Sciences Methods and Technologies International Journal (SciMeTech)

ISSN: 3085-5284, journal homepage: www.scimetech.com

Quasi-Symbiotic Domain Warfare: The Orbro Protocol A Low-Observable Defense Framework for AI-Saturated Threat Environments

Nicholette Lindsay
FLUX|NteL, Austin, TX, USA
FluxNteL@outlook.com

How to cite:
Nicholette Lindsay, "Quasi-Symbiotic Domain Warfare: The Orbro Protocol A Low-Observable Defense Framework for AI-Saturated Threat Environments", Sciences Methods and Technologies International Journal (SciMeTech), Vol 2, Issue 1, p 203-206

Keywords:
Symbiotic Domain Warfare
Quasi-Symbiotic Defense
Recurrent Palindromic Neural Network
Adversarial Machine Learning
Bio-Frequency Authentication
LEO Satellite Security
Low-Observable Cyber Operations
GAN-Based Cyber Threats
AI-Native Threat Detection

Abstract

Contemporary cybersecurity doctrine is fundamentally reactive, depending on anomaly detection against a known baseline. This model is collapsing in AI-saturated environments where synthetic data constitutes the atmospheric norm and adversarial signals are architecturally indistinguishable from legitimate ones. This paper introduces Symbiotic Domain Warfare (SDW): a doctrinal framework in which defense systems engage adversarial signals through deceptive co-occupation rather than exclusion. The Quasi-Symbiotic variant is operationalized through the Orbro Protocol, a recursive, self-validating security architecture whose core engine is the Recurrent Palindromic Neural Network (RPNN). The RPNN enforces a palindromic integrity condition over a temporally symmetric hash window and introduces an Adversarial Reflection Mechanism that appears cooperative to attacking models while forcing recursive computational exhaustion. A Low-Observable infrastructure layer, the Aethernox Lattice, distributes verification compute across non-terrestrial LEO orbital nodes, minimizing the defense system's detectable signature. Finally, the Skylink Nodule provides a bio-frequency-anchored cryptographic interface, replacing static multi-factor authentication with a dynamic, non-synthesizable physiological signal key derived from cardiac rhythm variability, galvanic skin response, and neural oscillation data. Together, these components constitute a baseline defense standard for post-kinetic AI-saturated threat environments, advancing the field from Defended Networks toward Symbiotic Domain Systems.

I. Introduction

For three decades, the dominant model of cybersecurity operated on a single implicit assumption: that normal is knowable. Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) platforms, and behavioral analytics engines all share this foundational premise—establish a baseline, monitor for deviation, and respond to the outlier. That assumption is no longer valid.

The widespread deployment of generative adversarial networks, large language models, and autonomous offensive AI agents has produced a new threat class: the synthetic-native adversarial signal. These attack vectors are not merely disguised as normal traffic—they are, by architectural design, statistically indistinguishable from it. A GAN-generated probe does not deviate from baseline; it defines a new one. A language model conducting a social engineering campaign does not violate behavioral norms; it exploits them with unprecedented precision [1, 2].

This is the condition we term **Symbiotic Domain Warfare (SDW)**: a threat environment in which adversarial and legitimate systems co-occupy the same computational domain in a state of apparent mutual coexistence. The adversary does not attack the perimeter—it inhabits the interior, parasitically consuming trust relationships and signal infrastructure while remaining statistically invisible. The Orbro Protocol operationalizes a Quasi-Symbiotic response through three integrated components: a computational engine that reflects adversarial energy back at its source, an infrastructure layer that minimizes its own detectable presence, and a human authentication interface that anchors identity to a living, non-synthesizable signal.

II. Methods

The Orbro Protocol is structured around three tightly integrated technical components, each addressing a distinct layer of the Symbiotic Domain Warfare problem.

A. Quasi-Symbiotic Engagement: The RPNN Architecture

The core computational engine of the Orbro Protocol is the Recurrent Palindromic Neural Network (RPNN)—an architecture designed to operationalize the Quasi-Symbiotic doctrine at the signal processing level. The RPNN operates over a bidirectional recurrent layer with hidden state h, producing forward and backward passes across a temporally symmetric window $W = [t , ..., t , ..., t]$ of length $2k+1$. The palindromic hash function φ computes a temporally symmetric integrity

$-k \quad 0 \quad +k$ digest:

$\varphi(S, W) = \Sigma \alpha \cdot g(H)$ *where* $\alpha = \alpha$ *(palindromic weight symmetry)* $t \quad t \quad t \quad -t$

This constitutes the Signal Integrity Condition (SIC): a signal S is sovereign if and only if its palindromic digest is invariant under temporal reversal. When a signal fails the SIC, the Adversarial Reflection Mechanism (ARM) activates, generating a phase-inverted response $S = \Psi(S)$ such that $\varphi(S , W) = \varphi(S , W)$ and $||S || >> ||S ||$. This forces the adversarial model into a r a r a r 2 a 2

computationally exhausting recursive loop—what we term the *Mute*. Existing deception defenses such as honeypots [3] and Moving Target Defense [4] attract or redirect adversaries; the RPNN consumes them within the live signal space itself.

• B. Low-Observable Infrastructure: The Aethernox Lattice

The Aethernox Lattice distributes RPNN verification compute across non-terrestrial orbital nodes integrated with low-Earth-orbit (LEO) satellite mesh networks. By relocating the verification layer to orbital infrastructure, the Lattice achieves four properties terrestrial Edge cannot match: Physical Interdiction Resistance, Jurisdictional Sovereignty, Electromagnetic Hardening, and Dynamic Topology. LEO constellation bandwidth has crossed the threshold required for sub-100ms round-trip verification latency in high-priority signal integrity checks [5], validating this as an operationally viable overlay network. The Quasi-LO designation acknowledges that some operational signature is unavoidable in active defense, while minimizing it to the greatest extent architecturally feasible—extending Moving Target Defense insights [6] to the physical infrastructure layer.

• C. Non-Synthesizable Authentication: The Skylink Nodule

The Skylink Nodule replaces static multi-factor authentication with a wearable bio-frequency interface anchoring cryptographic identity to a live physiological signal. The Nodule harvests a composite bio-frequency vector $\beta(t) \in R^m$ from cardiac rhythm variability (CRV), galvanic skin response modulation (GSR), and neural oscillation envelope data (NOE). The cryptographic key $K(t) = H(\beta(t) || nonce(t))$ is non-replayable because $\beta(t)$ is non-stationary—it changes with physical activity, stress state, and circadian rhythm. Deepfake biometric bypass attacks have demonstrated that static credentials—facial geometry, fingerprint, voice—are synthesizable given sufficient adversarial resources [7, 8]. A bio-frequency key resists synthesis not because it is complex, but because it is alive. The Nodule also performs continuous duress monitoring: if $D(\beta(t), \beta) > \theta$, the Hard Mute Protocol severs all uplinks and seals active sessions. Hardware lineage for the wearable platform is avg

established by Chuang et al. [9], Barki et al. [10], Lewis et al. [11], and the OmniBuds platform [12].

III. Results and Discussion

The Orbro Protocol is presented as a theoretical architecture—a formal specification preceding empirical validation, consistent with the established tradition of architectural proposals in adversarial ML defense research [1, 2, 3]. The palindromic integrity condition is computationally tractable: the SIC check adds $O(k)$ operations per signal relative to standard bidirectional RNN inference.

Under simulated conditions grounded in the GAN-based attack model of Dunmore et al. [1] and Macas et al. [2], consider an adversarial model A generating probes $P ...P$ against a target protected by the RPNN. Each detected probe P triggers Mute response $M = \Psi(P)$. Because $||M || >> ||P^1 ||^n$, the cost of each follow-on probe grows with each iteration—depleting A's^i i i i 2 i 2 resource budget at an exponential rate relative to the linear cost of generating Mute responses. A Muted adversarial model yields more intelligence than a blocked one: attack trajectory data, model architecture signals, and resource exhaustion metrics.

The Aethernox Lattice's Quasi-LO posture extends MTD's dynamic topology insight [6] to the physical substrate—a dimension prior MTD implementations operating on terrestrial fixed infrastructure cannot achieve. The Skylink Nodule advances the hardware lineage of earable biosignal platforms [9, 10, 11, 12] into a cryptographic key derivation pipeline, a novel application not addressed by any existing platform.

Future work will focus on: (1) full empirical validation of the RPNN on standard adversarial ML benchmarks (NSL-KDD,

UNSW-NB15, CICIDS) against Defense-GAN [13] and MTD ensemble baselines [4]; (2) hardware prototyping of the Skylink Nodule's bio-frequency interface; and (3) latency characterization of the Aethernox Lattice under operational LEO constellation conditions.

IV. Conclusion

The adversarial landscape has crossed a threshold. Symbiotic Domain Warfare names the new condition with precision: the adversary inhabits the defended domain, co-occupying computational space in a state of apparent normalcy that renders anomaly-based detection structurally obsolete. The Orbro Protocol responds with a doctrine of deceptive counter-occupation—its three pillars (RPNN, Aethernox Lattice, Skylink Nodule) address the problem at the level it actually exists, advancing cybersecurity from Defended Networks to Symbiotic Domain Systems. The threat is intelligent, recursive, and fluid. The defense must inhabit it back—deceptively, invisibly, and with the irreducible advantage of being alive.

"We are not building a wall. We are becoming the frequency the wall cannot touch." — Orbro Protocol Design Principle

References

[1] Dunmore, A., Kim, J., Thabtah, F., & Lu, J. (2023). A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3296707

[2] Macas, M., Wu, C., & Fuertes, W. (2024). Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecuritysystems. *Expert Systems with Applications*, 238, 122223.

[3] Zibaeirad, A., et al. (2025). Adversarial Defense in Cybersecurity: A Systematic Review of GANs for Threat Detection and Mitigation.arXiv:2509.20411.

[4] Walter, E., Ferguson-Walter, K., & Ridley, A. (2021). Incorporating Deception into CyberBattleSim for Autonomous Defense.arXiv:2108.13980.

[5] Yue, S., et al. (2024). On the Security of LEO Satellite Communication Systems. *IEEE Journal on Selected Areas in Communications*.

[6] Li, C., Sun, X., & Zhang, Z. (2021). Satellite Network Security Mechanism Based on Blockchain Technology. *IEEE Access*, 9, 113558–113565.

[7] Lei, C., et al. (2018). Moving Target Defense Techniques: A Survey. *Security and Communication Networks*. https://doi.org/10.1155/2018/3759626

[8] ISACA. (2024). Examining Authentication in the Deepfake Era. White Paper.

[9] Springer Nature / Cognitive Computation. (2025). Generative AI and Deepfake Detection in Biometric Systems.https://doi.org/10.1007/s12559-025-10469-3

[10] Chuang, J., Curran, M. T., Merrill, N., & Gandhi, S. (2019). One-Step, Three-Factor Passthought Authentication With Custom-Fit,In-Ear EEG. *Frontiers in Neuroscience*, 13, 354.

[11] Barki, H., Mai, N.-D., & Chung, W.-Y. (2025). Optimized XGBoost for Multimodal Affective State Classification Using In-Ear PPGand Behind-the-Ear EEG Signals. *IEEE JBHI*.

[12] Lewis, D., et al. (2023). Soft Smart Biopatch for Continuous Authentication-Enabled Cardiac Biometric Systems. *Advanced Sensor Research*.

[13] Montanari, A., et al. (2024). OmniBuds: A Sensory Earable Platform for Advanced Bio-Sensing and On-Device Machine Learning.arXiv:2410.04775.

[14] Samangouei, P., Kabkab, M., & Chellappa, R. (2018). Defense-GAN: Protecting Classifiers Against Adversarial Attacks UsingGenerative Models. arXiv:1805.06605.

[15] Tahayori, K., et al. (2025). HybridMTD: Enhancing Robustness Against Adversarial Attacks with Ensemble Neural Networks andMoving Target Defense. SCITEPRESS.

[16] Li, T., & Zhu, Q. (2024). Symbiotic Game and Foundation Models for Cyber Deception Operations in Strategic Cyber Warfare.arXiv:2403.10570.

[17] Putrevu, V. S., et al. (2024). ADAPT: Adaptive Camouflage Based Deception Orchestration For Trapping Advanced Persistent Threats.ACM.

[18] Wang, Z., et al. (2025). HoneyGPT: Breaking the Trilemma in Terminal Honeypots with Large Language Model. arXiv:2406.01882.
[19] Hussain, I., Aldwairi, M., & Wani, A. (2025). A Dynamic AI-Powered Honeypot Framework for Adaptive Cyber Threat Diversion.IEEE CSNet.
[20] Sengupta, S., Chakraborti, T., & Kambhampati, S. (2019). MTDeep: Boosting the Security of Deep Neural Nets Against AdversarialAttacks with Moving Target Defense. arXiv:1705.07213.
[21] Masse, G. C. T., et al. (2025). Deception-Based Defense Against Model Poisoning Attacks in Federated Learning Using GAN. IEEEICC.
[22] ENISA. (2024). Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment. European Union Agency for Cybersecurity.
[23] Zhang, T., et al. (2025). Moving Target Defense Meets Artificial-Intelligence-Driven Network: A Comprehensive Survey. *IEEE Journal of IoT*.
[24] Kozina, A., Galinec, D., & Steingartner, W. (2021). Threat Defense: Cyber Deception Approach and Education for Resilience in HybridThreats Model. *Symmetry*, 13(4), 597.
[25] Hong, M., Jiang, D., et al. (2026). Vulnerabilities of Audio-Based Biometric Authentication Systems Against Deepfake SpeechSynthesis. arXiv:2601.02914.