Strategic surprise in the 21st century:

Complexity, systems failure, and the rewiring of national security

REPORT

John Coyne, Justin Bassi, Chris Taylor, James Corera, Mike Hughes and Francesca Ciuffetelli

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

25 YEARS 2001–2026

MARCH 2026

About the authors

John Coyne is Director of National Security Programs at ASPI.

Justin Bassi is Executive Director of ASPI.

Chris Taylor is Head of Statecraft and Intelligence Policy Centre at ASPI.

James Corera is Director of Cyber, Technology and Security Program at ASPI.

Mike Hughes is Director of Defence Strategy Program at ASPI.

Francesca Ciuffetelli is Coordinator of National Security Programs at ASPI.

AI contributed no ideas to this report.

About 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. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

About Reports

Reports deliver original and deeply researched analysis and judgements on issues of strategic significance and ongoing importance. Reports aim to inform and influence national strategic choices with original, deeply researched analysis that surfaces implications, tests assumptions, and may consider future courses of action.

First published March 2026
Published in Australia by the Australian Strategic Policy Institute
ISSN: 3083-2853 (Online), 3083-2861 (Print)

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

@ASPI_org

Cover image: iStockphoto/Martin Nancekievill.

Contents

Executive summary

Despite popular conception, strategic surprise in the 21st century isn't necessarily a failure of intelligence collection or analytical competence. It's a structural consequence of operating in a system defined by interaction density, acceleration and interdependence. In such environments, disruption rarely emerges from a single, hidden threat. It accumulates through continuous pressure, concurrent stressors and cascading effects across political, economic, security and technological domains.

Australia is not unprepared. Its national security system is mature and legislatively grounded. The national intelligence community (NIC) operates as a coordinated enterprise, bringing together agencies established under their own distinct legislative mandates. While the NIC itself isn't constituted as a separate statutory body, it functions as a community under the coordinating responsibilities set out in the *Office of National Intelligence Act 2018* (Cth) (ONI Act). The Defence Strategic Review (2023), the Independent Intelligence Review (2024) and the National Defence Strategy (2024) explicitly recognise the convergence of defence, economic security and national resilience.[1] The challenge is therefore not institutional absence, but institutional alignment to tempo.

This report demonstrates that 20th-century risk models, built around ranking discrete threats and allocating resources accordingly, are no longer sufficient in high-interaction systems. Prioritisation remains necessary. However, when treated as the organising principle of governance, it risks creating blind spots. It privileges risk items over risk interactions. And it can reinforce portfolio optimisation over systemic coherence.

Drawing on intelligence failure scholarship,[2] complexity theory,[3] forecasting research[4] and polycrisis analysis,[5] this report shows that strategic surprise most often results from integration lag, in which the pace of institutional synthesis and decision-making falls behind the pace of environmental interaction.

The solution isn't omniscience, but 'strategic fitness'.

Strategic fitness is the adaptive capacity of national systems to integrate horizontally, to decide at tempo, and to recover quickly under concurrent stress. It shifts the performance standard from predictive precision to integration speed and recovery time. It recognises that surprise can't be eliminated, but it can be prevented from cascading into strategic defeat.

Australia's advantage in the coming decade won't depend on forecasting every contingency. It will depend on whether its institutions can observe earlier, synthesise faster, act decisively and sustain coherence under pressure.

This report provides a pragmatic reform pathway to embed strategic fitness within Australia's existing institutional architecture. This report isn't an academic exercise or an abstract theoretical intervention. It's the product of deep analysis and lived experience by intelligence practitioners who collectively bring more than a century of operational and strategic service within Australia's NIC, reflecting candidly on where the system has come from, what it has learned under pressure, and where it must now aim if it's to remain fit for purpose in an era of structural acceleration and complexity.

Recommendations

Recommendation 1: Establish a National Intelligence Community Systemic Risk Synthesis Capability. Consistent with Recommendation 23 of the 2024 Independent Intelligence Review, the Office of National Intelligence (ONI) should formalise and expand existing work by designating a small cross-domain synthesis and warning methodology cell, embedded in and reinforcing ONI's all-source analytical teams. Its mandate would be to map interaction risks across the economic, technological, infrastructure and security domains, strengthen NIC-wide warning tradecraft, and provide quarterly systemic risk briefings to the National Security Committee of Cabinet. This function wouldn't duplicate collection or portfolio analysis, nor create a stand-alone strategic warning centre; rather, it would focus on identifying cascade pathways, integration gaps and cross-portfolio friction points in a polycrisis environment. Progress should be measured through the delivery of quarterly cross-domain assessments and an independent review after two years, evaluating improvements in synthesis speed, warning tradecraft maturity and cross-portfolio integration across the NIC.

Recommendation 2: Mandate concurrency stress-testing in national-security exercises. All major national-level security exercises should incorporate multidomain concurrent stress scenarios, including economic coercion, cyber disruption and regulatory or information pressures. The objective is to test decision tempo and delegated authority under realistic conditions of simultaneity. Success should be measured by tracking reductions in cross-agency decision-cycle times across successive exercises and documenting the closure of identified integration bottlenecks within defined implementation windows.

Recommendation 3: Implement federated data interoperability across the NIC. Consistent with and enabled by the Top Secret (TS) Cloud initiative, agencies should adopt interoperable federated data standards that permit secure analytic access across classification levels while preserving custodianship and statutory accountability. TS Cloud should act as a catalyst for common architectures, identity management and cross-domain solutions that enable authorised discovery and analysis without centralising holdings or fragmenting Top Secret and lower classified data into isolated pools. Progress should be measured by the proportion of priority analytic datasets accessible through federated protocols on TS Cloud-enabled environments, demonstrable reductions in cross-agency data request processing times, and evidence that cross-classification synthesis is strengthened rather than siloed.

Recommendation 4: Embed cross-domain integration metrics in Senior Executive Service performance frameworks. Senior Executive Service performance agreements already include references to cooperation and collaboration, particularly with external stakeholders and across departments—and, where appropriate, across portfolios. However, cooperation isn't the same as integration. Cooperation implies consultation and information sharing; integration requires shared objectives, joint accountability and coordinated policy design, risk assessment and recovery planning across portfolios. This recommendation therefore represents a shift from encouraging collaborative behaviour to embedding measurable cross-domain integration outcomes. Those metrics should be designed to incentivise collaboration not merely across business units within agencies, but across departmental and functional boundaries where shared outcomes depend on joint effort. Performance frameworks should include explicit integration and recovery benchmarks—such as jointly owned risk modelling, coordinated contingency planning and shared system-level outcomes—with promotion and remuneration decisions reflecting demonstrated cross-portfolio effectiveness rather than evidence of goodwill alone.

Recommendation 5: Produce an annual Strategic Fitness Assessment. The government should institute a classified annual Strategic Fitness Assessment that measures integration speed, delegated authority effectiveness, and recovery performance across portfolios. This assessment should establish a baseline integration-lag index and track improvement over time. Success would be reflected in demonstrable reductions in cross-portfolio decision delays and improved recovery benchmarks during stress events.

Recommendation 6: Clarify and rehearse delegated authority in multidomain contingencies. Cabinet-endorsed protocols should define pre-delegated authority thresholds for responding to multidomain contingencies, including economic coercion, significant cyber incidents and critical infrastructure disruptions. Those authorities should be exercised regularly to ensure alignment between environmental tempo and institutional response. Progress should be measured through documented reductions in both escalation delay and precipitous escalation during exercises and real-world incidents.

Each recommendation could be implemented individually. Collectively, these recommendations align Australia's existing legislative and institutional foundations with the structural realities of interaction density and acceleration. The measurable outcome is straightforward: reduced integration lag, faster coordinated decisions under concurrent stress and demonstrably shorter recovery times across critical sectors. That's the practical expression of strategic fitness.

1. The structural persistence of strategic surprise

Strategic surprise has accompanied modern statecraft for decades, but its character has changed. The attacks of 11 September 2001, were not, in retrospect, a story of absent warning. The 9/11 Commission made clear that relevant information existed. Still, it was fragmented across agencies, constrained by institutional assumptions, and slowed by structural seams that proved more consequential than the signals themselves.[6] The lesson wasn't simply about intelligence tradecraft. It was about institutional design.

That pattern is neither uniquely American nor confined to terrorism. The literature on intelligence failure consistently emphasises cognitive bias, bureaucratic fragmentation and organisational inertia as central explanatory variables.[7] Richard Betts famously argued that intelligence failures are 'inevitable' not because analysts lack skill, but because organisations struggle to overcome ambiguity, conflicting evidence and political context.[8] Robert Jervis demonstrated how perceptual biases and entrenched assumptions shape the interpretation of signals, even when data is available.[9] Those insights remain salient, but they require updating for an era defined by acceleration and systemic interdependence.

Subsequent episodes, including the rise of the Islamic State in Iraq and Syria, the 7 October 2023 attacks in Israel and China's economic coercion of Australia, reveal a recurring structural pattern. Signals are generated. Reporting accumulates. Assessments circulate. Yet synthesis lags. Strategic surprise occurs not because information was invisible, but because systems couldn't integrate and respond at the speed that the environment demanded.

Australia's China policy turbulence in 2017–2018 illustrates this dynamic. Intelligence analysts had long identified the divergence between China's formal diplomatic engagement and its increasingly hostile strategic behaviour. However, policy agencies responsible for advancing the bilateral relationship struggled to integrate that evolving threat environment into strategic planning. The resulting policy sclerosis delayed coherent government response and left

ministers to make national-security decisions in the absence of timely, coordinated policy advice.

Strategic surprise in the 21st century is therefore not an episodic breakdown in otherwise stable planning systems. It's a structural feature of a strategic environment defined by complexity, speed and deep interdependence. Thomas Homer-Dixon's work on complex systems stresses that tightly coupled, high-speed systems are inherently more prone to cascading breakdown when buffers erode.[10] Charles Perrow's theory of 'normal accidents' similarly suggests that in complex, tightly coupled systems, failure isn't aberrational but systemic.[11] Applied to national-security governance, those insights suggest that surprise isn't an anomaly, but an emergent property of system design under conditions of interaction density.

For much of the late 20th century, strategic planning—by design as much as by circumstance—assumed that threats were relatively discrete, escalation broadly linear, and crises episodic, reflecting a conscious choice to organise policy around a unifying strategic objective that disciplined prioritisation and resource allocation. Risk-management frameworks were built around probability and consequence, reinforcing prioritisation as the central organising principle. In more stable environments, that provided coherence and focus; however, once that unifying goal fractured—particularly after 1991—the same structures proved less adaptive to diffuse, interacting risks. In complex environments, such assumptions can produce blind spots. Nassim Nicholas Taleb's analysis of 'black swan' events underscores the limits of probabilistic forecasting in fat-tailed systems, where rare but consequential events dominate outcomes.[12] The issue isn't merely statistical; it's institutional. Systems designed to optimise efficiency under known conditions become brittle when subjected to nonlinear stress. This report frames contemporary strategic surprise through the interaction of three structural dynamics (continuous, concurrent and cascading risk), amplified by volume, velocity and variety.

Risk is continuous because strategic competition is persistent rather than episodic. As Adam Tooze has described in the context of 'polycrisis,' modern pressures don't arrive sequentially; they overlap and reinforce one another.[13] Continuity erodes the distinction between crisis and normality, challenging institutions that rely on episodic mobilisation.

Risk is concurrent because multiple stressors materialise simultaneously across economic, technological, political and security domains. Barry Buzan's sectoral approach to security recognised decades ago that security dynamics extend beyond the military domain.[14] Today, concurrency across sectors is routine rather than exceptional. Economic measures, cyber activity and information campaigns unfold in parallel, overwhelming systems structured along portfolio lines. For example, Russia's 2022 invasion of Ukraine saw coordinated military operations accompanied by cyberattacks on critical infrastructure, energy coercion against Europe, sanctions and countersanctions. It sustained information campaigns that interacted in real time to compound strategic effects.

Risk is cascading because disruption propagates across interconnected systems. Work on systemic risk in financial and infrastructure networks shows how shocks can spread through tightly coupled nodes, producing second- and third-order effects that exceed the initial disturbance.[15] Cascades explain why manageable stress can transform into a systemic crisis when integration and recovery lag.

The 'three Vs' of complexity intensify these structural conditions.

Volume challenges cognition and institutional bandwidth. As Herbert Simon observed, 'a wealth of information creates a poverty of attention.'[16] Volume amplifies the difficulty of distinguishing signal from noise. It increases the likelihood that weak signals are missed amid routine reporting demands.

Velocity compresses decision cycles. David Snowden's Cynefin framework emphasises that, in complex environments, cause and effect are coherent only in retrospect, requiring adaptive rather than predictive responses.[17] Faster feedback loops reduce the time available for deliberation and heighten the risk of reactive rather than strategic decision-making.

Variety increases the heterogeneity of actors and methods. Philip Tetlock's research on expert political judgement demonstrated the inherent limits of forecasting accuracy in complex geopolitical environments.[18] Even with structured methods and aggregation, improvements in forecasting can't eliminate uncertainty.[19] This reinforces a structural conclusion: predictive refinement alone can't resolve systemic vulnerability.

Grey-zone and hybrid warfare concepts capture important features of today's competitive environment. Still, they primarily describe adversary behaviour rather than addressing whether our own institutional design is fit for purpose. The core issue is structural misalignment between how the environment now behaves—concurrent, cascading and cross-domain—and how governance systems, which often remain segmented, sequential and siloed, are organised. Strategic surprise is therefore best understood not as a failure to collect information, but as a failure to synthesise across domains, to decide under compression, and to act before cascading effects compound. Australia's exposure is real. Economic openness, reliance on global supply chains, infrastructure interdependence and democratic transparency increase both opportunity and vulnerability. Strategic surprise isn't hypothetical. It's an enduring condition of complex, accelerated systems.

The policy challenge isn't to eliminate surprise, which is impossible. It's to prevent surprise from cascading into strategic defeat. That requires building strategic fitness: the institutional capacity to integrate across domains, challenge assumptions, make high-consequence decisions within compressed time frames (even amid ambiguity), and absorb shocks while restoring functionality without prolonged degradation. In a world in which complexity is structural rather than episodic, resilience isn't a slogan. It's a governance imperative.

2. The inheritance of 20th-century risk models

Contemporary debates about strategic surprise often default to the language of 'unknowns' and 'black swans', as if uncertainty itself were new. It isn't. What's new is the degree to which our inherited approaches—how we structure planning, define priorities, allocate attention and govern risk—assume a world that behaves more sequentially and more legibly than the one we now inhabit.

Modern risk management emerged from actuarial science, economics and engineering reliability theory, and it delivered a powerful promise: if risks can be identified, measured and ranked, they can be managed. That logic (probability times consequence), translated into a prioritised list, became institutional common sense across both corporate governance and public administration. In business strategy, Porter's 'competitive strategy' helped to embed an analytical mindset that treated competition as a set of identifiable forces that could be mapped and countered through deliberate positioning.[20] In enterprise governance, frameworks such as the Committee of Sponsoring Organisations of the Treadway Commission's Enterprise Risk Management—Integrated Framework codified the idea that organisations could comprehensively identify events, assess risks and respond through structured control and reporting mechanisms.[21] International standards such as ISO 31000 reinforced similar principles—risk can be treated as a management process that's systematic, repeatable and applicable across sectors.[22]

Those frameworks weren't naive; they were fit for purpose in environments in which key risks were relatively bounded, crises were episodic, and decision cycles were slow enough to allow deliberation. Nevertheless, they were also frequently misinterpreted: management—fundamentally about mitigation and trade-offs—morphed in the eyes of some decision-makers into an expectation of risk elimination, reinforcing a false sense of controllability. They aligned with the operating logic of 20th-century institutions: organise vertically, optimise for efficiency, and treat disruption as an interruption of 'normal operations'. National-security planning inherited the same. Intelligence collection management, force-structure planning and contingency development all leaned towards the same design: identify major threats, rank them, and allocate scarce attention and resources accordingly. At its best, that produced discipline. It also shaped a professional culture: if you can't name the top priorities, you aren't serious; if you can't rank risks, you aren't governing.

The problem is that prioritisation became more than a technique. It became a world view.

One of the most persistent myths in national security is that strategic effectiveness requires narrowing attention to a small number of priorities. That belief is embedded in planning cycles, briefing templates, risk registers and ministerial expectations. Finite resources and limited cognitive bandwidth usually justify it. The justification is real. The conclusion is not. In complex strategic environments—particularly in Australia's experience over the past quarter of a century, as the strategic picture has intensified and diversified—prioritisation has often become less robust precisely as interdependence has increased. Excessive focus can be destabilising rather than clarifying.

Prioritisation doesn't eliminate risk; it redistributes it—often into blind spots, seams and 'grey areas' where accountability is diffused, and adversaries can operate with advantage. That doesn't mean abandoning organising principles. A central organising logic—such as managing the risks associated with coercive hegemony in the Indo-Pacific—can provide coherence in capability development and acquisition. However, it should function as a framing discipline, not as a narrowing device. In other words, a central organising principle should guide integration across domains—economic security, technology, critical infrastructure, influence, supply chains—not compress them into a single dominant threat lens that suppresses peripheral but compounding risks. The challenge is to combine strategic coherence with systemic breadth: aligning capability decisions with a unifying objective while preserving institutional capacity to detect, synthesise and respond to risks that don't neatly fit within the primary frame.

Conventional prioritisation assumes that threats can be ranked, probabilities estimated and responses staged. It assumes that risks emerge sequentially and can be handled one at a time. That logic depends on a relatively stable environment in which cause and effect are legible, and the main tasks are selection and allocation. However, contemporary strategic competition is defined less by isolated shocks than by interaction: economic pressure colliding with regulatory ambiguity, information activity amplifying political friction, cyber disruption compounding operational uncertainty, and all of it unfolding at a pace that compresses learning cycles.

This is where the inherited models begin to fail. They aren't 'wrong'; they're incomplete. They're optimised for managing known categories of risk under conditions of relative stability. They're brittle under interaction density.

Herbert Simon made the essential point decades ago: as information grows, attention becomes the binding constraint—organisations face 'an information-rich world' in which decision systems must be designed around the scarcity of attention and processing capacity.[23] Advances in computational power and artificial intelligence partially relax the processing constraint: machine-learning systems can ingest, sort and correlate volumes of data far beyond human capacity, accelerating pattern recognition and anomaly detection. Nevertheless, that doesn't dissolve Simon's dilemma. Artificial intelligence expands processing; it

doesn't replace judgement. The contemporary environment, therefore, intensifies Simon's warning: the challenge isn't simply collecting or even processing more, but deciding what deserves attention, integrating across fragments, exercising calibrated judgement under uncertainty, and acting before opportunities close. The human bottleneck has shifted from data handling to sensemaking, accountability and decision authority—and that constraint remains irreducibly institutional. Complexity theory sharpens the critique. Holland's work on complex adaptive systems emphasised that system-level behaviour can be emergent and not reducible to parts; interactions matter as much as—or more than—individual variables.[24] Snowden and Boone's Cynefin framework translated similar ideas into decision practice: in complex contexts, cause and effect are coherent only in retrospect, and leaders must privilege adaptation and sensemaking over linear prediction.[25] Taleb's critique of probabilistic confidence adds a further warning: in fat-tailed environments, rare and high-impact events dominate outcomes, and conventional models systematically underestimate the influence of extreme discontinuities.[26] These aren't abstract academic debates. They map directly onto why modern systems are surprised.

The deeper issue is that prioritisation frameworks, whether in corporate enterprise risk management or national-security threat ranking, are typically designed around risk items rather than risk interactions. They produce lists, not pathways. They allocate resources to 'top risks,' but often fail to examine how moderate stressors combine into systemic overload. They encourage confidence because they look controlled: colour-coded matrices, ranked registers, tidy dashboards. But control isn't the same as resilience.

Charles Perrow's theory of 'normal accidents' is a useful bridge between complexity theory and institutional reality. Perrow argued that in complex, tightly coupled systems, accidents aren't aberrations; they're an expected product of system design.[27] The analogue for strategic surprise is straightforward: in tightly coupled governance systems—in which decisions and dependencies are interlinked across infrastructure, markets, regulation and security—surprise becomes a normal output when integration lags interaction.

That's why narrow prioritisation can create the illusion of control while masking systemic fragility. It encourages the deferral of ambiguous, cross-cutting or uncomfortable risks—those that don't sit neatly in one portfolio, those that demand shared ownership, those that look 'low probability' until they combine with something else. It reinforces confirmation bias around what's already deemed important. Moreover, it rewards a bureaucratic behaviour that's rational at the unit level but corrosive at the system level: optimise your own lane, protect your mandate, and treat spillover as someone else's problem.

The point isn't to abandon prioritisation. In democratic systems with finite resources, prioritisation is politically and operationally unavoidable. The point is to end the belief that a single-ranked list is an adequate model of strategic risk. In a world characterised by continuous pressure, concurrent stressors and cascading effects—amplified by volume, velocity and variety—strategic surprise is the predictable result of treating interaction as a secondary issue.

The practical implication is that national security and enterprise governance should move from a selection model to a systems model. The organising question changes. It's no longer 'What are the top three threats?' It's 'Which combinations of stressors could overwhelm institutional capacity, and where will integration fail first?' That shift is demanding because it challenges the inheritance of 20th-century management: it requires institutions to look sideways across portfolios, to treat time and tempo as strategic variables, and to measure preparedness not only by plans and priorities, but also by recovery capacity and decision speed under pressure.

That's the transition this report argues for: from the comfort of prioritisation to the discipline of systems fitness—without losing strategic focus, but without mistaking focus for resilience.

3. Interaction density and environmental acceleration

Contemporary strategic environments aren't simply more dangerous; they're more densely interconnected. The defining feature of this era isn't the existence of risk, but the density of interaction among political, economic, security and technological systems. Strategic effect increasingly emerges from how pressures combine rather than from the magnitude of any single event.

Economic interdependence binds competitors together in ways that blur the line between cooperation and coercion. Global supply chains, capital flows and market access create both resilience and leverage. As Henry Farrell and Abraham Newman have argued, the architecture of global economic networks can be 'weaponised', allowing states to exploit central nodes in financial and informational systems to exert influence beyond traditional military means.[28] China's use of trade coercion against Australia in 2020–21—targeting barley, wine, coal and other exports following political disputes—illustrates how economic relationships can be mobilised for strategic

signalling without crossing the threshold of armed conflict. In such an environment, trade policy, sanctions regimes, export controls and regulatory decisions are no longer peripheral to national security—they're integral to it. Economic governance becomes a strategic terrain.

Cybertechnology compounds that interdependence. Civilian and defence systems rely on shared digital architectures, commercial providers and globally integrated platforms. As Martin Libicki observed, cyber operations collapse traditional distinctions between the battlefield and the homeland, and between the state and the private sector.[29] The 2017 NotPetya cyberattack—attributed to Russia—demonstrated how malicious code aimed at Ukrainian systems cascaded through global corporate networks, disrupting shipping, logistics and manufacturing far beyond the initial target set. Networked systems increase efficiency but also increase exposure. Disruption propagates rapidly across nodes, often crossing organisational and jurisdictional boundaries before attribution is clear. Cyber infrastructure doesn't simply create new vulnerabilities; it increases sectoral coupling, amplifying the risk of cascading effects.

Information ecosystems intensify those dynamics further. Digital platforms transmit narratives at scale, compressing the time between event and interpretation. Manuel Castells's analysis of the 'network society' highlighted how communication networks reshape power by altering how information flows and how identities mobilise.[30] During the Covid-19 pandemic, for example, misinformation campaigns intersected with public-health measures, economic disruption and geopolitical blame narratives, magnifying social polarisation and complicating policy responses. Influence activity is rarely decisive in isolation, but it accelerates and amplifies the political consequences of economic shocks, cyber incidents and regulatory disputes. In combination, those domains illustrate the central argument: interdependence doesn't merely create vulnerability in discrete sectors; it fuses them into a tightly coupled system in which stress in one domain rapidly transmits to others.

Regulatory decisions now generate geopolitical effects with increasing regularity—export controls, investment screening, competition-law enforcement and standards-setting shape technological ecosystems and alliance dynamics. As the World Trade Organization and multilateral institutions face strain, national regulatory choices often function as strategic signals.[31] What once appeared as technocratic policy can quickly acquire strategic meaning.

Adam Tooze's description of the present era as one of 'polycrisis' captures this structural shift.[32] Crises no longer arrive in isolation. They interact, overlap and compound. Financial instability intersects with energy shocks. Energy shocks interact with political fragmentation. Public-health emergencies intersect with supply-chain fragility. Continuous pressure erodes recovery time. Systems don't reset between shocks; they absorb one stressor while preparing for another. The cumulative effect is reduced strategic slack.

Concurrency overwhelms institutional bandwidth. Governments and corporations alike are structured around portfolios, committees and sequential decision cycles. When economic coercion, cyber incidents, regulatory disputes and alliance signalling occur simultaneously, coordination becomes the bottleneck. The constraint isn't information availability but synthesis and authority. This is the practical manifestation of Herbert Simon's insight that attention, not information, is the scarce resource in complex systems.[33]

Cascades amplify impact. Research on systemic risk in interconnected networks demonstrates how tightly coupled systems transmit disruption nonlinearly.[34] A shock in one sector can propagate through financial, infrastructural and political systems, generating consequences disproportionate to the initial trigger. In strategic terms, this means that moderate events can produce outsized geopolitical effects when interaction density is high. A contemporary illustration can be seen in the global convulsive effects following the 7 October 2023 attacks on Israel and the subsequent Gaza war. While the earlier intifadas were deeply consequential regionally, their international systemic effects were comparatively contained. By contrast, the 2023 shock propagated rapidly through energy markets, alliance politics, domestic social cohesion, digital information ecosystems and great-power positioning. The difference isn't solely the scale of violence, but the density and immediacy of global interconnection through which the disruption travelled. The now-familiar triad of volume, velocity and variety intensifies those structural conditions.

Volume challenges cognition. Decision-makers face unprecedented quantities of data, analysis and reporting. As Daniel Kahneman's work on cognitive bias illustrates, human judgement under uncertainty relies on heuristics that can distort interpretation when information is ambiguous or overwhelming.[35] Volume increases the risk that critical signals are buried or misclassified.

Velocity compresses deliberation. Events unfold faster than legislative cycles, procurement systems and interdepartmental coordination mechanisms. Snowden and Boone argue that, in complex contexts, decision-makers must privilege rapid experimentation and adaptive learning over predictive certainty.[36] However, many national-security institutions remain optimised for deliberate planning rather than iterative adjustment.

Variety complicates jurisdictional clarity. Threats no longer map neatly onto existing organisational boundaries. Economic security intersects with defence policy. Cyber resilience intersects with private-sector governance. Information operations intersect with domestic political discourse. Barry Buzan's expansion of security studies beyond the military sector anticipated this broadening

of the security agenda.[37] Today, that expansion is operational rather than theoretical. The 2024 Independent Intelligence Review, for example, commendably recognised economic security as central to Australia's future intelligence effort. Yet its implementation recommendations largely default to assigning primary responsibility to Treasury (recommendations 13 and 14).[38] That instinct reflects established portfolio structures, but it also illustrates the challenge identified here: as issue-variety expands across domains, responses continue to be anchored within traditional departmental lead-agency models. In a high-interaction environment, however, economic security isn't solely a fiscal or regulatory matter; it's simultaneously industrial, technological, strategic and geopolitical. Assigning a single portfolio lead might provide administrative clarity, but it doesn't resolve the systemic integration challenge that cross-domain risk now presents.

In this environment, the decisive metric isn't simply threat probability or consequence. It's an integration lag relative to environmental acceleration. When the pace of interaction across economic, technological and political systems exceeds the speed at which institutions can synthesise information and coordinate responses, strategic surprise becomes structurally likely. Integration lag isn't a matter of incompetence; it's a design issue. It reflects how authority, information flows and incentives are structured.

The implication is clear. Strategic resilience in high-interaction environments can't be built solely through better forecasting or more detailed risk registers. It requires institutional architectures capable of operating at tempo—structures that reduce friction across portfolios, integrate signals horizontally, and maintain recovery capacity under concurrent stress. That has both legislative and organisational implications. Australia's intelligence framework—shaped by the original Hope Royal Commission, embodied in the distinct statutory mandates of the ASIO Act and the Intelligence Services Act, and reaffirmed in the 2020 Richardson Review—deliberately constructs functional boundaries between security intelligence and foreign intelligence to protect civil liberties, clarify accountability and prevent mission creep. Those guardrails remain essential. But in a landscape where threats traverse domestic and international domains simultaneously—cyber intrusions, foreign interference, economic coercion—the operational seams between mandates can create latency in information flow, coordination and joint sensemaking if not actively managed.

The task, therefore, is not to dismantle legislative walls, but to ensure that they're complemented by lawful interoperability: clearer authorising provisions for information sharing, harmonised thresholds where appropriate, robust joint analytic mechanisms, and oversight arrangements capable of supervising integrated activity without diluting accountability. Interaction density is not temporary. It's the defining condition of the contemporary strategic landscape. The legal architecture should continue to safeguard rights and democratic control—but it should also enable authorised integration at the speed and scale that high-interaction risk now demands.

4. Strategic fitness as organising principle

The central argument of this report is that contemporary strategic environments have outgrown the linear governance models inherited from the 20th century. If surprise is a structural feature of complex, accelerated systems, then the appropriate response isn't marginal improvement in forecasting accuracy. It's an institutional redesign. Strategic fitness is the organising principle of that redesign.

'Strategic fitness' refers to the adaptive capacity of national systems under conditions of persistent interaction, compressed time and systemic interdependence. It shifts the evaluative standard of preparedness away from predictive precision and towards integration speed, decision tempo, action and recovery capacity. In other words, the question is no longer 'Did we forecast correctly?' but 'Can we observe, orient, decide and act quickly enough to prevent disruption from cascading into strategic defeat?'

This isn't semantic reframing. It's a substantive shift in how national power is conceptualised and measured.

For decades, national-security institutions have invested heavily in prediction—in collection systems, analytic methodologies, scenario planning, risk registers and warning thresholds. Those remain essential. But, as the earlier sections demonstrate, contemporary strategic effect often emerges not from invisible threats but from visible pressures that are mis-integrated or acted upon too slowly. Strategic fitness, therefore, requires a structural rebalancing: forecasting remains important, but adaptation becomes decisive.

Three interlocking pillars underpin strategic fitness.

1. Horizontal integration across systems

The first pillar is horizontal integration across political, economic, security and technological domains. Contemporary strategic competition exploits seams between portfolios. Economic coercion interacts with information activity. Cyber disruption intersects with infrastructure fragility. Regulatory decisions

generate geopolitical consequences. Systems designed vertically struggle to manage horizontally applied pressure.

Strategic fitness, therefore, requires permanent cross-domain synthesis functions. This isn't a duplication of intelligence assessment or policy development. It's institutionalised integration—capability explicitly tasked with mapping interaction risk, identifying cascade pathways and stress-testing systemic vulnerabilities before they're exploited.

This demands interoperable data architectures, shared analytic platforms and common operating pictures that transcend agency boundaries. More importantly, it requires cultural reform. Integration must be rewarded, not treated as an encroachment on mandate. The absence of horizontal integration isn't a technical shortcoming; it's a structural vulnerability.

2. Delegated authority aligned with tempo

The second pillar is authority aligned with tempo.

In environments characterised by velocity and concurrency, delay compounds vulnerability. Decision cycles that were once tolerable become strategically costly. When authority is overly centralised or procedurally constrained, systems accumulate integration lag. By the time consensus forms, adversaries have already secured an advantage.

Strategic fitness, therefore, requires clarity of delegated decision rights and rehearsed escalation pathways. Pre-delegation doesn't weaken accountability; it enhances responsiveness. It ensures that decisions can be made at the level where information is freshest and time compression is most acute.

Exercises should stress tempo, not just procedural compliance. They should simulate concurrency—multiple stressors applied simultaneously—to reveal where authority bottlenecks emerge. Institutions that can't decide under uncertainty will repeatedly experience surprise, regardless of the quality of their information.

Tempo isn't about recklessness. It's about alignment. Decision speed must match environmental speed. Where misalignment persists, vulnerability expands.

3. Recovery design embedded within a national deterrence framework

The third pillar is recovery design embedded within a national deterrence framework; specifically, what's increasingly been described as deterrence by resilience.

Traditional deterrence theory privileges capability and credibility. It assumes that the prospect of retaliation or denial constrains adversaries. Contemporary strategic competition complicates that logic. Strategic effect can now be generated below traditional thresholds, through economic coercion, regulatory leverage, infrastructure disruption, cyber operations or coordinated information campaigns. Those activities aim less at decisive defeat than at cumulative pressure against perceived vulnerabilities.

In this context, resilience isn't merely a protective function. It's a deterrent variable.

Deterrence by resilience rests on a simple strategic proposition: if an adversary assesses that disruption won't produce durable strategic leverage, the incentive to initiate coercion declines. What Australia requires, therefore, isn't the unrealistic capacity to prevent all disruption, but the demonstrable ability to withstand, fight through, and recover rapidly from it, and to communicate that capacity in ways that shape adversaries' perception.

Recovery capacity reduces adversary leverage. If a state can quickly reroute trade, stabilise markets, sustain infrastructure, maintain social cohesion and preserve decision-making coherence under stress, coercive pressure loses potency. Strategic fitness therefore integrates resilience into deterrence architecture. Redundancy in energy systems, diversification in supply chains, sovereign industrial capacity and robustness in digital infrastructure aren't economic luxuries; they're strategic assets.

However, embedding resilience within deterrence requires clarity. Whole-of-nation deterrence is exceptionally difficult to coordinate and implement, particularly in the absence of shared understanding about who or what's being deterred. Departments can't meaningfully contribute to deterrence effects if they don't understand the adversary, the coercive pathways available to that adversary, and the specific vulnerabilities being targeted.

Resilience investments can't be generic. They must be informed by assessment of how an adversary might attempt to coerce Australia, where leverage might be applied, how pressure might accumulate across domains, and which systemic dependencies could be exploited. Developing resilience-enhancing initiatives without this framing risks producing activity without deterrent effect.

Preparedness should therefore be measured not by the absence of disruption, but by recovery performance and maintained coherence under concurrent stress. A system that absorbs disruption and reorients rapidly sends a stronger signal of resolve than one that prevents minor shocks yet fragments under sustained pressure.

This requires changing what's measured. Traditional performance indicators emphasise compliance, process completion and predictive accuracy. In complex environments, the absence of disruption isn't proof of readiness. It may reflect luck, timing or adversary restraint. What matters is how systems behave when stress is applied.

Metrics should therefore include:

- integration speed across portfolios
- decision time under concurrent stress
- recovery duration for critical functions
- ability to sustain coordinated response across domains
- capacity to communicate resilience credibly to external audiences.

Those measures shift focus from static control to adaptive performance. They privilege system behaviour over planning artefacts.

The implications for intelligence communities are significant.

Collection management models historically reflect prioritisation logic: identify top-tier adversaries, allocate collection accordingly, and refine assessments against defined requirements. In interaction-dominated environments, that approach must evolve.

Strategic fitness requires:

- collection strategies that incorporate systemic vulnerability indicators alongside adversary intent
- analytic models that privilege cross-domain synthesis over single-stream depth
- warning frameworks that track stress accumulation and interaction density rather than binary thresholds
- cultural norms that reward integration and challenge dominant narratives.

We shouldn't expect that intelligence and security agencies can collect their way out of complexity. They must instead be empowered to integrate their way through it.

Ultimately, recovery design must sit within a broader mechanism that integrates the tools of statecraft. Defence capability, economic policy, regulatory settings, infrastructure planning, diplomacy and information operations must be coordinated not simply for efficiency, but for cumulative deterrent effect.

Integration itself has deterrent value.

When adversaries perceive that Australian capabilities, activities and investments are aligned and mutually reinforcing, rather than siloed and episodic, the credibility of deterrence increases. Fragmented tools invite probing. Integrated tools raise the expected cost of coercion and reduce confidence in achieving leverage.

Strategic fitness is therefore a whole-of-system standard.

It recognises that national power isn't the sum of portfolios but the product of their interaction. It treats time as a strategic variable and recovery as a performance metric. It acknowledges that strategic surprise can't be eliminated. The objective isn't omniscience, but resilience under pressure.

The decisive advantage accrues not to the actor who predicts every contingency, but to the actor whose institutions can absorb shock, adapt rapidly, and demonstrate that coercion won't achieve strategic effect.

Recovery design embedded within deterrence isn't an abstract concept. It's the practical organising principle for national security in an era in which complexity is permanent and acceleration is structural.

5. Institutional anchoring in Australia

Australia doesn't lack institutional architecture. Its national-security system is structurally mature, legally grounded and strategically aware. Central policy coordination resides within the Department of the Prime Minister and Cabinet (PM&C), which supports the National Security Committee of Cabinet and provides whole-of-government integration at the apex of decision-making. Intelligence leadership is anchored under the ONI Act, which established ONI as the head of the NIC and formalised enterprise-level coordination, assessment leadership and capability evaluation.[39] Critical infrastructure resilience is embedded within the legislative framework of the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), significantly strengthened through amendments that expanded sectoral coverage and cyber obligations.[40]

Strategically, recent policy documents demonstrate recognition of the complexity described throughout this report. The 2023 Defence Strategic Review acknowledged that Australia faces the most challenging strategic environment since the Second World War and emphasised the need for integrated deterrence, national resilience and alignment between defence capability and broader national settings.[41] The subsequent National Defence Strategy further articulated the necessity of whole-of-government approaches to deterrence, preparedness and industrial mobilisation.[42] Those documents don't treat resilience as peripheral. They frame it as foundational.

The institutional problem, therefore, is not absence, but alignment.

Australia's governance system remains predominantly portfolio-structured, legally segmented and procedurally sequenced. That's normal in Westminster systems. Departments are accountable through ministers; mandates are defined through legislation; authority is vertically organised. Under stable conditions, that structure delivers clarity and accountability.

Under conditions of concurrency and cascade, it can generate integration lag.

Cross-domain integration occurs through interdepartmental committees, taskforces, intelligence coordination forums and crisis-response mechanisms. But much of that integration is episodic—triggered by events rather than embedded as a permanent operating architecture. The system is capable of surging coordination. The strategic question is whether it's designed for persistent interaction density.

The ONI Act strengthened intelligence enterprise leadership by formalising ONI's role in coordinating national assessments and evaluating intelligence performance across agencies—building on, but broadening, the assessment coordination function historically exercised by the Office of National Assessments. Yet stronger integration within the NIC doesn't automatically translate into operational integration across economic, regulatory and industrial portfolios, where decision rights, data systems and accountability structures remain distributed.

Similarly, amendments to the SOCI Act have expanded obligations on asset owners and operators, embedding cyber- and risk-management requirements across critical sectors. But regulatory resilience—however necessary—isn't synonymous with systemic integration at tempo across portfolios during concurrent stress. This explains Home Affairs' focus, in parallel, on supporting the uplift of response capabilities by the SOCI operators themselves. The Defence Strategic Review explicitly called for a 'whole-of-nation' approach to national defence.[43] The challenge lies in operationalising that ambition amid acceleration. 'Whole-of-government' can't be reduced to periodic coordination meetings or shared language in strategic documents. It requires standing cross-domain mechanisms that are empowered, data-integrated and tempo-aligned.

This is where strategic fitness intersects directly with Australian institutional design. The structural gap isn't legal authority or strategic recognition. It's the absence of permanent integration functions explicitly tasked with mapping cascade pathways, stress-testing concurrency and aligning delegated authority with environmental speed.

For example, economic coercion, cyber disruption and regulatory responses often span multiple portfolios—Treasury, Foreign Affairs and Trade, Home Affairs, Defence, Industry and PM&C. Each portfolio may perform effectively within its mandate. The systemic vulnerability emerges when interaction across mandates is slower than the pace at which pressures accumulate. The decisive variable becomes integration speed relative to environmental acceleration.

Australia's federal structure adds complexity. States and territories hold significant responsibilities in infrastructure, emergency management and public health. Private-sector actors own and operate substantial portions of critical infrastructure. National resilience is therefore distributed across public and private systems. Legislative reform has improved oversight and reporting obligations, recognising security as a shared responsibility. However, the distribution of responsibility doesn't automatically or necessarily equate to coherent responses.

The institutional anchoring required for strategic fitness is therefore not about creating new bureaucracies for their own sake. It's about ensuring that cross-domain integration is continuous rather than reactive; that delegated authority is pre-aligned to tempo; and that recovery design is embedded across sectors, not layered on after disruption occurs.

Australia's recent strategic documents demonstrate awareness of the challenge. The next step is architectural refinement. Strategic surprise in a high-interaction environment won't result from institutional absence. It will result from institutional friction—where coordination is procedurally possible but temporally misaligned.

The policy implication is measured but clear: Australia's national-security advantage will depend less on adding new frameworks and more on hardwiring integration into the operating logic of existing ones. Strategic fitness needs to become a design principle, not simply a strategic aspiration.

6. Political economy constraints

The structural challenge isn't the absence of institutions. It's operational friction under conditions of concurrency and acceleration.

Reform proposals that imply wholesale structural redesign—such as new super-agencies, sweeping legislative overhauls or permanent cabinet reorganisation—are neither necessary nor politically feasible. Australia's system is designed around ministerial accountability, statutory clarity and portfolio-defined responsibilities. Those are features, not flaws. They provide legitimacy and democratic control. The task is to adapt within that framework, not attempt to replace it.

Portfolio protection is inherent in Westminster governance. Departments are accountable to ministers; ministers are accountable to parliament. Integration initiatives that appear to blur mandate boundaries will encounter resistance unless their purpose is tightly defined and authority clearly authorised. In practice, this means that integration mechanisms must be framed as enhancing, not diluting, ministerial accountability.

Budgetary silos are equally embedded. Appropriations flow through portfolios, and performance is assessed against portfolio outputs. Cross-domain initiatives that require pooled funding or shared

staffing will face scrutiny from central agencies and the parliament. Reform must therefore minimise structural fiscal disruption while demonstrating measurable operational benefit.

Statutory mandates further shape what's feasible. The ONI Act establishes ONI's leadership of the NIC and its role in enterprise evaluation and coordination. That authority provides a foundation for integration, but it doesn't extend into economic, regulatory or industrial portfolios. Similarly, the SOCI Act provides mechanisms for risk management and reporting in designated sectors, but it doesn't create a centralised resilience command structure. Legislative amendment is possible, but politically sensitive and procedurally demanding.

Ministerial risk aversion must also be acknowledged. Reforms that create visible disruption or appear to centralise authority excessively will be approached cautiously, particularly outside periods of acute crisis. Incremental adaptation is more consistent with Australia's political culture than radical restructuring.

Given those constraints, reform must be evolutionary rather than revolutionary. The most pragmatic pathway is to strengthen integrative functions within existing structures rather than create new ones. The NIC already operates as an enterprise under ONI's stewardship. A realistic enhancement would be to formalise a systemic risk synthesis capability within that framework, focused on cross-domain interaction mapping rather than additional collection. Such a function would integrate intelligence assessments with economic indicators, infrastructure stress signals and regulatory developments to identify potential cascade pathways. This wouldn't duplicate portfolio analysis; it would provide structured synthesis at tempo, report through established NIC channels, and preserve statutory clarity.

National exercises also provide a practical reform lever. Australia already conducts security and emergency-management exercises across agencies and jurisdictions. The adjustment required is conceptual rather than legislative: exercise design should deliberately incorporate concurrency and cascade dynamics rather than single-event contingencies. Applying simultaneous economic, cyber and informational stressors in controlled scenarios would reveal integration lag, authority bottlenecks and data friction before adversaries do. This approach requires no new legislation, only disciplined reorientation of planning assumptions and performance metrics.

Data integration should likewise be pragmatic. Centralised repositories often encounter privacy, security and custodial resistance. Federated data architecture—enabling interoperable access under defined protocols while agencies retain control—offers a feasible compromise. Australia's digital transformation initiatives already provide the scaffolding for such interoperability. Extending standards across NIC agencies and relevant economic portfolios would enhance integration speed without triggering institutional alarm over centralisation.

Performance metrics are another realistic reform vector. Senior Executive Service agreements and portfolio reporting frameworks can incorporate cross-domain coordination objectives without legislative amendment. If integration and recovery speed are visible components of performance evaluation, incentives begin to align with strategic fitness objectives. Integration becomes a professional expectation rather than a matter of discretionary cooperation.

It's equally important to acknowledge what's unlikely. Australia is unlikely to create a permanent super-ministry for economic and national-security integration, and it should not. Such centralisation would disrupt established accountability frameworks and encounter sustained resistance. Wholesale restructuring of cabinet or the NIC, absent crisis conditions, is similarly improbable. Proposals that ignore the embedded logic of Westminster governance risk becoming aspirational rather than executable.

Australia's institutional base is comparatively strong. The NIC provides enterprise-level coordination. PM&C anchors central oversight. Legislative frameworks embed resilience obligations across sectors. The practical challenge lies in aligning those mechanisms with environmental tempo and with awareness of cascades. Strategic fitness in the Australian context will emerge not from radical redesign but from the disciplined enhancement of existing authorities: clearer delegated decision pathways in exercises, structured cross-domain synthesis within the NIC, interoperable data standards, and performance metrics that privilege integration and recovery.

Political economy constraints don't negate reform. They shape its feasible trajectory. The realistic strategy is cumulative adaptation anchored in statutory authority and enterprise mechanisms already in place. That approach may lack drama, but it aligns with Australia's institutional culture and democratic norms. In a high-interaction environment, evolutionary integration is more durable than revolutionary change.

The harder question is impetus. In the absence of a crisis, institutional systems default to equilibrium: portfolios defend mandates, reform competes with day-to-day pressures, and integration is deprioritised in favour of immediate deliverables. Kickstarting adaptation, therefore, requires deliberate executive signalling and performance alignment. That can take the form of cabinet-endorsed integration mandates, explicit cross-portfolio key performance indicators tied to secretaries' performance agreements, and routine whole-of-system stress-testing exercises that expose friction points before failure does. Scenario-based exercises, red-teaming and independent capability audits can create constructive pressure by making latent seams visible—generating momentum without waiting for shock.

Sustaining adaptation requires institutionalisation. Reform needs to migrate from initiative to routine: quarterly cross-domain briefs embedded in the processes of the National Security Committee; shared data standards linked to budget incentives; joint analytic postings treated as career-enhancing rather than peripheral. Funding levers matter. Modest, ring-fenced integration funds tied to demonstrable cross-agency collaboration can shift behaviour over time. In short: absent a crisis, the impetus needs to be manufactured through governance design—by embedding integration into performance systems, budget processes and senior leadership expectations so that evolutionary change becomes self-reinforcing rather than episodic.

Conclusion

Strategic surprise in the 21st century isn't a failure of vigilance. It's a feature of the environment.

Australia won't forecast its way out of uncertainty. It won't legislate complexity into submission. It won't eliminate risk by narrowing attention to a ranked list of priorities, however disciplined that list appears. The structural conditions that define this era—interaction density, concurrency, cascade and acceleration—ensure that pressure will arrive from multiple directions at once, and that moderate stressors will combine in ways that outpace linear governance.

The choice isn't between certainty and uncertainty. It's between fragility and fitness.

Australia begins from a position of strength. Its national-security architecture is mature. The NIC operates as an enterprise. Legislative frameworks embed resilience obligations across critical sectors. Recent strategic documents recognise the convergence of economic security, technological competition and defence posture. The system isn't blind to complexity.

But recognition is not adaptation.

The decisive variable in the coming decade will be the speed of integration relative to environmental acceleration. Where integration lags, surprise will compound. Where authority is misaligned with tempo, delay becomes a vulnerability. Where recovery design is secondary to prevention, coercion will retain leverage. Strategic effect will increasingly be generated not by dramatic escalation but by cumulative pressure applied across seams.

Strategic fitness is therefore not a slogan. It's a design standard.

It demands permanent horizontal integration rather than episodic integration. It demands delegated authority aligned with tempo rather than constrained by procedural inertia. It demands recovery capacity embedded within deterrence, so that resilience reduces an adversary's advantage rather than merely mitigating damage after the fact.

This doesn't require revolutionary institutional upheaval. It requires disciplined enhancement of what already exists. It requires the NIC to prioritise cross-domain synthesis alongside depth of collection. It requires national exercises that test concurrency rather than rehearse single contingencies. It requires performance metrics that reward integration and recovery time, not just predictive accuracy. It requires leaders prepared to align incentives with systemic resilience rather than portfolio protection.

The states that prevail in high-interaction environments won't be those that predict every contingency. They'll be those whose institutions can absorb pressure without losing coherence; who can decide at speed without losing legitimacy; who can recover without losing credibility.

Australia doesn't need omniscience. It needs strategic fitness.

In an era where complexity is structural and acceleration is permanent, fitness is national power.

Notes

1 Australian Government, *Defence Strategic Review 2023*, Commonwealth of Australia, 2023; Australian Government, *National Defence Strategy 2024*, Commonwealth of Australia, 2024.

2 RK Betts, 'Analysis, war, and decision: why intelligence failures are inevitable', *World Politics*, 1978, 31(1):61–89. https://doi.org/10.2307/2009978; R Jervis, *Perception and misperception in international politics*, Princeton University Press, 1976.

3 JH Holland, *Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence*, MIT Press, 1992; C Perrow, *Normal accidents: living with high-risk technologies*, Basic Books, 1984.

4 PE Tetlock, *Expert political judgment: How good is it? How can we know?*, Princeton University Press, 2005.

5 A Tooze, 'Welcome to the world of the polycrisis', *Financial Times*, 28 October 2022.

6 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission report: final report of the National Commission on Terrorist Attacks Upon the United States*, US Government Printing Office, 2004.

7 Betts, 'Analysis, war, and decision: why intelligence failures are inevitable'; Jervis, *Perception and misperception in international politics*.

8 Betts, 'Analysis, war, and decision: why intelligence failures are inevitable'.

9 Jervis, *Perception and misperception in international politics*.

10 T Homer-Dixon, *The upside of down: catastrophe, creativity, and the renewal of civilisation*, Knopf, 2006.

11 C Perrow, *Normal accidents: living with high-risk technologies*, Basic Books, 1984.

12 NN Taleb, *The black swan: the impact of the highly improbable*, Random House, 2007.

13 Tooze, 'Welcome to the world of the polycrisis'.

14 B Buzan, *People, states and fear: an agenda for international security studies in the post-Cold War era* (2nd ed.), Harvester Wheatsheaf, 1991.

15 D Helbing, 'Globally networked risks and how to respond', *Nature*, 2013, 497(7447):51–59, https://doi.org/10.1038/nature12047.

16 HA Simon, 'Designing organisations for an information-rich world', in M Greenberger (ed.), *Computers, communications, and the public interest*, Johns Hopkins Press, 1971, 37–72.

17 DJ Snowden, ME Boone, 'A leader's framework for decision making', *Harvard Business Review*, 2007, 85(11):68–76.

18 Tetlock, *Expert political judgment: How good is it? How can we know?*.

19 PE Tetlock, D Gardner, *Superforecasting: the art and science of prediction*, Crown, 2015.

20 ME Porter, *Competitive strategy: techniques for analysing industries and competitors*, Free Press, 1980.

21 Committee of Sponsoring Organisations of the Treadway Commission (COSO), *Enterprise risk management—integrated framework*, AICPA, 2004.

22 International Organization for Standardization (ISO), *ISO 31000:2009 Risk management—principles and guidelines*, ISO, 2009.

23 Simon, 'Designing organisations for an information-rich world'.

24 Holland, *Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence*.

25 Snowden & Boone, 'A leader's framework for decision making'.

26 Taleb, *The black swan: the impact of the highly improbable*.

27 Perrow, *Normal accidents: living with high-risk technologies*.

28 H Farrell, AL Newman, 'Weaponised interdependence: how global economic networks shape state coercion', *International Security*, 2019, 44(1):42–79, online.

29 MC Libicki, *Cyber deterrence and cyberwar*, RAND Corporation, 2009.

30 M Castells, *The rise of the network society* (2nd ed.). Wiley-Blackwell, 2010.

31 CP Bown, 'How COVID-19 medical supply shortages led to extraordinary trade and industrial policy', *Asian Economic Policy Review*, 2020, 15(1):45–63, online.

32 Tooze, 'Welcome to the world of the polycrisis'.

33 Simon, 'Designing organisations for an information-rich world'.

34 Helbing, 'Globally networked risks and how to respond'.

35 D Kahneman, *Thinking, fast and slow*, Farrar, Straus and Giroux, 2011.

36 Snowden & Boone, 'A leader's framework for decision making'.

37 Buzan, *People, states and fear: an agenda for international security studies in the post-Cold War era*.

38 Australian Government, *2024 Independent Intelligence Review*, Commonwealth of Australia, 2024, online.

39 *Office of National Intelligence Act 2018* (Cth), Commonwealth of Australia, 2018.

40 *Security of Critical Infrastructure Act 2018* (Cth), Commonwealth of Australia, 2018.

41 Australian Government, *Defence Strategic Review 2023*.

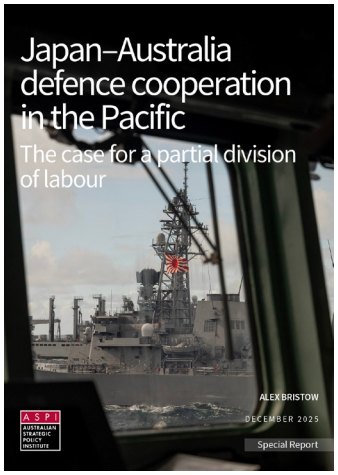
42 Australian Government, *National Defence Strategy 2024*.

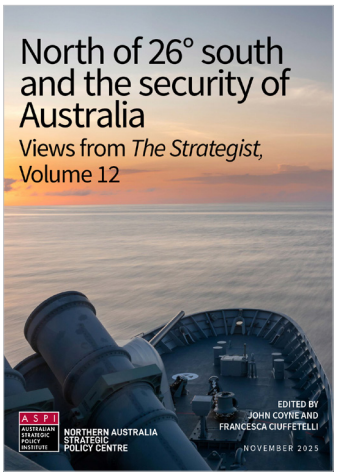
43 Australian Government, *Defence Strategic Review 2023*.

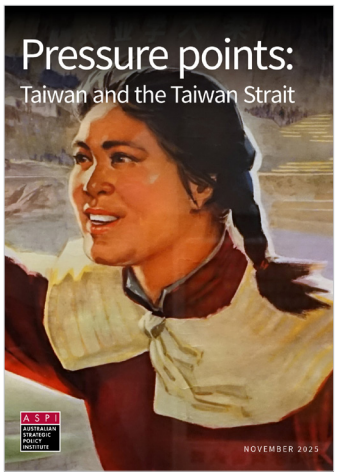
Acronyms and abbreviations

ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
NIC	national intelligence community
ONI	Office of National Intelligence
ONI Act	*Office of National Intelligence Act 2018* (Cth)
PM&C	Department of the Prime Minister and Cabinet
SOCI Act	*Security of Critical Infrastructure Act 2018* (Cth)

Some recent ASPI publications








ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
25
YEARS
2001–2026