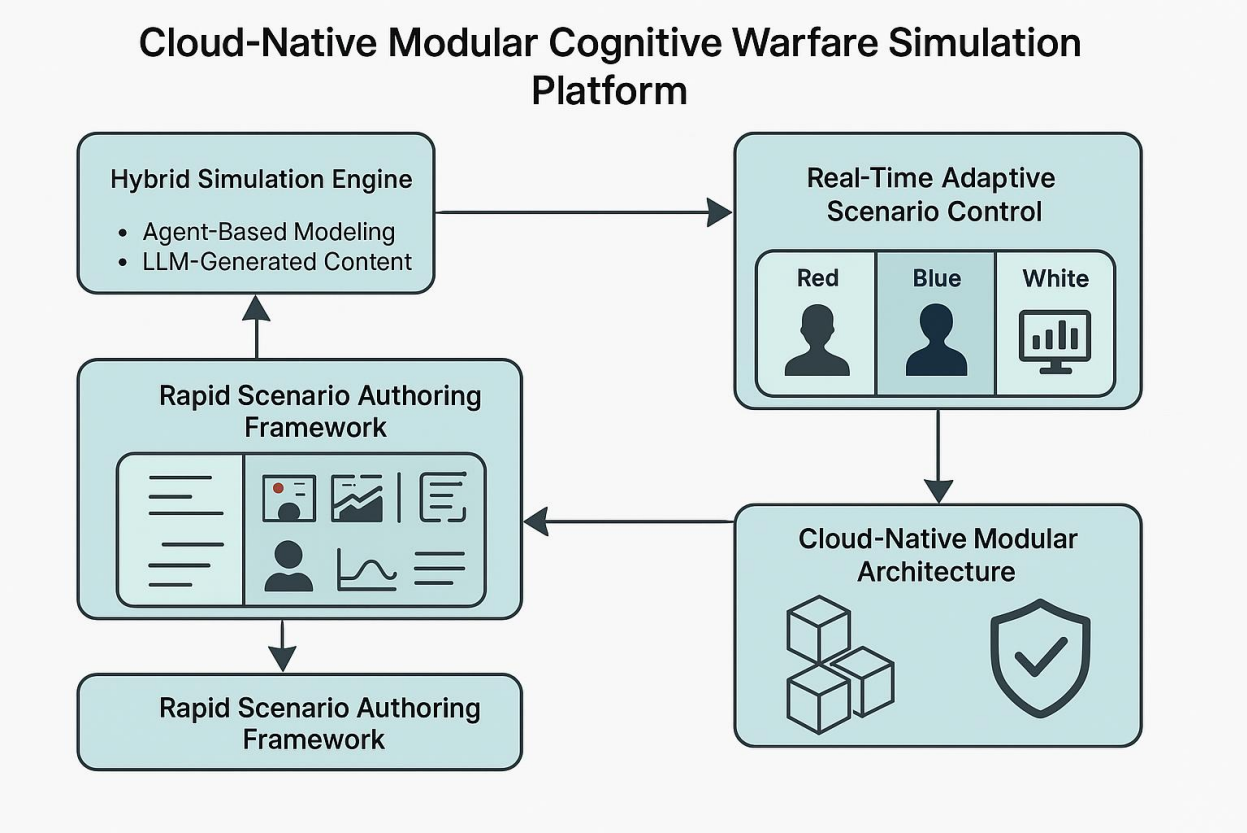
Cloud-Native Modular Cognitive Warfare Simulation Platform

Groundbreaker Solutions LLC
Author: Jason L. Lind (jason@groundbreaker.solutions)
Date: 23 April 2025

---

1. Introduction

Cognitive Warfare (CogWar) extends cyber warfare into the domains of perception and decision-making by leveraging techniques drawn from social engineering, game theory, and information manipulation to shape adversary behavior. This proposal addresses Navy SBIR Topic N252-110 by presenting a training platform that simulates cyber-attacks integrated with social media and influence operations. Traditional kinetic or cyber exercises do not capture the multifaceted nature of modern hybrid threats. Our solution delivers realistic, adaptive, and immersive multi-modal exercises for Red (adversary), Blue (defender), and White (control) teams.



---

2. Key System Components

2.1 Hybrid Simulation Engine

At the heart of the platform is a hybrid simulation engine that combines:

- **Agent-Based Modeling (ABM):** Simulating the behaviors, interactions, and decision-making processes of multiple entities including adversaries, defenders, and neutral actors. The ABM uses frameworks such as MITRE ATT&CK to define realistic tactics.
- **LLM-Driven Content Generation:** Real-time production of dynamic narrative content (social media posts, chat messages, news articles) that reflect the evolving simulation state. This ensures that every technical event is mirrored by a plausible information operation on social channels.

Together, these mechanisms create a synchronized simulation of cyber and social components that reinforce each other and offer an auditable chain-of-causality through after-action reviews.

2.2 Real-Time Adaptive Scenario Control

An RL-driven "game master" monitors trainee performance and the flow of events to modify the scenario in real time:

- **Dynamic Pacing:** The system can accelerate or decelerate events, introduce additional injects, or pause low-priority communications based on real-time feedback.
- **In-Exercise Hints and Injects:** Adaptive hints may be delivered to maintain optimal challenge levels without compromising scenario credibility. All decisions are logged to support later analysis.

2.3 Gamified Red/Blue/White Interfaces

- **Blue Team (Defenders):** Integrated dashboards displaying network alerts, threat intel feeds, and simulated social media narratives, requiring real-time cross-correlation of technical and human-centric cues.
- **Red Team (Adversaries):** Tools for initiating and managing cyber-attacks, generating misleading social media content, and monitoring defender actions.
- **White Cell (Control):** A central, comprehensive interface for exercise oversight, enabling manual event injection, scenario modification, and detailed event timeline review.

2.4 Cloud-Native Modular Architecture

The platform is built on a microservice architecture that:

- **Ensures Scalability and Flexibility:** Supports distributed, global training with seamless integration of components.
- **Implements Zero Trust Security:** Using robust mutual authentication and fine-grained access control.

- **Facilitates Rapid Updates:** Supports real-time scenario updates, new module integration, and minimal downtime.

---

3. Data Integration and Scenario Authoring

3.1 Hybrid Data Integration

A blended data strategy uses:

- **Live Data Feeds:** OSINT sources such as Twitter/X, Mastodon, cybersecurity logs, and RSS news feeds are ingested and mapped onto the simulation ontology.
- **Synthetic Data Generation:** LLMs augment real data with realistic narrative content that mirrors observed behaviors in real-world incidents. All content is annotated for provenance and designed to be fully auditable.

3.2 Scenario Framework and Authoring Tools

- **Structured Information Maneuver Framework:** Integrates elements from the MITRE ATT&CK framework and extended Cyber Kill Chain phases to map a complete sequence of attack steps.
- **Visual Authoring Toolkit:** Allows exercise planners to quickly assemble and customize scenarios using modular event blocks and pre-built templates. The tool supports the rapid creation of new scenarios and the dynamic swapping of Threat Model Packs to tailor adversary profiles.

---

4. Adaptive Cognitive Load and Data Audit

4.1 Adaptive Cognitive Load Management

The system actively monitors metrics indicating trainee stress:

- **Measurement of Interaction Metrics:** Scroll depth, dwell time, and decision latency are continuously tracked.
- **Dynamic Throttling:** When cognitive load is high, low-priority injects are deferred and critical alerts are highlighted, ensuring trainees focus on the most impactful actions.
- **Safety Interventions:** Integrated cool-down periods and resilience prompts are provided to help manage stress and improve overall learning.

4.2 Data Pipeline Compliance and Audit

- **Immutable Data Logging:** Cryptographic hashing and permissioned ledger technologies create an unalterable record of every event.
- **Full Transparency:** All automated decisions (including those by the RL controller) are fully traceable, meeting DoD compliance and ethical AI guidelines.

- **Content Moderation:** Constant validation through red-teaming and constrained decoding prevents inappropriate or off-script content from reaching trainees.

---

5. Detailed Multi-Modal Attack Scenario Descriptions

To fully exploit the platform's capabilities, we present multiple detailed attack scenarios that integrate technical exploits with information operations:

5.1 Targeted Phishing and Social Manipulation

Overview:
Adversaries launch a highly targeted spear-phishing campaign aimed at critical personnel. Emails are crafted using personal details gleaned from social media. In parallel, a coordinated misinformation campaign uses fake news and social media posts to create confusion about the attack's origin and intent.

Attack Flow:

- **Reconnaissance:** The attacker gathers detailed personal and professional data using OSINT techniques.
- **Phishing Deployment:** Spear-phishing emails, appearing as internal communications, are sent to target employees.
- **Social Media Amplification:** As initial intrusions occur, the attacker simultaneously seeds false narratives on platforms, suggesting insider sabotage or a larger covert campaign.
- **Defender Challenge:** Blue team members must quickly validate suspicious emails, correlate network anomalies, and discern legitimate alerts amid a flood of contradictory social media signals.
- **After-Action Analysis:** Logs from both the ABM and LLM modules allow review of how false social content impacted the detection timeline, emphasizing the need for integrated threat intelligence.

5.2 Insider Recruitment via Social Media

Overview:
Adversaries use social engineering on private online forums and encrypted messaging apps to target vulnerable employees. By manipulating personal grievances or ideological sympathies, adversaries recruit an insider to facilitate further compromise.

Attack Flow:

- **Initial Contact:** The attacker initiates seemingly benign conversations on niche forums and social networks.
- **Building Trust:** Through sustained interaction and exploitation of vulnerabilities (e.g., job dissatisfaction or ideological leanings), the attacker gradually builds a rapport with the target.

- **Insider Compromise:** Once the trust threshold is exceeded, the recruited insider is persuaded to provide access credentials or install malware.
- **Dual Channel Disruption:** Concurrently, a simultaneous misinformation campaign blurs the lines between external and internal threats.
- **Defender Challenge:** The Blue team must identify subtle behavioral shifts, monitor anomalous access patterns, and rapidly isolate the compromised account to stem further infiltration.
- **After-Action Analysis:** Detailed logs and simulated chat histories enable White Cell controllers to trace how insider recruitment contributed to downstream network compromises.

5.3 Ransomware Campaign with Public Pressure

Overview:
This scenario integrates a large-scale ransomware attack with a parallel public disinformation campaign. Attackers cripple essential systems while leaking falsified sensitive data designed to provoke public outrage and erode stakeholder confidence.

Attack Flow:

- **Ransomware Injection:** An initial ransomware attack encrypts core data assets and disrupts normal operations.
- **False Data Leak:** Simultaneously, fabricated internal emails and documents are released via social media, suggesting internal wrongdoing or incompetence.
- **Crisis Communications:** The public disinformation effort magnifies the disruption by fueling panic among stakeholders and eroding trust.
- **Defender Challenge:** The Blue team must engage in technical remediation—isolating systems, restoring backups—while also coordinating a counter-disinformation campaign through official media channels.
- **After-Action Analysis:** Performance metrics assess how quickly the team identified and contained both the ransomware spread and the misinformation, with lessons learned to enhance dual-channel response capabilities.

5.4 Supply Chain Compromise and Coordinated Malware Propagation

Overview:
This scenario emulates an attack where adversaries compromise a trusted third-party supplier to infiltrate multiple targets simultaneously. A misinformation component complicates attribution, as misleading evidence is distributed to direct blame and obscure the supply chain’s role.

Attack Flow:

- **Compromise Initiation:** Attackers insert malicious code into a software update distributed by a trusted vendor.
- **Propagation Mechanism:** The compromised update is installed across multiple organizations, embedding a dormant malware payload.
- **Misinformation Initiation:** Concurrently, adversaries use social media to disseminate conflicting reports about the breach's origin, including fabricated evidence that implicates innocent third parties.
- **Defender Challenge:** Blue team members must verify the integrity of software updates, coordinate with vendors to isolate the breach, and disambiguate the conflicting intelligence reports.
- **After-Action Analysis:** The simulation's audit logs help track the propagation timeline and validate how misinformation delayed the incident response, informing improvements in supply chain security protocols.

5.5 Fake News and Deepfake Disinformation

Overview:
Leveraging advanced AI techniques, adversaries create highly convincing fake media, including deepfakes of executive statements and doctored images. The campaign aims to damage reputation and destabilize internal decision-making processes.

Attack Flow:

- **Media Fabrication:** Adversaries produce deepfake videos and altered images that portray leadership in compromising scenarios.
- **Viral Distribution:** These media items are released via social networks and quickly picked up by less vetted news sources.
- **Public Reaction:** The rapid spread of the deepfakes creates temporary public panic and internal confusion.
- **Defender Challenge:** Blue team and public affairs personnel must validate media authenticity using forensic tools, counteract the disinformation with verified evidence, and communicate accurate narratives to the public.
- **After-Action Analysis:** The ability to cross-reference deepfake detection outputs with event logs reinforces the need for robust multimedia verification protocols in crisis management.

5.6 Critical Infrastructure Sabotage with Social Diversion

Overview:
This scenario targets cyber-physical systems controlling critical infrastructure. Prior to launching the attack, adversaries inundate the information channels with false emergency reports to distract defenders from the impending operational disruption.

Attack Flow:

- **Diversion Tactics:** Just before the cyber-physical breach, adversaries initiate a wave of sensationalized social media reports—either fabricated emergency events or irrelevant crises—to distract attention.
- **System Breach:** Under the cover of misinformation, malware is deployed to target systems such as power grids or water treatment facilities.
- **Simultaneous Response:** Blue teams face the dual challenge of filtering out diversionary content while quickly reacting to the actual infrastructure breach.
- **After-Action Analysis:** Detailed mapping of the injection and response times across technical and social platforms helps calibrate future scenarios aimed at improving rapid threat prioritization.

6. Development Phases

6.1 Phase I: Technical Feasibility

- **Use Case Definition:** Select and implement a prototype scenario (e.g., coordinated DDoS with social media recruitment).
- **Prototype Development:** Build a foundational simulation engine that integrates key aspects of ABM and LLM-driven narrative generation.
- **Interface Prototyping:** Develop initial dashboards for Blue and White cells to visualize evolving scenarios.
- **Preliminary Testing:** Execute controlled pilots to measure system performance and refine data logging.

6.2 Phase II: Prototype Enhancement

- **Expand Scenario Catalog:** Create and refine multiple detailed attack scenarios to form a comprehensive library.
- **Enhanced Data Modeling:** Fine-tune AI models using larger datasets and custom threat packs to generate realistic content.
- **Full Adaptive Control:** Deploy a robust RL-based controller capable of dynamic, multi-lever adaptation.
- **Advanced Authoring Tools:** Develop a complete suite for scenario construction and white cell oversight.

- **Live Demonstration:** Validate the end-to-end system through live, virtual, constructive (LVC) exercises and gather detailed performance metrics.
- **Documentation and Transition:** Finalize system documentation and prepare for operational deployment and dual-use applications.

7. Commercialization Potential

Dual-Use Market Strategy

- **Target Markets:** Commercial sectors such as finance, healthcare, critical infrastructure, and other government agencies.
- **Business Models:** Deployment via SaaS subscriptions, on-premises installations, and Training-as-a-Service offerings.
- **Value Proposition:** Realistic, adaptive training that improves incident response, enhances cross-team coordination, and reduces the impact of real-world threats by simulating the intricate dynamics of modern cyber and informational warfare.

---

8. Conclusion

The proposed cloud-native cognitive warfare simulation platform meets the Navy's urgent need for realistic, multi-modal training against hybrid cyber and information threats. By integrating an agent-based simulation engine, AI-driven narrative generation, and dynamic adaptive controls with dedicated interfaces and a modular cloud architecture, the platform delivers a "train as you fight" experience with unprecedented fidelity. Detailed attack scenarios further prepare defenders for the complexities of real incidents. With built-in cognitive load management, robust auditing, and strong ethical safeguards, this platform not only enhances military readiness but also holds significant dual-use potential in the commercial cybersecurity landscape.

Based strictly on your attached resume, here is a **one-page resume tailored for the Cloud-Native Modular Cognitive Warfare Simulation Platform SBIR submission**:

Jason L. Lind
Chief Architect | Cognitive Warfare Specialist

Professional Summary

Innovative software architect and defense technologist with 20+ years leading the design of secure, scalable systems for cognitive warfare simulation, blockchain-based governance, and AI-powered training environments. Recognized for delivering high-fidelity, multi-modal cyber-physical platforms that combine agent-based modeling, LLMs, microservices, and adaptive UIs. Proven track record architecting SBIR-backed, DoD-aligned simulation frameworks that integrate narrative generation, decentralized command, and zero-trust compliance.

Relevant Experience

President / Chief Architect
Groundbreaker Solutions LLC — *Dec 2023–Present*

- Lead architect of SBIR-funded projects for DoD modernization, including real-time cognitive warfare simulations and blockchain-enabled supply chain security.
- Designed AI-driven ABM frameworks for sentiment and narrative modeling using LLMs, Hofstede dimensions, and drama theory.
- Spearheaded Phase I & II proposals and implementation for adaptive, multi-modal cyber and information training systems.
  Skills: AI, LLMs, Architecture, SBIR, Smart Contracts, Zero Trust, Blockchain

Founder / Chief Architect
UNofficial CYBERCOM — *Dec 2023–Present*

- Engineered decentralized cybersecurity governance using Ethereum-based DAOs and Solidity smart contracts.
- Developed Red/Blue/White governance interfaces using Blazor Server, React, and MobX for real-time ops.
  Skills: DAO, Web3, Blockchain, React, SignalR, Nethereum

Freelance Architect
United States Space Force — *Dec 2023–Mar 2025*

- Overhauled legacy ASP.NET MVC app tracking weather balloon instrumentation.
- Introduced SignalR and Postgres-based integration for real-time data aggregation and monitoring.
  Skills: .NET Core, Postgres, SignalR, MVC, DoD Compliance

Core Technologies

- **Simulation & AI**: Agent-Based Modeling, ChatGPT, ReactiveUI, Delphi.ai
- **Architecture**: Blazor, .NET Core, ASP.NET, Microservices, UML/BPMN
- **Data & DevOps**: CosmosDB, Postgres, Azure Functions, CI/CD (GitHub Actions)
- **Cybersecurity**: Smart Contracts, DAO, Zero Trust, Ethereum, Solidity