

# Researchers develop quantum-inspired algorithm that improves cyber attack detection and opens AI's 'black box'

*Multiverse Computing and cybersecurity experts CounterCraft develop explainable AI model that can spot known and unknown attacks*

SAN SEBASTIÁN, SPAIN, March 26, 2024 /EINPresswire.com/ -- Researchers from [Multiverse Computing](#), a global leader in value-based quantum computing solutions, and CounterCraft, global leaders in deception-powered threat intelligence, have built a new quantum AI model that significantly improves attack detection over traditional methods. Trained on datasets from actual network traffic and system logs, the Matrix Product State (MPS) model identified 100% of attacks.



# Counter Craft

The MPS methodology employs adversary-generated threat intelligence instead of traditional rule-based systems to identify cyberattacks. This approach provides improved interpretability and clear insights into anomalies identified by the algorithm. Continuously advancing this model and enhancing its interpretability capabilities will pave the way for its real-world application in the near future, according to the researchers.

CounterCraft analysts had already identified the attacks within the training data, which provided a benchmark for evaluating the performance of Multiverse's new model. The model is described in a new paper submitted to arXiv: "[Tensor Networks for Explainable Machine Learning in Cybersecurity.](#)"

The model excels in reducing false positives with greater precision as compared to the majority of classical models, including isolation forest, one-class SVM and variational encoders. At the same time, the MPS model improved the explainability of the algorithm's results, an increasingly important capability for business users and regulators, according to the researchers.



The ability to detect unknown attacks both inside and outside the network is vital for early detection and response.”

*David Barroso, CounterCraft  
CTO and co-founder*

“Explainable AI supports robust decision-making by providing clear explanations for outcomes, while improving understanding of threats and ensuring compliance with increasingly stringent transparency regulations,” said Roman Orus, Chief Scientific Officer at Multiverse Computing and an author of the paper. “Our work with CounterCraft shows how quantum techniques can strengthen cybersecurity defenses against today’s threats and future ones while improving explainability.”

A cyber attack is generally not a single event but a series of 20-80 individual events. The MPS model identified 83.5% of these steps as well as finding several steps missed in the classical analysis.

The training data for this model from CounterCraft contained detailed incident reports covering various attack types, such as weak credential usage and exploits of known vulnerabilities. The model was trained to tell the difference between normal behavior and abnormal behavior, enabling it to identify attacks.

“We provide total visibility into an attackers' tactics and techniques to help customers anticipate and understand the strategies used by cyber adversaries, and this new model based on tensor networks will improve those capabilities,” said David Barroso, CounterCraft CTO and co-founder. “The ability to detect unknown attacks both inside and outside the network is vital for early detection and response and is one of CounterCraft's strengths.”

The model also creates synthetic data which can be used for training models and to simulate activity for deception strategies.

The software also includes a user-friendly risk tolerance slider so security analysts can adjust the sensitivity of the threat detection to their requirements. This ensures a high detection rate with a manageable number of alerts.

This work lays the foundation for future research in cybersecurity and quantum software. Next steps for the research could include robust testing to enhance the model’s effectiveness in diverse scenarios. The initial use case was cybersecurity, but this model can enhance anomaly detection across finance, healthcare, government, critical infrastructure, manufacturing and retail.

About CounterCraft

CounterCraft is a leading provider of deception-powered threat intelligence solutions that

empower organizations to proactively defend against cyber threats. CounterCraft's sophisticated deception technology offers full visibility into adversaries' tactics, techniques, and procedures. CounterCraft enables organizations to detect threats early, collect specific and actionable threat intelligence, stop threats before breach and defend their valuable data in real time. Their Gartner-recognized, award-winning technology and innovative approach to cybersecurity has keeping Fortune 500 companies and government agencies safe from cyber attacks since 2015. Discover how CounterCraft is redefining cybersecurity with intelligence-driven defense at [www.countercraftsec.com](http://www.countercraftsec.com).

#### CounterCraft Media Contact

Marti Buckley  
mbuckley@countercraftsec.com  
+34 943 122 320

#### About Multiverse Computing

Multiverse Computing is a leading quantum software company that applies quantum and quantum-inspired solutions to tackle complex problems in finance, banking, manufacturing, energy, and cybersecurity to deliver value today and enable a more resilient and prosperous economy. The company's expertise in quantum algorithms and quantum-inspired algorithms means it can secure maximum results from current quantum devices as well as classical high-performance computers. Its flagship product, Singularity, allows professionals across all industries to leverage quantum computing to speed up and improve the accuracy of optimization and AI models with existing and familiar software tools. The company also has developed CompactifAI, a compressor which uses quantum-inspired tensor networks to make AI systems such as large language models more efficient and portable. In addition to finance and AI, Multiverse serves enterprises in the mobility, energy, life sciences and industry 4.0 sectors. The company is based in San Sebastian, Spain, with branches in London, Toronto, Paris and Munich. For more information about Singularity and CompactifAI, contact Victor Gaspar at [victor.gaspar@multiversecomputing.com](mailto:victor.gaspar@multiversecomputing.com)

#### Multiverse Computing Media Contact

Veronica Combs  
veronica@hkamarcom.com  
812-987-6076

Christian Balzora  
HKA  
+1 714-422-0919  
[email us here](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/698902114>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.