MOSSÉ SECURITY

THE ENEMY GETS A VOTE

Analysing the Australian Cyber Security Strategy 2023-2030 Horizons 1&2 Through the Eyes of a Cyber Adversary

Author: Benjamin Mosse

Date: 29 August 2025

Table of Contents

Introduction

Imagine you are part of a cybercriminal gang, deciding which region of the world to target next. Australia has always been lucrative, but now there's talk of a new national cybersecurity strategy (1). Could this change the game? You start digging. The documents are public, so you read them closely, asking: *does this strategy raise the risks for us, push us elsewhere, or reassure us that Australia is still open for business?*

This is the approach I take in this paper. I built a threat actor profile and examined every intervention from Horizon 1 and every proposed action area in Horizon 2 through an adversary's eyes.

The purpose is not dramatics, but method: to stress-test the strategy and to counter the Framing Effect (3)—the bias that arises when we accept a policy on its own terms instead of questioning its underlying assumptions.

Methodology

I adopted a structured process to evaluate the Australian Cyber Security Strategy from an adversarial perspective known as Red Team Mindset (5,6).

The aim was to simulate how an adversary might interpret, adapt to, and even exploit the measures outlined in Horizons 1 and 2. The process comprised the following steps:

- **Step 1 – Threat Actor Profile Development:** I constructed a threat actor profile informed by my direct experience responding to major breaches in Australia, as well as publicly reported incidents.
- **Step 2 – Horizon 1 & 2 Analysis:** From the perspective of this threat actor, I evaluated Horizon 1 and 2 initiatives to assess their potential to deter, prevent, or impose material costs on the actor's operations.
- **Step 3 – Applied Critical Thinking:** Applied a technique from the Red Team Handbook (5) to deepen insights through an adversarial perspective.
- **Step 4 – Development of Recommendations:** Finally, I reviewed the Cyber Security Policy Model to identify opportunities for strengthening its design and the overall approach taken by Home Affairs, with the goal of reducing adversary advantages and improving policy effectiveness.

While this methodology has limitations, it offers a clear, repeatable process that others can refine. By substituting different threat actor profiles, it can stress-test a national cyber security strategy against varied adversaries, revealing how each might perceive and react to planned policy interventions. This makes it a practical tool for exposing blind spots and challenging assumptions in strategy and policy.

Objectives

The objective of this analysis is to surface the deep assumptions and blind spots embedded in Australia's Cyber Security Strategy 2023-2030.

As work on cognitive bias demonstrates, decision-makers often overlook critical variables when operating within familiar frames (4). By examining the policy through a lens entirely foreign to its design, the aim is to challenge narratives, expose overlooked risks, and reveal insights unlikely to emerge from conventional approaches (5,6).

Limitations

This assessment has clear limitations. Designing a fictitious threat actor profile inevitably reflects the biases and assumptions of the author, and no analysis can claim to know with certainty how a real adversary would think or act. The threat actor's perspective is therefore an informed approximation, not a definitive representation.

In addition, the analysis was constrained to a total of 8 hours, limiting the depth of review and the ability to explore alternative interpretations or scenarios.

Finally, this analysis was conducted independently, without the benefit of a diverse team of critical thinkers, which inherently limits the breadth of insights such an approach can otherwise yield. Nonetheless, despite these constraints, I trust that the perspective offered here will be of value to Home Affairs and may encourage the adoption of more robust Red Team assessments in the future.

Threat Actor Profile

<table>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">Policy Ghost is a fictitious financially motivated cybercriminal enterprise that impacts the confidentiality and integrity of sensitive data (personal and business) and revenue-generating business processes. Their operations have resulted in significant information privacy losses, proprietary data theft, prolonged business interruptions, and high-cost cyber extortions.

Policy Ghost is a moderately skilled adversary known to law enforcement that targets Australian organisations underinvested in cybersecurity. They adapt quickly to evade and bypass modern defences, but a well-trained, 24/7 security operations centre can stop them.

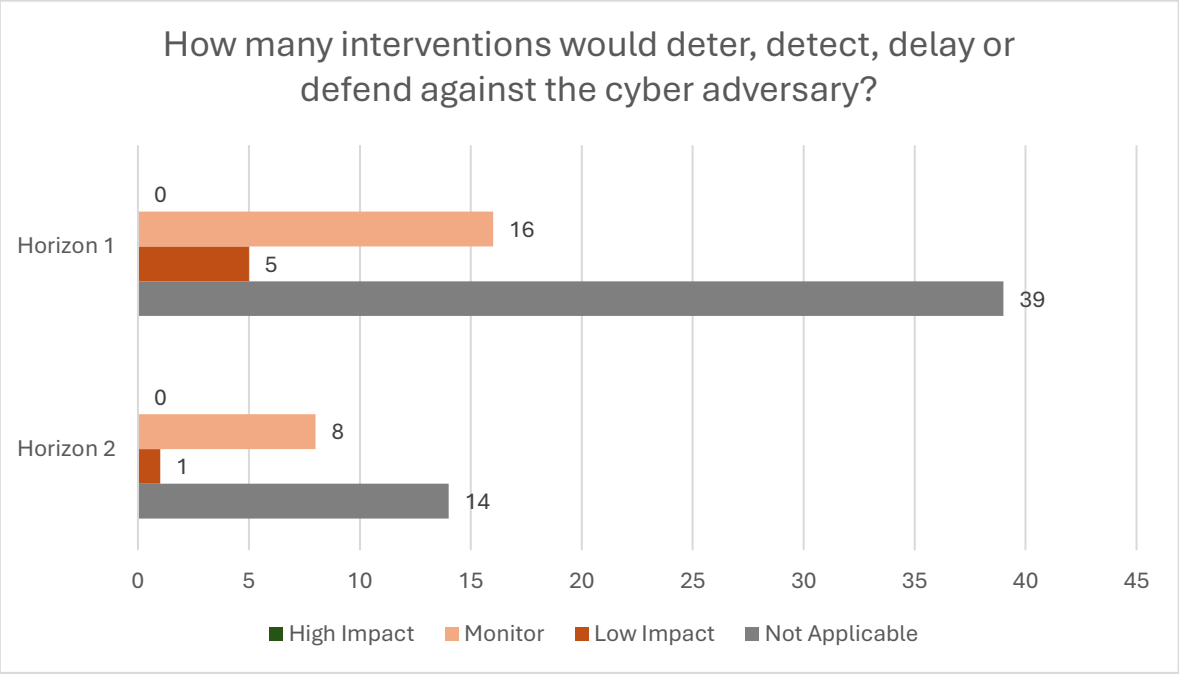
Policy Ghost targets the following industries: healthcare, finance, and retail.</td></tr>
<tr><th colspan="3">Methods</th></tr>
<tr><td>• Phishing
• Ransomware
• Data Exfiltration</td><td>• Malware
• Credential Stuffing
• Supply Chain</td><td>• Account Takeover
• Privilege Abuse
• Application Exploitation</td></tr>
<tr><th colspan="2">Primary Tactic: Business Interruption</th><th>Secondary Tactic: Data Breach</th></tr>
<tr><td colspan="2">Full-network ransomware deployment with concurrent data exfiltration, coupled with targeted psychological pressure campaigns to compel victim payment.</td><td>Theft of large volumes of sensitive personal data, confidential health records, or proprietary business information, followed by extortion demands to prevent release or sale of the data on dark web marketplaces.</td></tr>
</table>

Key Findings

Adversary-Centric Review of Horizon 1 & 2

I reviewed every intervention listed in Appendix B, *"Status of Horizon 1 Initiatives"*, as well as each proposed Action Area for Horizon 2, from the perspective of a cyber adversary.

For each item, I asked: *"Would this intervention/action deter, detect, delay, or defend against Policy Ghost?"* Each was assigned one of four ratings: **Low Impact**, **High Impact**, **Monitor** (relevant but insufficient information available), or **Not Applicable**.



In Horizon 1, 21 of the 60 interventions reviewed (35%) showed some relevance to impacting a cyber adversary such as Policy Ghost. In Horizon 2, 9 of the 23 action areas (39%) were assessed as relevant.

Both horizons include items relevant to adversaries like Policy Ghost, but none qualify as "High Impact" due to:

- **Weak Causal Linkages:** The link between many interventions and actual disruption of the cybercrime model is unclear. For instance, it is not evident how participation in the International Counter Ransomware Task Force (ICRTF) would measurably affect a group like Policy Ghost. Rhetoric is not enough—impact must be demonstrated with data to justify a "high impact" classification; otherwise, it should be considered low.
- **Insufficient Information:** Several interventions that appeared potentially relevant lacked adequate publicly available information to enable a robust evaluation of their effectiveness.

SWOT Analysis – Cyber Adversary vs. Home Affairs

The table below presents a SWOT analysis, written from the perspective of Policy Ghost, comparing its own capabilities against the nationwide initiatives outlined in the Australian Cyber Security Strategy.

Strengths	Weaknesses
• Located overseas and out of reach • Known to law enforcement, but not a national security threat • Ability to recruit talented hackers and maintain strong operational capabilities that defeat legacy and modern security protections (with some exceptions)	• Inability to evade Australian threat sharing capabilities • Inability to prevent long-term law enforcement tracking and pursuit if considered a top-priority threat
Opportunities	**Threats**
• Most Australian businesses will not adopt threat intelligence capabilities. Even if they did, it's unlikely that they would know how to leverage such capabilities • Senior business leaders face limited to no personal consequences for negligence in cybersecurity	• Ongoing risk of getting arrested • Adoption of more modern security controls that raise the cost of Policy Ghost maintaining operational dominance over Australian targets

Recommendations for Home Affairs

Recommendation 1: Define clear and measurable strategic goals

The strategy is structured around 6 “cyber shields”:

The challenge is that these cyber shields are not measurable. It is difficult to determine what success looks like for broad aspirations such as “strong businesses and citizens” or “safe technology.”

The cyber shields could be strengthened by linking them to clear, measurable outcomes such as:

Strategic Goal	What it means
Drive cyber-crime down	• Achieve a 5-year downward trend on data breaches • Reduce the average cost of a data breach • Reduce the average cost of a ransomware compromise
Achieve better Value for Money on cyber spending in government	• Save from consolidating duplicate tools/contracts • Achieve same or better outcomes at lower cost
Impose real consequences on businesses that fail to meet their cybersecurity and privacy obligations	• Expand and intensify regulatory investigations and enforcement actions • Impose stronger penalties and fines for negligent cybersecurity and privacy practices • Achieve demonstrable year-on-year improvements in compliance rates

Recommendation 2: Use metrics already at your disposal

The term “metrics” appears three times in the Horizon 2 Policy Discussion Paper, yet no metrics are proposed, and none of the “end-state” statements on page 9 are quantified. I therefore recommend adopting simple, measurable indicators such as:

- **Increase in cybersecurity budgets** – e.g., from 5% of IT spend to 15%.
- **Growth in the number of CISOs** defending critical infrastructure – e.g., from 100 to 300.
- **Increase in government agency compliance** with the Essential 8.
- **Reduction in data breaches** reported to the OAIC.
- **Reduction in incidents** responded to by the ASD.
- **Reduction in the average cost** of a data breach in Australia.

Surveys and reports tracking these metrics already exist. While each has limitations, they could provide Home Affairs with a practical basis for measuring and assessing the strategy’s effectiveness.

Recommendation 3: Understand and validate before you intervene

In a volatile, uncertain, complex and ambiguous domain such as cybersecurity, it can be tempting to pursue many initiatives at once. Yet this approach rarely delivers consistent results. A more effective path is to first build a clear understanding of the system, validate that it reflects reality, and then identify targeted interventions most likely to achieve strategic goals.

Accordingly, I recommend that Home Affairs establish a dedicated team tasked with mapping identities, components, relationships, and perspectives across the system. This work should be guided by the DSRP framework (Distinctions, Systems, Relationships, Perspectives) and supported by structured tests to confirm alignment with reality. Only after this validation should interventions be advanced, framed within a comprehensive business case.

- Do we understand the full system?
- Is our understanding aligned to reality?
- Which intervention is most likely to achieve our strategic goal(s)?
- Can we meet the standard of a full business case?
- Do we have exit criteria in case the intervention causes negative effects?

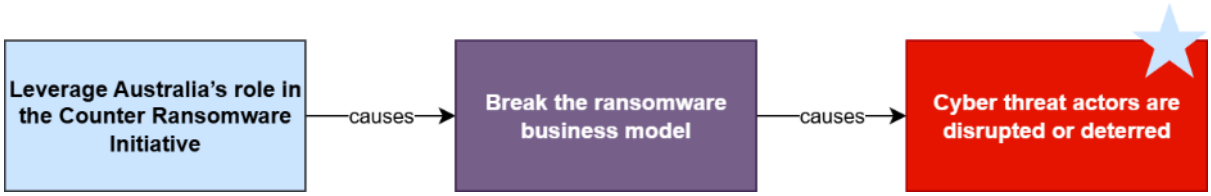
Recommendation 4: Use scientific thinking and approaches

Incorporate rigorous, evidence-based methods — including literature reviews, systematic reviews, meta-analyses, systems thinking, red team analysis, game theory, and quantitative modelling — into the strategy development process.

Without the application of such scientific approaches, policy interventions are unlikely to be effective, and cyber adversaries will maintain a clear and enduring advantage.

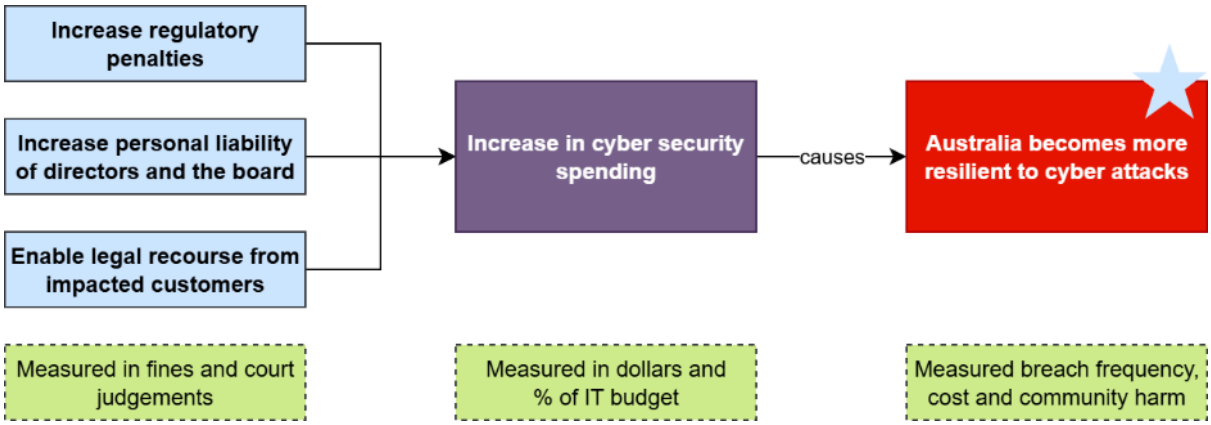
Recommendation 5: Prioritise strong causal links

Here's an example of a causal link implied in the Cyber Security Strategy Horizon 1:



The principal issue is the absence of a clearly articulated mechanism by which the Counter Ransomware Initiative disrupts the operational model of ransomware actors – indeed, it remains uncertain whether such disruption is achievable at all. Furthermore, empirically demonstrating that threat actors are being materially deterred or disrupted presents significant methodological challenges. Consequently, while the initiative may be conceptually appealing, establishing and evidencing a measurable return on investment (ROI) will be highly problematic in practice.

It is therefore recommended that the strategy incorporate interventions with well-defined and demonstrable causal linkages to desired outcomes – linkages that are both measurable and supported by empirical evidence of effectiveness. For example:



In the example above, it is feasible to measure whether negligent businesses are being subjected to penalties, or whether customers are successfully pursuing legal action against such entities following the compromise of their personal data.

It is likewise possible to track changes in cybersecurity budget allocations over time.

Finally, existing datasets from the Australian Signals Directorate (ASD) and the Office of the Australian Information Commissioner (OAIC) can be utilised to evaluate whether the frequency and impact of breaches are demonstrably decreasing.

Recommendation 6: Mandate measurement for all interventions

If one truly understands the mechanism by which an intervention disrupts a cyber adversary, then its effectiveness can be measured. Established methodologies, such as Douglas Hubbard's *Applied Information Economics* or the FAIR Institute's *Factor Analysis of Information Risk*, offer rigorous means of doing so – and proving it.

Instituting a requirement that *every* intervention be measured imposes a deliberate and salutary burden: it compels your team to articulate, with clarity and precision, the rationale for the expenditure of resources, the probable range of return on investment (ROI), and the prioritisation of interventions with demonstrably superior ROI.

It also functions as a quiet but revealing diagnostic – exposing ideas whose foundations are insufficiently developed or inadequately understood.

Recommendation 7: Map interventions to risk scenarios

In cybersecurity, the process begins by identifying the critical "doomsday" scenarios and selecting the most effective controls to mitigate them. Their value should then be validated through before-and-after measurements that prove actual risk reduction.

To illustrate this approach with a simple example: we might assess how many accounts rely on weak passwords without MFA, or commission a penetration test to demonstrates the exploitation of critical vulnerabilities. After implementing controls, we can then demonstrate that specific attack methods are no work – and we have therefore proven that the risk has been reduced.

The same approach should be used with the Australian Cyber Security Strategy:

Threat Actor(s)	Intervention	Measurement
Label/Name	*Describe the intervention*	*Where's the proof that the intervention works?*

One should note that:

- Not all interventions will affect threat actors – that's acceptable if they serve another strategic goal
- Some interventions will impact multiple threat actors
- Some threat actors might be capable of avoiding or evading all the interventions
- The risk of some threat actors should be accepted based on your risk appetite

Conclusion

Applying an adversarial methodology to the Australian Cyber Security Strategy enabled a systematic review of every intervention in Horizon 1 and every action area in Horizon 2, assessing their potential effectiveness against a defined threat actor. While this approach has limitations, it rendered the strategy both quantifiable and measurable, and it is replicable by any subject matter expert seeking to “soft test” the strategy against adversaries they regard as priority targets.

The analysis revealed two key findings:

- First, just over one-third of the strategy’s measures appear directly relevant to impacting threat actors (this is not necessarily a problem).
- Second, many interventions are articulated only at a high level, with insufficient data to verify their likely effectiveness – this should be addressed.

This creates an opportunity for Home Affairs, working together with industry and subject matter experts, to sharpen strategic goals, ensure interventions are measurable, strengthen causal links, use scientific methods, and align all actions with reducing the risks posed by specific scenarios and threat actors.

Appendix A - Analysing Horizon 1 Interventions from the Perspective of a Cyber Adversary

All interventions listed in Horizon 1 were reviewed and assessed by asking: "*Does this intervention deter, detect, delay or defend against a cyber adversary like Policy Ghost?"*

Four possible ratings were used:

- **Not Applicable:** No effect on Policy Ghost's operations.
- **Low Impact:** Minimal effect.
- **Monitor:** Relevant, but current effectiveness could not be measured.
- **Strong Impact:** Would measurably deter, disrupt, or increase the cost of their operations.

Detailed Results:

#	Interventions	Impact
1a	Create cyber 'health checks' for small and medium businesses	**Not Applicable**
1b	Small Business Cyber Security Resilience Service	**Not Applicable**
2a	National Cyber Security Awareness Campaign	**Low Impact**
2b	Fund grants to community organisations	**Not Applicable**
3a	Amplify current cybercrime disruption activities	**Monitor**
3b	Drive global cooperation to effectively prevent, deter and respond to cybercrime	**Monitor**
3c	Build regional capabilities to fight cybercrime	**Monitor**
4a	Mandatory no fault, no liability ransomware reporting obligation	**Not Applicable**
4b	Create a ransomware playbook	**Low Impact**
4c	Leverage Australia's role in the Counter Ransomware Initiative	**Monitor**
5a	Provide industry with additional information on cyber governance obligations under current regulation	**Not Applicable**
5b	Cyber Incident Review Board	**Not Applicable**
6a	Single reporting portal for cyber incidents	**Not Applicable**
6b	Limited use obligation is now law	**Not Applicable**
6c	Code of practice for cyber incident response providers	**Monitor**
7a	Expand the Digital ID program	**Low Impact**
7b	Continue support for victims of identity crime	**Not Applicable**
8a	International security standards for consumer grade smart devices	**Not Applicable**
8b	Labelling scheme to measure the cyber security of smart devices	**Not Applicable**
8c	Voluntary cyber security code of practice for app stores and app	**Not Applicable**
8d	Work with Quad partners to harmonise software standards for government procurement	**Not Applicable**
8e	Framework for assessing the national security risks	**Not Applicable**
9a	Review to identify and develop options to protect Australia's most sensitive and critical data sets	**Not Applicable**

#	Interventions	Impact
9b	Review Commonwealth legislative data retention requirements	**Not Applicable**
9c	Review the data brokerage ecosystem	**Not Applicable**
9d	Design a voluntary data classification model	**Not Applicable**
10a	Embed cyber security into our work on responsible AI to help ensure that AI	**Not Applicable**
10b	Set standards for post-quantum cryptography	**Not Applicable**
11a	Executive Cyber Council as a coalition of government and industry leaders	**Not Applicable**
11b	Enhance ASD's existing threat sharing platforms	**Monitor**
11c	Launch a threat sharing acceleration fund	**Monitor**
11d	Encourage and incentivise industry to participate in threat sharing platforms	**Monitor**
12a	Next-generation threat blocking capabilities across Australian networks	**Monitor**
12b	Encourage and incentivise threat blocking across the economy	**Monitor**
13a	Align telecommunication providers to the same standards as other critical infrastructure entities	**Not Applicable**
13b	Clarify the regulation of managed service providers under the SOCI Act	**Not Applicable**
13c	Incorporate cyber security regulation as part of expanded 'all hazards' requirements for the aviation and maritime sectors.	**Not Applicable**
13d	Protect the critical data held, used and processed by critical infrastructure	**Monitor**
14a	Activate enhanced cyber security obligations for Systems of National Significance	**Monitor**
14b	Finalise a compliance monitoring and evaluation framework	**Not Applicable**
14c	Expand crisis response arrangements to ensure they capture secondary consequences from significant incidents	**Not Applicable**
15a	Enable the National Cyber Security Coordinator to oversee the implementation and reporting of cyber security uplift	**Not Applicable**
15b	Develop a whole-of-government zero trust culture	**Not Applicable**
15c	Conduct regular reviews of the cyber maturity of Commonwealth entities	**Not Applicable**
15d	Designate 'Systems of Government Significance' that need to be protected with a higher level of cyber security	**Not Applicable**
15e	Developing the cyber skills of the APS	**Not Applicable**
16a	Expand our National Cyber Exercise Program	**Monitor**
16b	Develop incident response playbooks	**Low Impact**
17a	Attract global cyber talent through reforms to the migration system	**Not Applicable**
17b	Provide guidance to employers to target and retain diverse cyber talent	**Not Applicable**
17c	Build a framework for the professionalisation of the cyber workforce	**Not Applicable**
18a	Provide cyber start-ups and small-to-medium enterprises with funding to develop innovative solutions to cyber security challenges	**Not Applicable**

#	Interventions	Impact
19a	Refocus Australia's cyber cooperation efforts	**Not Applicable**
19b	Build a regional cyber crisis response team	**Monitor**
19c	Pilot options to use technology to protect the region at scale	**Monitor**
20a	Collaborate with partners in international standards development forums	**Not Applicable**
20b	Advocate for digital trade rules	**Not Applicable**
20c	Continue to defend an open, free, secure and interoperable internet in international forums	**Not Applicable**
20d	Continue to uphold and improve the framework of responsible state behaviour in cyberspace	**Monitor**
20e	Increase costs for malicious cyber actors	**Low Impact**

My time for this assessment was limited, and I do not claim special insight into all these interventions. Nonetheless, it serves as a starting point to highlight which measures could meaningfully impact a threat actor like Policy Ghost, and to prompt the strategy's authors to clearly articulate why they believe their interventions will be effective – and provide the evidence.

Appendix B - Analysing Horizon 2 Action Areas from the Perspective of a Cyber Adversary

All action areas listed in Horizon 2 were reviewed and assessed by asking: "*Does this intervention deter, detect, delay or defend against a cyber adversary like Policy Ghost?"*

Four possible ratings were used:

- **Not Applicable:** No effect on Policy Ghost's operations.
- **Low Impact:** Minimal effect.
- **Monitor:** Relevant, but current effectiveness could not be measured.
- **Strong Impact:** Would measurably deter, disrupt, or increase the cost of their operations.

Detailed Results:

#	Interventions	Impact
1a	Consolidate our cyber awareness messages across the economy	**Not Applicable**
1b	Increase cyber literacy in school programs	**Not Applicable**
1c	Target resilience uplift to small entities that cannot adequately protect themselves, including through giving small business clear and low- or no-cost cyber standards to apply	**Low Impact**
1d	Enhance support for citizens and victims of cybercrime to help them bounce back quicker	**Not Applicable**
1e	Harmonise and simplify cyber regulation to promote best practice and efficiency	**Not Applicable**
2a	Interventions to protect Edge devices	**Not Applicable**
2b	Interventions to protect Consumer energy resources	**Not Applicable**
2c	Interventions to protect Operational technologies	**Not Applicable**
2e	Interventions to manage vendor risks	**Not Applicable**
2f	Promote the safe use of emerging technology	**Monitor**
3a	Encourage and enable the private sector to block threats and take a more proactive posture against cyber threat actors	**Monitor**
3b	Amplify existing government and industry models for threat sharing and blocking	**Monitor**
3c	Reviewing policy frameworks as necessary for resilience to a widespread incident, conflict or crisis situations to protect Australia's national interests	**Not Applicable**
3d	Managing vulnerability disclosure	**Not Applicable**
4a	Maturation of our regulatory framework for critical infrastructure security	**Monitor**
4b	Centralising cyber security risk management and prioritisation of investment and policy interventions to drive Commonwealth cyber uplift	**Not Applicable**
5a	Promote a sustainable and diverse cyber workforce and business ecosystem	**Not Applicable**

#	Interventions	Impact
5b	Provide greater support for academic research and strengthen collaboration between academia, industry and government	**Not Applicable**
5c	Nurture the growth and development of robust sovereign capabilities	**Not Applicable**
6a	Continuing to use all arms of statecraft to deter and impose costs on state and non-state malicious cyber actors	**Monitor**
6b	Strengthening cyber resilience and cooperation on critical technologies in the region and reinforcing Australia's partner of choice status	**Monitor**
6c	Continuing to shape, uphold and defend international cyber rules norms and standards in our interests	**Monitor**
6d	Driving a program of international regulatory alignment and enhancing regional cyber policy and regulatory capacity	**Monitor**

My time for this assessment was limited, and I do not claim special insight into all these action areas. Nonetheless, it serves as a starting point to highlight which measures could meaningfully impact a threat actor like Policy Ghost, and to prompt the strategy's authors to clearly articulate why they believe their interventions will be effective – and provide the evidence.

References

1. Australian Department of Home Affairs, “Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy” (2025). Available at: https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/consultation-horizon-2-of-2023-2030-australian-cyber-security-strategy [Accessed 10 August 2025]

2. FAIR Institute, “Announcing a FAIR Taxonomy for Cyber Risk Scenarios” (2025). Available at: https://www.fairinstitute.org/blog/announcing-a-fair-taxonomy-for-cyber-risk-scenarios

3. Wikipedia, “Framing Effect (psychology)”. Available at: https://en.wikipedia.org/wiki/Framing_effect_(psychology)

4. Paulina Kovic, Seth Doyle, Victor Tyler, “Cognitive Biases in Strategic Decision-Making: Unravelling the Psychological Barriers to Rational Leadership”. Available at: https://www.researchgate.net/publication/391704738_COGNITIVE_BIASES_IN_STRATEGIC_DECISION-MAKING_UNRAVELING_THE_PSYCHOLOGICAL_BARRIERS_TO_RATIONAL_LEADERSHI

5. University of Foreign Military and Cultural Studies, Red Team Handbook (2018). Available at: https://home.army.mil/wood/application/files/6115/8222/0759/RedTeamHB.pdf

6. UK Ministry of Defence, Red Teaming Handbook, Third Edition (2021). Available at: https://assets.publishing.service.gov.uk/media/61702155e90e07197867eb93/20210625-Red_Teaming_Handbook.pdf

7. Home Affairs, “Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy” (2025). Available at: https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/charting-new-horizons-horizon-2-policy-discussion-paper.pdf