USE CASE

Enhancing Real-Time Decision-Making

with AI and Cross Domain Solutions in Bandwidth-Constrained Environments

Challenge

Modern military operations increasingly rely on real-time data from a wide range of sources—surveillance cameras, sensors, partner networks, and mission systems. However, ships and tactical edge environments face severe bandwidth constraints, making it impractical to stream all data, particularly video to decision-makers operating on classified, high-side networks. Additionally, data must be trusted and validated to ensure mission-critical decisions—such as kinetic strikes—are based on accurate and complete information.

The Solution

To address evolving mission requirements and support timely, informed decisions, organizations are adopting a dual-AI architecture. This approach leverages edge-based AI on the low-side network for initial data processing, paired with a more advanced decision-support AI on the high-side network. The two environments are securely connected using a Cross Domain Solution (CDS), which enforces strict policy controls to ensure that data transfers between classification levels are secure and compliant.

However, a key challenge in maintaining the effectiveness of this architecture is model drift—the gradual decline in AI model accuracy as operational environments and data patterns change. This degradation can create vulnerabilities or degrade decision quality if not managed proactively.

Organizations are adopting dual-AI architectures with secure data transfer and real-time data validation to combat model drift, ensuring AI accuracy and security in dynamic environments.

Continuous training is required to keep models up-to-date and resilient. But selecting and validating training and test data is resource-intensive. Worse, without controls, adversaries could inject malicious data to poison the model, accelerating drift or manipulating outcomes.

To mitigate this, organizations can implement pre-screening mechanisms that validate incoming data in real time. By verifying the integrity and trustworthiness of data at the point of collection—ideally on the low side—you reduce the risk of training on compromised datasets. This not only improves security posture but also streamlines retraining cycles, ensuring models remain accurate without requiring massive resources.

Here's how it works:

AI on the Low Side (Edge)

Low-side AI models are embedded at the edge—on ships or forward-deployed systems—behind surveillance sensors or camera feeds. These models continuously analyze data locally and detect events of interest (e.g., a hijacking attempt or suspicious movement). Instead of streaming all video or sensor feeds, which would overwhelm the limited bandwidth, only the relevant data is flagged and queued for transfer.

Cross Domain Transfer

Once flagged, the data passes through a CDS. This ensures only validated, policy-compliant information crosses into the high-side network, mitigating risks such as data poisoning, compromised sensors/sources or accidental disclosure of sensitive sources. This "smart filtering" enabled by AI and enforced by CDS dramatically reduces unnecessary traffic while preserving mission-critical insight.

AI on the High Side (Core Decision-Making)

On the high side, AI models correlate incoming prioritized data from multiple domains—including coalition partners and unclassified networks—to generate decision recommendations. These models aid in decision making and can suggest target prioritization or risk assessments, but human operators retain control over final actions.

Impact

Bandwidth Optimization: AI at the edge ensures only urgent, relevant data is transmitted, preserving precious bandwidth while maintaining situational awareness.

Faster, Trusted Decisions: High-side AI models are only as good as the data they receive. CDS enables real-time ingestion of trusted, multi-domain data to improve decision speed and accuracy.

Security & Integrity: CDS validates data provenance, protecting high-side systems from corruption, spoofing, or unvetted inputs—key to maintaining trust in AI-generated insights.

Mission Enablement: This architecture empowers forces to act faster and smarter in environments where every second and byte matters.

Future Outlook

With growing interest from naval stakeholders, this architecture is actively advancing through pilot programs and technical evaluations. Shipboard teams are prioritizing AI-driven event detection and secure, CDS-enabled data transfer to enhance safety, accelerate collaboration, and strengthen command decision-making—particularly in contested and bandwidth-constrained environments such as the Indo-Pacific. These early deployments are shaping the next generation of mission-critical infrastructure, positioning Owl's cross-domain and diode solutions as foundational to secure, real-time information sharing at scale.

Executive Insight: Trusted AI at Mission Speed

Maximize AI ROI and mission impact by ensuring only validated, high-integrity data is used for model retraining—directly at the point of collection. Owl's cross domain solutions proactively defend against adversarial attacks and data poisoning, dramatically reducing retraining cycles and operational overhead. This approach keeps AI models accurate, resilient, and compliant with federal security standards—enabling faster, more trusted decision-making in bandwidth-constrained and high-threat environments.

OWL Cyber Defense™

Owl Cyber Defense Solutions, LLC, headquartered in Columbia, MD, is a pure play cybersecurity company solely focused on purpose-built, made-in-the-USA data diode and cross domain solutions. Trusted to protect the most sensitive government and commercial networks worldwide, our technologies are developed and manufactured to meet the strictest U.S. security standards. Owl enables secure, near-instantaneous collaboration across network boundaries—powering faster, safer, and smarter decisions for military, federal, and commercial critical infrastructure organizations. With a focus on scalability, interoperability, and regulatory compliance, Owl ensures resilient communication in the most high-threat environments. Rigorously tested. Globally trusted.

Visit **www.owlcyberdefense.com** or contact us at **info@owlcyberdefense.com** for more details.