Unconventional deterrence in Australian strategy

SALLY BURT
DAVID KILCULLEN
IAN LANGFORD
ANDREW MAHER

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

OCTOBER 2025

Special Report

About the authors

Dr Sally Burt is Senior Lecturer in Cyber Strategy and Diplomacy in the School of Humanities and Social Sciences at UNSW. Her current research includes examination of the use of cyber-enabled mechanisms to engage in international relations and statecraft, such as deterrence and coercion, attribution, cyber governance and the conduct of influence campaigns.

Prof. David Kilcullen is a former soldier and diplomat, and a scholar of guerrilla warfare, terrorism, urbanisation and the future of conflict, who served 25 years for the Australian and United States governments. He has taught at universities and military colleges in the United States and Europe, making scholarly contributions to the theory of guerrilla warfare, insurgency and counterinsurgency, future conflict, human geography, urban studies, and fieldwork methods for conflict ethnography and remote observation.

Prof. (Brigadier, retd.) Ian Langford, DSC and Bars, has 30 years of experience as a senior officer in the Australian Defence Force. Operational service includes deployments to Timor-Leste, Afghanistan, Bougainville, Solomon Islands, Iraq, Israel, Lebanon, Syria, and the South-West Pacific. He is presently the Executive Director of the Security and Defence PLuS Alliance and co-author of *Lets Trade, Not Argue- A strategy to secure a respectful relationship with China*, published in 2025.

Dr Andrew Maher is a former Australian military officer with a particular interest in operations conducted by, with and through foreign forces, via operational experience in Afghanistan and Iraq. His research and teaching focus is towards Irregular Warfare, and he is soon to publish his first book, *Riding Tigers: The Strategic Logic of Proxy Warfare*.

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.

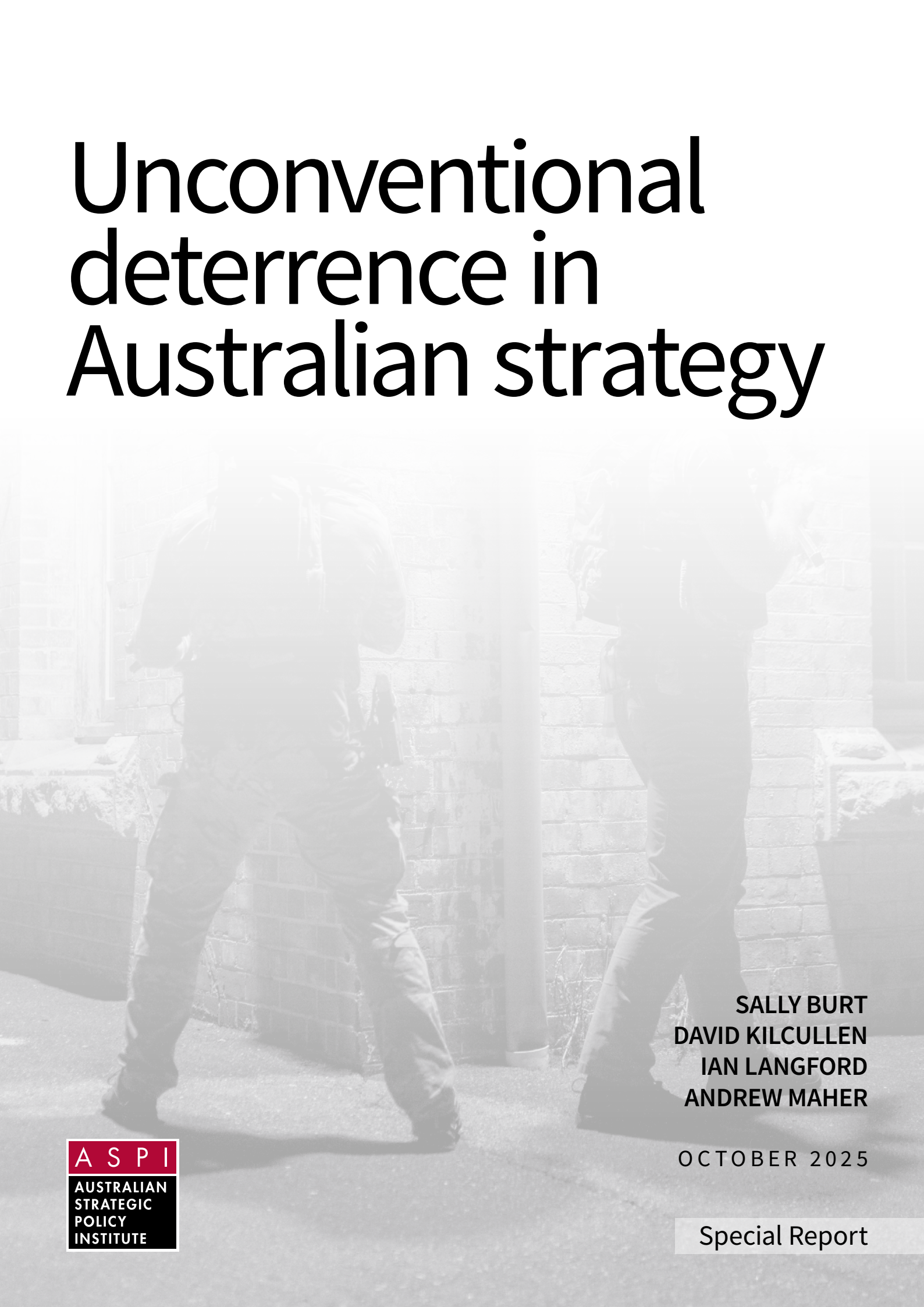
ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal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

About Special Reports

Special Reports are written by both internal and external authors, they are intended to deepen understanding on critical questions facing key strategic decision-makers and, where appropriate, provide policy recommendations.

Cover image: Defence image library, online.

Unconventional deterrence in Australian strategy



SALLY BURT
DAVID KILCULLEN
IAN LANGFORD
ANDREW MAHER

OCTOBER 2025

Special Report

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Important disclaimer
This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services.

© The Australian Strategic Policy Institute Limited 2025

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

First published October 2025

Published in Australia by the Australian Strategic Policy Institute

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

Contents

Executive summary

As Australia prepares its 2026 National Defence Strategy (NDS), the nation must recognise that a window of strategic risk exists *now* and will do so into the early 2030s. The medium-term acquisition of nuclear-powered, conventionally armed submarines under AUKUS, intended to deter conflict, is irrelevant to the short-term problem of maintaining deterrence through the coming five-year period of heightened risk (2027–2032). That's because the first AUKUS submarines—US Virginia-class boats—won't be delivered until 2032, while the purpose-built SSN-AUKUS won't arrive until the early 2040s. We can't, in effect, solve a 2027 deterrence problem with a 2032 deterrent capability.

Australia's traditional reliance upon 'great and powerful friends' and extended nuclear deterrence now seems no longer assured. There's no equivalent to NATO's Article V for Indo-Pacific security; even if there were, adversaries' demonstration of 'grey zone' capabilities—aiming to weaken alliances, isolate targets, erode resolve and impose costs—suggests that formal alliance commitments may be insufficient.

Conflicts in Eastern Europe and the Middle East are demonstrating that smaller players—both middle powers and non-state actors—can generate strategic asymmetry against major powers, in turn deterring them from initiating conflict or escalating in conflict. As recently identified in the UK's Strategic Defence Review (2025), Ukraine is pioneering a new way of war; British decision-makers have recognised the need to rapidly adapt and are using special operations capability to drive that adaptation.

This paper explores asymmetric methods of deterrence and asks whether they might be appropriate for Australia. We organise those methods under the term *unconventional deterrence* to differentiate them from traditional concepts of conventional and nuclear deterrence, which broadly conform to deterrence-by-punishment or deterrence-by-denial logic. Today's technologies, however—along with the emergent realities of information and influence operations in a post-industrial information age—offer new asymmetries, new ways to create and apply both military and non-military elements of national power, and thus new mechanisms to deter beyond-peer adversaries from armed aggression.

This paper explores those options, offering the concept of unconventional deterrence as an organising principle for special operations, cyber and other specialised capabilities that might be rapidly fielded by Defence and other agencies, and could best be orchestrated through an empowered National Security Adviser reporting directly to the National Security Committee of Cabinet. It also offers a comparative analysis, demonstrating that like-minded middle powers have embraced unconventional deterrence concepts in their military strategies, and are using them to face down their own beyond-peer threats.

Australia has options to fill today's deterrence gap: we just need to look beyond conventional paradigms.

Introduction

Australia's 2023 Defence Strategic Review (DSR) and 2024 National Defence Strategy (NDS) established deterrence as a core strategic output for Defence. The NDS defined deterrence in conventional terms as the 'use of the military and other elements of national power to discourage or restrain a potential adversary from taking unwanted actions' through 'measures and responses that change a potential adversary's risk assessment and therefore decision-making calculus'.[1] Shaping Australia's strategic environment, projecting force to deter adversary power projection, holding at risk adversary assets that could target our interests during a conflict, and improving Australia's preparedness and resilience are all identified as key requirements for national deterrence.

Conventional military power typically relies on the application of relative *superiority*—in mass, firepower, logistics, technology and/or tempo—against enemy combat forces at a time and place of one's own choosing.[2] For Australia, however, the threat posed by our most likely major-power adversary—the Chinese Communist Party (CCP) and its military arm, the People's Liberation Army (PLA)—is such that we would face relative *inferiority* at the outset of any conflict, certainly if operating alone, and possibly as part of a coalition.

Today's strategic challenge, implicitly recognised in the NDS, is thus to deter a beyond-peer adversary, from a position of relative inferiority, across multiple elements of national power. Conventional deterrence, in isolation, may lack the critical component of credibility: the ability to convince an adversary that we possess both the intent and the capability to deter armed aggression, or to impose significant costs should such deterrence prove unsuccessful.

But history has shown that conceptual innovation can, and often does, trump technological inferiority. British strategist Colin Gray's account of the Battle of Britain in 1940 describes an action involving German pilots with better experience, flying more capable aircraft, who were nevertheless defeated because Britain fought as a national integrated air defence system.[3]

Some 50 years later, Chechen guerrillas imposed unacceptable costs on a 40,000-strong Russian invasion force, eventually forcing a negotiated end to the First Chechen War.[4] The lesson: under certain circumstances conceptual asymmetry can temporarily mitigate inferiority in mass and/or firepower, while irregular actors (defined as non-state armed groups working either alone or in concert with special operations forces) can defeat the aims of conventionally superior opponents.

Given Australia's current situation of conventional inferiority against a beyond-peer adversary, a key challenge in implementing the NDS is to develop innovative and unorthodox operating concepts sufficient to mitigate our conventional military inferiority in mass, firepower and specific technologies. Such concepts align with deterrence theory, but they extend it from purely pre-conflict considerations to include in-conflict (sometimes called 'intra-war') deterrence, which occurs after the outbreak of war.[5] Intra-war deterrence seeks to deter an enemy from escalation and compel de-escalation. Operating concepts must assume a starting position of conventional relative inferiority and recognise that we're unlikely to achieve superiority through alliances or following mobilisation.

We call this approach *unconventional deterrence*. The term 'unconventional' in this context means concepts and capabilities that lie outside conventional (state-on-state, force-on-force, battlefield-centric) military war-fighting and indeed, outside conventional manifestations of state power through diplomacy and statecraft. Unconventional methods operate indirectly against an adversary's vulnerabilities, exerting influence and imposing costs through a target population or audience, and using methods such as resistance warfare, guerrilla operations, unarmed or armed propaganda, subversion and sabotage—a set of activities sometimes also termed *special warfare*. Such means and methods may potentially be combined with cyber, information or political warfare, if directed by government.

Ivan Arreguín-Toft proposed the idea of 'unconventional deterrence' within the context of relative state power, in the sense that, as opposed to conventional wisdom, the weak can win wars—through protraction, asymmetry, or both—thus gaining a potential to deter stronger powers.[6] His work analyses how weak actors can deter strong actors, suggesting that, while relative power matters, the interaction of opponents' strategies matters more.[7] 'When actors employ similar strategic approaches', strong actors 'win quickly and decisively', he argues. The implications of this work are that an Australian war-fighting concept that relies upon conventional deterrence only, faced by a much more powerful opponent, is risky indeed and unlikely to successfully deter. For weaker actors, strategies asymmetric to those of the stronger actor are far more likely to result in success '*even when everything we think we know about power says they shouldn't*'.[8]

An expanded concept of unconventional deterrence might operate independently from, or in concert with, conventional deterrence, responding flexibly to counteract an adversary's approach. Former US Secretary of Defense Lloyd Austin's challenge to allies—of generating collective 'integrated deterrence'—could partly be addressed in this manner.

Australia currently has no official doctrine that approximates to the idea of unconventional deterrence, but our history—particularly during World War II, when we faced a superior conventional enemy across the same geography in which a future deterrent capability would operate—offers important insights.

Other countries have successfully adopted concepts that explicitly or implicitly employ unconventional deterrence. For example, during World War II, Switzerland successfully deterred Nazi Germany by presenting itself as a 'porcupine'.[9]

Switzerland communicated an ability to hold at risk key rail and road connections into Italy and demonstrated a credible capacity to wage a prolonged campaign of large-scale resistance warfare if invaded. In changing German decision-makers' calculus, the Swiss approach was different from, and markedly more successful than, the failed conventional deterrence efforts of Poland, Denmark, Norway, Belgium, the Netherlands and France. Similarly, credible Spanish threats to protect that country's neutrality through wide-ranging guerrilla resistance similarly deterred Hitler from embarking upon Operation Felix—the seizure of Gibraltar.[10]

In combination with conventional defences, such unconventional methods contributed to an emergent doctrine termed 'total defence'.[11] Importantly, Swiss deterrence wasn't solely a pre-conflict activity. Rather, it sought to continue imposing deterrent effects throughout the conflict: Hitler returned to the Swiss question several times throughout World War II and was repeatedly deterred from specific actions due to Switzerland's 'total defence' posture. Drawing from that experience, Switzerland maintained its armed neutrality during the Cold War.[12]

The ability to alter an adversary's calculus by credibly communicating a capacity for resistance warfare, or for total defence more broadly, constitutes a form of unconventional deterrence-by-denial.

An unconventional deterrence logic emerged following Russia's successful seizure of Crimea in 2014. NATO nations—notably the UK, through Operation Orbital—supported Ukraine's establishment of territorial defence brigades (formally termed 'territorial defence forces'—TDF).[13] In December 2021, then-Chairman of the US Joint Chiefs of Staff, General Mark Milley, communicated to his Russian counterpart, General of the Army Valery Gerasimov, that the US would support in Ukraine 'a bloody insurgency, similar to the one that led to the Soviet retreat from Afghanistan'.[14] Milley's communication of capability, leveraging multi-year investment in Ukraine's TDF and Special Operations Forces (SOF) capabilities, indicated an American *belief* that preparations for prolonged resistance could deter a conventional aggressor.

Ukrainian TDF worked with Ukrainian SOF, alongside conventional capabilities, to defeat Russia's attempted *coup de main* near Kyiv at the outset of its full-scale invasion in February 2022.[15] As the full-scale invasion developed, SOF supported resistance warfare in Russian-occupied territories and online, imposing costs across a range of categories including time, space, materiel and reputation, and thereby changing enemy commanders' calculus.[16] Resistance capabilities covered gaps in conventional capability, enabling Ukrainian manoeuvre units to regain their balance, and buying time for the international community to rally in support. By April 2022, having suffered significant attrition, Russia abandoned its attempt to seize Kyiv, withdrew from northwestern Ukraine, and engaged in peace talks in Istanbul.

Beyond 2022, Ukrainian partisan warfare and people's resistance activities in Russian territory have further increased the costs of Russia's campaign once it was launched. Ukraine's experience in its current war against a beyond-peer enemy thus demonstrates the contribution of irregular warfare to pre-conflict deterrence-by-denial, to in-conflict compellence to desist current actions, and further deterrence of Russian expansion through deterrence-by-punishment logic.

While unsuccessful in preventing the invasion, Ukraine's unconventional capabilities and demonstrated capability likely dissuaded Russia from further conventional escalation and helped compel Russian forces to withdraw from Kyiv in March 2022.[17] Importantly, we must also note Russian threats against Finland and the Baltic states made post-February 2022. Costs imposed in Ukraine are likely to have influenced the Russian cost–benefit calculus in such contingencies.

The lesson to be drawn is that unconventional deterrence logic was demonstrated and tested and, while still pressured by the crucible of conflict, Ukraine continues efforts to employ this deterrent messaging, in concert with conventional capabilities.

In a similar vein, after being labelled a member of the 'Axis of Evil' in 2002, and up until June 2025, Iran successfully deterred the US and Israel from conventional military action against it, using regional proxies including Hamas in Gaza, Hezbollah in Lebanon, Kata'ib Hezbollah and other popular mobilisation forces in Iraq, and the Houthi movement in Yemen.[18] That 'axis of resistance' allowed Iran to threaten penalties for attacks on its territory or interests and to shift the point of contestation against more powerful adversaries, raising the costs of any attack.[19] Iran's proxy

support to non-state actors such as Hezbollah during that period can thus be viewed as an unconventional form of deterrence-by-punishment.

The failure of Iran's unconventional deterrence in 2025 is equally instructive in this regard. Israel's 2024 campaigns against Hezbollah and Hamas—along with the fall of Iran's ally, Bashar al-Assad's regime in Syria, and Israel's subsequent incursions into Lebanon and Syria—severely degraded Iran's unconventional deterrence.[20] Simultaneously, Iranian missile strikes on Israel, commencing in April 2024, shifted the ground of regional competition away from unconventional, asymmetric 'grey zone' activity—in which Iran had demonstrated its deterrent capacity—and towards direct conventional military confrontation, in which Tehran was at a significant disadvantage against Tel Aviv.[21] That emboldened Israel to launch an air and missile campaign against Iran in June 2025, in turn triggering US air strikes against Iranian nuclear sites during the so-called 'Twelve-Day War'. In effect, the collapse of the 'axis of resistance', achieved by undermining the unconventional component of Iranian deterrence, shifted the conflict onto conventional ground, opening space for Israeli, and then American, attacks.[22]

With that as background, we can define unconventional deterrence in this context as *the use of irregular warfare means to deter an adversary from initiating or escalating hostilities and/or to compel an enemy to cease or de-escalate hostilities once initiated*. Unconventional deterrence may operate independently, or in concert with conventional means, and may deter by denial, by punishment, or both.

Part 1 of this paper sets a historical baseline for the concept of unconventional deterrence in Australian strategy, examining Australian adaptations early in World War II in response to the Japanese threat. Part 2 examines the application of irregular and improvised means of deterrence, exemplified by the proliferation of uncrewed systems in both the Nagorno-Karabakh war of 2020 and the ongoing Ukraine conflict. It also examines how SOF worldwide have adapted to the changing environment, ranging from support by NATO SOF to Ukraine and other partner nations to the employment by Iran's Islamic Revolutionary Guard Corps Quds Force of proxy forces across the 'Axis of Resistance'. Building on that context, Part 3 develops further the idea of unconventional deterrence, examining how irregular forces and means, along with unorthodox approaches, can credibly communicate an ability to frustrate an adversary's plans, and thus deter-by-denial. Finally, Part 4 considers capabilities, policy adaptations and force-generation changes needed to realise Australian unconventional deterrence.

This paper seeks to inform the implementation of Australia's 2024 NDS and examine some of the implications and issues it raises to inform the development of the 2026 NDS, mitigating the risk that conventional deterrence may prove ineffective during the 'deterrent capability gap' between now and the arrival of the first AUKUS submarines in 2032. The concepts herein may well augment those future deterrent capabilities well beyond 2032.

We present an alternative option, a 'Plan B', for policymakers and planners seeking to complicate an adversary's calculus, using unconventional deterrence delivered partly, but not solely, through Special Operations Command (SOCOMD) and related ADF capabilities.[23] 'Plan B' focuses upon supporting the resilience and resistance capabilities of Southeast Asian partners, recognising the defence-in-depth effect that Australia would thereby gain from such efforts.[24]

This approach comports well with those of major allies. The recently released UK Strategic Defence Review argued that: 'the UK must pivot to a new way of war … and think differently about what conventional "military power" is and how to generate it. In modern warfare, simple metrics such as the number of people and platforms deployed are outdated and inadequate.'[25] In addition to a range of organisational, training, education and acquisition changes, the review articulated a new role for UK special forces, to lead the way 'in innovation of new technologies and systems across all domains'.[26] This is a profound shift, born in part from battlefield lessons from Ukraine and elsewhere, which recognises the role of unconventional deterrence in improving strategic readiness.

We don't suggest in this paper that unconventional deterrence can replace traditional, conventional deterrent capabilities. Rather, we argue that in combination, conventional and unconventional concepts executed together, whether unilaterally or alongside allies and partners, might yield an integrated deterrence effect greater than the sum of its parts.

Part 1: Historical context

Australian and a beyond-peer adversary: 1942–1945

Australia has faced a first-class great-power adversary before, across the same physical terrain that would be relevant in a future conflict. That competition, preceding World War II, offers insight into today's challenges and opportunities.

In the lead-up to the outbreak of the European war in 1939, a pattern of autocratic subversion and proxy warfare was recognised at the highest levels of Allied governments. On 3 September 1939, Australian Prime Minister RG Menzies noted that:

> The technique of German propaganda; of carefully fomented agitations in neighbouring countries; the constant talk of persecution and injustice; these are all nauseatingly familiar to us. We made the acquaintance of all of them during the dispute over Czecho-Slovakia, and we may well ask what has become of the Czech minority and the Slovak minority since the forced absorption of their country into the German state … It is plain—indeed it is brutally plain—that the Hitler [sic] ambition has been, not as he once said, to unite the German peoples under one rule, but to bring under that rule as many European countries, even of alien race, as can be subdued by force.[27]

British policymakers in 1940, shaken by Nazi expansion in Austria, Czechoslovakia and Poland, and then facing Nazi subversion into France, Norway, Belgium and the Netherlands, believed that a 'new form of warfare' had been developed by Germany. That new form of warfare used secret organisations for espionage, provocation, subversive propaganda and 'whispering' campaigns, creating a framework for underground activities termed a 'Fifth Column'.[28] This wasn't a stand-alone activity but an operational-level adjunct to conventional campaigning. The Soviet Union and the Axis powers (then comprising Nazi Germany and Fascist Italy) had competed via proxies in the Spanish Civil War (1936–1939), refining their understanding and application of this form of warfare.

In response, the British Government established the Special Operations Executive (SOE) in 1940, with the purpose of counteracting subversive German organisations. As a 'counter-subversive' force, SOE would:

> hinder the enemy's regimentation of conquered nations by promoting disaffection, passive resistance, active revolt, and guerrilla warfare among the peoples of the occupied countries; to hamper the enemy's war production by sabotage, propaganda and other subversive activities in enemy and enemy-occupied countries; [and] deny the enemy access to outside resources by conducting anti-Axis and pro-Allied activities of a similar, but less drastic nature in neutral countries.[29]

British planners, from a position of relative weakness vis-à-vis Nazi Germany, developed the 'detonator concept' in which, with appropriate political warfare preparation, small SOE teams could be inserted (like a detonator) into the explosive environment of national resistance to Nazi occupation, then 'explode' into coordinated violence, hindering the enemy at a time and place of strategic utility. That idea spread across the Commonwealth, including to Australia.[30] Australian planners in particular took note, given abundant evidence of Imperial Japan's grey-zone activity before the attack on Pearl Harbor.[31]

In Asia, the detonator concept was applied through SOE's establishment of the ORIENTAL mission, which sought throughout 1940–41 (that is, before hostilities against Japan) to establish stay-behind resistance networks able to impose costs on any Japanese invasion or occupation.[32] For example, the Commonwealth deployed 250–300 advisers, known as 'Tulip Force', under Mission 204 in July 1941 in response to a request for support from Chiang Kai-shek.[33] The mission of supporting the Nationalist Chinese by raising guerrilla warfare battalions was expressly intended to deter Japan from aggression against Southeast Asia, to 'lock up' the maximum number of Japanese forces, and thus would 'have as its primary object the strengthening of our defensive position on our own frontiers [i.e. Commonwealth colonies]'.[34] From an Australian Government perspective, it was believed that quiet assistance to the Chinese would have a diversionary effect, as 'a means of absorbing Japanese energy and aggression'.[35]

Simultaneously, the Japanese were refining their own subversive warfare techniques through competition with the Soviet Union and China during the 1920s and 1930s. To support Japanese expansion into Southeast Asia, the Imperial Japanese intelligence concept was to:

> … combine local organisations which had subversive aims or tendencies with a superior organisation whose task it would be to coordinate their activities throughout the whole area of operations … In their plan of expansion in GEA [Greater East Asia] the Japanese fully realised the great tactical value of this doctrine 'Asia for the Asiatics' and the whole force of their propaganda was turned to the fullest exploitation of this doctrine among the peoples of this area.[36]

In the Pacific theatre, Japanese preparation for the invasion of the Australian territories of Papua and New Guinea—to take one example among many—involved long-range, long-duration reconnaissance teams operating under academic, commercial and diplomatic cover.[37] Commercial ship visits to Salamaua, Lae, Port Moresby and Rabaul, the establishment of commercial front companies, botanical and zoological research expeditions, the acquisition of local guides and maps, coastal and beach surveys, route reconnaissance—even the collection of grass (to test its suitability for pack animals) at Wau airstrip—were undertaken by civilian intelligence officers and members of the Imperial Japanese Navy and Army from 1931 onward, and those activities were stepped up after 1937.[38] They formed part of a suite of intelligence, surveillance and reconnaissance (ISR) and 'operational preparation of the environment' (OPE) activities conducted by Japan throughout potential conflict areas. The Japanese attempted to develop local influence networks in targeted areas through contact with local populations and, in the former German territory of New Guinea, with Nazi-sympathising German settlers and at least one neutral citizen, Swiss national Josef Anton Hofstetter.[39]

Japanese ISR and OPE—in strategic terms, a form of pre-conflict shaping—were well known to Australian authorities in Papua and New Guinea, to the Director of Military Intelligence, and to the Security Service of the Commonwealth Investigation Branch—the forerunner of the Australian Security Intelligence Organisation (ASIO). Australian intelligence maintained a watch on those networks and activities and sought to limit Japanese commercial presence and political influence in Papua, New Guinea, Solomon Islands and mainland Australia.[40]

Intensifying pre-war competition laid the foundations for the establishment of Special Operations Australia (SOA) after the outbreak of war in Europe, based on a clear recognition of growing Japanese use of subversion in concert with other forms of military and non-military coercion.[41] SOA, like SOE, was a counter-subversion organisation that sought to 'fight fire with fire' by coordinating resistance movements, hampering invaders through sabotage and competing in grey-zone activities. Unfortunately, such efforts began only shortly before the outbreak of the Pacific War and were inhibited by perceptions that such preparations represented 'defeatism'. Both of those factors undermined the deterrence effects.

Prime Minister John Curtin gave his formal approval for raising SOA in March 1942: 'for the establishment of a bureau for the purpose of undertaking espionage in enemy-occupied territory, the dissemination of propaganda amongst the native races of occupied territories and the issue to the enemy of misleading information'.[42] The Prime Minister's words highlighted the political and information-warfare goals of SOA, which sought not only to carry out kinetic operations but also to affect adversary decision-making, and to influence local and global audiences.

SOA, like SOE and like the Royal Australian Navy's Operation Ferdinand—the region-wide coastwatching program designed to give early warning of adversary presence and activity across Australia's maritime and littoral approaches—thus emerged from pre-war competition, and from political leaders' perceived need to make prudent (and low-cost) preparations for conflict, amid grey-zone competition.[43] Those preparations—though far from universally successful in the months after Pearl Harbor—were a critical enabler for Australian and Allied operations later in the war.[44] SOA's activities were neither stand-alone operations nor an end in themselves, but a means of maintaining visibility and influence across Japanese-occupied territories in Australia's approaches, and an adjunct to conventional war-fighting.

Along with the Navy's coastwatchers and the Army's independent companies and commandos, SOA constituted an Australian multidomain special operations capability during the war. The Royal Australian Air Force (RAAF) also established a comprehensive special operations capability including personnel and cargo movement, ISR and long-range strike, with RAAF PBY Catalina aircraft mining harbours and maritime choke-points as far afield as Manila.[45] In addition to raiding and sabotage, Australian and Allied special operations organisations conducted guerrilla warfare in Portuguese Timor, supported resistance in Borneo, Malaya, Burma and Indochina, and engaged in strategic strike and ISR across the region. Such multidomain special operations imposed costs upon the Japanese that supported Australia's overall theatre strategy via a compellence-through-punishment logic.

This history suggests that Australia is perfectly capable of projecting influence and altering an opponent's decision-making calculus both before and during large-scale, high-intensity warfare against a beyond-peer adversary. It also suggests a useful distinction between conventional and unconventional deterrence. Whereas conventional forces focus upon overt warfare and a force-on-force battlefield-centric struggle between competing military formations, unconventional organisations (military or civilian) use an indirect approach, working through local populations or target audiences, to alter an adversary's decision-making calculus in political, economic and military terms.

History thus suggests that—subject to certain key conditions discussed below—unconventional deterrence could feasibly be achieved by establishing regional resistance networks, working among local audiences and with like-minded partner nations, attacking the implicit consent of regional populations to adversary influence and, in the event of conflict, undermining the enemy's ability to operate in or through a contested area.

Of course, to achieve a deterrent effect, Australia's capability for such operations would need to be credibly communicated ahead of hostilities. It would thus involve relatively overt activity in a pre-conflict environment, while maintaining the ability to transition to clandestine or covert operations at the approach of war. Likewise, credibly communicating the capacity to reveal an adversary's pre-conflict actions—through strategic communication of declassified intelligence material, bolstering regional resistance to adversary influence—might form an important aspect of unconventional deterrence.

Australia's World War II history likewise suggests that efforts to develop deterrence and national resilience—central to the NDS—should include unconventional deterrence through irregular warfare, including regionally focused special operations. Unity of effort among SOF, general-purpose forces, cyber and sensitive capabilities and non-military elements of national power could be enhanced via division of labour, with SOF credibly communicating the ability to impose costs across moral, material, human, political, economic and reputational dimensions—and across time and space—before and during any future conflict.[46] The indirect cost-imposition capabilities of SOF were believed by Australian planners in 1939–45 to complement general-purpose forces with the application of deterrence-by-punishment logic.

Part 2: Contemporary unconventional deterrence

Technology and grey-zone activity

Australia's most likely adversary—the Chinese Communist Party (CCP) and its military arm, the People's Liberation Army (PLA)—conducts grey-zone activity across the globe, including the Indo-Pacific, directly or indirectly targeting Australia and Australian interests. That includes cyberwarfare, cognitive domain operations, political warfare, covert influence, economic coercion and infrastructure exploitation, rather than directly sponsoring non-state armed groups (with exceptions, notably in northeast India).[47] In many ways, in fact, CCP actions today resemble those of pre-1941 Japan, as well as those described in the other examples noted above.

Communist China doesn't currently sponsor proxies (such as guerrilla groups or surrogate forces) to the same degree, or in the same way, as do Russia and Iran in their respective areas of influence. Chinese intelligence did, however, support guerrillas and insurgents until the end of the 1980s and maintains liaison relationships with non-state actors in Australia's region. For example, Chinese support pivoted following the collapse of the Burmese Communist Party in 1989 to support the United Wa State Army, which has between 20,000 and 30,000 fighters, is the largest narcotics-trafficking organisation in Southeast Asia, and presently controls an area of Shan State in Myanmar that's approximately the size of Belgium.[48]

China's 'three warfares'—psychological warfare, legal warfare (or 'lawfare') and public opinion warfare—are forms of non-kinetic irregular warfare operating through a distributed influence network sponsored by PLA SOF.[49] PLA SOF in a future conflict would probably optimise for enabling tasks such as special reconnaissance, *coups de main* to secure objectives ahead of a conventional force, covert emplacement of anti-access/area-denial and counter-intervention capabilities such as anti-ship ballistic missiles, or strategic raiding.[50] China's maritime militia (中国海上民兵) conducts 'people's war at sea' alongside the PLA Navy and Chinese Coast Guard, applying maritime irregular warfare techniques to intimidate rivals and block adversaries from contested locations.[51]

All or most of those activities would have been familiar to any Australian planner confronting Japanese strategic shaping in the 1930s, but today a great deal of ISR and OPE takes place not in the physical environment but in cyberspace. In the early to mid-2010s, the Chinese cyber activities that received the greatest public response from the US and its allies were those involving theft of proprietary information and corporate secrets. The February 2013 identification of China's cyber activities by commercial cybersecurity firm Mandiant exposed the fact that PLA units were operating in cyberspace to gather economic intelligence and commercially sensitive information.[52] That exposure was followed by the indictment of five PLA service members on 31 counts of cyber-espionage in May 2014.[53] In late 2014 and early 2015, a Chinese cyber unit successfully breached the US Office of Personnel Management, accessing the security clearance files of about 4 million US Government employees.[54] That alarming breach presented a challenge to intelligence agencies and operations. Since the breach, China's target range has expanded. According to 2024 testimony by then-FBI Director Christopher Wray to the House Select Committee on Strategic Competition, Chinese hacking is sustained, occurs at enormous scale, and telegraphs the types of targets that might be sabotaged through malware.[55]

Those actions indicate a logic of deterrence-by-punishment, in which threats to impose costs are so severe for an adversary that it refrains from taking the action in the first place. The US now knows that China is using cyber capabilities to target critical US domestic infrastructure such as communications, energy, transportation systems, the electrical grid and the water supply.[56] Consequently, US planners must calculate that in the event of conflict over, say, Taiwan, the CCP could punish the US by activating malware that would cause domestic chaos and potentially inflict civilian casualties, with attendant political ramifications. To the extent that organisations such as the FBI believe that they can't protect fully against such threats, the US could be deterred. Reflecting this, recent analyses use the term *digital weapons of mass destabilisation*, conveying the application of deterrence theory to the CCP's cyber capabilities.[57]

A further challenge is posed by the sheer scale of the CCP's operations, in which millions of individuals are involved—a number of personnel dedicated to cyber activities that can't be matched by friendly powers. When augmented by artificial intelligence (AI)—as PLA planners are increasingly emphasising—the challenge of mass becomes acute.

PLA planners refer to the latter approach as 'cognitive domain operations'. To support it, the PLA and other CCP agencies have developed a set of operational-level capabilities for a multidomain (or, in PLA parlance, 'full-dimensional') campaign across land, air, sea, space, the electromagnetic spectrum, cyberspace and in the cognitive or information domains.[58] That approach—described in PLA concepts since 2015 as 'winning local informationised wars'—blends conventional with irregular forces, kinetic and non-kinetic means, and cross-domain capabilities to rapidly and thoroughly destroy an adversary's war-making capacity.[59]

Cognitive domain operations seek, if possible, to win without fighting by undermining an adversary's morale, intimidating and demoralising decision-makers and the general population, isolating a target from sources of support, and obfuscating the initial stages of a campaign so that the adversary remains unaware that it's at war, and unable to respond, until too late.[60] As AI proliferates, 'intelligentised (智能化) warfare'—in which AI accelerates and deepens the effect of such a campaign—is becoming increasingly prominent in PLA discussions of full-dimensional campaigning.[61]

In totality, CCP statecraft today resembles the pre-1941 pattern of subversion and proxy employment (including the use of commercial entities as proxies for the state) pursued by totalitarian powers, but it also covers the information and cyber space as well as physical domains. Once a target's cohesion and will to resist are sufficiently weakened, PLA concepts suggest that it would then directly threaten to employ uniformed elements to deter, dissuade or compel its opponents.

That approach is echoed in Russian statecraft, described by Dima Adamsky as 'cross-domain coercion'.[62] Examining Russian unconventional warfare in Ukraine, analysts noted in 2024 that 'the consistent features of the Soviet methodology are: elite capture through the recruitment of agents within a faction of a state's political elite; the use of information operations and subversion to create political destabilisation; and escalation through violence to create a crisis through which Russian allies can seize power'.[63] There's thus a certain consistency in autocratic methods of subversion and grey-zone activity to advance strategic objectives.

Considering this emerging array of threats, Australia's 2023 DSR noted 'the return of major power strategic competition, the intensity of which should be seen as the defining feature of our region and time'.[64] The 2024 NDS builds on the DSR's analysis, noting that 'entrenched and increasing strategic competition between the United States and China is a primary feature of our security environment. It is being accompanied by an unprecedented conventional and non-conventional military build-up in our region, taking place without strategic reassurance or transparency. The challenges to regional stability and prosperity arising from this competition are being compounded by a range of other security risks, including climate change, grey-zone activities and technological advancements.'[65] The NDS further notes that 'grey-zone activities have also expanded in the Indo-Pacific. In addition to conventional military forces, some countries are employing paramilitary forces more frequently, including China's actions in the South China Sea. Threats posed by state and non-state actors in the cyber domain are also multiplying.'[66]

The NDS references to paramilitary and grey-zone activity weren't present a year earlier in the DSR, perhaps indicating increased awareness of a 'competition gap'. Australian civilian strategists and military decision-makers have historically demonstrated little appetite for irregular warfare, constraining their understanding of the ambiguous, liminal nature of the grey-zone threat, and in turn limiting policy options for government.[67] Consideration of grey-zone subversive activity is a hopeful sign that Australian strategists recognise that they can't ignore irregular warfare, lest they fail to recognise the pre-conflict cognitive warfare and grey-zone competition to which the nation is already being subjected.

Arguably the most important world event to occur between the publication of the DSR in 2023 and the NDS in 2024 was the October 2023 attack on Israel by Hamas, which triggered an Israeli invasion of Gaza and set in motion escalatory actions by Iranian proxies in Iraq, Jordan, Yemen and Lebanon, followed by Israel's war with Hezbollah and the collapse of the Assad regime in Syria. The Hamas attack, the Israeli offensive and Iranian-sponsored counteractions precipitated pro-Palestinian and pro-Hamas protests worldwide.

Those events suggest that 'informationatised' conflict, as noted by Chinese planners, won't be geographically contained. Rather, it will spread across multiple locations and networks, becoming a competition for influence at global scale—something NATO terms 'boundless' conflict.[68] This is key to understanding the transitional character of contemporary conflict: Australia now faces Information or Digital Age warfare with different dynamics and conceptions of military power from the Industrial Age. Conventional military capabilities still matter, but information dynamics, economic pressure points and 'crowdsourced' open-source intelligence in an environment of ubiquitous technical surveillance now matter more. As Mick Ryan and PW Singer have argued, today it isn't just about winning the war; one needs to win the story of the war.[69]

Unconventional deterrence: a comparative analysis

How are Australia's allies and like-minded countries adapting to this evolving threat environment? This section builds on the previous one, offering a comparative analysis which shows that the democratisation of lethal and non-lethal technologies, across the spectrum of competition, offers opportunities to improve resilience, complicate adversaries' decision-making and impose costs before and during conflict, generating unconventional deterrence.

The case of Ukraine—not a treaty ally, but a major recipient of Australian military assistance since 2022, the sovereignty and territorial integrity of which Australia continues to support—is instructive.[70] As Kori Schake has noted, unconventional means and methods were central to Ukraine's adaptation between 2014 and 2022. Ukraine surprised the world with its ability to withstand Russia's onslaught and inflict damage early in the invasion. In February 2023, Schake pointed out that:

> [F]or the expense of just five percent of the US defence budget, Ukraine has fought a war that has decimated the Russian military and deflated its reputation … Russia has been taken off the board as a major adversary. Zero Americans died to produce that outcome; Ukraine has paid the butcher's bill for us—something we should never forget. Even China is weaker as a consequence of the war because Beijing has shackled itself to a weak and snarling Russia; and despite professions of unlimited friendship, it is fearful enough of Western sanctions to restrict loans and arms to Russia. The performance of Russia's military may even give China's leaders pause about the prospects for their own military ambitions.[71]

Although its circumstances today look bleaker than in 2023–24, Ukraine's experience nonetheless offers significant lessons for Australia. In the eight years between Russia's seizure of Crimea in 2014 and its full-scale invasion of February 2022, Ukraine evolved a 'total defence' strategy integrating conventional manoeuvre forces, territorial defence brigades, civilian resilience networks (which evolved into 'popular resistance' groups in areas occupied by Russia), an SOF 'partisan warfare' capability oriented towards 'support to resistance', and a civil–military cyberwarfare partnership, with assistance from US and NATO nations' SOF. The Baltic states of Latvia, Lithuania and Estonia, Scandinavian countries including new NATO members Finland and Sweden, and others including Poland have adopted similar concepts.[72] In June 2025, Kazakhstan followed suit by establishing territorial defence units within a similar model of total defence strategy.[73]

Though the geographic, economic and political contexts differ, the logic of total defence is not dissimilar to the approach evolved by SOE and SOA 85 years ago: to counter an aggressor's subversive practices ahead of conflict, and to develop and support resistance networks in order to asymmetrically impose costs and affect the aggressor's calculus should war break out.

In Ukraine's case, we see at least three subvariants of unconventional deterrence, including deterrence-by-detection, asymmetric strike, and resistance warfare.

Deterrence-by-detection

Throughout November 2021 – January 2022, the US and some allies attempted what's been described as 'deterrence by detection': changing Russian planners' calculus through rapid declassification and release of intelligence about their plans. This approach, first proposed by the Center for Strategic and Budgetary Assessments, argued that adversaries can be denied grey-zone objectives 'if they know they are being watched constantly and that their actions can be publicised widely, can generate and maintain real-time situational awareness that can contribute to meeting the fait accompli challenge'.[74] By detecting and publicising an adversary's grey-zone activities, a nation being targeted by hybrid aggression can alter the aggressor's risk calculus. In deterrence theory terms, we consider this a mechanism of deterrence-by-denial, since the revelation of covert activities alters an aggressor's calculus by demonstrating that its plan has been detected, thereby increasing the risk of failure and forcing reappraisal.

Deterrence-by-detection can also assist in the attribution of cyber activities, influencing global opinion against sponsors and reducing the benefits of such activities. Plausible deniability can thus be invalidated by establishing a clear pattern of adversary behaviour—as Western countries are now doing against Russia's campaign of state-orchestrated sabotage in Europe.[75] Nonetheless, detection without credible follow-on consequences risks being a hollow deterrent, as was the case in Ukraine during 2021 and 2022. Rapid declassification of intelligence in fact failed to deter Russia, even alongside the threat of sanctions and well-telegraphed capabilities for resistance.[76] Arguably, the broader loss of credibility by the US and its allies after the disastrous withdrawal from Afghanistan in August–September 2021 outweighed any deterrence-by-detection effect specific to Ukraine. There's a lesson here: effective deterrence requires the capacity to credibly communicate both the will and the ability to act against aggression, across any and all geographies or domains of competition. Arguably, deterrence in the European theatre in 2021, effective as it might have been in isolation, was fatally undermined by events in Afghanistan.

Despite that failure, allied deterrence-by-detection efforts in 2021–22 arguably achieved a different objective. By building a credible picture of Russia's aggressive intent, intelligence releases spurred alliance- and consensus-building across Europe and globally, denying Russia liminal manoeuvre space and making global opposition stronger and more cohesive when the invasion came.[77] Lessons from Ukraine may deter future aggressors confronted with a similar loss of initiative in the 'battle of the narrative', as 'false flags' are pre-bunked by the defender being first with the truth. Isolation of a target through mis- and disinformation—a key component, noted earlier, of Chinese cognitive warfare operations—may thus be harder to achieve.

Sensitive reporting—collected through strategic reconnaissance, technical surveillance and special intelligence, among other means—exists today within a different environment from the Cold War or the post–Cold War period. Sensitive collection capabilities that were once the preserve of well-resourced nation-states are now commercially available and proliferating across a broader range of nations, corporations and non-state armed groups.

That makes deterrence-by-detection more feasible, since sensitive sources and methods need not be disclosed in the process of revealing an adversary's actions or intentions. This unconventional concept differs from the traditional notion of technological asymmetry, in which smaller countries seek exquisitely sensitive capabilities to offset numerical and size disadvantages. At the same time, special reconnaissance and intelligence activities remain critical in order to verify open-source intelligence or to tip and cue commercial collection means. SOF, along with the agencies of the national intelligence community, would play key roles in deterrence-by-detection.

Asymmetric strike

Since Russia's full-scale invasion, Ukrainian SOF have demonstrated an asymmetric maritime strike capability that has forced Russian naval planners to alter deployment plans, allowing Ukraine to temporarily seize the initiative in the Black Sea from a much more powerful beyond-peer aggressor. The technology involved is new, but the concept—as for unconventional deterrence writ large—is not.

A century ago, a handful of British Royal Naval Volunteer Reserve personnel seconded to the Secret Intelligence Service used shallow-draft torpedo boats, in concert with air attack by naval aviation, to bypass torpedo nets and sea mines protecting the Bolsheviks' Baltic Fleet at Kronstadt, near St Petersburg.[78] During two raids in August 1919 (that is, during a period of competition rather than conflict), that irregular strike force sank a cruiser and two battleships, removing the Soviet threat to the British Baltic Fleet, which was then supporting the nascent armed forces of independent Estonia. The Bolsheviks realised that any effort to reassert Russian control over Estonia could be blocked by British support. That shifted the Soviet calculus, securing Estonia's independence and, perhaps unsurprisingly, diverting Bolshevik effort to Poland.

The past three years in Ukraine have seen similar developments in naval warfare through the application of uncrewed surface vehicles (USVs) as littoral loitering munitions, striking Russian naval bases and warships and imposing significant human and material costs on Russia's Black Sea Fleet.[79] The USVs were operated by Ukrainian SOF, built to a crowdsourced design, and crowdfunded through the Ukrainian Government's *United24* website, creating an information effect by building an international community of interest around the operations' success, and exploiting USV-generated footage for influence purposes, as well as inflicting physical damage on Russian naval platforms.

The startling success of Ukraine's Operation Spider's Web in early June 2025 underscores the evolution of asymmetric strike, or more broadly of unconventional strategic strike—a pattern common to Ukraine's operations inside Russia and to those of Israel in Lebanon and Iran.[80] One-third of one leg of Russia's nuclear triad was removed at a stroke, with the destruction of 13 strategic bombers. Overall, some 41 platforms were hit across four air bases, inflicting US$7 billion in damage.[81] That operation, in turn, generated an information effect out of all proportion to the effort expended, by demonstrating Ukraine's continued ability to inflict strategic damage in the immediate run-up to critical negotiations with Russia. The audience for the strike may also have included US President Donald Trump, as Ukraine demonstrated that it did indeed have 'cards left to play'. Although it's too early to be certain, it's possible that Operation Spider's Web helped shift both Russian and American perceptions of Ukraine in ways that favoured Kyiv's strategic interests via deterrence-by-punishment logic.

Asymmetric strike, as employed here by Ukraine, strongly resembled the British attack on Kronstadt a hundred years earlier: material and reputational costs were imposed by the innovative application of cutting-edge technologies, denying manoeuvre space (physical or political) to an adversary with numerically superior conventional capabilities. The Ukrainian strike clearly changed Russia's calculus, frustrating the original plan to blockade Ukraine's Black Sea coast and forcing the Russian Navy out to sea, uncovering land forces previously protected by shipboard air defences and limiting Russia's options across multiple domains at limited cost for Ukraine.

Asymmetric strike using SOF, unorthodox capabilities such as robotics and autonomous systems and a combination of physical, information and cyber effects offers insights into what Australia would need for unconventional deterrence. Demonstrating, pre-conflict, the ability to conduct asymmetric strike across a contested area may create doubt in the minds of adversary planners, while being insufficiently aggressive to provoke conventional escalation. In Australia's case, this might clearly signal willingness to escalate, conventionally or unconventionally, if an aggressor did not desist from a particular course of action. If conducted covertly, perhaps through non-state partners, the destruction of key adversary capabilities at a critical time might also be deniable for both parties, offering an off-ramp from vertical escalation by saving face for an aggressor.

Again, deterrence through asymmetric strike isn't unique to Ukraine: Iran has orchestrated similar effects via its proxy in Yemen, the Houthi movement, targeting commercial shipping in a critical global maritime choke-point, the Bab el-Mandeb strait, as a form of horizontal escalation. That had important strategic benefits for Iran, though those were undone, as we've noted, when Tehran shifted to vertical escalation via its direct strikes on Israel after April 2024. Likewise, and in response, Israel demonstrated a capability for asymmetric strike in its attacks on Hezbollah electronic devices before its September 2024 war with Lebanon, and in its operations immediately before the Twelve-Day War of 2025.[82] Cyber-kinetic activities—those combining effects in physical and cyberspace and integrating kinetic action with the information domain—also offer promise in this regard.

Resistance warfare

As we've noted, Russia's seizure of Crimea in 2014 and the subsequent conflict in eastern Ukraine prompted the development of resistance warfare as a component of Ukrainian national strategy, along with a reinvigorated focus on support to resistance by Ukraine's international partners, including the UK and the US. After the full-scale Russian invasion of 2022, pre-war efforts to develop national resilience and 'total defence' structures enabled resistance warfare (***народний спротив***, 'popular resistance') networks within occupied areas, alongside unconventional warfare (***партизанська війна***, 'partisan warfare') within Ukrainian SOF and an interagency Resistance Directorate. Resistance, in this context, means:

> a nation's organised, whole-of-society effort, encompassing the full range of activities from nonviolent to violent, led by a legally established government (potentially exiled/displaced or shadow) to re-establish independence and autonomy within its sovereign territory that has been wholly or partially occupied by a foreign power.[83]

Nine months before the full-scale invasion, Ukrainian legislation (Bill #5557 of 25 May 2021) authorised the establishment of national resistance in Ukraine. The Bill promoted 'the widest possible involvement of the population in actions aimed at ensuring the sovereignty and territorial integrity of the state'.[84] That legislation, alongside practical support for the development of resistance networks in Ukraine and elsewhere in Eastern Europe, was aided by advice from US Special Operations Command – Europe (SOCEUR) and several NATO nations.[85] Once the full-scale invasion occurred, Ukraine established a National Resistance Centre (Центр національного спротиву) as a coordination mechanism under Ukraine's Ministry of Defence.[86]

Ukraine's approach was to become a metaphorical 'indigestible hedgehog' through capabilities for resistance to occupation, credibly communicated to the Russian aggressor. This strategy of becoming indigestible (that is, demonstrating that even if an adversary succeeds in occupying territory, it will face unacceptable costs in attempting to secure it) has also been adopted in Estonia[87] and Finland,[88] among others. Concepts including 'total defence', 'national defence' or 'comprehensive defence' were articulated in the 2012 Czech Defence Strategy,[89] the 2016 Latvian National Defence Concept, the 2017 Lithuanian National Security Strategy, the 2015 Swedish National Defence Bills, and the 2017 Finnish Security Strategy for Society.[90] That all those adaptations occurred in response to the Russian threat after the seizure of Crimea in 2014 is significant: in effect, those nations created an unconventional complement to their existing conventional deterrence.

'Total defence' concepts are evident in the Indo-Pacific to a lesser or greater degree, within Indonesia's Total People's Defense and Security System (*Sistem Pertahanan dan Keamanan Rakyat Semesta: Sishankamrata*), Singapore's Total Defence, the Philippines Civilian Armed Forces' Geographical Units, and historical examples ranging from the Timorese resistance movement (1975–1999) to the Bougainville Revolutionary Army, Malaitan Eagle Force and other regional groups.

Resistance strategy can't be implemented without a pre-existing level of societal resilience, as recognised by NATO more than a decade ago in its Resilience Agenda, which was mentioned in Australia's DSR in 2023 and incorporated as a national goal in the 2024 NDS. In Australia's region, resilience includes protecting the supply-chain ecosystem and responding to weather disasters and natural emergencies or future pandemics, among other things. The scale of national resilience challenges will probably require 'crowdsourced' solutions similar to those in Ukraine and elsewhere. Certain preparations are scalable from pre-conflict national resilience through to resistance during conflict. Those measures create resilience, which over time (and subject to national will) may evolve into resistance tools.[91]

Implications of Ukraine's experience

These examples from Russia–Ukraine illustrate only some of the contributions SOF, in concert with other unorthodox capabilities and general-purpose forces, and operating alongside allies and partner forces, can make to realising multidomain unconventional deterrence. They demonstrate the requirement for personnel—within SOCOMD, in the broader ADF, and across government—capable of innovating conceptually and technologically in a politically sensitive,

multidomain operating environment against a beyond-peer adversary. There's precedent in Australia's World War II history, as noted above, but it would be a mistake to regard this as unique or exclusive to SOF, or to the ADF. Rather than engaging in turf battles, SOCOMD should see itself as a team player, a connector, catalyst, and enabler—akin to SOE's 'detonator' concept of 1940—for a much larger ecosystem of unconventional deterrence capabilities.

For its part, the US is currently adapting to the need for unconventional deterrence in great-power competition against a background of grey-zone and conventional aggression by Russia, Iran, North Korea and the People's Republic of China. A recent RAND report aggregated lessons from those adversaries under the term 'strategic disruption'.[92] Disruptive efforts deter by denial, frustrating 'adversary-preferred strategies through five unique pillars of capability—resist, support, influence, understand, and target'.[93] Those pillars closely resemble Australia's unorthodox capabilities developed in 1939–45 and reflect the unconventional deterrence logic outlined above. Importantly, those concepts are intended to enable broader instruments of national power and act as a catalyst for existing and future security capabilities.[94]

The logic of unconventional deterrence, and the adaptations described above, represent an expansion of concepts beyond Australia's traditional focus on physical defence problems (range, fuel consumption, weapons range etc.) appropriate for the Industrial Age, to include informational and cognitive factors appropriate to the Information/Digital Age. They also involve mixed methods of deterrence, combining both unconventional and conventional capabilities or blurring the lines between doctrinal distinctions of deterrence. For example, naval blockade of a shipping lane could perform a deterrence-by-denial function by frustrating an adversary's plans. Simultaneously, submarine warfare in a separate theatre could perform deterrence-by-punishment by shifting the point of conflict or form of action and imposing costs on an adversary's wartime economy.

In isolation, deterrence-by-detection, asymmetric strike and support to resistance might or might not deter aggression. In aggregate, however, particularly alongside conventional deterrence as described in the NDS, such methods can communicate a credible cost-imposition threat, enhancing Australia's deterrence-by-denial strategy, having altered an adversary's strategic calculus.

For Australia, unconventional deterrence is a policy imperative if we're to meet the aspirations outlined in the NDS, and to cover the deterrence gap between now and 2032 when the first AUKUS submarines are planned to arrive and which, by definition, must be covered by current capabilities. The adoption of such ideas may well yield benefit well beyond 2032 as concepts mature into a multifaceted deterrence-by-denial posture, allowing for combinations of conventional and unconventional deterrence to be used to address a range of threat scenarios. But capabilities and operational concepts are not enough: the next section considers what's needed to effect unconventional deterrence options.

Part 3: What's needed to effect unconventional deterrence?

A whole-of-government approach is best for organising and implementing unconventional deterrence within Australia's overall national defence. Given the need to unify and coordinate Australian statecraft across all phases of competition and conflict, no single department or agency in Australia is appropriately resourced and mandated to do so in its current form.

The nature of unconventional deterrence means that command, control and coordination, particularly pre-conflict, require unified oversight and management at the highest levels of government. This is particularly important given the sensitivity, risk and levels of operational security required for unconventional deterrence.

As a first step, government should consider re-establishing the role of National Security Adviser (NSA). The significance of the NSA for unconventional deterrence can't be overstated. Grey-zone and hybrid warfare occur across multiple different domains and dimensions simultaneously—the 'cross-domain coercion' noted above—and therefore efforts to counter such activity also require an integrated, cross-domain or whole-of-government structure that can mobilise resources across multiple agencies in a timely, integrated manner. Writing recently for ASPI, former Australian Secret Intelligence Service Director-General Paul Symon argued for:

> … ideally, a statutory appointment with clear responsibilities and accountabilities—to harness the full suite of capabilities across government, to initiate desktop wargames at the strategic level, to harmonise information strategies and to test individual department and agency plans. The existence of such an office would clarify the primacy of coordination and help orchestrate a close and continuing affinity to the national interest.[95]

A re-established NSA, working directly for the Prime Minister, would enormously improve Australia's ability to integrate and coordinate unconventional deterrence. To do that, the NSA would need agency-level powers to include a dedicated staff, all-source intelligence feeds and a 24-hour watchkeeping capability. The NSA would provide principal advice to the Prime Minister in the event of a crisis, lead the formulation of national-security policy, coordinate the development of strategic capabilities and liaise with allies and partners as needed. Bureaucratic rivalries would be managed through the NSA, which would be empowered by the Prime Minister (as the ultimate 'Defence Minister' in crisis). Senior committees, including the National Security Committee of Cabinet and the Secretaries' Committee on National Security, would be privy to all capabilities and operations, including but not limited to those for unconventional deterrence. Governance and oversight would come via the Inspector-General of Intelligence and Security, who would annually report to a responsible oversight committee chaired by a member of the Joint Standing Committee on Foreign Affairs, Defence and Trade.

Legislative reforms would be needed to support unconventional deterrence, with particular focus on ensuring that the *Defence Act 1903*, the *Intelligence Services Act 2001*, the *ASIO Act 2012* and the *Telecommunications Act 1979* are fit for purpose to enable unconventional deterrence during pre-conflict, when their impact is likely to be most strategically significant but also most politically controversial.

To be effective, Australian unconventional deterrence also needs robust institutional machinery including all interagency elements from Defence (including the Australian Signals Directorate), Home Affairs, the Attorney-General's Department, the Department of Foreign Affairs and Trade and the national intelligence community. Those agencies, coordinated by a reinvigorated NSA, could facilitate collaborative, multiagency taskforces with the time and space to engage in pre-conflict detection, attribution and assessment during an emerging security crisis. Such taskforces would operate via centralised command-and-control elements, in much the same way that an interdepartmental emergency taskforce coordinates whole-of-government responses to overseas crises, or Home Affairs (through the National Emergency Management Authority's national coordination mechanism and the Australian Government National Situation Room) manages domestic crises.

Directed capabilities needed for unconventional deterrence

Singaporean statesman Lee Kuan Yew's prescriptions, in the mid-20th century, for deterring larger Asian powers from interfering in Singaporean affairs or seeking to annex the island state apply to Australia and its neighbours in the 21st century. Drawing on a Chinese proverb, Lee said at a conference in 1966 that:

> In a world where the big fish eat small fish, and small fish eat shrimps, Singapore must become a poisonous shrimp … There are various types of shrimps. Some shrimps stay alive … Species in nature develop defence mechanisms. Some shrimps are poisonous: they sting. If you eat them, you will get digestive upsets.[96]

An attendee asked what he meant in the context of Singapore's dependence on commercial relations with its 'big fish' neighbours: China, Malaysia and Indonesia. Lee replied, 'our separate existence having been accepted and conceded, we then deal with them on equal and fair terms.'[97] This 'poisonous shrimp' approach—similar to the 'indigestible hedgehog' or 'porcupine' strategies adopted by Switzerland, the Baltic states and others—is a useful way to think about conventional and unconventional deterrence, working in tandem.

Effective unconventional deterrence contributes to a broad deterrence-by-denial strategy through the aggregation of unconventional and conventional military and non-military capabilities. That pushes adversary options to the margins, where conventional military power—the source of a likely aggressor's key advantage—is neither effective nor appropriate. For Australia, a strong ADF is essential for unconventional deterrence. Once an adversary chooses to avoid a traditional, conventional military confrontation and commences grey-zone operations as an alternative, unconventional deterrence comes into its own. The imaginative and effective employment of unconventional capabilities, as both a deterrent and a force option, is thus critical to Australia's overall national-security strategy.

The initial focus for Australian unconventional deterrence should be to enhance regional partners' capacity to resist external interference and coercion. The development of mutually beneficial counterterrorism partnerships between Australia and regional partners during the Global War on Terror provides a model for this. So, too, does the Australian Federal Police, which has spent significant effort this past decade developing connections with regional partners to thwart transnational crime such as drug, arms and people trafficking. The Royal Australian Navy likewise cooperates with neighbours for border protection and surveillance of exclusive economic zones. Defence international engagement programs offer a mechanism by which Australia can set conditions for unconventional deterrence in partnership with like-minded countries in the region, while also pursuing other policy goals.

The ability to fight across land, sea, air, space and cyber—before and during conflict, in and beyond declared war zones—offers new ways to deter adversaries in unexpected ways

Traditional missions, including strategic strike (often with terminal guidance via local partner forces), special recovery, strategic reconnaissance and specialist support operations all have utility as components of deterrence. Increasingly, however, offensive cyber, electronic warfare (including the penetration of adversaries' critical mission systems), space access and control, persistent surveillance of high-value targets (including chemical, biological, radiological and nuclear systems) and technical enablement of other military and national-security capabilities are key.

To generate all those deterrent effects, Australia's unconventional deterrence capabilities must match the scale of ambition and commitment from government and policymakers to include AUKUS and the 'REDSPICE' capability investments currently underway in the Australian Signals Directorate.[98] The force design required for that deterrent capability must also be unconventional in nature. Given the relatively limited role of Australian special forces in the grey zone, and the broad range of capabilities required in terms of demography, skills, background, technical literacy and martial skills, the only feasible method of force-generating such an organisation is via a whole-of-nation approach, similar to Australia's efforts in establishing SOA during World War II.[99] Under that approach, responsible

government departments, coordinated by the NSA, would generate diverse but complementary capability sets, to be force-assigned to missions commanded by a supported agency, working directly to the NSA as circumstances dictate.

Unconventional deterrence complicates the calculus of potential adversaries by limiting their strategic options before conflict and imposing costs across a range of categories both before and during conflict. In particular, adversaries may be less inclined to pursue goals in the grey zone if they know Australia is able to contest them in that space. Through the combined efforts of all interagency partners, effective strategic leadership and the re-establishment of an Australian NSA, Australia can complement conventional deterrence with an unconventional capability comprising both traditional and emerging capabilities, thereby countering hostile actions by adversaries both inside and outside traditional conflict.

Part 4: Conclusions

Today's environment involves heightened tension amid strategic competition among democratic states and autocracies. To be strategically useful, Australian capabilities must cover an extraordinarily wide range of tasks across both conventional and irregular warfare, against both states and non-state actors, in multiple domains and campaign phases, at all points on a competition continuum, and in an unforgiving technological setting.

Australia's history offers insight into policy options for both the enduring nature and the evolving character of competition. Japanese strategic competition with Australia before World War II was not dissimilar, as noted above, to the actions of today's CCP.

Yet, as noted, there's a 'deterrence gap' in the NDS, which doesn't directly address the need to deter an adversary between now and 2032, when the first of the planned AUKUS submarines is due to arrive. Likewise, there's a 'competition gap' in that Australian concepts of deterrence don't address the nature of competition as currently practised by China and other autocratic regimes such as Russia, North Korea and Iran. Lessons can be drawn from our historical experience of strategic competition, including successes and failures. The historical record offers insight into asymmetric policy options and capabilities against a beyond-peer adversary.

Despite Australia's inferiority in terms of size against an adversary like the CCP, history demonstrates that innovative concepts and asymmetric capabilities can achieve deterrent effects ahead of and during conflict. Most recently, unconventional deterrence logic was demonstrated by US, NATO and Ukrainian SOF before and during the current Ukrainian conflict, with deterrence-by-detection, asymmetric strike and support to resistance all playing a role. As Australia considers the implementation of the NDS, such adaptations are worth considering as ways to generate the asymmetry that Australia's situation demands.

The policy options discussed here are collectively termed 'unconventional deterrence'—a concept developed for this paper, but in no way a new idea, as World War II history demonstrates. Unconventional deterrence might unmask grey-zone activities, informing public opinion against subversion by an adversary. It might pose an asymmetric strike threat, communicating the ability to impose disproportionate financial, materiel, human, reputational and temporal costs against an adversary, while providing off-ramps to avoid runaway escalation in a crisis.

Supporting regional partners and like-minded countries to realise their 'total defence' strategies is a key element of this approach: indeed, in terms of Australia's relations with our neighbouring continent, the strategic premise for unconventional deterrence is the need to develop security *with* Asia, as opposed to security *against* Asia (as in the 'defence of Australia' strategy of the 1990s) or security *in* Asia (the 'forward defence' strategy of the 1950s–1970s).

Unconventional deterrence offers a conceptual basis for a strategic approach implicit but not spelled out in the NDS—which in a best-case scenario might deter a more powerful adversary from using force against Australia altogether or, in case of conflict, might deter an enemy from specific actions or targets.

Notes

1 Australian Government, *National Defence Strategy*, 2024, 23, online.
2 This paper uses the term 'enemy' to denote a hostile belligerent applying armed force against us in an ongoing (declared or undeclared) conflict, and 'adversary' to denote a potential enemy engaging in opposition or competition or undermining of our interests but that isn't currently an armed enemy.
3 Colin S Gray, *Another bloody century*, Weidenfeld & Nicholson, London, 2005, 121.
4 Carlotta Gall, Thomas De Waal, *Chechnya: a small victorious war*, Pan Books, London, 1997.
5 Brad Roberts, *Between tragedy and catastrophe: taking intra-war deterrence seriously*, Livermore Papers on Global Security no. 16, Lawrence Livermore National Laboratory, Center for Global Security Research, September 2025, 11–15.
6 Ivan Arreguín-Toft, 'Unconventional deterrence: how the weak deter the strong', in TV Paul, Patrick M Morgan, James J Wirtz (eds), *Complex deterrence: strategy in the global age*, University of Chicago Press, Chicago, 2009, 222–259.
7 Ivan Arreguín-Toft, *How the weak win wars: a theory of asymmetric conflict*, Cambridge University Press, Cambridge, 2005, 6.
8 Arreguín-Toft, *How the weak win wars*, 18, 45; emphasis in the original.
9 Stephen P Halbrook, *The Swiss and the Nazis: how the alpine republic survived in the shadow of the Third Reich*, Casemate, Philadelphia, Pennsylvania, 2006.
10 Michael Howard, *Grand Strategy: Volume IV: August 1942 – September 1943*, History of the Second World War United Kingdom Military Series, JRM Butler (ed.), Her Majesty's Stationary Office, London, 1972, 462–463.
11 Gjermund Forfang Rongved (ed.), *European total defence: past, present and future*, Routledge, London and New York, 2025.
12 See Pascal Lottaz, '"Cooperation" before "neutrality": Switzerland's new security doctrine', *Schweizer Standpunkt,* 22 August 2023, online; Kevin D Stringer, 'Building a stay-behind resistance organization: the case of Cold War Switzerland against the Soviet Union', *Joint Force Quarterly*, December 2020, vol. 86, online.
13 See Claire Mills, 'Military assistance to Ukraine 2014–2021', Parliamentary Research Briefing no. 7135, UK Parliament, 4 March 2022, online.
14 David Sanger, Eric Schmitt, 'US details costs of a Russian invasion of Ukraine', *New York Times,* 8 January 2022, online.
15 Andrew Maher, 'Resistance strategy: lessons from the Russo-Ukraine conflict for Europe, Australia and the Indo-Pacific', *Australian Journal of Defence and Security Studies*, 2023, 5(1).
16 'The digital component of Ukraine's resistance to Russian aggression', Atlantic Council, 17 May 2022, online (accessed 2 November 2023).
17 Discussed in Maher, 'Resistance strategy: lessons from the Russo-Ukraine conflict for Europe, Australia and the Indo-Pacific'.
18 J Matthew McInnis, *Iran at war: understanding why and how Tehran uses military force*, American Enterprise Institute, December 2016; see also Jean-Loup Samaan, *Non-state actors and anti-access/area denial strategies: the coming challenge*, Strategic Studies Institute, US Army War College, February 2020.
19 See David Leonhardt, 'Iran's Axis of Resistance', *New York Times,* 4 April 2024, online.
20 See Nicholas Carl, *The reshaping of Iran's Axis of Resistance*, Institute for the Study of War, 10 December 2024, online; see also Andrew J Tabler, *Why Assad fell*, Washington Institute for Near East Policy, 10 December 2024, online.
21 For contemporaneous US/Israeli commentary on the strikes, see Afshon Ostovar, Aaron Stein, *Tempting fate: the implications of Iran's attack on Israel*, Foreign Policy Research Institute, 15 April 2024, online.
22 See Sinem Adar, Muriel Asseburg, Hamidreza Azizi, Margarete Klein, Guido Steinberg, *The fall of the Assad regime: regional and international power shifts*, Stiftung Wissenschaft und Politik, Berlin, February 2025, online.
23 Andrew Maher, 'A "Plan B" for the ADF: supporting resistance as a strategy', *The Strategist*, 21 July 2023, online.
24 This idea is examined in detail in Andrew Maher, 'A plan B: an Australian support to resistance operating concept', *Australian Army Journal*, 2024, 20(2):77–79.
25 Ministry of Defence (MoD), Strategic Defence Review: Making Britain safer: secure at home, strong abroad, UK Government, 2025, 12, online.
26 MoD, *Strategic Defence Review*, 21.
27 'Broadcast message by Mr RG Menzies, Prime Minister', 3 September 1939, in Neale (ed.), *DAFP, 1937–49:* volume II, 226.
28 CA Brown (ed.), *The official history of special operations—Australia, volume 1—Organisation*, National Library of Australia, 2011, 13.
29 Brown, *The official history of special operations—Australia, volume 1—Organisation*, 13.
30 David Stafford, 'The detonator concept: British strategy, SOE and European resistance after the fall of France', *Journal of Contemporary History*, April 1975, 10(2).
31 These 'grey zone' activities have been discussed in Andrew Maher, *History rhymes: lessons from Indo-Pacific competition and confrontation in the grey zone*, Irregular Warfare Initiative, 18 May 2023, online.
32 Alan Ogden, *Tigers burning bright: SOE heroes in the Far East*, Bene Factum Publishing Ltd, London, 2013, 42–3; Eric Andrews, 'Mission 204: Australian commandos in China, 1942', *Journal of the Australian War Memorial*, April 1987, no. 10.
33 Lionel Gage Wigmore, 'Appendix 1—Australians in Mission 204', in *Australia in the War 1939–1945*, Official History series 1—Army, volume IV—The Japanese Thrust (1st edition, 1957), 643; War Office to C in C Far East, desp. 88880, WO106/3555A, 9 Sep 1941; C in C Far East, 41239, WO106/3555A, 5 Sep 1941.
34 War Office to C in C Far East, 76963, WO106/3555A, 9 July 1941.
35 Andrews, 'Mission 204', 11.
36 'Japanese security services', 30 June 1945, Australian War Memorial barcode 8729774, 25.
37 For a useful summary, see Peter Williams, *The Kokoda campaign: myth and reality*, Australian Army History Series, Cambridge University Press, Melbourne, 2012, 24*ff*.
38 Williams, *The Kokoda campaign: myth and reality*, 24–25.
39 Williams, *The Kokoda campaign: myth and reality*, 28–30.
40 Williams, *The Kokoda campaign: myth and reality*, 26–27.
41 The term 'SOA' is used for consistency here: several names were used over time to describe this organisation and related entities. The term SOA as used here describes thematically the full range of special operations activities undertaken by Australia.
42 Brown, *The official history of special operations—Australia, volume 1—Organisation*, 17.
43 Eric Feldt, *The coast watchers*, Oxford University Press, London, 1946, 2–5, 7–11.

44 For an assessment of these operations, see Gavin Long, *Australia in the war of 1939–45*, series 1, vol. VII, *The Final Campaigns,* Appendix 4, 'The Allied Intelligence Bureau', Australian War Memorial, Canberra, 1963, 617–622.

45 See Robert Cleworth, John Suter Linton, *RAAF Black Cats: the secret history of the covert Catalina mine-laying operations to cripple Japan's war machine*, Allen and Unwin, Sydney, 2020.

46 The language of 'indirect approach' channels BH Liddell Hart, *Strategy,* 2nd revised edition, First Meridian Printing, New York, originally printed in 1954.

47 A modified version of some parts of the following section will appear in David Kilcullen, 'Irregular and unconventional warfare', in Sebastian Kaempf, Artur Gruszczak (eds), *Routledge handbook on the future of warfare*, Routledge, London, forthcoming, 166–177; see also Rajeev Bhattacharya, 'How China's "aid" to rebel groups sustained northeast insurgency', *The Quint*, 1 July 2020, online; Lyle Morris, 'Is China backing Indian insurgents?', *The Diplomat,* 22 March 2011, online.

48 Tom Kramer, *The United Wa State Party: narco-army or ethnic nationalist party?,* policy studies 38 (Southeast Asia), East–West Center, Washington DC, 2007, xv; Bertil Lintner, *The United Wa State Army and Burma's Peace Process*, report no. 147, United States Institute of Peace, Washington DC, April 2019, 2; Dominique Dillabough-Lefebvre, 'The Wa art of not being governed: the Wa are keen to shed their image as Myanmar's drug lords or China's proxies', *The Diplomat*, 28 May 2019, online; further, it was recently reported that the United Wa State Army is protecting new rare-earth mines operated by Chinese companies. Shoon Naing, Devjyot Ghoshal, Napat Wesshasartar, Eleanor Whalley, Naw Betty Han, 'China-backed militia secures control of new rare earth mine in Myanmar', *The Japan Times*, 12 June 2025, online.

49 See Elsa Kania, 'The PLA's latest strategic thinking on the three warfares', *China Brief*, 22 August 2016, 16(13), online.

50 See Dennis J Blasko, 'Chinese Special Operations Forces: not like "Back at Bragg"', *War on The Rocks,* 1 January 2015, online.

51 See Andrew S Erickson, *Understanding China's third sea force: the maritime militia*, Harvard Fairbanks Center for Chinese Studies, 8 September 2017, online; Andrew S Erickson, Conor M Kennedy, 'Meet the Chinese maritime militia waging a "people's war at sea"', *Wall Street Journal*, 30 March 2015, online.

52 'APT1: Exposing one of China's cyber espionage units', Mandiant, 2013.

53 Department of Justice, 'US charges five Chinese military hackers for cyber espionage against US corporations and a labour organization for commercial advantage', media release, US Government, 19 May 2014.

54 D Rushe, 'OPM hack: China blamed for massive breach of US Government data', *The Guardian*, 5 June 2015; Committee on Oversight and Government Reform, *The OPM data breach: how the government jeopardized our national security for more than a generation*, US House of Representatives, 114th Congress, majority staff report, 7 September 2016.

55 'Director Wray's opening statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party', Federal Bureau of Investigation, Washington DC, 31 January 2024, online.

56 'Director Wray's opening statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party'.

57 Brian David Johnson, Jason C Brown, Josh Massad, *Digital weapons of mass destabilisation: the future of cyber and weapons of mass destruction*, Threatcasting Lab, Arizona State University, no date, online.

58 See Edmund J Burke, Kristen Gunness, Cortez A Cooper III, Mark Cozad, *People's Liberation Army operational concepts*, RAND Corporation, Santa Monica, 2020, 13.

59 Burke et al., *People's Liberation Army operational concepts*.

60 David Kilcullen, *The dragons and the snakes: how the rest learned to fight the West*, Oxford University Press, New York, 2020, 221–223.

61 Burke et al., *People's Liberation Army operational concepts*, 21

62 Dmitry (Dima) Adamsky, *Cross-domain coercion: the current Russian art of strategy*, Institut Français des Relations Internationales, Paris, 2015).

63 Jack Watling, Oleksandr V Danylyuk, Nick Reynolds, *The threat from Russia's unconventional warfare beyond Ukraine, 2022–24*, Royal United Services Institute, London, February 2024, 5.

64 Department of Defence, *National defence: Defence Strategic Review*, Australian Government, 2023, online, 17.

65 Australian Government, *National Defence Strategy*, 2024, 5–6.

66 Australian Government, *National Defence Strategy*, 14.

67 The broader context of this statement is: 'The strategic risks we face require the implementation of a new approach to planning, force posture, force structure, capability development and acquisition … It is clear that a business-as-usual approach is not appropriate'. Department of Defence, *National defence: Defence Strategic Review*, 24.

68 North Atlantic Treaty Organization, *NATO Warfighting Capstone Concept*, Allied Command Transformation, Norfolk, Virginia, 2021, 5.

69 Mick Ryan, Peter Warren Singer, 'The future of deception in war: lessons from Ukraine', *New America*, May 2025, 41.

70 See Richard Marles, 'Australia continues to stand with Ukraine,' media release, 27 April 2024, online.

71 Kori Schake, Joseph Tavares, 'A beneficial war? How Russia's invasion of Ukraine has enhanced the United States' strategic position in the world', in Zeno Leoni, Maeve Ryan, Gesine Weber (eds), *War in Ukraine: one year on,* King's College London, February 2023, 40.

72 Discussed in detail in Maher, 'Resistance strategy: lessons from the Russo-Ukraine conflict for Europe, Australia, and the Indo-Pacific'. The Swedish total defence strategy is instructive with regard to the belief in what we term unconventional deterrence concepts; see 'Main elements of the government bill Totalförsvaret 2021–2025', Swedish Government, 21 June 2021, online (accessed 30 January 2023) and Psychological Defence Agency, online.

73 Alexander Kim, 'Kazakhstan reinforces multivector foreign policy', *Eurasia Daily Monitor*, Jamestown Foundation, 9 July 2025, 22(100), online.

74 Thomas G Mahnken, Travis Sharp, Grace B Kim, *Deterrence by detection: a key role for unmanned aircraft systems in great power competition*, Center for Strategic and Budgetary Assessments, 2020, iii; Travis Sharp, Thomas G Mahnken, Tim Sadov, *Extending deterrence by detection: the case for integrating unmanned aircraft systems into the Indo-Pacific Partnership for Maritime Domain Awareness*, Center for Strategic and Budgetary Assessments, 2023.

75 Sophia McGrath, *Spotlight on the shadow war: inside Russia's attacks on NATO territory*, US Helsinki Commission, November 2024, 7.

76 Wyn Bowen, Matthew Moran, 'Sanctions, deterrence and the recent case of Russia', in Ksenia Kirkham (ed.), *The Routledge handbook of the political economy of sanctions*, Routledge, Oxon, 2024, 59–77.

77 For a discussion of 'liminal warfare' and 'liminal manoeuvre', see Kilcullen, *The dragons and the snakes: how the rest learned to fight the West*, 115–119.

78 Keith Jeffery, *MI6: the history of the Secret Intelligence Service 1909–1949*, Bloomsbury, 2010, 176–177; Harry Ferguson, *Operation Kronstadt*, Arrow Books, 2008, 2009, e-reader version.

79 Sam Skove, 'Navies face "dreadnought moment" as Ukraine destroys more Russian warships, British admiral says', *Defence One*, 13 September 2023, online.

80 David Kilcullen, 'Israel–Iran war reveals rising age of unconventional conflict', *The Australian*, 21 June 2025 online.

81 Katja Bego, *Ukraine's Operation Spider's Web is a game-changer for modern drone warfare. NATO should pay attention*, Chatham House, 6 June 2025, online.

82 Kilcullen, 'Israel–Iran war reveals rising age of unconventional conflict'.

83 Otto Fiala (ed.), *Resistance operating concept*, Swedish Defence University and Joint Special Operations University, Stockholm and Tampa, Florida, 2019. An alternate, but similar, definition is: 'a form of contention or asymmetric conflict involving participants' limited or collective mobilisation of subversive and/or disruptive efforts against an authority or structure.' Jonathan B Cosgrove, Erin N Hahn, *Conceptual typology of resistance: assessing revolutionary and insurgent strategies*, US Army Special Operations Command and John Hopkins University Applied Physics Laboratory, February 2021.

84 'Ukrainian Parliament (Verkhovna Rada) register a bill #5557 "About foundations of national resistance"', Ukrainian Security and Cooperation Centre, 25 May 2021, online (accessed 30 June 2022).

85 Otto C Fiala, 'Resistance resurgent: resurrecting a method of irregular warfare in great power competition,' *Special Operations Journal*, 2021, 7(2).

86 Government of Ukraine, 'National Resistance Centre' (Центр національного спротиву), online.

87 Estonian Defence League, online (accessed 4 June 2022).

88 The short film, *Taistelukenttä* [*Battlefield*], produced by the Finnish Ministry of Defence, is notable in its visual demonstration of the Finnish understanding of Russian hybrid warfare tactics and the way military and civilian resistance preparations stand ready to counter grey-zone actions, online (accessed 4 June 2022).

89 The Defence Strategy of the Czech Republic, Prague, 2012.

90 Stephen J Flanagan, Jan Osburg, Anika Binnendijk, Marta Kepe, Andrew Radin, *Deterring Russian aggression in the Baltic states through resilience and resistance*, research report, RAND Corporation, Santa Monica, April 2019, 2, online.

91 For additional detail, see David Kilcullen, 'Mobilisation and Australia's national resilience', *Australian Army Journal*, 2024, XX(3):121–161.

92 Eric Robinson, Timothy R Heath, Gabrielle Tarini et al., *Strategic disruption by special operations forces: a concept for proactive campaigning short of traditional war*, RAND Corporation, Santa Monica, 2023.

93 Robinson et al., *Strategic disruption by special operations forces*, v.

94 Robinson et al., *Strategic disruption by special operations forces*, vii.

95 Paul Symon, 'Yes, Australia does need a national security adviser', *The Strategist*, 20 December 2023, online (accessed 7 September 2024).

96 'Transcript of a talk given by the Prime Minister, Mr Lee Kuan Yew on the subject "Big and Small Fishes in Asian Waters" at a meeting of the University of Singapore Democratic Socialist Club at the University campus on 15th June, 1966', media release, Singapore Government, MC.JUN.22/66(PM), online (retrieved 20 June 2020).

97 'Transcript of a talk given by the Prime Minister, Mr Lee Kuan Yew on the subject "Big and Small Fishes in Asian Waters" at a meeting of the University of Singapore Democratic Socialist Club at the University campus on 15th June, 1966'.

98 REDSPICE = resilience, effects, defence, space, intelligence, cyber and enablers.

99 David Horner, *SAS: Phantoms of war, a history of the Australian Special Air Service*, updated edition of *SAS: Phantoms of the jungle*, Allen & Unwin, Sydney, 2002, 20–68.

Acronyms and abbreviations

ADF	Australian Defence Force
AI	artificial intelligence
ASIO	Australian Security Intelligence Organisation
CCP	Chinese Communist Party
DSR	Defence Strategic Review
FBI	Federal Bureau of Investigation
ISR	intelligence, surveillance and reconnaissance
NATO	North Atlantic Treaty Organization
NDS	National Defence Strategy
NSA	National Security Adviser
OPE	operational preparation of the environment
PLA	People's Liberation Army
RAAF	Royal Australian Air Force
SOA	Special Operations Australia
SOCEUR	Special Operations Command – Europe (US)
SOCOMD	Special Operations Command
SOE	Special Operations Executive (UK)
SOF	special operations forces
TDF	territorial defence forces
USV	uncrewed surface vehicle

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

What's your strategy?

The Strategist, ASPI's commentary and analysis website, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at www.aspistrategist.org.au

THE STRATEGIST

To find out more about ASPI go to www.aspi.org.au or contact us on 02 6270 5100 and enquiries@aspi.org.au.

Stay informed via the field's leading think tank, the Australian Strategic Policy Institute.

facebook.com/ASPI.org @ASPI_org

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

ISSN 2200-6648