

Technology & Innovation

Artificial Intelligence and Machine Learning for Mission Assurance in Cyber-Contested Air and Space Operations

Manish Khaware¹ 

¹ Australian Defence Force

Keywords: Cyber Resilience, Air and Space Operations, Artificial Intelligence, Machine Learning

<https://doi.org/10.58930/bp55099098>

Vol. 4, Issue 1, 2026

Networked air and space operations depend on continuous digital connectivity, creating acute vulnerability to cyber and electromagnetic disruption. Advanced air forces increasingly rely on integrated command-and-control, space-enabled communications and distributed sensor–shooter networks, making cyber resilience a prerequisite for mission success. Artificial intelligence (AI) and machine learning (ML) offer capabilities to enhance mission assurance through rapid threat detection, adaptive network management and continuous operational risk assessment. This paper examines how AI/ML can strengthen mission assurance in cyber-contested air and space operations. It first clarifies AI/ML in an applied military context and analyses key challenges related to data integrity, network latency, access control and mission continuity. It then proposes a generic AI-enabled mission assurance reference architecture comprising dynamic risk scoring, continuous authorisation based on Zero Trust principles, intelligent cyber defence, electromagnetic spectrum (EMS) resilience and adaptive network prioritisation. Finally, the paper discusses implications for force design, doctrine, workforce development and international interoperability. The framework is intended to be transferable across advanced air forces operating networked integrated air and missile defence and joint all-domain command-and-control architectures.

1. Introduction

Contemporary air and space power is inseparable from digital networks and data-driven decision systems, making cyber resilience a core determinant of operational effectiveness (Barlet, 2025; Snyder et al., 2021). Modern combat aircraft, space systems and ground-based command-and-control (C2) nodes are interconnected through complex digital infrastructures that enable sensor fusion, distributed targeting and coordinated effects across domains. While this connectivity enhances operational reach and tempo, it also expands the attack surface available to adversaries seeking to degrade missions through cyber and electromagnetic means (United States Air Force, 2021; United States Department of Defense [US DoD], 2023).

Advanced militaries are increasingly pursuing joint, networked battle management architectures that integrate air, missile defence, space, cyber and maritime operations into unified digital ecosystems, such as the Joint All-Domain Command and Control (JADC2) (United States Department of Defense [US DoD], 2022a). These architectures are designed to accelerate decision cycles and enable distributed operations across contested environments. However, their dependence on continuous data exchange introduces systemic vulnerabilities: disruptions to data flows, corruption of sensor inputs or compromise of authentication mechanisms can have cascading mission effects (Schneider, 2020).

Cyber mission assurance therefore extends beyond traditional information security concerns and focuses on pre-

serving operational outcomes despite cyber disruption (Snyder et al., 2021). The objective is not merely to prevent intrusions but to ensure that essential mission functions continue under attack, including in degraded modes. Achieving this requires adaptive, intelligent defensive mechanisms capable of responding at machine speed, which increasingly motivates the integration of artificial intelligence (AI) and machine learning (ML) into cyber defence and network management functions (Rassler, 2019).

This paper argues that AI/ML technologies can enable a shift from static cyber protection towards dynamic mission assurance in networked air and space operations. It proposes a reference architecture designed to maintain operational continuity under cyber-contested conditions. The framework is intentionally generic and intended for applicability across advanced air forces operating integrated, networked combat systems, rather than prescribing solutions for specific national programs.

2. AI and ML in the military cyber context

Public discourse often conflates AI with general-purpose or generative systems, yet most military applications employ narrow/task-specific AI designed to support bounded operational functions (Kainikara, 2019). In defence contexts, AI typically refers to computational systems capable of pattern recognition, classification, optimisation and automated decision support within constrained environments (US DoD, 2022a). These systems augment, rather than re-

place, human decision makers by operating at scales and speeds beyond human cognitive capacity.

ML represents a subset of AI methods that enable systems to improve performance through data-driven adaptation (Rassler, 2019). In cyber and network operations, ML techniques commonly support anomaly detection, behaviour profiling, predictive analytics and adaptive routing (Schneider, 2020). Supervised learning models can identify known threat patterns, while unsupervised models detect deviations from established baselines, making them valuable for identifying novel or stealthy cyber intrusions (Barlet, 2025).

Importantly, most operationally relevant AI systems today do not possess autonomous intent or broad reasoning capabilities. Instead, they operate as decision-support tools embedded within sensors, networks and command systems, executing pre-defined policies and constraints (US DoD, 2022a). This distinction is critical for mission assurance applications, where human oversight and command authority remain essential, even as automation accelerates detection and response cycles.

The reference architecture proposed in this paper assumes near-term AI maturity levels and focuses on evolutionary integration of ML-driven analytics and automation into existing C2 and cyber defence infrastructures. It does not rely on speculative assumptions about artificial general intelligence or fully autonomous command systems, aligning instead with realistic operational and governance constraints (Rassler, 2019).

2.1. Cyber dependence of networked air and space operations

Networked air and space operations rely on continuous digital connectivity across platforms, domains and coalition partners, making cyber resilience foundational to operational effectiveness (Snyder et al., 2021). Modern combat aircraft function as network nodes that collect, process and disseminate sensor data, while space systems provide global communications, navigation and intelligence services that underpin joint operations (United States Air Force, 2021). Disruption to any layer of this digital ecosystem can rapidly degrade mission performance.

Integrated air and missile defence (IAMD) systems further increase cyber dependence by linking disparate sensors and shooters into unified engagement networks (Snyder et al., 2021). These architectures require precise timing, high-integrity data and reliable authentication mechanisms to enable coordinated defensive and offensive actions. As system integration increases, failures propagate more readily across interconnected subsystems, amplifying operational risk (Schneider, 2020).

Coalition interoperability introduces additional complexity, as data must traverse heterogeneous networks governed by differing security policies and technical standards (NATO Allied Command Transformation, 2024). While interoperability enhances collective defence, it also expands trust relationships and increases exposure to supply chain vulnerabilities, insider threats and misconfigurations that adversaries may exploit (United States Air Force, 2021).

As militaries adopt cloud computing, software-defined networking and virtualised mission systems, cyber resilience becomes inseparable from overall force survivability (Barlet, 2025). Traditional perimeter-based security models are insufficient for protecting dynamic, distributed architectures, necessitating adaptive, continuously monitored security postures that align directly with mission priorities (Schneider, 2020).

2.2. Mission assurance challenges in cyber-contested operations

Data integrity and trust. Operational decision making depends on trustworthy sensor and intelligence data, making data integrity a central mission assurance concern (Snyder et al., 2021). Adversarial manipulation of sensor feeds, navigation signals or logistics databases can degrade situational awareness without triggering obvious system failures. AI systems are particularly sensitive to data poisoning and adversarial input manipulation, which may degrade performance in subtle ways that are difficult to detect through conventional monitoring (Rassler, 2019).

Loss of confidence in data undermines operational tempo and can force reversion to slower, manual processes, negating the advantages of networked warfare. Maintaining continuous validation of data provenance and behavioural consistency is therefore critical to sustaining trust in automated decision-support systems.

Network latency and denial of service. Many air and space missions require low-latency communications to support remote sensing, autonomous systems and dynamic targeting (United States Air Force, 2021). Cyber attacks that increase latency or disrupt bandwidth can render time-sensitive missions ineffective even without complete network outages. In high-tempo operations, delays of seconds may be operationally significant.

Cyber and electromagnetic interference often co-occur, with jamming and malware targeting communications simultaneously (NATO, 2022). Ensuring resilient connectivity therefore requires integrated management of both digital networks and spectrum resources, rather than treating them as separate operational domains.

Access control and lateral movement. Complex operational networks involve thousands of users, devices and automated services, creating challenges for enforcing least-privilege access (Schneider, 2020). Credential compromise or insider threats can enable lateral movement across interconnected systems, allowing localised breaches to escalate into enterprise-wide mission disruption (United States Air Force, 2021).

Traditional static access controls are poorly suited to dynamic operational contexts, where users may shift roles rapidly and systems must integrate coalition partners and deployed platforms (NATO Allied Command Transformation, 2024). Continuous behavioural verification becomes necessary to detect compromised credentials and anomalous activity in real time.

Mission continuity under degradation. Mission assurance requires not only preventing cyber compromise but sustaining operational capability despite partial system

failures (Snyder et al., 2021). Adversaries may pursue persistent, low-level disruptions designed to degrade performance rather than trigger overt outages. Forces must therefore be able to prioritise essential functions, degrade gracefully and recover rapidly from cyber incidents (Schneider, 2020).

Future adversaries may deploy AI-enabled malware capable of adapting to defensive measures, increasing the speed and complexity of cyber engagements (Rassler, 2019). Human-only response models may be insufficient to counter machine-speed attacks, necessitating automated defensive mechanisms integrated with mission command structures.

3. Related work and doctrinal context

Cyber mission assurance and AI in military operations cyber mission assurance has emerged as a distinct research domain concerned with preserving operational outcomes under sustained cyber pressure rather than solely preventing network intrusions (Snyder et al., 2021). Prior studies emphasise that complex weapon systems should be treated as socio-technical enterprises in which human operators, digital infrastructure and physical platforms are inseparably linked (Schneider, 2020). Within such systems, failure modes may propagate non-linearly, meaning that small cyber disruptions can generate disproportionate operational effects.

Research on joint all-domain operations highlights that decision advantage increasingly depends on resilient information flows across distributed nodes (US DoD, 2022a). When command structures rely on continuous digital connectivity, adversaries may target data integrity, timing and authentication rather than attempting complete denial of service. This aligns with observations from conflict simulations indicating that persistent low-level cyber interference can degrade operational tempo more effectively than overt network outages (United States Air Force, 2021).

AI-enabled cyber defence has attracted growing attention due to the volume and velocity of telemetry generated by modern networks (Barlet, 2025). Machine-learning models can process network flows, endpoint behaviour and access logs at scale, enabling detection of subtle deviations that may escape human analysts (Rassler, 2019). However, scholars caution that overreliance on automation introduces new risks, including model brittleness, false positives and adversarial exploitation of learning systems (US DoD, 2021). Effective mission assurance therefore requires hybrid human-machine approaches rather than fully autonomous defensive systems.

Studies of electromagnetic spectrum operations further underscore the convergence of cyber and electronic warfare (NATO Allied Command Transformation, 2024). Adaptive jamming, spoofing and spectrum denial techniques increasingly target both digital protocols and physical waveforms, requiring integrated defensive strategies that address cyber and EMS resilience simultaneously. AI-enabled cognitive radios and adaptive signal processing have been proposed as mechanisms to enhance survivability in con-

tested spectrum environments, though operational validation remains limited.

Collectively, this literature suggests that cyber resilience in air and space operations must be treated as a multi-layered systems problem rather than a discrete technical function. The reference architecture proposed in this paper synthesises these insights by aligning AI-enabled cyber defence mechanisms directly with mission-level priorities and operational command structures.

The reference architecture presented in this paper was developed using a systems engineering approach that integrates doctrinal analysis, operational workflow mapping and cyber threat modelling. Rather than deriving requirements from specific platforms or acquisition programs, the methodology focuses on generic operational functions common to networked air and space enterprises, including sensing, command and control, data distribution and engagement coordination.

First, operational workflows were decomposed into mission-critical information dependencies, identifying data flows whose disruption would generate disproportionate mission impact (Snyder et al., 2021). These dependencies informed prioritisation logic within the architecture, ensuring that resilience mechanisms align with operational objectives rather than purely technical metrics.

Second, cyber threat vectors were mapped against each workflow component, incorporating both traditional network-based attacks and spectrum-based interference (United States Air Force, 2021). This enabled identification of cross-domain vulnerabilities where cyber and electronic warfare effects may compound one another.

Third, candidate AI/ML techniques were evaluated for suitability based on explainability, training data requirements and operational deployment constraints (US DoD, 2022b). Preference was given to methods that support continuous learning from operational telemetry while maintaining transparency for human oversight.

Finally, architectural components were integrated into layered defensive functions corresponding to prevention, detection, response and recovery phases of cyber incidents. This lifecycle perspective ensures that mission assurance is maintained not only during attack onset but throughout prolonged periods of contested operations.

4. Operational scenarios and mission-level application

To illustrate how the proposed architecture supports mission assurance, consider a generic integrated air defence scenario involving distributed sensors, airborne interceptors and joint command nodes. During routine operations, AI-driven risk scoring identifies elevated threat activity on external data links, prompting pre-emptive routing of sensor data through alternative communication paths while increasing authentication thresholds for external interfaces.

If adversarial cyber activity escalates to active interference, intelligent cyber defence agents detect anomalous traffic patterns indicative of attempted data manipulation. Affected network segments are isolated while validated

sensor feeds are prioritised for interceptor tasking. Simultaneously, EMS resilience mechanisms adjust communication waveforms to mitigate jamming, preserving low-latency control channels.

In a separate space-enabled ISR scenario, spectrum congestion and cyber intrusion attempts degrade satellite downlink performance. Adaptive network prioritisation restricts non-essential data transmissions, ensuring that time-sensitive targeting information continues to reach command nodes. Human operators retain authority over engagement decisions, but AI-enabled systems manage network and security adaptations at machine speed.

These scenarios illustrate how mission assurance emerges from coordinated defensive actions across cyber, network and spectrum domains rather than isolated security controls. The architecture therefore supports operational continuity even when adversaries employ multi-vector disruption strategies.

5. AI limitations, assurance and human oversight

Despite their advantages, AI systems introduce new operational and governance challenges that must be addressed through rigorous assurance processes (US DoD, 2022b). Machine-learning models are sensitive to training data quality and may exhibit degraded performance when operating outside previously observed conditions. In contested environments, adversaries may deliberately manipulate inputs to induce misclassification or overwhelm anomaly detection thresholds (Rassler, 2019).

To mitigate these risks, the reference architecture incorporates confidence scoring and human-in-the-loop validation for high-consequence decisions. Automated responses are constrained by predefined policy boundaries, ensuring that escalation remains subject to command authority. Continuous model retraining using operational data supports adaptation to evolving threat patterns while preserving traceability of decision logic.

Model verification and validation processes should be integrated into operational readiness cycles, analogous to aircraft certification regimes. Red-teaming, adversarial testing and simulation-based stress testing are essential to identify failure modes prior to deployment (Barlet, 2025). Without such governance mechanisms, AI-enabled cyber defence may introduce operational fragility rather than resilience.

Ethical considerations also arise when automated systems influence operational outcomes. Transparency, accountability and compliance with legal frameworks must be maintained even when defensive actions are executed autonomously at machine speed. These requirements reinforce the need for hybrid human-machine command structures rather than fully autonomous cyber defence.

Military cyber doctrine increasingly recognises mission assurance as distinct from information security compliance (United States Air Force, 2021). Rather than focusing solely on preventing intrusions, cyber resilience strategies emphasise continuity of essential functions under attack, aligning cyber defence with operational outcomes (Snyder et al., 2021).

NATO's Federated Mission Networking (FMN) doctrine highlights the need for resilient digital interoperability across coalition forces, including dynamic reconfiguration of networks under contested conditions (NATO Allied Command Transformation, 2024). FMN—established in 2015—has continued to mature through spiral specifications that codify policy-aware interoperability and rapid reconfiguration for contested operations (Federated Mission Networking (FMN), 2022, 2023; NATO Allied Command Transformation, 2020). Similarly, US JADC2 concepts stress survivable connectivity and distributed command architectures to maintain operational effectiveness despite adversarial disruption (US DoD, 2022a).

Academic research on 'hyperwar' and algorithmic warfare suggests that future conflicts will increasingly feature automated decision loops operating at machine speed, amplifying the importance of resilient data and communications infrastructures (Allen & Husain, 2017; Euhus, 2018; United States Department of Defense [US DoD], 2022a). Without resilient cyber foundations, accelerated operational tempo may magnify vulnerabilities rather than confer advantage.

Emerging work on adversarial AI highlights risks associated with deploying ML systems in contested environments, including model exploitation and data manipulation (Rassler, 2019). This reinforces the need for defence-in-depth approaches that combine AI-driven detection with robust governance, testing and fallback procedures (US DoD, 2022a).

6. Proposed AI-enabled mission assurance reference architecture

This paper proposes a five-layer AI-enabled mission assurance architecture designed to preserve operational outcomes under cyber-contested conditions. The framework is applicable to networked air and space forces operating in integrated C2, IAMD and space-enabled ISR systems.

AI-driven mission risk scoring. ML models aggregate cyber threat intelligence, network telemetry, system vulnerabilities and mission dependencies to generate continuous mission risk assessments (Snyder et al., 2021). These risk scores inform commanders of potential cyber impacts on operational objectives and trigger automated mitigations when thresholds are exceeded. Predictive modelling enables identification of single points of failure prior to mission execution, supporting proactive resilience measures such as redundancy activation and route diversification (Schneider, 2020).

Zero Trust architectures enforce continuous verification of users, devices and services based on behavioural and contextual analysis rather than static credentials (United States Department of Defense [US DoD], 2022a; US Department of Defense Chief Information Officer, 2024). ML-based behaviour analytics detect deviations indicative of compromise, enabling rapid containment of intrusions and preventing lateral movement across mission systems (Barlet, 2025). Micro-segmentation combined with adaptive policy enforcement helps localise breaches and preserve mission functions even when peripheral systems are com-

promised (National Institute of Standards and Technology, 2023a, 2023b, 2025).

ML-enabled intrusion detection systems analyse network flows and system logs to identify both known threats and novel anomalies (Rassler, 2019). Automated response mechanisms can isolate affected segments, reconfigure network routes and deploy deception techniques to contain adversaries at machine speed. Human oversight remains essential for high-consequence actions, but automation accelerates detection and initial containment, buying critical time for commanders and cyber operators (US DoD, 2022b).

Electromagnetic spectrum resilience. AI-enabled cognitive radios and adaptive signal processing support dynamic spectrum management under jamming and interference (NATO Allied Command Transformation, 2024). ML algorithms can identify interference patterns and optimise frequency selection, power allocation and waveform adaptation in real time. Integrating EMS awareness with cyber defence enhances situational awareness across digital and physical layers of communication infrastructure, supporting resilient connectivity in contested environments (United States Air Force, 2021).

Network prioritisation and graceful degradation. AI-driven traffic management dynamically allocates bandwidth to mission-critical data flows during congestion or attack (Snyder et al., 2021). Quality-of-service policies aligned with the commander's intent ensure essential functions retain connectivity when resources are constrained. Graceful degradation strategies allow systems to continue operating in reduced capability modes, preserving operational coherence even when full functionality cannot be maintained (Schneider, 2020).

6.1. Operational and force design implications

Implementing AI-enabled mission assurance architectures requires integration with broader force modernisation efforts and C2 system development (US DoD, 2022a). Cyber resilience must be embedded into system design rather than added as an afterthought, ensuring interoperability between cyber defence, network management and operational command functions.

Workforce development is equally critical, as AI-enabled cyber defence demands expertise in data science, software engineering and operational cyber analysis (Barlet, 2025). Training programs must integrate cyber resilience into operational exercises to build trust in automated support systems under realistic conditions (Snyder et al., 2021).

Doctrinal evolution is required to integrate cyber mission assurance into operational planning processes, including explicit consideration of cyber risk during mission design and execution (NATO, 2022). Decentralised command models may be necessary to sustain operations when connectivity is degraded, supported by autonomous local decision aids.

6.2. Policy, governance and ethical considerations

AI-enabled cyber defence raises governance challenges related to automation authority, accountability and escalation control (US DoD, 2022a). Clear policies must define thresholds for autonomous defensive actions and ensure human oversight of responses with strategic implications.

Model assurance, testing and validation processes are essential to mitigate risks of false positives and adversarial exploitation (Rassler, 2019). Continuous red-teaming and adversarial testing support resilience of AI systems deployed in contested environments. See also the Australian Signals Directorate's Information Security Manual for baseline controls (Australian Signals Directorate, 2026).

International collaboration on standards and threat intelligence sharing enhances collective resilience, particularly in coalition operations where interoperability is operationally essential (NATO Allied Command Transformation, 2024).

6.3. Implications for defence policy and capability acquisition

Embedding cyber mission assurance into future force design requires shifts in defence policy and acquisition practice. Traditional procurement models often treat cyber security as a compliance requirement addressed late in the development cycle, whereas mission assurance demands that resilience be engineered into system architectures from inception (United States Air Force, 2021). Capability development processes should therefore incorporate operational cyber resilience requirements alongside performance, safety and reliability criteria.

Contracting frameworks must also evolve to support continuous software updates, model retraining and adaptive security configurations over system lifecycles. Static accreditation approaches are poorly aligned with AI-enabled systems that evolve in response to changing threat environments (US DoD, 2022b). Instead, risk-based continuous authorisation models are required to enable rapid deployment of defensive improvements without introducing unacceptable operational delays.

From an investment perspective, cyber mission assurance should be prioritised as an operational capability rather than an overhead cost. Funding lines dedicated to resilience analytics, spectrum management and AI assurance tooling may yield disproportionate operational benefits by preserving the effectiveness of existing platforms under contested conditions. This reframing is essential for sustaining capability relevance in high-intensity conflict scenarios.

6.4. Coalition operations and interoperability

Future air and space operations are likely to be conducted in coalition environments where networks must interconnect across national boundaries and security domains (NATO Allied Command Transformation, 2024). While coalition integration enhances collective situational

awareness and force projection, it also introduces governance, trust and technical interoperability challenges that complicate cyber mission assurance.

Differences in national security policies, data handling standards and cyber response authorities may constrain implementation of fully integrated AI-enabled defence mechanisms. For example, automated containment actions may be permissible within national networks but restricted when operating across coalition links. Mission assurance architectures must therefore support policy-aware segmentation and graduated trust models that adapt security controls based on partner agreements and operational context.

Shared situational awareness regarding cyber and EMS threats is equally critical. Federated data-sharing frameworks and common operational pictures for cyber and spectrum environments can improve collective responsiveness while respecting national sovereignty. AI-enabled fusion of threat intelligence across partners may enhance early warning and coordinated defence, but such approaches require robust governance structures and transparent data stewardship mechanisms.

Technological solutions alone are insufficient to deliver effective cyber mission assurance. Organisations must develop workforces capable of operating, supervising and continuously improving AI-enabled defence systems (Bartlett, 2025). This requires integration of cyber, data science and operational expertise rather than maintaining these functions in isolated professional communities.

Training programs should expose operational personnel to cyber-contested scenarios in realistic exercises, fostering understanding of how network degradation affects mission execution and how automated resilience mechanisms can support decision making (Snyder et al., 2021). Conversely, cyber specialists must understand operational priorities to ensure defensive actions align with mission objectives rather than purely technical metrics.

Organisational structures may also require adaptation to enable rapid coordination between operations centres, network management teams and cyber defence units. Flattened communication pathways and shared situational awareness tools can reduce response latency during cyber incidents, improving overall mission assurance. Leadership development programs should emphasise systems thinking and cross-domain integration to prepare future commanders for managing digitally dependent forces.

7. Conclusion and recommendations

As air and space operations become increasingly dependent on digital networks and automated decision systems, cyber resilience is no longer a supporting function but a core determinant of mission success. Adversaries are expected to pursue persistent, multi-layered cyber and electromagnetic campaigns designed to degrade operational effectiveness rather than simply disrupt individual systems. In this environment, mission assurance requires adaptive, intelligence-enabled mechanisms that preserve essential functions even under sustained attack.

This paper has presented a transferable reference architecture for AI-enabled cyber mission assurance in networked air and space operations. By integrating continuous risk scoring, Zero Trust-based authorisation, intelligent cyber defence, electromagnetic spectrum resilience and adaptive network prioritisation, the framework supports operational continuity across integrated command-and-control and air defence networks. Rather than replacing human command authority, the architecture augments decision making by automating detection, triage and response functions at machine speed, enabling commanders to retain control while operating in compressed decision cycles.

To operationalise this approach, defence organisations should embed cyber resilience requirements into system design and acquisition processes, invest in AI-literate cyber and operational workforces, and integrate cyber-contested scenarios into routine operational training and exercises. Clear governance frameworks are also required to define appropriate levels of autonomous defensive action and to ensure accountability in AI-enabled cyber operations. Finally, international collaboration on standards, interoperability and threat intelligence will remain essential, as future air and space operations are likely to be conducted in coalition contexts. With deliberate investment and institutional adaptation, AI-enabled cyber mission assurance can become a foundational enabler of credible, resilient air and space power in future high-intensity conflicts.

.....

The views expressed in this article are the author's own and do not represent the view of the Department of Defence.

Submitted: November 18, 2025 AEST. Accepted: January 13, 2026 AEST. Published: August 11, 2026 AEST.



This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CCBY-4.0). View this license's legal deed at <http://creativecommons.org/licenses/by/4.0> and legal code at <http://creativecommons.org/licenses/by/4.0/legalcode> for more information.

References

- Allen, J. R., & Husain, A. (2017). On Hyperwar. *Proceedings*, 143(7). <https://www.usni.org/magazines/proceedings/2017/july/hyperwar>
- Australian Signals Directorate. (2026). *Information Security Manual*. Australian Government. <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism>
- Barlet, G. (2025). Advances in Artificial Intelligence Require New Level of Cyber Security. *Defense Opinion*.
- Euhus, B. T. (2018). A Clausewitzian Response to “Hyperwarfare.” *Parameters*, 48(2). <https://doi.org/10.55540/0031-1723.2767>
- Federated Mission Networking (FMN). (2022). *FMN Spiral 5: Overview of Standards and Profiles (Supplement to the Final FMN Spiral 5 Specification)*. NATO Interoperability Standards and Profiles (NISP). https://storage.nisp.nw3.dk/20221202_FM_N_Spiral_5_Standards_Profile.pdf
- Federated Mission Networking (FMN). (2023, October 16). *FMN Spiral 5 Specification*. NATO Interoperability Standards and Profiles (NISP). https://nisp.nw3.dk/fmn_spiral_5_specification-20231016.html
- Kainikara, S. (2019). *Artificial Intelligence and the Future of Air Power*. Air Power Development Centre. <https://airpower.airforce.gov.au/publications/algorithmic-warfare-applying-artificial-intelligence-warfighting>
- National Institute of Standards and Technology. (2023a). *NIST Special Publication 800-82 Revision 3: Guide to Operational Technology (OT) Security*. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>
- National Institute of Standards and Technology. (2023b). *NIST Special Publication 1800-35 (Parts A–D): Implementing a Zero Trust Architecture*. National Institute of Standards and Technology.
- National Institute of Standards and Technology. (2025). *NIST Special Publication 1800-35: Implementing a Zero Trust Architecture*. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-35.pdf>
- NATO Allied Command Transformation. (2020). *FMN Spiral Compliance for NRF (Spirals 4–6) (RFI-ACT-SACT-20-45, Annex A-1)*. North Atlantic Treaty Organisation Headquarters Supreme Allied Commander Transformation. <https://www.act.nato.int/wp-content/uploads/2023/05/rfi020045.pdf>
- NATO Allied Command Transformation. (2024, June). *Federated Mission Networking (Trifold)*. <https://www.act.nato.int/wp-content/uploads/2024/06/Federated-Mission-Networking-Trifold.pdf>
- North Atlantic Treaty Organization [NATO]. (2022). *Federated Mission Networking*. NATO Communications and Information Agency. <https://www.act.nato.int/activities/federated-mission-networking/>
- Rassler, D. (2019). Adversarial AI and the future of conflict. *Modern War Institute at West Point*.
- Schneider, J. (2020). Resilient by design: Cyber mission assurance in modern warfare. *Journal of Information Warfare*, 19(2), 1–15.
- Snyder, D., Mayer, L. A., Brosmer, J. L., Bodine-Baron, E., Hodgson, Q. E., Hura, M., Fujiwara, J., & Hamilton, T. (2021). *Wing-Level Mission Assurance for a Cyber-Contested Environment*. RAND. https://www.rand.org/pubs/research_reports/RRA580-1.html
- United States Air Force. (2021). *Cyber Resiliency Office for Weapon Systems: Systems Security Engineering Cyber Guidebook Version 4.0*. <https://apps.dtic.mil/sti/citations/AD1173807>
- United States Department of Defense [US DoD]. (2021). *U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway*. Department of Defense.
- United States Department of Defense [US DoD]. (2022a). *DoD Zero Trust Strategy*. US Department of Defense Chief Information Officer. <https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>
- United States Department of Defense [US DoD]. (2022b). *Summary of the Joint All-Domain Command and Control (JADC2) Strategy*. <https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF>
- United States Department of Defense [US DoD]. (2023). *Summary of the 2023 Department of Defense Cyber Strategy*. U.S. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf
- US Department of Defense Chief Information Officer. (2024). *DoD Zero Trust Capability Execution Roadmap (v1.1)*.