LOCH TECHNOLOGIES

Trusted AI Countermeasures

CAPABILITIES STATEMENT

1285 66th Street,
Emeryville, CA 94608
www.loch.io
Company Tel : 888-725-9434

Primary Contact:
Garry Drummond, CISSP, CWNA, CWSP
Direct Tel: 510-703-6149
gdrummond@loch.io

The Impact of AI/ML on Advanced Command and Control and the Rising Cyber Threats

Revolutionizing Cyber Protection of AI/ML Algorithms with Resilient Machine Learning Systems (rMLS)

The recent advances in Artificial Intelligence (AI) and machine learning (ML) algorithms drive the proliferation of data-driven intelligent applications in many areas including advanced command and control (AC2) missions, decision support systems, recommender systems, computer vision, autonomous vehicles, as well as intrusion detection and prevention systems. Many AI/ML algorithms have been integrated in decision support applications to improve analysis performance and prediction. Due to the wide-spread usage of AI/ML in critical decision processes (e.g., DoD AC2 mission critical applications), there is an exponential growth in cyberattacks that target the AI/ ML algorithms and consequently influence their decision process in favoring of the attackers.

Differentiators

- **Resilient Machine Learning Systems (rMLS):** The use of Moving Target Defense (MTD) dynamically changes the machine learning algorithms, making it difficult for attackers to target specific models.
- **Focus on Securing AI/ML Systems:** Instead of using AI/ML solely for building cybersecurity solutions, LOCH focuses on protecting AI/ML algorithms themselves from adversarial attacks, ensuring resilient AI operations in critical environments like defense, autonomous systems, and cyber infrastructure.
- **Broad Market Application:** The rMLS technology is targeted for both DoD mission-critical applications (e.g., Advanced Command and Control, UAS, Satellite systems) and commercial markets (e.g., smart cities, utilities, and transportation).
- **Emerging Threats from Large Language Models (LLMs):** The technology addresses the risks posed by LLM-based attacks, such as those from GPT-4 and BERT, making it uniquely equipped to defend against sophisticated AI-driven cyberattacks.
- **Strategic Partnerships and Funding:** LOCH Technologies, has already secured $1.8M from the Air Force Research Laboratory (AFRL) to develop this cutting-edge solution, showcasing strong industry partnerships and government backing.

PAST PERFORMANCE $15M FOR CYBERSECURITY

1. AFRL Direct to Phase II ($1.8M), Resilient Adversarial Machine Learning, Starting Date: August 2024.
2. NAVY SBIR Phase II ($1.8 M) (August 22- July 2025) – Autonomous Protection for Unmanned Maritime Autonomous Architecture (UMAA)Services.
3. US Air Force: Department of Defense $5M contract (April 2023 – April 2024) for Enhanced Cybersecurity Sensors to detect threats in near and far field emissions.
4. US Army Phase II ($2 M) (November 2019- December 2021) – Tactical Cyber Immune System
5. AFRL and US Army STP Project ($1.5 M) (Nov 2019- Nov 2021) – Autonomic Security Operations Center (ASoC) for OT and Industrial Control Systems.
6. US Army Materiel Command (AMC) project ($400K) to develop a commercial product, AMC Security Operations Center as a Service (AMCaaS).
7. US Navy SBIR Phase I and Option Phase ($237K, starting July 2021- October 2022): Autonomic Protection for Unmanned Maritime Contract Number: N68335-21-C-0555.
8. US Army CERDEC STTR Phase II ($1M, December 2019- December 2021): Tactical Cyber Immune System.).
9. US AFRL and Army Technology Transition Project ($1.5 M, September 2019- September 2021): Autonomic Security Operations Center (ASoC).
10. AFRL SBIR Phase II ($750K, Sep. 2016 – Nov. 2018): Autonomic Monitoring, Analysis and Mitigation (AMAP), Contract Number: FA8750-17-C-0279
11. ONR STTR Phase I ($150K, Jun. 2018 – Dec. 2018): Multi-Layer Mapping of Cyberspace - Contract Number: N68335-18-C- 0416
12. USA CERDEC STTR Phase I ($150K, Aug. 2016 – Feb. 2017): Tactical Cyber Immune System (TCIS), Contract Number: W56KGU-16-C-0065

LOCH TECHNOLOGIES

Trusted AI Countermeasures

CAPABILITIES STATEMENT

1285 66th Street,
Emeryville, CA 94608
www.loch.io
Company Tel : 888-725-9434

Primary Contact:
Garry Drummond, CISSP, CWNA, CWSP
Direct Tel: 510-703-6149
gdrummond@loch.io

The Impact of AI/ML on Avanced Command and Control and the Rising Cyber Threats

Core Competencies

- **Moving Target Defense (MTD):** rMLS uses dynamic and constantly evolving machine learning algorithms to prevent attackers from exploiting known vulnerabilities. By frequently altering the internal models, rMLS creates an unpredictable environment, which makes it challenging for adversaries to understand and target the system.
- **Resilience to Adversarial Attacks:** A core feature of rMLS is its ability to detect, withstand, and recover from adversarial AI/ML attacks. The system ensures continued operation even under attack by adapting to threats in real-time, thus minimizing the impact on decision-making processes.
- **Real-Time Adaptability:** rMLS systems are built to adapt instantly to potential threats without interrupting their operations. This adaptability ensures that critical AI/ML systems, such as those used in defense or critical infrastructure, continue to function effectively, even when targeted by cyberattacks.
- **Cross-Domain Application:** rMLS technology can be applied across various industries and domains, including defense, autonomous systems, smart cities, and critical infrastructure. This flexibility makes it a versatile solution for protecting mission-critical applications in both military and commercial environments.
- **Protection Against Advanced AI/ML Threats:** As AI/ML technologies evolve, so do the types of attacks, including those that target large language models (LLMs) and advanced decision-making systems. rMLS incorporates countermeasures to mitigate these emerging threats, ensuring that AI/ML models remain secure in increasingly complex environments.
- **Autonomous and Self-Healing Capabilities:** rMLS systems are designed to autonomously recognize, respond to, and recover from cyberattacks without the need for manual intervention. These self-healing capabilities are critical for maintaining uptime and ensuring the continued reliability of AI/ML systems.

Vendor Information

- GSA # G535F01454
- CAGE # 92U44
- SAM # FZPXBVF4UPB
- CMMC #
- NIST #
- DUNS # 05414-6235
- NAICS -541514,541512, 511210, 423430,

Patents

- Access Security by Interrogation - # 10,257,226
- Access Security by Interrogation - # 10,764,755.00
- P25 Trunked Radio Vulnerability Management -# 10,999,309
- Zero Trust for Wireless Security - # 11.540,130
- RF Security by Interrogation - # 10,764,755
- Real-Time Interference Monitoring -# 11,595,429
- Behavior Based Monitoring for Radio Frequency - # 11,716,623
- Vulnerability Management, Real-Time Interference - # 11,936,680