where you personally believe Australian investment should be prioritised to advance Australia's economic prosperity: *(please note: investment holistically covers this area of technology, from research right through to skills and manufacturing/production)*

1. _____
2. _____
3. _____

2A. Of the three technologies you selected above, please circle on the scale below where you believe this investment should come from:

1) Private funding |___I___I___I___I___|___I___I___I___I___| Australian Government funding

100% 50/50 100%

2) Private funding |___I___I___I___I___|___I___I___I___I___| Australian Government funding

100% 50/50 100%

3) Private funding |___I___I___I___I___|___I___I___I___I___| Australian Government funding

100% 50/50 100%

2B. Should there be any limitations on foreign investment in Australian businesses that develop or manufacture critical technologies due to economic prosperity concerns?

a No limitations on foreign investment

b Some limitations on foreign investment

c A total ban on foreign investment.

2C. If you answered 'some limitations on foreign investment', should there be:

a Some limitations on foreign investment

i from certain countries

ii from all countries

iii unsure as of yet

b Some limitations on foreign investment

i from certain technologies

ii for all technologies

iii unsure as of yet

3. Please circle the degree to which you agree or disagree with the following statement in respect to each area of technology listed below:

'It is important for Australia's national security that it develops a sovereign capacity to produce in the following areas of critical technology' *('sovereign capacity' is defined holistically as Australia's domestic capacity in an area of technology, from research right through to skills and manufacturing/ production).*

5G	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Quantum technologies	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Artificial intelligence	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Synthetic biology	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Internet of things	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Cybersecurity	Strongly agree / Agree / Disagree / Strongly disagree / Don't know

3A. If it's not important for Australia to have a sovereign capacity in these areas, is it important to have access to a reliable, secure supply from other nations *for national security*?

Yes / No

4. Please circle the degree to which you agree or disagree with the following statement in respect of each area of technology listed below:

'It is important for Australia's economic prosperity that it develops a sovereign capacity in the following areas of critical technology' *('sovereign capacity' is defined holistically as Australia's domestic capacity in an area of technology, from research right through to skills and manufacturing/ production).*

5G	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Quantum technologies	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Artificial intelligence	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Synthetic biology	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Internet of things	Strongly agree / Agree / Disagree / Strongly disagree / Don't know
Cybersecurity	Strongly agree / Agree / Disagree / Strongly disagree / Don't know

4A. If it's not important for Australia to have a sovereign capacity in these areas, is it important to have access to a reliable secure supply from other nations for economic prosperity?

Yes / No

5. Do you personally agree or disagree that technology reflects the values of the countries it is designed and produced in?

Strongly agree / Agree / Disagree / Strongly disagree / Don't know

6. Do you personally believe it is OK or not OK to deploy technologies designed and produced in authoritarian states in Australia?

a It is always OK

b It is OK in some circumstances

c It is never OK

d Don't know

7. Do you personally believe Australia is doing enough to shape international standards on critical technologies?

Yes / No / Don't know

[Questions 7A, 8, 9, 10 to be answered in interview]

7A. If you answered 'No', in what areas do you believe Australia should be focusing, and what should be done?

8. What do you foresee as the biggest challenge facing Australia in respect of critical technologies in the next five years? Why?

9. What policy or regulatory changes need to be introduced to address this challenge?

10. What critical technology/technologies are you interested in and would like to know more about?

Section 2: Cybersecurity

This section asks about cybersecurity issues. It asks you to assess the 'cyber resilience' of different sectors and where investment is needed in order to address vulnerabilities. These are followed by open-ended questions regarding future issues and an assessment of the current regulatory/ policy responses.

11. Do you personally feel safe online against scams / cyber threats?

a Always

b Sometimes

c Never

[Questions 11A, 12, to be answered in interview]

11A. If you answered A or B, what kind of scams / cyber threats are you worried about?

12. From an Australian national security perspective, are you more concerned about state- or non-state-backed malicious cyber activity?

13. On a scale of 1–3, please rank the top three threats you personally are most concerned about for Australia *(the lower the number, more concerned you are; the higher the number, the less concerned you are).*

Cybersecurity issue	Rank
State-backed cyberattacks on critical infrastructure	
Non-state cyberattacks on critical infrastructure	
State-backed cyber-enabled commercial IP theft	
Non-state cyber-enabled commercial IP theft	
State-backed cyber espionage	
Non-state cyber espionage	
State-backed cyber-enabled foreign interference	

Non-state cyber-enabled foreign interference	
Data breaches from badly designed systems or negligence (i.e. not from a malicious attack)	
Other:	

14. On a scale of 1–10, how 'cyber resilient' do you consider the following to be (1 being not at all cyber resilient and 10 being very cyber resilient). *Cyber resilience is a measure of how well an organisation or individual can manage a cyberattack or data breach while continuing to operate effectively. Cyber resilience also reduces the likelihood of successful cyberattacks.*[9] *Cyber resilience is measured on a spectrum and is achieved (1) by having effective arrangements in place for managing cyber risks, (2) by monitoring and reporting against cybersecurity deliverables and (3) by having a culture of cyber resilience.*[10]

Federal government agencies (excluding Defence and intelligence agencies)	1 2 3 4 5 6 7 8 9 10 not sure
Federal defence and intelligence agencies	1 2 3 4 5 6 7 8 9 10 not sure
State and territory government agencies	1 2 3 4 5 6 7 8 9 10 not sure
Local councils	1 2 3 4 5 6 7 8 9 10 not sure
The offices of MPs and senators	1 2 3 4 5 6 7 8 9 10 not sure
Democratic and 'national identity' institutions (e.g. Australian Electoral Commission, National Archives)	1 2 3 4 5 6 7 8 9 10 not sure
Political parties	1 2 3 4 5 6 7 8 9 10 not sure
The communications sector	1 2 3 4 5 6 7 8 9 10 not sure
The data storage or processing sector	1 2 3 4 5 6 7 8 9 10 not sure
The financial services and markets sector	1 2 3 4 5 6 7 8 9 10 not sure
The water and sewerage sector	1 2 3 4 5 6 7 8 9 10 not sure
The energy sector	1 2 3 4 5 6 7 8 9 10 not sure
The health care and medical sector	1 2 3 4 5 6 7 8 9 10 not sure
The higher education and research sector	1 2 3 4 5 6 7 8 9 10 not sure
The food and grocery sector	1 2 3 4 5 6 7 8 9 10 not sure
The transport sector	1 2 3 4 5 6 7 8 9 10 not sure
The space technology sector	1 2 3 4 5 6 7 8 9 10 not sure
The defence industry sector	1 2 3 4 5 6 7 8 9 10 not sure
Individuals	1 2 3 4 5 6 7 8 9 10 not sure

15. From the previous list, which three sectors should receive prioritised investment in the next 12 months to assist with improving their cyber resilience?

1. _____
2. _____
3. _____

16. Of the three sectors you selected above, please indicate on the scale below where you believe this investment should come from:

1) Private funding |___I___I___I___I___|___I___I___I___I___| Government funding

100% 50/50 100%

2) Private funding |___I___I___I___I___|___I___I___I___I___| Government funding

100% 50/50 100%

3) Private funding |___I___I___I___I___|___I___I___I___I___| Government funding

100% 50/50 100%

17. Should the federal government have a data management strategy for the public sector; i.e. government agencies, government business enterprises?

a Yes

b No

c Don't know

[Question 17A to be answered in interview]

17A. Why / Why not?

18. Should the federal government have a data management strategy for the private sector, i.e. critical infrastructure operators?

a Yes

b No

c Don't know

[Question 18A to be answered in interview]

18A. Why / Why not?

19. **In Estonia,[11] citizens own their personal data and approve the information that can be used by government agencies. It is a criminal offence for government agencies to access unauthorised personal data. Should Australians own their personal data?**
    a Yes, but only in relation to access by government agencies
    b Yes, but only in relation to access by private companies
    c Yes, in relation to both access by government agencies and private companies
    d No

20. **What types of federal government data or federal information should it be mandatory to store on servers located in Australia?** As opposed to being stored on offshore servers, which would be under the sovereign jurisdiction of another country, and therefore be subject to the law of that country. (Circle all that apply)
    a Classified data or information
    b Unclassified nationally significant data or information
    c Identifiable citizen-related data or information
    d Non-identifiable citizen data or information
    e Other: (please explain)

21. **What types of state/territory government data should it be mandatory to store on servers located in Australia?**
    a Classified data or information
    b Unclassified significant data or information
    c Identifiable citizen-related data or information
    d Non-identifiable citizen data or information
    e Other: (please explain)

22. **What types of local council data should it be mandatory to store on Australian servers?**
    a Sensitive and confidential data or information
    b Unclassified significant data or information
    c Identifiable citizen-related data or information
    d Non-identifiable citizen data or information
    e Other: (please explain)

23. **In your opinion, when it comes to legacy ICT systems that support critical national infrastructure, what is the best way to manage these from a cybersecurity perspective?**
    a A complete and comprehensive renewal of existing systems, no matter the cost, because the risks are too high and cannot be effectively mitigated and managed
    b A major update to existing systems to save on cost, because the risks are high, but they can be effectively mitigated and managed
    c A gradual update to existing systems because the cost is too high, the risks are medium to low and they can be effectively mitigated and managed
    d No update is needed
    e Don't know
    f Other: (please explain)

24. Should it be legal or illegal in Australia to pay ransomware demands?

Legal / Illegal

[Questions 24A to be answered in interview]

24A. Why / Why not?

25. From your perspective, is there a federal government department/agency that has the lead responsibility for cybersecurity issues?

Yes / No

[Questions 25A, 25B to be answered in interview]

25A. If you answered 'yes', please state which government department that is:

25B. From your perspective, which federal government department <u>should</u> have the lead responsibility for cybersecurity issues?

26. Which one of the below comes closest to describing how often you are engaged by constituents and industry on issues relating to cybersecurity?

a Every day
b A few times a week
c A few times a fortnight
d A few times a month
e A few times a year
f Less than once a year

[Questions 26A, 27, 28, 29 to be answered in interview]

26A. What issues do they focus on?

27. What do you foresee as the biggest challenge facing Australia in respect of cybersecurity in the next five years? Why?

28. What policy or regulatory changes need to be introduced to address this challenge?

29. What cybersecurity issues are you interested in and would like to know more about?

Appendix 4: List of figures

Notes

1 Australian Signals Directorate, 'Cyber security terminology', Australian Government, online.

2 Australian National Audit Office (ANAO), *Cyber resilience*, performance audit report no. 53 of 2017–18, Australian Government, 28 June 2018, 53, online.

3 Department of Industry, Science and Resources, 'List of critical technologies in the national interest', Australian Government, 2021.

4 Millie Muroi, 'Medibank hack: APRA hit health insurer with $250m extra capital requirement', *Sydney Morning Herald*, 27 June 2023, online.

5 The authors note that the data collection for this study was completed prior to the government's release of a draft Data and Digital Government Strategy on 9 May 2023, online. This draft strategy considers public sector data integration and efficiencies, privacy and security. While it does not specifically address private sector data, data standards or data storage, many of the issues raised by Parliamentarians in our study were reflected in the mid-2023 public consultation process, online. The final version of the Strategy and an accompanying Implementation Plan, is due for release by the end of 2023.

6 There were, however, a range of highly variable votes allocated to investment contributing to these averages: two participants' allocated votes to AI investment allotted at least 70% of funding to the private sector, while three participants' vote allocations favoured at least 80% government investment.

7 Brandon How, 'New parliamentary office would improve tech policy: Violi', *InnovationAus.com*, 7 March 2023, online. In March 2023, Aaron Violi MP, Liberal Member for Casey, and Dr Daniel Mulino MP, Labor Member for Fraser, proposed the establishment of a Parliamentary Technology Assessment Office to advise policymakers on the impact that emerging technologies may have on proposed policy and how to ensure that regulations keep pace with technological change and development. The bipartisan proposal suggests modelling a technology assessment office on the UK's Parliamentary Office of Science and Technology, established in 1992, and the former (1974–1995) US Congressional Office of Technology Assessment. Like the Parliamentary Budget Office, the Technology Assessment Office would be independently staffed to ensure the provision of objective advice.

8 Data from the Parliamentary Library's *Parliamentary handbook* for the 46th parliament, online. Note that data on 'Status' was taken from 29 May 2019 from the Australian Parliament's 46th parliament ministry list, online, and from 2 June 2019 for the shadow ministry, online.

9 ANAO, *Cybersecurity follow-up audit*, performance audit no. 42 of 2016–17, Australian Government, 2017, 8, online.

10 ANAO, *Cyber resilience*.

11 Imtiaz Khan, Ali Shahaab, 'Estonia is a 'digital republic'—what that means and why it may be everyone's future', *The Conversation*, 8 October 2020, online.

Acronyms and abbreviations

ACIC	Australian Criminal Intelligence Commission
ACSC	Australian Cyber Security Centre
ADF	Australian Defence Force
AEC	Australian Electoral Commission
AI	artificial intelligence
ASIO	Australian Security Intelligence Organisation
CCP	Chinese Communist Party
DFAT	Department of Foreign Affairs and Trade
FTA	free trade agreement
ICT	information and communications technology
IP	intellectual property
IT	information technology
OECD	Organisation for Economic Co-operation and Development
NAA	National Archives of Australia
PJCIS	Parliamentary Joint Committee on Intelligence and Security

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE