Simulating the Skies: Unleashing AI for Adaptive Airborne Defense

Robin Grimes, Connor Green, Jeff Souder, William Marx, Ph.D., Chanler Cantor
Intuitive Research and Technology Corporation (*INTUITIVE*®)
Huntsville, Alabama
robin.grimes@irtc-hq.com, connor.green@irtc-hq.com, jeff.souder@irtc-hq.com,
william.marx@irtc-hq.com, chanler.cantor@irtc-hq.com

ABSTRACT

The rapid advancement and proliferation of airborne threats – including Uncrewed Aerial Systems (UAS), hypersonic weapons, and other emerging platforms – pose significant challenges in modern warfare. Adversaries deploy these systems for reconnaissance, targeting, and direct strikes, often aiming to destroy Air and Missile Defense (AMD) sensors to secure air dominance. While overall threat data is abundant, details on individual variants remain limited and quickly become obsolete. Traditional Modeling and Simulation (M&S) techniques, which depend on comprehensive datasets and finite Subject Matter Expert (SME) resources, cannot keep pace with these dynamic adversaries. Consequently, the United States must develop agile solutions to analyze vast quantities of evolving threats despite incomplete data.

This paper explores methods to combine advanced M&S's automated data generation with sparse real-world samples to train Artificial Intelligence (AI) to assess options within complex threat spaces. We examine how AI techniques can infer missing characteristics and build adaptive operational models that mirror fluid tactics. Central to our methodology is the Sensor Testbed for Allocation, Resilience, and Survivability (**STARS**), an open-architecture platform created to simulate and assess novel strategies. By enabling AI to "connect the dots" between incomplete observations and then interface with **STARS**, our approach can enhance real-time decision-making and empower commanders to optimize sensor deployment, prioritize critical areas, and deploy countermeasures effectively. Moreover, this methodology aligns with initiatives like Golden Dome for America (GDA), which seek to strengthen layered defense through AI-driven integration, offering a scalable solution for adapting to rapidly evolving airborne dangers while preserving essential human oversight.

ABOUT THE AUTHORS

Ms. Robin Grimes is a Systems Engineer at *INTUITIVE* and supports PM STARE, PEO Missiles and Space, as the Modeling and Simulation Lead for the AN/MPQ-64A4 - Sentinel A4, an active electronically scanned array (AESA) 3D radar. She holds a BS in Electrical Engineering with a minor in Mathematics and MS in Electrical Engineering (Intelligent Systems) from Clemson University.

Mr. Connor Green is a Senior Digital Engineer at *INTUITIVE;* as a member of the research team, he specializes in AI, radar, and data analysis. He has experience in RF seeker technology, hardware-in-the-loop simulations, RF test chambers, and computer-vision AI. He received a BS in Electrical Engineering from Mississippi State University.

Mr. Jeff Souder is a Vice President at *INTUITIVE*, where he serves as a senior strategic advisor, leveraging his Air, Space and Missile Defense experience to guide the company's continued growth in this mission-critical domain. He also completed a distinguished 25-year career in the Army, where his final and most significant assignment was serving as Project Manager at the Missile Defense Agency, leading the establishment of ballistic missile defense sites in Poland and Romania. He received graduate degrees from Florida Institute of Technology and The US Naval War College and a BS in Electrical Engineering from Penn State University.

Dr. William Marx is the Senior Vice President and Chief Technology Officer of *INTUITIVE*. He is responsible for planning, managing, and executing research and development programs aligned with the technology priorities of the U.S. military and commercial customers. Dr. Marx received his PhD and MS in Aerospace Engineering from the Georgia Institute of Technology and his BS in Aerospace Engineering with a minor in Mathematics from Embry-Riddle Aeronautical University. He was a NASA Langley Graduate Student Researchers Program (GSRP) Fellow.

Ms. Chanler Cantor is an Area Manager at *INTUITIVE*. She is responsible for managing the internal research and development portfolio where projects include AI, data analytics, and complex visualization. She received her MS in Systems Engineering from The Johns Hopkins University and her BS in Electrical Engineering from The University of Alabama.

Simulating the Skies: Unleashing AI for Adaptive Airborne Defense

Robin Grimes, Connor Green, Jeff Souder, William Marx, Ph.D., Chanler Cantor
Intuitive Research and Technology Corporation (*INTUITIVE*®)
Huntsville, Alabama
robin.grimes@irtc-hq.com, connor.green@irtc-hq.com, jeff.souder@irtc-hq.com, william.marx@irtc-hq.com, chanler.cantor@irtc-hq.com

INTRODUCTION

Modern warfare is increasingly dominated by airborne threats such as Uncrewed Aerial Systems (UAS), hypersonic weapons, and other emerging platforms which challenge conventional defense strategies through their speed, sophistication, and adaptability. Adversaries exploit these systems for reconnaissance, targeting critical assets, and degrading Air and Missile Defense (AMD) capabilities by seeking to destroy or blind sensors. While the overall volume of threat data continues to grow, critical gaps persist in understanding specific threat variants, their evolving characteristics, and dynamic operational tactics which may be directed by Artificial Intelligence (AI) controllers making decisions in real-time (Bondar, 2025). These gaps are exacerbated by the rapid obsolescence of existing intelligence, rendering traditional Modeling and Simulation (M&S) approaches inadequate.

M&S platforms provide the capability to explore hypothetical defense scenarios and sensor interactions, but they generally depend on extensive input model libraries and expert time. Although sensor networks now produce terabytes of data daily – from high resolution radar returns to infrared imagery and electronic warfare intercepts – critical details about new threat variants remain hidden. The data volume creates a saturation problem: important signals are buried in noise, Subject Matter Experts (SME) teams cannot manually sift through every byte, and adversary innovations slip through the cracks. As a result, Intelligence Centers struggle to balance the data analysis workload with the need to rapidly update threat models. Ironically, amidst this mountain of data, analysts are also hampered by how little we know about each individual threat. Due to the numerous and transient UAS configurations, it is impossible to have well defined models for each of them. When attackers can deploy modified UAS or novel hypersonic profiles within weeks, standard M&S processes churn out models that are obsolete before they're even finalized.

This paper investigates how integration of advanced M&S with AI enhances threat analysis and decision-making in environments characterized by incomplete or sparse data. Our approach embeds AI directly into high-fidelity M&S frameworks to automate data-triage and inference. The proposed Sensor Testbed for Allocation, Resilience, and Survivability (STARS) serves as the representative simulation environment for our research. By leveraging AI-driven data compression, we distill excessive sensor output data into concise feature sets that highlight anomalies while preserving potential threat indicators. In subsequent sections, we detail four core AI applications—data compression, synthetic gap filling, resource optimization, and adversarial scenario generation—and demonstrate how AI-augmented M&S transforms data saturation into a strategic advantage.

Our work aligns with broader initiatives such as Golden Dome for America (GDA) and the Defense of Guam mission which envision layered, all-domain defense networks capable of leveraging AI to adapt faster than adversaries can innovate (U.S. Department of Defense, 2025). The methodology proposed here offers a scalable path to adapt defensive systems to rapidly evolving threats, ensuring that U.S. forces can respond effectively without over-reliance on outdated or incomplete data. By combining the strengths of automated simulation and machine learning, this paper contributes to the development of agile, data-efficient solutions that empower tactical commanders to maintain situational awareness and operational resilience in contested airspace.

CURRENT STATE OF SIMULATIONS

M&S is an indispensable tool for military organizations, serving as the cornerstone for risk reduction, performance validation, and system integration. The utility spans multiple defense domains, from acquisition to training, analysis, and mission planning. Hardware-in-the-Loop (HWIL) configurations integrate physical sensors, subsystems, or even full-scale equipment into closed-loop simulation environments. Real hardware components, including radar assemblies or signal processors, are exercised against a simulated environment, allowing engineers to verify physical systems without deploying them to the field. Similarly, Software-in-the-Loop (SWIL) uses tactical code with virtual platforms to emulate complete systems. The capability facilitates both catching potential issues early and the exploration of novel techniques. Sim-over-Live (SoL) is a technique whereby real assets integrate with virtual entities during test events. This capability permits personnel to engage simulated targets alongside physical ones.

These established techniques work most effectively when threat characteristics are well understood and change slowly, but they face significant limitations when applied to more dynamic and potentially AI-directed threats. In a traditional M&S cycle, like the one depicted in Figure 1, threat scenarios are defined based on inputs from the intelligence community, models are built to reflect known features, calibration occurs based on flight test data, and a lengthy accreditation process must be completed. This accreditation process typically involves collaboration between several contractor and Government stakeholders and often takes numerous iterations over months before the results are released to the threat M&S community. In contrast, the modern battlefield is increasingly characterized by rapid technological advances and emerging threats. UAS platforms may be introduced or altered in a matter of weeks by altering payloads, swapping components, or experimenting with electronic countermeasures, thus making M&S setups obsolete before they're even completed.

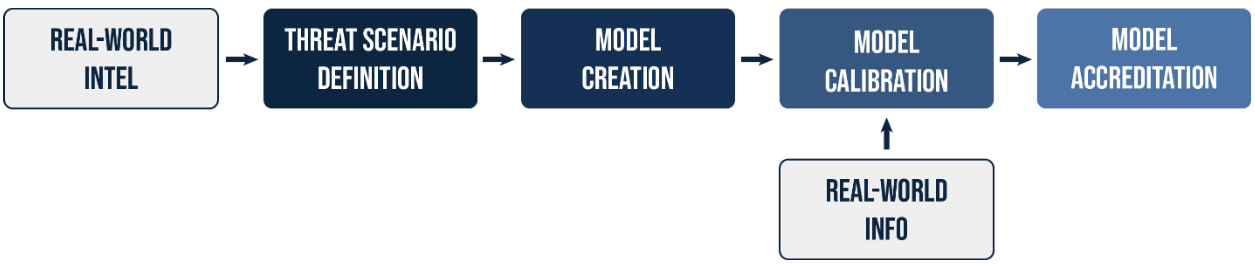

Figure 1. Traditional M&S Approach

The Duality of Data

A significant barrier to effective threat modeling is the sparsity of real-world data. Event Target Files (ETFs) are recorded datasets of raw sensor data – mainly radar returns – captured during a specific adversary event, which are then processed by intelligence agencies to extract relevant information. Though a primary source of empirical threat information, they still offer only a snapshot view. Similarly, Overhead Persistent Infrared (OPIR) systems provide intermittent detections of new threats – often limited to brief thermal signatures – without revealing full behavioral patterns. When challenged by rapid evolution of the threat, analysts must constantly update models based on new, yet incomplete data. In practice, when simulation teams rely on these fragments of information (e.g. recorded videos or relayed data) to "fill in" models, it results in high uncertainty.

Defense organizations also face an overwhelming influx of raw data (Taylor, 2025). Satellite imagery streams, OPIR detections, fielded sensor logs, SIGINT intercepts, or even social media reports all require processing at a level far beyond the capacity of SMEs. These SMEs must sift through vast datasets to identify meaningful information, and much information is left on the digital cutting room floor either due to human oversight or simple data processing limitations. In a scenario such as the Defense of Guam, multiple sensor streams must be analyzed concurrently. We rely on SMEs to triage the data, to pick out the most pertinent and leave the less certain behind. And undoubtedly, we leave important information unexamined.

EMERGENCE OF AI AND MACHINE LEARNING (ML)

In recent years, AI has emerged as a transformative force, enabling systems to process vast datasets, identify patterns, and adapt to complex environments. At the forefront of this revolution are Machine Learning (ML) techniques that empower algorithms to learn from data and make informed decisions even in scenarios with incomplete or dynamic information. Among the most influential ML approaches are neural networks—such as Convolutional Neural

Networks (CNNs) and Recurrent Neural Networks (RNNs)—which have proven particularly valuable in defense applications. Figure 2, below, shows the various subsets of AI that will be discussed in this paper. CNNs excel at spatial data analysis, such as parsing radar imagery or sensor outputs to extract critical features for threat identification, while RNNs specialize in sequential data, enabling the prediction of adversarial behaviors over time and the modeling of evolving tactics. The authors' method uses CNNs as a replacement for RNNs, because the sequential data for multiple columns can be visually correlated in a plot. These advancements have expanded AI's capacity to infer missing information, simulate plausible scenarios, and optimize resource allocation, even when data is sparse or rapidly changing.

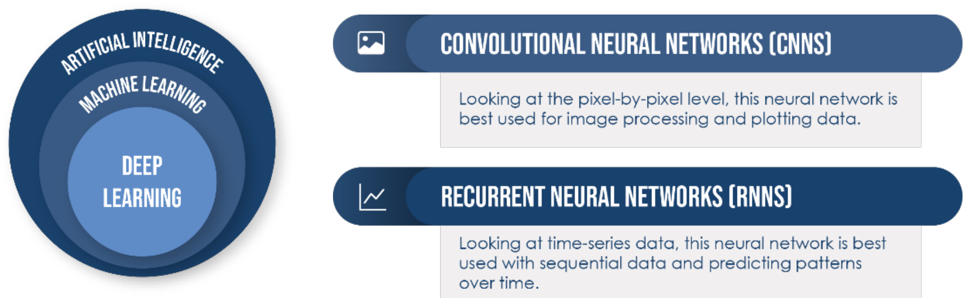

Figure 2. Subsets of AI

Training an ML Model

When training an ML model, there are many different training methods including behavioral, supervised, unsupervised, etc. The goal is to teach a model to fit a general pattern from specific examples. In simulation terms, one example of ML model training could be exposing the model to simulation results created from specific scenario parameters to predict which parameters created a particular scenario result in a future simulation run. This example is further detailed in the "Gap-Filling in Simulations" section.

Data is the key bottleneck for all AI solutions, and it's why commercial companies focus so much on collecting and labeling it. For this paper, our research has primarily focused on supervised learning. However, many other training methods can be applied to create ML models for the M&S community. Supervised learning is training an AI on labeled data where the AI is given both the question and answer. In a human scenario, this type of training could be visualized as learning via flashcards where the front of the card is a sample's data (question) and the back is the sample's label (answer). Labeling data is the most important part of the dataset, because it determines the output the AI will provide.

Labeled Datasets

Labeled datasets are critical for supervised learning in AI systems. Simulations, despite their computational intensity, represent a largely untapped resource for generating vast, automatically labeled datasets. By leveraging simulations, domain experts can create synthetic scenarios that replicate real-world conditions, producing labeled outputs such as radar survival rates, threat detection probabilities, or environmental interference metrics. This automated labeling process is pivotal, as manual annotation of thousands of data samples is impractical and prone to human error. The quality and structure of these labels directly influence the AI's ability to discern patterns and generalize across scenarios. For instance, if a simulation outputs radar performance metrics tied to specific configurations, the AI can learn to correlate input variables (e.g., sensor placement, environmental clutter) with outcomes, enabling data-driven optimization of survivability strategies.

When analyzing data, humans spend time simplifying and filtering the data for the most important features and ignore the rest of the data until time permits a search for less obvious patterns. An AI model does not need the same data culling and prioritization, because it will use trial and error math to determine what data is important to the output since the weights (i.e., coefficients) for useless data (e.g., columns in a csv file) will trend towards zero. Compressing raw data into useful metrics can be the final step for aiding human decision making, or it can be the first step of an optimization problem where another AI or classical system provides a sensor deployment strategy to maximize survivability. Due to the volume of samples needed, labeling needs to be an automated process, or it needs a structured system for a group of humans to interact with at scale (e.g., captcha image tests). Simulations provide an interesting opportunity for automatically labeling data, or using AI models trained on labeled real world data (i.e., statistical brute force) as subsystems within the simulation instead of devoting significant time to algorithm development.

INTEGRATING AI INTO M&S

A key advantage of using AI within simulation environments lies in its capacity to extract and retain information from large datasets, surpassing human limitations in pattern recognition and analytical depth. By training on comprehensive, labeled simulation data, AI models can identify subtle relationships between system parameters and operational outcomes, even in complex, multi-variable scenarios. Furthermore, AI's ability to extrapolate from existing data—particularly when gaps exist in the dataset—allows it to fill in missing information through learned patterns. This capability is especially valuable in defense applications, where simulations may lack coverage for edge cases or niche environments. Figure 3, below, shows how AI data can be integrated into the traditional M&S approach.

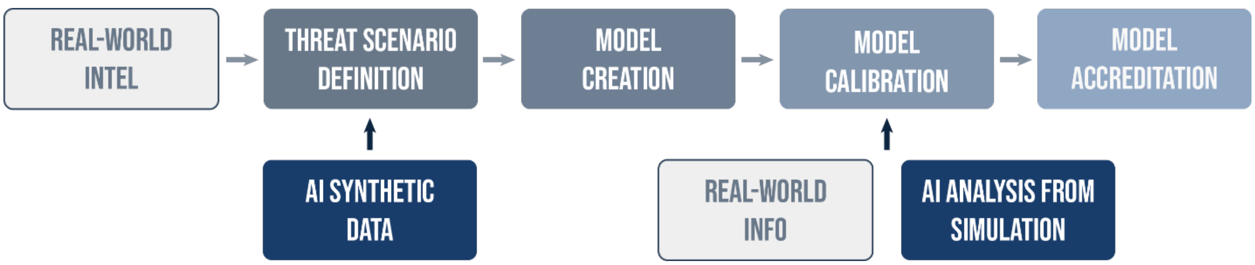

Figure 3. M&S Approach Including Synthetic AI Data

Simulation owners hold a unique position in this ecosystem, as they possess the tools and expertise to generate high-quality, labeled datasets that can be used to train AI models. By structuring simulation outputs into AI-friendly formats—such as tabular data or visual representations of tabular data—sim owners can provide the critical input required for model development. This not only accelerates the training process but also fosters collaboration across defense teams by enabling dataset sharing. Importantly, AI's reliance on input-output relationships means it can function effectively within black-box systems, as it does not require explicit knowledge of internal subsystems. This property is particularly advantageous in scenarios involving proprietary or sensitive technologies, such as radar waveforms and algorithms, and allows parties who wouldn't otherwise have access to train AI models on internal simulation data without exposing proprietary or classified algorithms.

PRIOR RESEARCH

Since the widespread adoption of AI in the commercial domain, many researchers have hypothesized ways to use these AI advances to benefit the military domain. The following sections compose a literature review on the application of AI technologies and methodologies to the M&S domain.

Computer Vision to Evaluate and Provide Training Data

The potential of AI in radar simulation is further amplified by advancements in computer vision techniques. Typically, computer vision is a type of AI used on real world pictures. A common example is using a computer vision model to explain what elements are contained in the picture. However, computer vision can also be applied to visualize and

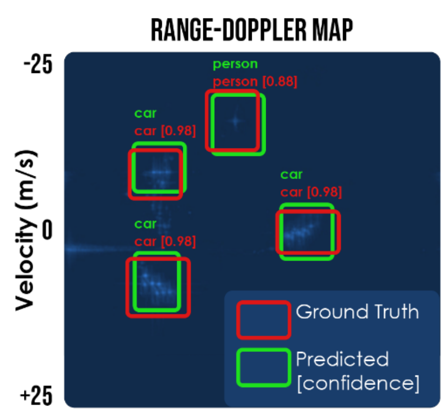

Figure 4. Example of how AI can supplement visualization data. Image adapted from Silgar (2020).

interpret data. A recent paper demonstrated how visualizing data for an AI made it better at evaluating model performance compared to a conventional numbers-based approach (Li, 2025). Simulations produce tabular data with time-series measurements, which can be transformed into visual formats—such as plots or battlefield diagrams—while preserving contextual information. These visual representations serve as effective training inputs for CNNs, which excel at identifying spatial and temporal patterns.

Predictive Modeling

Velazquez (2024) provided a methodology for applying a combination of CNNs and RNNs to process and predict complex military scenarios. Velazquez's assertion is that trained AI technologies can provide a more accurate and dynamic predictive modeling approach. Predictive modeling, compared to traditional, static modeling, enables a more adaptive and dynamic simulation that can adapt and evolve with less collected, real-world input data. In other words, predictive models can fill in the gaps where real-world input data might be scarce. This predictive modeling approach can benefit M&S scenarios that involve emerging threats where there is minimal existing threat data.

ML Training Methods

As mentioned previously, there are many different training methods that can be applied to create a ML model. While our research contained in this paper is focused on supervised learning, other researchers have explored other types of training methods to solve different M&S problems. Velazquez (2024) also asserted that deep learning, a subset of machine learning that uses multi-layered neural networks to mimic human neurons, enables military simulations to dynamically adapt in real-time based on trainees' actions, moving beyond static scenarios. This adaptability prepares personnel for the unpredictability of real-world operations by fostering tactical agility, encouraging both proactive and reactive decision-making essential for modern warfare. Black and Darken (2024) researched the application of Reinforcement Learning (RL) to the M&S domain. In RL, an agent learns to make decisions by performing actions in an environment and receiving feedback through rewards or penalties. In complex scenarios, training RL agents becomes increasingly challenging as complexity often leads to exponential increases in required training time. Black and Darken proposed a new abstraction method to enable more efficient AI training. This research has the potential to enhance RL's applicability in complex M&S.

Trust in AI

In high-consequence decision-making domains such as battlespace management or defense applications, the integration of AI models raises significant legal, moral, and ethical concerns. To address these challenges, our research team has focused on advancing trust in AI since 2021, initially concentrating on behavioral cloning and analysis of black box AI models. In 2021, we began exploring the feasibility of cloning human decision-making for a simple board game into an AI model. This effort revealed insufficient human data to replicate behavior. However, by incorporating AI models, we demonstrated that an observer agent could predict observed model behavior with sufficient data coverage (Etheredge et al., 2022). This finding spurred further inquiry into the trustworthiness of cloned models, culminating in our 2023 work, which proposed a system to build trust by identifying model behaviors under specific conditions, as applied to autonomous vehicles (Russell et al., 2023). In 2024, our team introduced a quantitative approach leveraging variational autoencoders (VAEs) and gradient-based stability/uncertainty quantification techniques to evaluate model trustworthiness (Baugh et al., 2024).

Collectively, these studies aim to accelerate AI adoption in the defense community by providing rigorous methodologies to assess model reliability and transparency. By quantifying trustworthiness through observable behaviors and stability metrics, our work seeks to ensure that AI systems can be safely and effectively deployed in critical defense scenarios.

OUR RESEARCH

Our research does not seek to present an all-encompassing solution for integrating AI into sensor defense systems but instead examines a series of targeted, smaller-scale applications designed to enhance scalability and practical utility. These approaches aim to address specific challenges within sensor survivability planning, such as data management, simulation fidelity, and real-time decision-making, offering tools that could be readily adapted to diverse contexts.

Central to this work are four key applications of AI: data compression, gap-filling in simulations, resource optimization, and adversarial testing. Throughout these applications, the focus remains on leveraging AI's strengths—pattern recognition, rapid computation, and scalability—while addressing its limitations, such as the "black box" nature of its decision-making processes. By decomposing tasks into stages and providing interpretable metrics, the strategy ensures that human SMEs retain ultimate authority over critical decisions. This balance between automation and oversight is essential for maintaining trust and operational relevance in defense planning. The examples provided, though rooted in simulations like STARS, are intended to inspire broader applications, encouraging practitioners to adapt these principles to their own systems and scenarios.

Data Compression

In the M&S space, where high-dimensional data from distributed sensor networks strains computational resources and delays decision-making, data compression is indispensable for maintaining simulation fidelity and enabling real-time analysis. AI can process vast, unlabeled datasets in their entirety—without prior filtering—to identify critical patterns, thereby reducing the cognitive burden on SMEs. This capability leverages advanced techniques such as autoencoders (a type of neural network) and dimensionality reduction algorithms, which systematically distill terabytes of sensor data (e.g., radar, infrared, or electronic warfare feeds) into compressed representations while preserving key features like speed, altitude, or trajectory anomalies.

By minimizing data complexity, M&S frameworks can efficiently iterate through scenarios, test hypotheses, and validate strategies without being overwhelmed by raw input volumes, ensuring simulations remain agile and responsive to evolving threat dynamics. For instance, in a simulation environment like STARS, compressed data from distributed sensors allows rapid generation of probabilistic threat models, which commanders can use to prioritize defensive resources or adjust sensor allocation in real time. This approach addresses the "data deluge" problem by transforming raw inputs into interpretable metrics—such as threat probability scores or spatial correlation maps—that align with initiatives like GDA to enhance layered defense systems (Taylor, 2025).

Crucially, data compression is vital for scalability: as sensor networks expand or threat tactics grow more sophisticated, compressed data remains actionable, enabling AI and SMEs to collaboratively maintain situational awareness in contested airspace. By automating outlier identification (e.g., unusual UAS flight patterns or hypersonic weapon maneuvers), AI-driven summarization tools free SMEs to focus on high-value analysis rather than sifting through raw data. The method also ensures that simulations can run faster and more iteratively, allowing defense planners to explore countermeasure effectiveness and adversarial adaptations under time-sensitive, resource-constrained conditions.

Gap-Filling in Simulations

In the M&S community, addressing gaps in simulations is critical to ensuring models remain relevant and effective in preparing for real-world threats, which often exhibit incomplete or evolving characteristics that static simulations cannot capture. Leveraging our prior research and experimentation, the authors propose two mitigation strategies. First, synthetic sample generation through sample duplication and iterative censorship of Radar Cross-Section (RCS) data—such as obscuring portions of RCS values for commonly encountered UAS—could train AI models to extrapolate complete threat profiles from incomplete data, enhancing predictive accuracy for emerging threats. For example, by masking RCS features of stealthy UAS or hypersonic glide vehicles in simulated environments, AI learns to infer missing parameters (e.g., altitude, speed, or trajectory anomalies) using contextual cues, thereby mirroring real-world scenarios where adversaries employ low-observability tactics to evade detection. This approach not only prepares AI systems to handle partial or degraded data but also reduces reliance on SMEs to manually curate datasets.

In the second mitigation strategy, partial real-world data would be used to calibrate simulation parameters, ensuring modeled scenarios align more closely with operational realities. By integrating fragmented data (e.g., limited observations of enemy UAS swarms or hypersonic maneuvering) into simulations, AI can refine its understanding of threat behaviors, environmental variables (e.g., atmospheric conditions affecting RCS), and sensor limitations (e.g., radar blind spots or jamming effects). As an example, the authors created a dataset from running a scenario with a number of simulation parameters being swept (i.e., standard Monte Carlo test runs), and then the dataset was used to train an AI on how to calibrate the parameters to get the desired output. Next, the AI was given a test flight, and the

AI provided the simulation parameters needed to recreate the real-world result; thus, allowing for confidence when simulating similar runs in that environment where real-world data was not collected. This calibration process bridges the gap between idealized simulations and dynamic battlefields. These strategies combined, improve the ability to generate robust threat models, simulate adversarial adaptations, and optimize defensive responses while maintaining the critical role of SME validation.

Resource Optimization

Resource optimization is a foundational requirement in the M&S community because modern warfare demands decisions that balance competing priorities under extreme constraints. In contested environments, military systems face adversaries who exploit resource limitations—such as sensor coverage, countermeasure availability, or personnel bandwidth—to disrupt operations. For instance, UAS or hypersonic weapons may target high-value sensors to degrade situational awareness, forcing defenders to allocate resources strategically. Traditional M&S approaches often fail to account for these trade-offs at scale, as they rely on simplified assumptions or require excessive computational power to explore all possibilities. Without optimized resource allocation, simulations risk producing unrealistic strategies that overpromise defensive capabilities or underprioritize critical vulnerabilities. This disconnect between simulated outcomes and real-world feasibility jeopardizes preparedness, as commanders may deploy tactics that are either too risky (e.g., overexposing sensors to enemy targeting) or too conservative (e.g., underutilizing assets due to uncertainty). Resource optimization ensures that simulations reflect the operational realities of scarcity and complexity, enabling planners to identify configurations that maximize effectiveness while minimizing risks—a requirement for credible defense readiness.

The dynamic nature of airborne threats further underscores the need for resource optimization in M&S. Adversaries continuously adapt their tactics, from employing AI directed stealthy UAS swarms compromising an entire defense layer). Resource optimization thus ensures that M&S outputs remain actionable, scalable, and resilient to the fluidity of modern threats, bridging the gap between theoretical models and the unpredictable demands of combat.

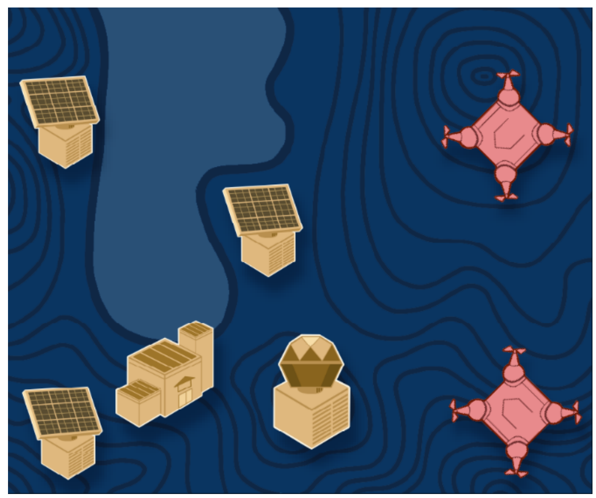
Figure 5. Notional threat landscape

By training AI on Monte Carlo-style simulation runs, the system can rapidly assess sensor configurations against hypothetical threat scenarios, such as the decision snapshot depicted in Figure 5. This decision snapshot is a visualization of automated radar placement in a simulation platform such as STARS under threat from detected UAS; it is a snapshot of a decision point for deciding which radar to enable to track the threat. Not all radars are the same, and risk must be balanced to ensure the UAS threat is defeated while minimizing the looming threat of active radars being targeted.

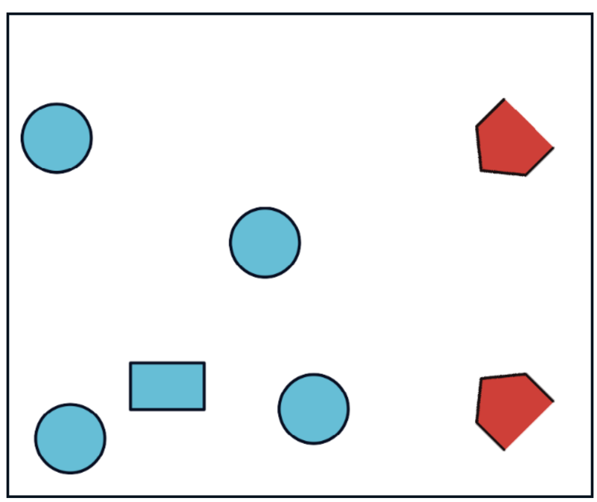
Figure 6. Simplified notional threat landscape

To simplify and improve this process, the authors' solution is to feed an AI model with a streamlined visualization (depicted in Figure 6), which abstracts key variables (e.g., sensor range, cost, or criticality) into the visualization via arbitrary color and shape. This streamlined visualization depicts how the STARS positional data is converted into a simple image. Computer-vision AI cares about feature proximity and the pixel value used as color since it's performing matrix math; thus, a simple image, with important shapes and colors being tied to sim values, is all that is needed. The images are then labeled automatically by output metrics of the sim run, like average survival rating for this configuration. Since the image is the input and the output is a survival metric, the AI learns the relationships in the image that maximizes the survival metrics.

The simplified picture of the threat landscape enables the AI model to predict survivability ratings for proposed sensor setups, as illustrated in Figure 7, offering SMEs a real-time, data-driven supplement to their judgments. This visualization allows for humans to have oversight on the AI's output instead of trusting it to make the decision and demonstrates how the AI can compress an overwhelming amount of information into a simpler number to be reviewed quickly. Crucially, the AI's role is not to replace human oversight but to support it through structured, high-speed analysis.

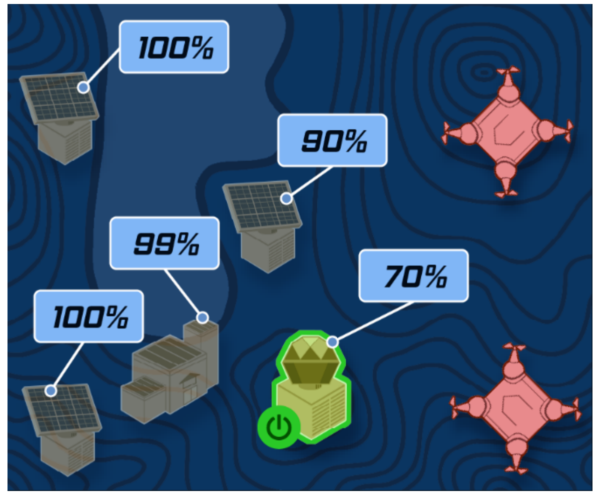

Figure 7. Notional survivability dashboard

Adversarial Testing

Adversarial testing further extends this framework by introducing AI-driven threat scenarios. Instead of relying on static or blindly randomized parameters, an adversarial AI could dynamically adjust threat characteristics—such as loosening constraints on speed or altitude—to simulate evolving UAS capabilities. This dual-AI approach allows for iterative "what-if" analyses, testing defensive configurations against increasingly sophisticated threats. The integration of adversarial models also underscores the importance of robust dataset design: effective AI performance hinges on well-sourced, labeled data where outcomes can be meaningfully tied to input variables. Without this foundational rigor, even advanced models may fail to deliver actionable insights.

A Real-World Scenario

These modular AI applications readily extend to concepts such as GDA which relies on layered sensor networks to cover the United States mainland. Figure 8 depicts a notional example of a sensor network where each circle represents a sensor's range. In this context, data compression AI could ingest separate feeds of radar data, OPIR constellations, and early warning sensors scattered across multiple states. A virtual environment could simulate sensor outages, deny zones, or even jamming states. Simulated scenarios would allow planners to quantify how data voids impact detection probabilities, and then eventually mitigate blind spots through sensor geometry or signal processing thresholds before actual system deployment. The innovative use of images tailored for computer processing also allows for the data to be understood easier for both SMEs and non-SMEs when iterating and reviewing the AI models, resulting in faster development and strategy cycles need for a massive system of systems like GDA.

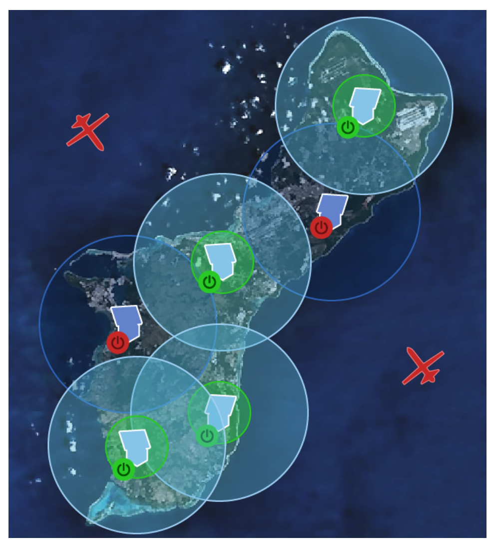

Figure 8. Notional sensor network

Closer to Beijing than to Hawaii, the US island territory of Guam is referred to as "the tip of the spear" for the United States military within the Indo-Pacific theatre. Guam faces persistent risk of attack due to its high strategic value. The Defense of Guam mission includes a range of strategies, sensors, and Command/Control (C2) systems to safeguard the island. In a simulated representation of the Defense of Guam, tactical data streams from hypothetical on-island radars, maritime sensors, and Airborne Early Warning (AEW) platforms feed into a complex joint environment that creates massive datasets. AI modules can process these concurrent virtual feeds to generate compressed threat summaries and identify critical patterns faster than manual review by SMEs, thus providing a better data dashboard for SMEs to review in real-time. Deviations from the identified patterns are key indicators for threats such as UAS swarms and allow for rapid detection and response (Fong & Roy, 2024).

Across both GDA and Defense of Guam M&S ecosystems, embedding AI into the simulation pipelines directly addresses the challenge of rapidly changing threats amid limited empirical data. By combining AI-driven data compression and synthetic gap filling, defense planners can produce probabilistic threat assessments without waiting for fully characterized models. SMEs leverage these AI-augmented outputs alongside limited available real-world observations to refine both AI tools and the underlying model fidelity. This approach ensures that commanders receive actionable insights even when adversaries innovate faster than traditional M&S can generate new threat models.

CONCLUSION

The evolving threat landscape of modern warfare, driven by the rapid proliferation of airborne systems such as UAS, hypersonic weapons, and emerging platforms, necessitates transformative approaches to sustain defensive superiority. Traditional M&S methodologies, hindered by reliance on exhaustive datasets and limited SME resources, are increasingly outpaced by adversaries who innovate faster than defense systems can adapt. This paper postulates that integrating AI with advanced M&S frameworks is a critical force multiplier, enabling defense planners to navigate incomplete data, infer missing threat characteristics, and dynamically model adversarial behaviors—all while preserving human oversight. For our hypothesis testing, the STARS platform exemplifies this synergy: an AI strategy assistant can be developed from the simulation, and the simulation can be improved by embedding the open-architecture environment with AI capabilities such as data compression, synthetic gap filling, resource optimization, and adversarial scenario generation. This approach produces probabilistic threat estimates that directly inform operational decisions, such as sensor placement, waveform selection, and countermeasure timing, across critical missions like homeland protection under GDA and strategic outposts like Guam.

AI-augmented M&S not only compresses vast sensor and intelligence data into actionable summaries but also stimulates new defensive strategies by predicting adversary tactics from sparse observations and generating war-game scenarios that challenge conventional assumptions. Optimization AI models further empower commanders by identifying resource allocations aligned with mission objectives, all within a rapid iterative cycle that prioritizes SME expertise while minimizing time consuming tasks. By translating complex, multi-domain data into interpretable metrics, this methodology accelerates decision-making without sacrificing the critical judgment of human operators.

Future efforts must address both technical and procedural challenges to further elevate realism. These include refining environmental models, expanding electronic warfare libraries, integrating live operational data, and establishing robust validation processes for AI-generated models. Additionally, ethical considerations and real-time SME-AI feedback mechanisms warrant deeper exploration to ensure trust and adaptability in high-stakes scenarios. As adversaries continue to innovate, the agile, AI-based approach presented here provides a durable foundation for anticipating and countering emerging airborne threats.

REFERENCES

Baugh, C., Camlic, K., Etheredge, C., Marx, W., Hill, T. & Cantor, C. (2024). Mapping trust in AI: Right tool, right task. *I/ITSEC 2024*. https://s3.amazonaws.com/amz.xcdsystem.com/44ECEE4F-033C-295C-BAE73278B7F9CA1D_abstract_File18333/FinalPaperStage3_24264_0825085709.pdf

Black, S., & das, C. (2024). Localized observation abstraction using piecewise linear spatial decay for reinforcement learning in combat simulations. ModSim 2024.

Bondar, Kateryna. (2025, June 2). How Ukraine's spider web operation redefines asymmetric warfare. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare.

Etheredge, C., Russell, K., Marx, W., Hill, T. & Drown, D. (2022). The use of AI/ML to replicate threat behavior for nonlinear simulation. I/ITSEC 2022. https://s3.amazonaws.com/amz.xcdsystem.com/44ECEE4F-033C-295C-BAE73278B7F9CA1D_abstract_File16562/PaperUpload_22230_0630041243.pdf

Fong, C., & Roy, D. (2024). Guam's strategic importance in the indo-pacific. Council on Foreign Relations. Retrieved June 5, 2025, from https://www.cfr.org/in-brief/guams-strategic-importance-indo-pacific

Li, W. (2025). Advances in artificial intelligence for data visualization: Developing computer vision models to automate reading of data plots, with application to regression diagnostics. Monash University. Thesis. https://doi.org/10.26180/28141406.v1

Russell, K., Green, C., Etheredge, C., Yohe, M., Marx, W., Hill, T., Odom, L., Drown, D. (2023). Using AI to increase trust in AI - yes, we're serious. *I/ITSEC 2023*. https://s3.amazonaws.com/amz.xcdsystem.com/44ECEE4F-033C-295C-BAE73278B7F9CA1D_abstract_File17275/FinalPaper_23316_0822051122.pdf

Sligar, A. (2020). Machine learning-based radar perception for autonomous vehicles using full physics simulation. IEEE Access, vol. 8 pp. 51470-51486, doi: 10.1109/ACCESS.2020.2977922.

Taylor, D. (2025). Managing the data deluge: How military radar systems are getting smarter. Military Embedded Systems. Retrieved June 5, 2025, from https://militaryembedded.com/radar-ew/rf-and-microwave/managing-the-data-deluge-how-military-radar-systems-are-getting-smarter

U.S. Department of Defense (2025, May 20). Secretary of defense Pete Hegseth statement on golden dome for America [Press release]. https://www.defense.gov/News/Releases/Release/Article/4193417/secretary-of-defense-pete-hegseth-statement-on-golden-dome-for-america/

Velazquez, L. E. (2024). Harnessing deep learning for enhanced military simulations: A comprehensive approach. ModSim 2024.