
© hamara – stock.adobe.com

Faster Than the Threat

AI-Enabled Decision Advantage for NATO Integrated Air and Missile Defence

By Lieutenant Colonel Sebastian Kurzepa, POL Air Force, JAPCC

It begins subtly, much like any other day on duty. Sensor networks deployed along NATO's Eastern Flank start registering small deviations from expected patterns. At the same time, satellite imagery reveals launchers for advanced missile systems relocating away from their permanent garrisons. Open-source intelligence reports unusual convoy activity towards less significant areas, accompanied by a rise in encrypted, command-level communications between key adversary nodes.

Considered in isolation, none of these indicators are necessarily decisive. Analysts and operators have encountered similar signals before, and over time they can grow desensitised to such minor deviations. Currently, Integrated Air and Missile Defence (IAMD) operators must manually classify the threat, estimate the manoeuvring trajectory, identify assets at risk and coordinate effectors. These steps can limit the pace at which the overall system can respond, particularly when the recognised air picture (RAP) is highly saturated by both friendly and threat tracks from high-volume assets such as unmanned aerial systems (UAS).

An AI-supported IAMD architecture changes this dynamic by fusing multi-domain sensor inputs at machine speed, identifying the weapon class, calculating

Large-scale UAS attacks compress decision timelines and challenge traditional air defence architectures.

the path a threat is likely to follow, and ranking the available defensive responses. Commanders must retain decision authority while AI compresses the Sense, Make Sense, Act cycle from minutes to seconds by automating multi-sensor correlation, pre-classifying threat types and generating ranked courses of action (COAs) prior to human decision.

This article argues that NATO must accelerate the responsible integration of artificial intelligence/machine learning (AI/ML) into IAMD, as traditional architectures are no longer sufficient for modern, multi-vector, high-speed attack environments.

Compressed Timelines: NATO IAMD Challenges

Isolated indicators only become significant in combination. On its own, a sensor anomaly, a vehicle movement or a rise in message traffic means little. Correlated at scale, the same indicators may reveal pre-launch preparations for hypersonic systems, low-observable missiles or UAS swarms. Such correlation, increasingly dependent on advanced data-processing methods, remains difficult to achieve when it relies entirely on human-centric processes. Multiple factors add to the difficulty of detecting, predicting and responding to complex threats quickly:

Advanced hypersonic threats: Hypersonic glide vehicles (HGVs) and hypersonic cruise missiles combine high speed with manoeuvrability, complicating prediction and cueing.

Outpaced traditional kill chains: The war in Ukraine demonstrates that the use of AI is compressing decision-making cycles and increasing both the speed and complexity of battlefield operations, posing a significant challenge to traditional, human-centric air and missile defence architectures.[1]

UAS saturation and low-observable cruise missiles: Ukraine has also demonstrated how large UAS swarms can overwhelm surveillance and classification systems, reducing to mere seconds the available time for an operator to react.[2]

Fragmented multinational sensor networks: NATO relies on national systems of varying age, capability, and interoperability levels. While the Alliance aims to build a unified, 360-degree operational picture, differing data formats, classification rules and system architectures slow cross-domain fusion. This reflects longstanding capability development challenges, documented in broader European IAMD assessments.[3]

Insufficient real-time decision agility: Traditional command and control (C2) architectures were not designed for ambiguous, rapidly evolving threat environments, which require near-instantaneous assessment. The increasing density and complexity of airspace further degrade the cognitive ability of humans to distinguish between decoys, hostile platforms, Allied assets and

© 2022 VLADJ55/Shutterstock.

AI-enabled sensor fusion can transform fragmented observations into a coherent operational picture, supporting faster decision-making.

civilian traffic. Compounding this, contested electromagnetic environments mean IAMD cannot assume continuous connectivity to a central node, forcing critical processing toward the tactical edge.

While NATO recognises these challenges and acknowledges the need for deeper technological integration and improved resilience, as the NATO IAMD Policy reflects, progress has not kept pace with the threat environment.[4] IAMD remains effective for now, but sustained investment in innovation is needed to ensure long-term credibility, particularly in emerging and disruptive technologies such as AI/ML.

Potential Applications of AI/ML

Each AI/ML application that follows reduces a different kind of uncertainty. Sensor and data fusion establishes what has been detected; trajectory prediction narrows where it is going. Historical trend analysis then widens the frame, indicating when particular threat types tend to appear, while intent modelling infers what a detected object is likely to do next.

Sensor and Data Fusion for Threat Detection and Classification

Threat detection relies on radar systems supported by infrared detectors, satellites, signals intelligence (SIGINT), airborne early warning (AEW) platforms, cyber intelligence data and open-source information. This has historically required manually processing, fusing and analysing large quantities of data. AI/ML algorithms can collate this data across varying formats from disparate sources in real time, integrating radar and other multi-sensor inputs into a single analytical process.[5] The resulting datasets can then be compared against historical baselines, providing operators with more holistic and probabilistic threat assessments. This is particularly useful for detecting targets with low radar cross sections (RCS), such as small drones or cruise missiles, as their radar signatures appear sporadically or are inconclusive without further corroboration and analysis.

A relevant example is Ukraine's capability to detect UAS using an extensive network of acoustic sensors.[6] AI/ML-enabled fusion could integrate this acoustic data with radar and SIGINT inputs at scale, particularly under overwhelming saturation where manual rule-based correlation becomes infeasible. In such settings, AI/ML can merge dispersed and inconsistent signals, difficult for human operators to correlate, into a coherent IAMD Common Operational Picture (COP) to generate warnings significantly faster than today's systems.

Trajectory Prediction

Prediction algorithms can be used to reduce uncertainty about an object's future position. This is critical in

USS Hopper launches a Standard Missile-3 during an exercise, intercepting a short-range ballistic missile target in the Pacific.

scenarios involving hypersonic weapons and cruise missiles. Stabilising engagement geometry earlier in the kill chain enables faster effector assignment and improves sensor-shooter alignment, converting warning time into usable engagement time. Those valuable seconds can be the difference between life and death in IAMD scenarios.

Classic estimation techniques such as Kalman filtering have long underpinned trajectory prediction. They have demonstrated their ability to enhance position and velocity estimations of ballistic missiles, which directly translates into a higher probability of a successful interception.[7] Practical research on ballistic trajectories provides the mathematical frameworks and algorithms used for rapidly determining the predicted interception point (PIP) and dynamically shaping trajectories in real time.[8] These techniques perform best against threats whose flight paths follow predictable physical models. Manoeuvring threats such as hypersonics and UAS do not follow ballistic trajectories, and the assumptions that make classic estimation fast and reliable hold less well against them.

AI/ML approaches the problem differently, learning flight behaviour rather than assuming it. Existing AI models can be trained on both simulation and flight-test data. These include deep learning systems that identify motion states and predict hypersonic glide vehicle trajectories,[9] and long short-term memory (LSTM) architectures whose attention mechanisms model complex manoeuvres.[10] Once trained, they generate predictions updated with each successive sensor input, enabling commanders to determine the threat vector far more precisely and quickly than with classic estimation techniques to allow for effective and timely defensive actions.

Historical Trend Analysis and Intent Modelling for Strategic Cueing

Historical trend analysis supports predictive cueing in IAMD, as AI/ML assists analysts in identifying long-term behavioural patterns across large, disparate datasets. ML-supported simulation can reveal recurring tendencies in beyond visual range (BVR) engagements and track how adversaries adjust their behaviour over time,[11] while multi-agent modelling highlights patterns in UAS swarm coordination, preferred attack timings and evolving multi-vector strike profiles.[12] Taken together, these studies suggest that adversary behaviour may be patterned,

AI-driven decision support has the potential to improve effector allocation under conditions of simultaneous multi-vector attack.

and that with sufficient data those patterns are learnable. Incorporating such patterns into predictive processes lets NATO ready sensors, effectors and rules of engagement (ROE) before a threat emerges rather than after.

While historical trend analysis helps indicate where and when threats are most likely to emerge, intent modelling addresses what a detected object will do next. AI/ML-enabled intent modelling draws on observed behaviours (e.g., flight profiles, sensor signals, and communications) to infer probable objectives and future adversary actions. In the air domain, deep learning methods and structural behaviour models can transform kinematic tracks into probabilistic assessments of intent, including attack, transit, reconnaissance or deception.[13,14]

By distinguishing between kinematically similar but behaviourally distinct flight profiles, intent modelling helps prioritise effector employment and may reduce false alarm rates. Drawing on multiple sensor types together, rather than any one in isolation, improves the accuracy of intent estimates.[15]

Data and Interoperability

While AI/ML models are evolving rapidly, the data required to train them remains the limitation. Models trained on fragmented or poorly governed inputs will produce assessments no commander should act on. The risks compound from there, across operational, technical and ethical dimensions.[16] Misclassification, predictive errors, operator overreliance and system-level vulnerabilities under degraded data conditions can all undermine the assessments these systems output. So can deliberate adversary manipulation, such as spoofed radar signals or injected malicious data.

AI/ML must rely on trustworthy data sources, secure supply chains, and robust cybersecurity processes to prevent the spread of corrupted inputs or compromised models across defence networks.[17] Another major challenge involves interoperability issues across the Alliance, including potentially inconsistent data standards, heterogeneous national architectures, and restrictions resulting from classification levels, all of which hinder effective information sharing and coordinated action.

Recommendations for NATO Decision-Makers

NATO's AI Strategy already recognises AI as a foundational capability that must enhance interoperability, resilience, and decision-making across all Alliance tasks. Realising that potential within the NATO Integrated Air and Missile Defence System (NATINAMDS), however, requires a systematic and institutionalised approach to adoption rather than opportunistic fielding. The preceding sections identified where current architectures fall short: fragmented data, slow cross-domain fusion, limited decision agility, and unresolved questions of trust and interoperability. The following recommendations address those shortfalls through four architectural requirements essential to an AI-ready IAMD.

Data readiness: The article establishes that data, not algorithms, is the binding constraint: models trained on fragmented or poorly governed inputs produce assessments no commander should act on, and differing national data formats already slow cross-domain fusion. NATO must therefore transition from data availability to data readiness. The Data Exploitation Framework Policy (DEFP) recognises data as a strategic resource and establishes the foundations for its secure, interoperable use.[18] Within IAMD this means operationalising the DEFP through harmonised data standards, structured metadata, disciplined data preparation and lifecycle management of AI models. This spans training; test, evaluation, verification and validation (TEV&V); and implementation.[19] NATO must also establish federated data pipelines, supported by secure sandbox environments, that allow controlled experimentation on operational data while preserving responsible-use safeguards.

Interoperability and security by design: The preceding sections both identify interoperability as a first-order obstacle: national systems of varying age and capability, inconsistent data standards, and heterogeneous architectures that impede shared action. AI integration must therefore be interoperable and secure from the outset, resting on standardised interfaces, shared data taxonomies and secure supply chains.[20] Doctrine, training, and exercises must evolve in parallel to enable effective human-AI teaming, mitigate automation bias, and preserve the primacy of human command authority. Standardised model documentation, certification, and recertification underpin the transparency on which multinational trust depends.

Institutionalised trust and responsible use: The preceding section identifies the ethical exposure directly: gaps in explainability and accountability, potential algorithmic bias, and the escalation risk of rapid AI-enabled responses. Responsible adoption requires human oversight, rigorous testing, resilient architectures, and adherence to NATO's Principles for Responsible Use of AI – legality, accountability, explainability and traceability, reliability, governability, and bias mitigation.[21] Engineering practice must give these principles effect through continuous monitoring of fielded models, resilience testing, red-teaming and validation under degraded data conditions.

'Data, not algorithms, is the binding constraint: models trained on fragmented or poorly governed inputs produce assessments no commander should act on...'

A distributed edge-core architecture: IAMD must function when connectivity is contested or lost. Accordingly, AI/ML capability should be distributed rather than centralised: edge systems providing real-time decision support at the tactical level, while a protected core retains model development, training, and governance. This division must be codified in a NATO reference architecture to guarantee coherence and interoperability across the two layers.

These four requirements cannot be pursued in isolation. Alignment with the NATO AI Strategy and integration into the NATO Defence Planning Process (NDPP) are essential to coherent capability development, sustained funding and lasting interoperability across the Euro-Atlantic area. Only through such a structured and consistent approach can the Alliance maintain its technological edge while ensuring that the adoption of AI remains controlled, responsible, and operationally effective.

Conclusion

Accelerated AI adoption across NATO's air and missile defences is not optional. Adversaries' use of proliferated UAS, HGVs and low-observable long-range fires compresses IAMD engagement timelines irrespective of Allied adoption choices. The decisive question is therefore not whether these threats exist, but whether NATO can adapt quickly enough to meet them. NATO must develop a comprehensive strategy that uses AI/ML to accelerate and sharpen decision-making in an increasingly complex and data-rich operating environment, while building the political consensus its broader use will require in the face of real ethical and legal challenges. Without timely adaptation, the strengths of today's IAMD architecture will erode; with it, AI offers a realistic means of preserving NATO's operational and strategic edge. ●

1. Onderco, M., 'Navigating the AI frontier: Insights from the Ukraine conflict for NATO's governance role in military AI', Journal of Strategic Studies 48, no. 3 (2025): pp. 602-626, https://doi.org/10.1080/01402390.2025.2463451.
2. NATO Integrated Air and Missile Defence Centre of Excellence, The Evolving UAS Threat: Lessons from the Russian–Ukrainian War since 2022 (Šiauliai: IAMD COE, 2024), https://iamd-coe.org/wp-content/uploads/2024/02/The-Evolving-UAS-Threat-Lessons-from-the-Russian-Ukrainian-War-Since-2022-on-Future-Air-Defence-Challenges-and-Requirements.pdf.
3. Muravska, J., European Integrated Air and Missile Defence in NATO: Progress and Persistent Challenges (London: Freeman Air & Space Institute, 2023), https://www.kcl.ac.uk/warstudies/assets/paper-16-julia-muravska-european-integrated-air-and-missile-defence.pdf.
4. NATO, NATO Integrated Air and Missile Defence Policy (Brussels: NATO, 13 February 2025), https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-integrated-air-and-missile-defence-policy.
5. Koch, W., 'Perspectives on AI-Driven Systems for Multiple Sensor Data Fusion', tm – Technisches Messen 90, no. 3 (2023): pp. 166-176, https://doi.org/10.1515/teme-2022-0094.
6. Center for Army Lessons Learned, Listening to the Sky: Acoustic Drone Detection Systems – Ukraine and Emerging Technologies, No. 26-1115 (Fort Leavenworth, KS: CALL, April 2026), https://www.army.mil/article/292099/.
7. Kalman, R. E., 'A New Approach to Linear Filtering and Prediction Problems', Journal of Basic Engineering 82, no. 1 (1960): pp. 35-45, https://doi.org/10.1115/1.3662552.
8. Lee, J., Kim, S., and Park, Y., 'Intercept Point Prediction of Ballistic Missile Defence Using Neural Network Learning', International Journal of Aeronautical and Space Sciences 21, no. 2 (2020): 345–357.
9. Zhang, J., Xiong, J., Li, L., Xi, Q., Chen, X., and Li, F., 'Motion State Recognition and Trajectory Prediction of Hypersonic Glide Vehicles Based on Deep Learning', IEEE Access 10 (2022): 21095–21108.
10. Xu, Y., Pan, Q., Wang, Z., and Hu, B., 'Hypersonic Target Trajectory Estimation Based on Long Short Term Memory and Multi-Head Attention', Entropy 26, no. 10 (2024): 823.
11. Costa, A. N., Dantas, J. P. A., Scukins, E., Medeiros, F. L. L., and Ögren, P., 'Simulation and Machine Learning in Beyond Visual Range Air Combat: A Survey', IEEE Access (2025), https://www.joaopadantas.com/files/costa2025simulation.pdf.
12. Sosa, C., SWARM of UAS Modelling and Simulation Methodology, STO MP SAS 192 (Brussels: NATO Science and Technology Organization, 2025), https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-192/MP-SAS-192-31.pdf.
13. Niu, Q., Zhang, L., Ren, S., Gao, W., and Wang, C., 'Attention Enhanced Contrastive BiLSTM for UAV Intention Recognition under Information Uncertainty', Drones 9, no. 4 (2025): 319.
14. Erukude, S. T., Veluru, S. R., and Marella, V. C., 'Multimodal Deep Learning: A Survey of Models, Fusion Strategies, Applications, and Research Challenges', International Journal of Computer Applications 187, no. 19 (2025): pp. 1–7, https://doi.org/10.5120/ijca2025925264.
15. Ibid.
16. NATO, Summary of NATO's Revised Artificial Intelligence Strategy (Brussels: NATO, 10 July 2024), https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy.
17. NATO, AI and Data Exploitation: Policies Landscape in NATO (Brussels: NATO HQ Innovation, Hybrid and Cyber Division, 2024).
18. NATO, Data Strategy for the Alliance (Brussels: NATO, 5 May 2025), https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance.
19. Chochtoulas, A., Nayyar, N., Stensberg, L., and Samso Pericon, L., The JAPCC AI Handbook (JAPCC, March 2026).
20. Madison, A., McDowell, K., Goecks, V. G., Hansberger, J., Olney, C. M., Ahern, C., Marathe, A., Waytowich, N., Kenney, C., and Kelshaw, C., Commanding Soldier–Machine Partnerships, STO HFM 239 (Brussels: NATO Science and Technology Organization, 2025), https://www.sto.nato.int/document/new-challenges-for-future-c2-commanding-soldier-machine-partnerships/.
21. NATO, Summary of NATO's Revised Artificial Intelligence Strategy (Brussels: NATO, 10 July 2024).

ABOUT THE AUTHOR

Lieutenant Colonel Sebastian Kurzepa
POL Air Force, JAPCC

Lieutenant Colonel Sebastian Kurzepa joined the Polish Armed Forces in 2000. He holds an MSc in Radar Systems from the Military University of Technology in Warsaw. During his career, he has served in a variety of command and staff positions across air operations, command and control, communications and information systems, logistics and aircraft maintenance. He also served at the 22nd Control and Reporting Centre and at the Polish Air Operations Centre – Air Component Command. Since July 2025, he has been a Staff Officer in the Assessment, Coordination and Engagement (ACE) Branch at the Joint Air Power Competence Centre (JAPCC). His professional interests include Integrated Air and Missile Defence, air command and control, and the integration of emerging technologies into military operations.