Journal of Military and Strategic Studies

VOLUME 24, ISSUE 4

Counterintelligence for Hybrid Threats in Large-Scale Joint Operations: A Divisional Model from the Australian Defence Force

Henry Prunckun*

Deakin Yates*

Introduction

Background

Hybrid intelligence threats now sit at the heart of strategic competition. Adversaries combine espionage, cyber-enabled collection, insider recruitment, and cognitive operations to weaken decision-making advantage and cohesion long before open confrontation. For democratic militaries, these challenges pose a structural question rather than merely a technical one: how should counterintelligence (CI) be organised at

* **Henry W. Prunckun**, BSc, MSocSc, MPhil, PhD, is an Adjunct Associate Research Professor at the Australian Graduate School of Policing and Security.

* **Deakin Yates** is a Sergeant in the Australian Defence Force. *The views expressed in this paper are his own and do not reflect those of the Australian Army or the Department of Defence.*

* *Acknowledgments: The authors wish to thank Charles Sturt University for access to its invaluable library resources.*

ISSN : 1488-559X

operational and divisional levels so that it can counter hostile intelligence activities while remaining within existing legal authorities and civil–military norms? This paper addresses that question through the case of the Australian Defence Force (ADF), which operates under strict statutory constraints and relies on a civilian security service to exercise many of its mandatory powers. Based on Prunckun's theory of counterintelligence and a strengths–opportunities analysis of doctrine, historical experience, and allied practice, the study develops a principles-based CI posture for large-scale, joint operations and features a practical vignette to show how embedded CI practitioners, joint processes, and CI–PSYOPS–cyber integration can be used to counter hybrid threats.

In this context, hybrid intelligence threats present a substantial challenge. For this study, *hybrid intelligence threats* are defined as activities whose primary purpose is to gain intelligence advantage against the ADF—collection, denial and deception, subversion, and decision-shaping—rather than the full spectrum of hybrid warfare effects.

The terms *hybrid warfare* and *hybrid threats* are used inconsistently across doctrine and scholarship and are sometimes criticised as overly elastic labels that risk bundling disparate activities into a single paradigm. In this paper, *hybrid intelligence threats* are therefore treated as a pragmatic organising construct: a doctrinally salient shorthand for a recurring bundle of intelligence-driven behaviours (espionage, cyber-enabled collection, insider activity, and decision-shaping) that can converge against divisional decision cycles. The argument does not depend on "hybridity" being a settled theory of war; it depends on the operational reality that these vectors can be synchronised and must be countered within existing legal authorities and joint command processes.

The analysis is confined to divisional command and joint operational interfaces, excluding strategic political warfare except where those activities directly impose CI requirements on divisional and HQJOC processes.

This study does not develop a political–economic counter-interference doctrine. It interfaces with those domains only insofar as pressures in the political or economic environment generate tactical.[1]CI requirements—for example, a false rumour affecting

[1] The term *tactical* here generally refers to the Divisional level as the tactical unit of action, around which, in conflict, a joint formation may be organised. Alternatively, tactical could also describe joint formations, such as

pay that degrades cohesion—become a CI problem when it targets decision advantage within the force. Where activities would require statutory powers or whole-of-government action, responsibility rests with legislated partners; the tactical CI posture engages by defining requirements, liaising, and synchronising effects under command authority.

These threats encompass a range of adversarial activities, including espionage, sabotage, special operations, cyber-enabled intelligence operations, insider threats, and psychological warfare—all aimed at undermining a military force's decision-making and operational effectiveness. Considering Australia's strategic environment and increasing participation in joint and coalition operations, it is suggested that the Australian Defence Force (ADF) could enhance its counterintelligence (CI) capabilities to address these threats effectively.

Counterintelligence plays a crucial role in military operations by identifying, assessing, and neutralising threats to security posed by hostile intelligence entities and insider threats. However, in the face of hybrid intelligence threats, the ADF's existing CI structures may need to be adapted to stay effective in large-scale combat operations (LSCO). Unlike traditional CI approaches that focus mainly on peacetime security and counterespionage, modern conflict environments require a more dynamic and integrated CI framework that can operate efficiently at different levels of command, both domestically and overseas, the likes of which have not been tested since World War II.

A challenge is determining how CI should be structured within the ADF to best support commanders at the tactical and operational levels in a joint operational environment, as part of a broader Defence structure. Historically, CI has been associated with intelligence and security functions at the higher strategic level. Still, large-scale conflicts necessitate robust CI support closer to the tactical and operational theatres, where commanders require timely intelligence to inform security and force protection decisions. Furthermore, given the increasingly joint nature of modern operations, any proposed CI structure must also support and complement the Royal Australian Air Force (RAAF), the Royal Australian Navy (RAN), the Australian Regular Army (ARA), and

task forces, that have an operational requirement for tactical CI below the nominal resourcing threshold of a Divisional structure.

Defence civilian intelligence staff elements to ensure cross-domain coordination and a unified Defence posture.

Without an adaptive CI framework, it is posited that the ADF risks gaps in its intelligence posture, vulnerabilities to hybrid intelligence threats, and degradation of advantageous decision-making at the divisional level. Addressing this issue requires a considered approach to structuring CI to counter hybrid intelligence threats effectively while ensuring its integration into joint force operations.

Research Question

To address these challenges, this study sought to answer the following question: How should the Australian Defence Force structure its counterintelligence to address hybrid intelligence threats in large-scale combat operations, and how can it best support commanders, particularly at the tactical level, within a joint operational environment? By exploring this question, this study analysed existing CI structures, doctrinal approaches, historical case studies, and best practices from allied forces to propose an optimised framework for the ADF's counterintelligence capabilities in large-scale combat operations.

The contribution presents a principles-based design proposal for how divisional-level CI could be structured and integrated into joint operations under existing Australian authorities. It does not claim to validate the model through comparative performance testing; instead, it argues for plausibility and coherence in light of doctrine, allied practice, and historical cases, and frames the outputs as propositions suitable for evaluation through exercises and post-activity review.

Literature Review

Theoretical Base

Counterintelligence is a pillar of military intelligence dedicated to identifying, assessing, and mitigating threats to security posed by foreign intelligence entities, as well

as espionage, sabotage, and insider threats.[2] Unlike traditional intelligence, which focuses on gathering and analysing information about adversaries, CI is inherently defensive, aiming to safeguard a military force's decision-making processes, personnel, and operational security.[3] In contemporary warfare, CI plays a role in countering adversarial activities aimed at manipulating or degrading military effectiveness.[4]

Historically, CI has been associated with strategic-level operations focused on counterespionage and the protection of military information during peacetime.[5] However, the evolving nature of conflict—characterised by hybrid warfare—demands CI capabilities that extend beyond traditional security functions.[6] Modern adversaries employ a range of tactics, including conventional and irregular methods, such as cyber intrusions, disinformation campaigns, and psychological operations, to undermine military cohesion and decision-making superiority.[7] Consequently, CI must operate across multiple levels of command to ensure real-time detection and mitigation of threats.[8]

Hybrid warfare is widely used to describe the blending of conventional operations with cyber, influence, and intelligence-enabled subversion.[9] However, its definition and explanatory value remain contested. Some accounts treat it as an analytically distinct mode of conflict, while others regard it as a repackaging of long-standing practices of political warfare, deception, and subversion. For the purposes of counterintelligence design, the key point is not so much whether *hybrid* constitutes a discrete category as that

[2] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 8th ed. (Thousand Oaks, CA: CQ Press,2020); Michael Warner, *The Rise and Fall of Intelligence: An International Security History* (Washington, DC: Georgetown University Press, 2009).
[3] Defence Intelligence Organisation, *Defence Intelligence Doctrine* (Canberra: Commonwealth of Australia, 2021).
[4] Frank Hoffman, *Hybrid Warfare and Challenges* (Arlington, VA: Potomac Institute for Policy Studies, 2009); James Renz and Thomas Smith, "The Evolving Role of Counterintelligence in Hybrid Warfare," *Journal of Strategic Studies* 42, 4 (2016): pp. 547–64.
[5] David Betz and Rory Cormac, *Defence Intelligence and the Cold War: Britain and the Bomb* (London: Edinburgh University Press, 2019).
[6] Ofer Fridman, Russian Hybrid Warfare: Resurgence and Politicisation (London: Oxford University Press, 2018); NATO, Comprehensive Concept for Hybrid Warfare (Brussels: NATO, 2021).
[7] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020); Ben Buchanan, *The Hacker and the State* (Cambridge, MA: Harvard University Press, 2020).
[8] Australian Department of Defence, *Future Joint Operating Concept 2035* (Canberra: Commonwealth of Australia, 2020).
[9] NATO, Comprehensive Concept for Hybrid Warfare; Fridman, Russian Hybrid Warfare.

modern adversaries can integrate collection, denial/deception, insider enablement, and cognitive shaping to target decision advantage across echelons.[10]

CI plays a particularly important role in hybrid warfare, as adversaries often seek to weaken their opponents before confrontation through intelligence-driven tactics.[11] Espionage, insider threats, and human and cyber-enabled intelligence operations enable hostile actors to infiltrate decision-making structures, disrupt cohesion, and manipulate public perception.[12] Additionally, adversaries employ disinformation and psychological operations to erode trust within military and civilian institutions, complicating the mobilisation of forces and strategic planning.[13]

For the Australian Defence Force, the implications of hybrid warfare necessitate a reassessment of traditional CI structures.[14] Rather than operating in isolation as a purely analytical function, CI would be better served by being operationalised and embedded within broader intelligence frameworks, collaborating with cyber defence, electronic warfare, and psychological operations to counter hybrid threats.[15] This integrated approach ensures a proactive CI posture, neutralising direct intelligence threats and mitigating adversarial influence campaigns that could undermine military effectiveness.[16]

Joint operations demand coordination from service branches to achieve strategic and operational objectives.[17] In modern conflict environments, where hybrid threats exploit gaps in intelligence-sharing and coordination, service-level CI must also support joint force structures to provide comprehensive protection against adversarial

[10] Hoffman, Hybrid Warfare and Challenges.
[11] Australian Department of Defence, *Defence Strategic Update 2022* (Canberra: Commonwealth of Australia, 2022).
[12] Rid, Active Measures; Buchanan, The Hacker and the State.
[13] Australian Cyber Security Centre (ACSC), *Threat Report 2023* (Canberra: Commonwealth of Australia, 2023); Thomas Czosseck and Kenneth Geers, eds., *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: IOS Press, 2011).
[14]Rid, Active Measures; Richard A. Clarke and Robert K. Knake, The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats (New York: Penguin Press, 2019).
[15] Australian Department of Defence, *Future Joint Operating Concept 2035*.
[16] Australian Strategic Policy Institute (ASPI), *Countering Hybrid Threats* (Canberra: ASPI, 2023); NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Hybrid Conflict Handbook* (Tallinn: NATO CCDCOE, 2020).
[17] Joint Chiefs of Staff, *Joint Publication 2-0: Joint Intelligence* (Washington, DC: Department of Defense, 2020).

intelligence activities.[18] Traditionally, CI has been managed strategically, with intelligence and security functions segmented across the Royal Australian Navy, the Royal Australian Air Force, the Australian Regular Army and the Defence Security Division. It is subject to resource prioritisation consistent with the direction of service-specific intelligence.[19] However, the growing complexity of joint operations necessitates a more unified strategic CI framework to facilitate cross-domain coordination and rapid threat mitigation, while balancing service-level operational needs.[20]

A primary challenge in joint operations is ensuring that CI functions are effectively synchronised across different military components.[21] Each service branch operates within distinct operational domains, requiring tailored CI approaches that address service-specific vulnerabilities while maintaining an integrated defence posture.[22] A fragmented or *siloed* CI approach—absent centralised coordination—risks intelligence gaps that adversaries could exploit through cyber intrusions, insider threats, or human intelligence operations.[23]

To address these vulnerabilities, CI within joint operations must prioritise interoperability, information-sharing, and real-time threat analysis.[24] Effective CI structures should be embedded within joint task structures, ensuring that commanders at operational and tactical levels receive timely intelligence to support manoeuvre planning and force protection.[25] Additionally, as hybrid warfare increasingly targets military-civilian interfaces, joint CI efforts must extend beyond traditional military boundaries, collaborating with civilian intelligence agencies, cyber defence units, and law enforcement to counter threats.[26]

[18] Australian Department of Defence, *Defence Strategic Update 2022*; Joint Chiefs of Staff, *Joint Intelligence*, 2022.
[19] Betz and Cormac, *Defence Intelligence and the Cold War*; U.K. Ministry of Defence, *Intelligence Doctrine* (London: MOD, 2022).
[20] Defence Intelligence Organisation, *Defence Intelligence Doctrine*.
[21] Australian Defence College, *Joint Professional Military Education Handbook* (Canberra: ADC, 2021).
[22] Joint Chiefs of Staff, *Joint Intelligence*, 2022.
[23] Andrew Davies and Edward Gustafson, *Joint Force Integration* (Canberra: ASPI, 2013); Australian Department of Defence, *Defence Strategic Update 2022*.
[24] Czosseck and Geers, The Virtual Battlefield; ACSC, Threat Report 2023.
[25] Australian Department of Home Affairs, *Security and Intelligence Framework* (Canberra: Commonwealth of Australia, 2021); NATO CCDCOE, *Hybrid Conflict Handbook*.
[26] Joint Chiefs of Staff, *Joint Intelligence*.

The emergence of hybrid warfare has fundamentally altered the operational landscape for CI, necessitating a shift from traditional security intelligence measures toward a coordinated approach across several fields of operation.[27] Hybrid threats leverage intelligence-driven tactics—such as cyber-enabled espionage, disinformation campaigns, and proxies—to degrade a military force's decision-making ability, disrupt command and control structures, and manipulate the information environment.[28] In this context, CI must evolve beyond a conventional defensive role to actively identify, neutralise, and pre-empt adversarial intelligence operations across multiple domains.[29]

Unlike traditional conflicts, in which CI focuses on detecting enemy spies and preventing security breaches within military installations, hybrid warfare requires a more proactive, outward-looking approach.[30] Adversaries in hybrid conflicts exploit not only military vulnerabilities but also political, economic, and social fault lines, making CI engage in continuous threat monitoring beyond the immediate battlespace.[31] For example, cyber-enabled intelligence operations can compromise sensitive military planning, while influence campaigns designed to sow distrust within the ranks can weaken operational effectiveness before a conventional battle begins.[32]

CI within the ADF must integrate with cyber defence, electronic warfare, and psychological operations to address these threats and form a holistic counter-hybrid threat strategy.[33] This requires a doctrinal shift from compartmentalised intelligence functions toward a fusion of CI with broader security and operational planning efforts.[34] Additionally, CI personnel must be trained to operate in digital environments, identifying and countering adversarial intelligence activities in real-time.[35]

[27] Clarke and Knake, The Fifth Domain; ASPI, Countering Hybrid Threats.
[28] Hoffman, Hybrid Warfare and Challenges; NATO, Comprehensive Concept for Hybrid Warfare.
[29] Rid, Active Measures; Buchanan, The Hacker and the State.
[30] Australian Department of Defence, *Defence Strategic Update 2022*.
[31] Fridman, Russian Hybrid Warfare; Betz and Cormac, Defence Intelligence and the Cold War.
[32] Renz and Smith, "The Evolving Role of Counterintelligence"; ACSC, *Threat Report 2023*.
[33] Rid, Active Measures; Clarke and Knake, The Fifth Domain.
[34] Australian Department of Defence, Future Joint Operating Concept 2035; NATO CCDCOE, Hybrid Conflict Handbook.
[35] Joint Chiefs of Staff, *Joint Intelligence*; UK Ministry of Defence, *Intelligence Doctrine*.

The *Grounded Theory of Counterintelligence* offers a conceptual framework for understanding counterintelligence beyond its security-oriented focus.[36] This theory posits that CI is not merely a defensive discipline but an active and analytical function that plays a central role in shaping intelligence operations. Rather than viewing CI as an isolated function solely concerned with detecting and preventing espionage, it is presented as a core intelligence activity that integrates offensive (i.e., counterespionage) and defensive (i.e., security intelligence) strategies.[37] At the foundation of this theory, three axioms define CI operations: surprise, all-source data collection, and universal targeting.[38] Two operational categories of CI are established from these axioms: defensive CI and offensive CI, the latter incorporating deception and neutralisation.[39]

While all three axioms are integral to CI's effectiveness, surprise is critical in military and intelligence operations. Denying adversaries accurate intelligence enhances decision superiority, allowing military forces to act with greater operational freedom.[40] In hybrid warfare, where adversaries rely on cyber espionage, insider threats, and disinformation, maintaining the element of surprise ensures that defensive measures remain unpredictable and adaptable.[41] Without surprise, CI operations become reactive rather than proactive, making it easier for adversaries to exploit vulnerabilities.

By applying this theoretical framework, the ADF can refine its CI doctrine to incorporate defensive and offensive elements, ensuring a more resilient intelligence posture. The framework provides a structured approach integrating surprise, multi-source intelligence collection, and broad targeting—essential for countering hybrid intelligence threats in large-scale combat operations.[42]

[36] Hank Prunckun, "A Grounded Theory of Counterintelligence." *American Intelligence Journal*, Vol 29, 2, December 2011, pp. 6–15; Hank Prunckun, *Counterintelligence Theory and Practice, 2nd Ed*. (Lanham, MD: Rowman & Littlefield, 2019).
[37] Betz and Cormac, Defence Intelligence and the Cold War; UK Ministry of Defence, Intelligence Doctrine.
[38] Joint Chiefs of Staff, *Joint Intelligence*.
[39] U.K. Ministry of Defence, *Intelligence Doctrine*.
[40] Hoffman, Hybrid Warfare and Challenges; Joint Chiefs of Staff, Joint Intelligence, 2022.
[41] Fridman, *Russian Hybrid Warfare*; Renz and Smith, "The Evolving Role of Counterintelligence."
[42] Australian Department of Defence, *Future Joint Operating Concept 2035*; Defence Intelligence Organisation, *Defence Intelligence Doctrine*.

Methodology

Approach

Given the classified nature of contemporary Australian Defence Force counterintelligence capabilities and the limited availability of primary data, this study relied on secondary sources. This methodological choice is supported by established research practices, where indirect data—particularly validated doctrinal documents and historical case studies—inform analysis in contexts where primary collection is impractical or restricted.[43]

This study uses a strengths–opportunities (S–O) design because the research question focuses on capability development within institutional and legal constraints, rather than comparing performance against an adversary. S–O provides normative, design-focused insights about how existing ADF assets can be aligned with realistic development paths; *weaknesses* and *threats* are not ignored but are treated as boundary conditions, later defined as feasibility limits. To reduce selection and recency bias from secondary sources, information was triangulated across doctrine, policy, and allied practices; findings are presented as propositions with specific plausibility conditions rather than as prescriptive instructions.

Historical sources on large-scale combat operations involving Australia and allied doctrinal publications provide considerable depth and breadth to this study.[44] These materials encompass institutional learning, tactical evolution, and operational adjustments responsive to diverse geopolitical environments. Furthermore, allied publications from militaries recently engaged in tactical CI operations offer practical insights and proxy indicators of best practices directly relevant to the ADF's evolving needs.[45]

---

[43] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge, MA: MIT Press, 2005).

[44] John Blaxland, *The Australian Army from Whitlam to Howard* (Melbourne: Cambridge University Press, 2016); Albert Palazzo, *The Australian Army: A History of Its Organization, 1901–2001* (Melbourne: Oxford University Press, 2011); David Horner, *Australia's Military History for Dummies* (Milton: Wiley, 2017).

[45] U.S. Army, Army Techniques Publication (ATP) 2-22.2: Counterintelligence (Washington, DC: Department of the Army, 2020); UK Ministry of Defence, Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations, 3rd ed. (Shrivenham: Defence Academy of the UK, 2018).

The reliance on secondary sources also presents analytical advantages, which allowed the study to draw from a range of geographically and temporally diverse experiences. While the historical nature of some sources might pose limitations, their inclusion enables longitudinal analysis, revealing patterns of capability development and doctrinal adaptation over time.[46] This approach ensures that the study remains both relevant and reflective of broader trends beyond the immediate operational context of the ADF.

A Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis was considered to structure the analysis. However, it was deemed that a targeted Strengths–Opportunities (S–O) analysis was more suitable for assessing the Australian Defence Force's current and potential counterintelligence capabilities in support of a joint divisional force. This approach is derived from the well-established SWOT framework, a structured analytic technique widely used in strategic planning, organizational assessment, and security studies.[47] However, in alignment with this study's capability-focused nature, only the strengths (internal enablers) and opportunities (external developmental vectors) were analyzed.

Applying a focused S–O lens reflects the intent to identify how the ADF's existing institutional strengths—such as doctrine, training, and structural assets—can be leveraged to realise emerging opportunities for enhancing CI in large-scale combat operations. By omitting weaknesses and threats, the analysis prioritizes solution-oriented insights and reflects a strengths-based theoretical orientation aligned with Prunckun's *Grounded Theory of Counterintelligence*.[48]

The S–O analysis was structured around the central research question, which examined how to counter hybrid intelligence threats in joint operations while aligning with current doctrinal and operational requirements.[49] The resulting findings were

[46] Hugh White, *How to Defend Australia* (Carlton: La Trobe University Press, 2019).
[47] Pieter Puyt et al., "The SWOT Analysis: A Tool for Security Strategy Evaluation," *Journal of Strategic Security* 13, 2 (2020): pp. 68–80.
[48] Hank Prunckun, "A Grounded Theory of Counterintelligence." *American Intelligence Journal*, Vol. 29, No. 2, December 2011, pp. 6–15; Hank Prunckun, *Counterintelligence Theory and Practice, Second Edition* (Lanham, MD: Rowman & Littlefield, 2019).
[49] James Kiras, Special Operations and Strategy: From World War II to the War on Terrorism, 2nd ed. (London: Routledge, 2020).

categorized according to current operational capabilities and future developmental needs across key functional groupings: 1) organizational structure, 2) required CI activities, and 3) critical skills. This methodological approach also addressed data access constraints by triangulating doctrinal sources, training materials, and policy documents, thereby enhancing the validity and practical relevance of the conclusions. The analysis, therefore, informs immediate operational readiness and long-term capability development within the ADF's CI enterprise.

Feasibility and Scope Limits

Statutory directives, personnel pipelines, and training capacity limit implementation. The tactical embedding proposed here assumes modest reallocation of analyst billets across the Army's intelligence structure and phased training development in partnership with DIG schools; offensive CI activities are restricted to deception and neutralization that can be conducted under command authority with deconfliction among statutory authorities. The paper does not assume new legislation, new agencies, or wholesale restructuring of the ADF.

Data Collection

Given the classified nature of current operational data and limited primary access, this research relied on secondary data sources, including allied and domestic defence doctrines, policy documents, and historical case studies.[50] These materials were selected for their credibility, relevance, and capacity to provide insights into institutional practices, operational adaptations, and doctrinal evolution.

Defence doctrine publications were obtained from open-source repositories maintained by the Australian Department of Defence and allied military institutions, including the United States Department of Defense and the United Kingdom Ministry of Defence.[51] Priority was given to documents outlining counterintelligence structures, threat frameworks, and organizational integration at the divisional level or within joint operations. Allied doctrines were particularly valuable due to the ADF's limited direct experience with divisional-level deployments that require robust CI support. These allied

[50] George and Bennett, Case Studies and Theory Development.

[51] Australian Defence Force, *ADF Publication 2.0: Intelligence*, 2nd ed. (Canberra: Defence Publishing Service, 2017); UK Ministry of Defence, *Joint Doctrine Publication 2-00*; US Army, *ATP 2-22.2*.

documents offered proxy models and comparative benchmarks for assessing gaps and potential pathways for the ADF's CI development.

Policy documents, white papers, and strategic defence reviews were sourced from official government sources, as well as defence think tanks such as the Australian Strategic Policy Institute (ASPI). [52] These documents provided a macro-level understanding of national security priorities and defence capability roadmaps, identifying institutional challenges relevant to intelligence and counterintelligence functions. Including policy and documentation ensured that the analysis was grounded in operational realities and aligned with national strategic objectives and future capability planning frameworks.

Historical case studies were selected from peer-reviewed academic literature, military histories, and defence analysis publications.[53] Preference was given to studies examining the application of CI in joint and large-scale operations, particularly concerning hybrid intelligence threats and organizational learning outcomes. Case studies were drawn from various geopolitical contexts to ensure a balanced and comprehensive dataset, including operations in the Middle East, Southeast Asia, and Europe.

All data sources were catalogued and coded for thematic analysis to ensure consistency in categorizing information under the S–O framework and subsequent functional analysis. This study ensured analytical robustness by triangulating data from doctrinal, policy, and historical sources. It mitigated the limitations associated with the absence of primary field data.[54]

Results and Analysis (S-O)

Strengths

The current ADF doctrine employs a multi-disciplinary counterintelligence (MDCI) approach, as reflected in its definition of counterintelligence. By recognizing that MDCI entails an all-source appreciation of CI, the doctrine establishes an analytical

[52] Australian Government, *2020 Defence Strategic Update* (Canberra: Commonwealth of Australia, 2020); Peter Jennings and Malcolm Davis, "ADF's Role in National Intelligence," *ASPI Strategist*, 2022.
[53] Horner, Australia's Military History; Kiras, Special Operations and Strategy.
[54] George and Bennett, *Case Studies and Theory Development*; Puyt et al., "The SWOT Analysis."

foundation for assessing threats relevant to the tactical and operational Commander's planning and operations in a Joint operating environment.[55]

The ADF's current CI structure (J2 model) and functions are aligned with the MDCI approach—particularly in enabling CI staff to support the production of the CI Estimate. This structure is predominantly implemented at the Brigade equivalent (BDE(e)) / Joint Task Force level and above.[56]

ADF training programs currently support the MDCI-led methodology, particularly by training analysts to apply the CI Estimate as a core analytical instrument for identifying and understanding all-source CI threats against a commander.[57]

The ADF, notably the Army, retains significant historical expertise in human-threat-based counterintelligence. Much of this is grounded in the *Manual of Land Warfare 2-1-4: Counterintelligence* (1996), which encompasses the full range of human-threat CI functions necessary to generate security intelligence under the MDCI framework. This institutional knowledge enhances the ADF's ability to identify and counter threats to security from hostile intelligence services, terrorism, espionage, sabotage, and subversion.[58]

The Army also maintains a deep reservoir of historical and relevant doctrine for traditional CI, dating back to World War II and extending at least to 1996. This provides a strong procedural basis for executing MDCI and traditional CI, including CI staff support to commanders, as well as the operational conduct of CI activities that deliver security intelligence—a critical input to MDCI analysis.[59]

The Army retains a specialized psychological operations (PSYOPS) capability within the divisional intelligence unit, the 1st Intelligence Battalion. Development of an Army-specific CI practitioner capability would also potentially be generated in the same unit, subject to operational requirements. Co-location with other specialized intelligence

55 Australian Defence Force, *ADF Publication 2.0: Intelligence*, 2nd ed. (Canberra: Defence Publishing Service, 2018).
[56] Australian Army, *Land Warfare Doctrine LWD 2-0: Intelligence* (Canberra: Australian Army, 2021).
[57] Australian Defence College, *Joint Professional Military Education Handbook* (Canberra: ADC, 2022); Australian Army Research Centre, *Future Army Professional Education Study* (Canberra: AARC, 2019).
[58] Department of Defence, Manual of Land Warfare, Volume 2: Intelligence, Pamphlet 1 – Counterintelligence, 2-1-4 (Canberra: Commonwealth of Australia, 1996).
[59] Australian Army, LWD 2-0: Intelligence.

capabilities enhances opportunities for integration and coordination to support CI outcomes at the tactical and operational levels.

Each Service is currently developing its own CI capabilities tailored to its domain-specific requirements, creating unique advantages that, when combined, are expected to strengthen the Joint CI capability and effect across the ADF.[60]

Without dedicated legislation, the ADF may seek to leverage Command authorities—deconflicted with legislated or policy-empowered agencies—to conduct operational CI activities effectively within its operational remit.[61]

Australia benefits from a world-leading national security agency, the Australian Security Intelligence Organisation (ASIO), which, under legislation, is responsible for countering threats to Australia's national security and defence system. As part of this system, the Australian Defence Organisation (ADO)—comprising the ADF and the Defence Department, along with its subordinate Defence agencies—is afforded protection under ASIO's mandate.[62]

Establishing the Defence Intelligence Group (DIG) has centralised coordination of critical intelligence capabilities across the Defence intelligence enterprise. This includes Defence's civilian intelligence agencies and aspects of the ADF's intelligence capabilities, including counterintelligence (CI), enabling a coordinated and cooperative approach between Defence and the National Intelligence Community.

Offensive CI activities by the ADF—such as deception and neutralisation—must stay within command authority and be coordinated with ASIO's legal responsibilities when conducted domestically or involving Australian persons. Investigations and activities requiring compulsory powers remain under the jurisdiction of ASIO or civilian police. The model presented here relies on ADF–ASIO liaison efforts, DIG coordination, and HQJOC standardisation to ensure that tactical and operational CI practitioners plan and carry out only those measures authorised by Defence, with partner agencies leading where statutory powers are involved.

[60] Department of Defence, *Defence Intelligence Enterprise Review* (Canberra: Commonwealth of Australia, 2019).
[61] Department of Defence, *ADF Command and Control Handbook* (Canberra: Commonwealth of Australia, 2021).
[62] Australian Government, Australian Security Intelligence Organisation Act 1979, Act No. 113 of 1979.

Opportunities

There is scope to expand beyond analytical CI to develop a dedicated operational CI capability—aligned with U.S. and U.K. models—that incorporates the doctrinally recognised CI activities of investigations, collection, operations, analysis, and dissemination, as well as foundation services.[63] For the Army, they can leverage historical doctrine and Field Security practices to reconstitute ground-based CI practitioner roles responsible for conducting defensive and offensive CI activities, reintegrating security intelligence as a core input to inform MDCI analysis.[64]

The ADF CI doctrine has an opportunity to adopt a principles-based theoretical model for CI, similar to those employed by strategic partners. This would provide a coherent doctrinal framework to support long-term capability development, training, and integration that encompasses analytical-based MDCI and operational CI activities.[65]

Joint CI processes can be developed at the Headquarters Joint Operations Command (HQJOC) level to ensure Joint CI standards are met, regardless of Service-specific activities. This enables cohesive planning and execution of CI in joint and combined environments and leverages domain advantages provided by Service-specific CI capabilities.[66]

Another opportunity lies in formalising partnerships with psychological operations capabilities. As hybrid warfare increasingly targets cognitive and informational domains, integrating CI practitioners with PSYOPS elements creates the potential for coordinated efforts to disrupt adversarial influence, protect friendly decision-making, and reinforce operational security.

While CI remains primarily concerned with identifying and neutralising hostile intelligence activities, the complementary nature of PSYOPS, which focuses on shaping perceptions and influencing behaviour, presents an avenue for more comprehensive defensive and offensive counterintelligence operations in competition, crisis, and conflict. Developing formal liaison mechanisms or co-located planning cells between CI and

[63] Department of Defence, Manual of Land Warfare, Volume 2: Intelligence, Pamphlet 1 – Counterintelligence.
[64] Amanda Clarke, "Counterintelligence in the Information Age," in *Contemporary Intelligence Studies: A Reader*, ed. Philip Davies and Kristian Gustafson (London: Routledge, 2016), pp. 213–227.
[65] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 8th ed. (Thousand Oaks, CA: CQ Press, 2020).
[66] Australian Defence Force, ADF Publication 2.0: Intelligence.

PSYOPS at the tactical and joint operational levels would enhance the ADF's ability to detect and pre-empt hybrid threats across security and cognitive domains.

Strengthening engagement with partner CI training institutions, such as the U.K.'s Joint Intelligence Training Group and the U.S. Army CI School, offers opportunities to co-develop interoperable training courses and align doctrinal concepts for operational CI in coalition operations.[67] ADF CI should also draw on its own and partner's extensive history and expertise to conduct operational CI to develop sovereign training accessible to partner CI organisations.

The exploration and development of Command authorities for the conduct of counterintelligence (CI) in the Australian Defence Force (ADF)—deconflicted with legislated or policy-empowered agencies—could enable the ADF to conduct operational CI activities aligned with Defence's specific needs and requirements. Aligning these activities with the ASIO would likely enhance Defence's security posture with greater resourcing and capacity to address increasing security needs.

Developing Defence-wide CI capabilities in services, appropriately coordinated at the strategic level by an organisation such as the DIG, would enable Defence to complement ASIO's statutory role more effectively, thereby enhancing national security outcomes across both domestic and expeditionary environments.[68]

Discusions

Leveraging Strengths to Maximize Opportunities

In large-scale combat operations and hybrid threat environments, the Australian Defence Force possesses several institutional strengths that can be strategically leveraged to develop a more adaptive and operationally integrated counterintelligence capability. Drawing on the *Grounded Theory of Counterintelligence*, this section analyses how the ADF can align its existing doctrinal, structural, and training strengths with key opportunities to enhance its counterintelligence posture. This discussion is framed by the theory's three

[67] Australian Defence College, Joint Professional Military Education Handbook.
[68] Australian Security Intelligence Organisation (ASIO), *Annual Report 2022–2023* (Canberra: Commonwealth of Australia, 2023).

foundational axioms—surprise, all-source data collection, and universal targeting—and its division of CI into defensive and offensive operational categories.[69]

In this paper, offensive counterintelligence is defined narrowly for an ADF context as deception and neutralisation actions designed to deny, distort, or channel adversary intelligence processes in support of the commander's intent. It is distinct from counterespionage investigations and offensive cyber operations; it is an effects contribution planned by CI practitioners in coordination with operations, fires, and PSYOPS, and executed under command authority with deconfliction amongst statutory authorities where necessary.

Cyber-CI integration is specified at the task level: counter-reconnaissance in Defence networks through decoy assets and beaconing; analytic support to identify insider-enabled collection patterns; and CI requirements imposed on defensive cyber for ISR denial, all linked to deception schemes of manoeuvre. This advances beyond generic *disinformation* language to define the behaviours of analysts and operators needed to support divisional decision advantage.

First, we will discuss multi-disciplinary doctrine and structural alignment. An important strength of the ADF is its adoption of a multidisciplinary counterintelligence (MDCI) approach, embedded in its current doctrine.[70] This doctrine emphasises consideration of multi-disciplinary threats, using all-source intelligence to assess and mitigate threats to commanders in joint operational environments, aligning closely with Prunckun's axiom of all-source data collection. Additionally, the current intelligence structure—specifically the J2 model—supports MDCI by enabling staff to generate the Counterintelligence Estimate, a critical analytical method in threat assessment.[71]

This doctrinal foundation presents an opportunity to evolve beyond a primarily analytical CI model to one incorporating a dedicated operational CI capability. Allied models, particularly in the United States and the United Kingdom, enhance analytical MDCI with operational CI functions provided by specialist CI personnel and other

[69] Hank Prunckun, "A Grounded Theory of Counterintelligence." *American Intelligence Journal*, Vol. 29, No. 2, December 2011, pp. 6–15; Hank Prunckun, *Counterintelligence Theory and Practice* (Lanham, MD: Rowman & Littlefield, 2019).
[70] Australian Defence Force, *ADF Publication 2.0: Intelligence*, 2nd ed. (Canberra: Defence Publishing Service, 2018).
[71] Australian Army, *Land Warfare Doctrine LWD 2-0: Intelligence* (Canberra: Australian Army, 2021).

specialist disciplines, such as threat disruption and deception planning.[72] Developing similar capabilities would enable the ADF to maintain operational surprise and adopt a more proactive stance in countering hybrid threats, thereby enhancing decision superiority in contested battle spaces.[73]

The contribution extends current ADF MDCI doctrine by formalising three deltas: tactical embedding of CI practitioners for security-intelligence production and deception support; HQJOC-level standardisation of joint CI processes, irrespective of Service of origin; and routine integration of CI–PSYOPS planning. Historical doctrine is retained as scaffolding for practitioner roles, while present-day joint processes anchor the model in contemporary practice.

Institutional knowledge and legacy doctrine are other areas that deserve discussion. The ADF—especially the Army—retains extensive institutional knowledge of human-threat-based counterintelligence, supported by doctrinal artifacts such as the *Manual of Land Warfare 2-1-4: Counterintelligence* (1996). This historical foundation presents a unique opportunity to reconstitute the roles of ground-based CI practitioners, particularly those focused on security intelligence as a critical input to MDCI analysis. This would enable targeting a wider range of threats, including state and non-state actors, thereby fully operationalising the universal targeting axiom.

Restoring these roles would also facilitate integrating deception and the historical role of field security within operational formations, thereby contributing to effective CI operations. In doing so, CI would become more deeply embedded at the tactical level, enabling the detection, disruption, and deception of hostile actors before they can exploit vulnerabilities.

CI training and operational integration can also play a vital role. The ADF's current training programs reinforce MDCI principles, with CI Estimate methodology as a cornerstone of analytic practice.[74] A critical opportunity exists to embed CI practitioners within the tactical structure, such as the 1st Intelligence Battalion in the Army intelligence

[72] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Thousand Oaks, CA: CQ Press, 2017); UK Ministry of Defence, *Intelligence Doctrine* (London: MOD, 2022).
[73] Joint Chiefs of Staff, *Joint Publication 2-0: Joint Intelligence*, 2022 ed. (Washington, DC: Department of Defense, 2022); Frank Hoffman, *Hybrid Warfare and Challenges* (Arlington, VA: Potomac Institute, 2009).
[74] Department of Defence, Manual of Land Warfare, Volume 2: Intelligence, Pamphlet 1–Counterintelligence, 2-1-4 (Canberra: Commonwealth of Australia, 1996).

structure, replicable within RAAF and RAN. This move would enhance the delivery of CI support at the tactical level, allowing for a more direct integration of CI functions into operational planning and tactical execution.[75]

Building on the need for embedded CI capability at the tactical level, an additional consideration is integrating counterintelligence with complementary disciplines such as psychological operations to enhance the ADF's ability to counter hybrid threats.

Hybrid threats increasingly exploit cognitive and informational vulnerabilities, making it essential for CI and PSYOPS to coordinate efforts. While CI identifies and neutralises hostile intelligence activities, PSYOPS shapes perceptions and disrupts adversary cohesion. Formal liaison between CI practitioners and PSYOPS elements would enable mutual support: CI informing PSYOPS targeting based on threat assessments, and PSYOPS reinforcing CI objectives through influence and deception operations.

At the operational level, co-locating CI and PSYOPS planners would facilitate integrated planning, particularly during competition and crisis phases where shaping the environment is critical. Standardising CI–PSYOPS cooperation processes at the joint level would strengthen operational security and decision superiority. Integration must maintain clear role boundaries, ensuring that CI remains focused on threat neutralisation while supporting influence activities where appropriate. This coordination would enhance the ADF's capacity to pre-empt hybrid threats and protect operational cohesion across domains.

The following worked example demonstrates the indicator-to-function-to-effect pathway proposed in this section.

Worked Example

Divisional movement deception amid insider-enabled targeting. In the week before mobilisation, CI detects three converging indicators: unusual probing of movement tables through unit S4 accounts; targeted phishing against those duplicate accounts; and the rapid spread of a rumour claiming a pay system outage on closed

[75] Australian Defence College, *Joint Professional Military Education Handbook* (Canberra: ADC, 2022).

messaging channels. These are cross-vector signals—technical, human, and cognitive—of adversary intelligence-gathering and insider-enabled collection targeting divisional decision cycles.

The CI section combines indicators from the CI Estimate with network telemetry from defensive cyber measures and HUMINT from unit security inspections, producing an updated threat picture and a task-specific set of requirements for operations, fires, and PSYOPS. An embedded CI practitioner at a tactical HQ holds a planning meeting that sequences three lines of effort, potentially requiring operational support. First, defensive cyber uses counter-reconnaissance tactics with decoy data and beaconed honey artifacts linked to movement tables, enabling attribution while blocking accurate ISR.

Second, CI and PSYOPS coordinate corrective messaging to address the pay rumour at its source and inoculate key audiences, while maintaining ambiguity about actual movement times. Third, CI-PSYOPS drafts deception inputs for the scheme of manoeuvre and co-chairs legal review to ensure measures fall within command authority and do not trigger thresholds for compulsory powers. The ASIO liaison channel is notified when appropriate to prevent overlap and to route any investigative leads requiring statutory powers. The tactical commander receives a CI-led decision brief with options: maintain tempo with deception; adjust convoy schedules; or activate a broader deception operation if probes escalate. The commander approves the deception-based course of action. Follow-up battle damage assessment shows adversary ISR diverted to decoys, rumour propagation reversed in target areas, and attempted insider access disrupted. According to Prunckun's axioms, this approach preserves surprise, exploits all-source collection, and treats both state and non-state vectors as universal targets. In terms of CI functions, the process integrates analysis (CI Estimate refresh), collection (telemetry and HUMINT), operations (deception and neutralisation), and dissemination (decision brief and requirements) with PSYOPS integration.

Regarding commander effects, the outcome preserves surprise, disrupts ISR, decreases insider threats, and supports deception, all without new legislation and with ASIO deconfliction. This shows the integration of CI practitioners at the tactical level, coordination with PSYOPS and defensive cyber at the task level, and the viability of limited offensive CI—such as deception and neutralisation—under current authorities.

Such embedded capability aligns with Prunckun's emphasis on CI as an active, integrative function rather than a siloed security activity. It would enable real-time support for manoeuvre commanders and help maintain surprise, a decisive factor in modern hybrid warfare.[76]

Service-specific capabilities and joint integration cannot be overlooked. This institutional strength lies in developing service-specific CI capabilities tailored to the distinct operational needs of the Royal Australian Navy, the Royal Australian Air Force, and the Australian Regular Army.[77] While these capabilities are not yet completely harmonised, they offer a valuable starting point for creating a cohesive joint CI framework.

An important opportunity is the development of joint CI processes at the Headquarters Joint Operations Command (HQJOC) level. Such processes would benefit from Army's established expertise while ensuring CI planning and execution are coordinated across domains. Moreover, adopting a principles-based theoretical model—similar to those of strategic partners—would enhance long-term interoperability and doctrinal cohesion.[78] This harmonisation supports joint force commanders in hybrid environments where the speed and coherence of intelligence operations are critical to mission success.

Finally, there is a combined effect of national security and legal flexibility. ADF benefits from the statutory protection provided by the Australian Security Intelligence Organisation, which is legislatively empowered to counter threats to Australia's national defence system.[79] While the ADF does not currently possess its legislative authority for offensive CI activities, it can leverage command operational authorities—carefully deconflicted with statutory remit—to conduct operational CI within its mission space and

[76] Australian Army, LWD 2-0: Intelligence.
[77] Ofer Fridman, *Russian Hybrid Warfare: Resurgence and Politicisation* (London: Oxford University Press, 2018); James Renz and Thomas Smith, "The Evolving Role of Counterintelligence in Hybrid Warfare," *Journal of Strategic Studies* 42, 4 (2016): pp. 547–564.
[78] Mark M. Lowenthal, *Intelligence: From Secrets to Policy, 7th ed*. (Thousand Oaks, CA: CQ Press, 2017); U.K. Ministry of Defence, *Intelligence Doctrine* (London: MOD, 2022).
[79] Australian Government, Australian Security Intelligence Organisation Act 1979, Act No. 113 of 1979.

relevant limitations, whether domestically or overseas, to contend with an increased threat environment.[80]

This legal flexibility presents an opportunity to develop ADF-wide CI capabilities that complement ASIO's national mandate, particularly in expeditionary or deployed contexts. Such development would allow the ADF to extend its CI posture from the domestic sphere into operational theatres, creating a seamless continuum of protection against hybrid threats.

Conclusion

This study suggests, rather than mandates, an ADF counterintelligence posture for hybrid intelligence threats at the divisional level. Based on an S–O analysis rooted in Prunckun's axioms, we advance three design propositions: embedding CI practitioners at the tactical level will likely improve deception planning and ISR denial; HQJOC standardisation can leverage cross-Service differences for greater joint CI outcomes; and formal CI–PSYOPS integration can strengthen resilience against cognitive shaping. Each idea is subject to feasibility constraints—no new legislation assumed; liaison dependencies with the ASIO; staged training development—and should be tested through exercises and post-activity reviews before wider implementation.

The analysis indicates that the ADF already possesses a robust foundation, including a multi-disciplinary counterintelligence doctrine[81] and a J2-aligned intelligence structure[82].[83] Additionally, the Army retains extensive institutional knowledge in human-threat-based CI and field security, supported by historical doctrine that remains relevant in contemporary contexts. [84] These strengths present actionable opportunities to operationalise CI at lower command levels, primarily by embedding CI practitioners within divisional headquarters, expanding joint CI planning at HQJOC, [85] and

[80] Department of Defence, *ADF Command and Control Handbook* (Canberra: Commonwealth of Australia, 2021).
[81] Australian Defence Force, *ADF Publication 2.0: Intelligence, 2nd ed*. (Canberra: Defence Publishing Service, 2018).
[82] Defence Intelligence Organisation, *Defence Intelligence Doctrine* (Canberra: Commonwealth of Australia, 2021).
[83] Australian Defence College, *Joint Professional Military Education Handbook* (Canberra: ADC, 2022).
[84] Department of Defence, Manual of Land Warfare, Volume 2: Intelligence, Pamphlet 1–Counterintelligence, 2-1-4 (Canberra: Commonwealth of Australia, 1996).
[85] Department of Defence, *Defence Intelligence Enterprise Review* (Canberra: Commonwealth of Australia, 2019).

harmonising service-specific CI capabilities into an integrated Defence-wide framework.[86]

Critically, the study underscores the need to transition CI from a compartmentalised, primarily defensive function into an operationally embedded capability that supports real-time threat mitigation, deception planning, and multi-domain integration. Such a shift could enable the ADF to maintain operational surprise, harness all-source data collection, and extend CI efforts to both state and non-state adversaries—tenets of the theoretical framework guiding this research.

This paper offers a design rationale for reconceptualising CI as a core enabler of operational effectiveness in joint and hybrid warfare environments. By leveraging its existing strengths and seizing current opportunities for doctrinal and structural reform, the ADF can develop a more agile, integrated, and forward-leaning CI capability—one that is not only responsive to today's hybrid threats but also anticipatory of tomorrow's complex intelligence challenges. The vignette demonstrates the proposed indicator-to-function-to-effect sequence; the next step is to trial the pathway in exercises and post-activity reviews to confirm its feasibility under existing command authorities and liaison arrangements.

[86] See Prunckun, "A Grounded Theory of Counterintelligence," pp. 7–10.

Bibliography

Australian Army. *Land Warfare Doctrine LWD 2-0: Intelligence*. Canberra: Australian Army, 2021.

Australian Army Research Centre. *Future Army Professional Education Study*. Canberra: AARC, 2019.

Australian Cyber Security Centre (ACSC). *Threat Report 2023*. Canberra: Commonwealth of Australia, 2023.

Australian Defence College. *Joint Professional Military Education Handbook*. Canberra: ADC, 2021.

----------. *Joint Professional Military Education Handbook*. Canberra: ADC, 2022.

Australian Defence Force. *ADF Publication 2.0: Intelligence*. 2nd ed. Canberra: Defence Publishing Service, 2017.

----------. *ADF Publication 2.0: Intelligence*. 2nd ed. Canberra: Defence Publishing Service, 2018.

Australian Department of Defence. *Defence Strategic Update 2022*. Canberra: Commonwealth of Australia, 2022.

----------. *Future Joint Operating Concept 2035*. Canberra: Commonwealth of Australia, 2020.

Australian Department of Home Affairs. *Security and Intelligence Framework*. Canberra: Commonwealth of Australia, 2021.

Australian Government. *Australian Security Intelligence Organisation Act 1979*. Act No. 113 of 1979.

----------. *2020 Defence Strategic Update*. Canberra: Commonwealth of Australia, 2020.

Australian Security Intelligence Organisation (ASIO). *Annual Report 2022–2023*. Canberra: Commonwealth of Australia, 2023.

Australian Strategic Policy Institute (ASPI). *Countering Hybrid Threats*. Canberra: ASPI, 2023.

Betz, David, and Rory Cormac. *Defence Intelligence and the Cold War: Britain and the Bomb*. London: Edinburgh University Press, 2019.

Blaxland, John. *The Australian Army from Whitlam to Howard*. Melbourne: Cambridge University Press, 2016.

Buchanan, Ben. *The Hacker and the State*. Cambridge, MA: Harvard University Press, 2020.

Clarke, Amanda. "Counterintelligence in the Information Age." In *Contemporary Intelligence Studies: A Reader*, edited by Philip Davies and Kristian Gustafson, 213–227. London: Routledge, 2016.

Clarke, Richard A., and Robert K. Knake. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press, 2019.

Czosseck, Thomas, and Kenneth Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, 2011.

Davies, Andrew, and Edward Gustafson. *Joint Force Integration*. Canberra: ASPI, 2013.

Defence Intelligence Organisation. *Defence Intelligence Doctrine*. Canberra: Commonwealth of Australia, 2021.

Department of Defence. *ADF Command and Control Handbook*. Canberra: Commonwealth of Australia, 2021.

----------. *Defence Intelligence Enterprise Review*. Canberra: Commonwealth of Australia, 2019.

----------. *Manual of Land Warfare, Volume 2: Intelligence, Pamphlet 1 – Counterintelligence*. Canberra: Commonwealth of Australia, 1996.

Fridman, Ofer. *Russian Hybrid Warfare: Resurgence and Politicisation*. London: Oxford University Press, 2018.

George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005.

Hoffman, Frank. *Hybrid Warfare and Challenges*. Arlington, VA: Potomac Institute for Policy Studies, 2009.

Horner, David. *Australia's Military History for Dummies*. Milton: Wiley, 2017.

Joint Chiefs of Staff. *Joint Publication 2-0: Joint Intelligence*. Washington, DC: Department of Defense, 2020.

----------. *Joint Publication 2-0: Joint Intelligence*. 2022 ed. Washington, DC: Department of Defense, 2022.

Jennings, Peter, and Malcolm Davis. "ADF's Role in National Intelligence." *ASPI Strategist*, 2022.

Kiras, James. *Special Operations and Strategy: From World War II to the War on Terrorism*. 2nd ed. London: Routledge, 2020.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 7th ed. Thousand Oaks, CA: CQ Press, 2017.

----------. *Intelligence: From Secrets to Policy*. 8th ed. Thousand Oaks, CA: CQ Press, 2020.

NATO. *Comprehensive Concept for Hybrid Warfare*. Brussels: NATO, 2021.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Hybrid Conflict Handbook*. Tallinn: NATO CCDCOE, 2020.

Palazzo, Albert. *The Australian Army: A History of Its Organization, 1901–2001*. Melbourne: Oxford University Press, 2011.

Prunckun, Hank. "A Grounded Theory of Counterintelligence." *American Intelligence Journal* 29, no. 2 (2011): pp. 6–15.

----------. *Counterintelligence Theory and Practice*. Lanham, MD: Rowman & Littlefield, 2019.

Puyt, Pieter, et al. "The SWOT Analysis: A Tool for Security Strategy Evaluation." *Journal of Strategic Security* 13, 2 (2020): pp. 68–80.

Renz, James, and Thomas Smith. "The Evolving Role of Counterintelligence in Hybrid Warfare." *Journal of Strategic Studies* 42, 4 (2016): pp. 547–564.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.

UK Ministry of Defence. *Intelligence Doctrine*. London: MOD, 2022.

----------. *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations*. 3rd ed. Shrivenham: Defence Academy of the UK, 2018.

U.S. Army. *Army Techniques Publication (ATP) 2-22.2: Counterintelligence*. Washington, DC: Department of the Army, 2020.

Warner, Michael. *The Rise and Fall of Intelligence: An International Security History*. Washington, DC: Georgetown University Press, 2009.

White, Hugh. *How to Defend Australia*. Carlton: La Trobe University Press, 2019.