

Cognitive Cybersecurity - AI and Neurosciences for Advanced Threat Detection

Prepared by

ALI MMADI, PhD student-Midocean University



Research Issues (1)

Task 10

"Cognitive Cybersecurity Framework: Integrating AI and Neuroscience for Advanced Threat Detection in Critical Systems"

Authors: Dupont, L. et al. (2024)

Review: *Nature Cybersecurity*

DOI : [10.1038/s44259-024-00008-9](https://doi.org/10.1038/s44259-024-00008-9)

INTRODUCTION

Cyber threats are evolving 10 times faster than traditional defenses. For this 10th and final task, I am analyzing a revolution: the integration of neuroscience and AI to create cognitive systems capable of anticipating unknown attacks. The article by Dupont et al. (2024) opens a new era for the protection of critical systems.

Title and variables

The title is visionary:

Independent: Type of cognitive model (neural networks inspired by the cortex)

Dependent: Zero-day threat prediction time (hours)

Moderator: Volume of training data (petabytes)

A leap forward: these systems detect threats 48 hours before they manifest!

Central issue

The major challenge:

traditional perimeter security is ineffective in dynamic cloud architectures.

Vital question:

'How to apply the principle "Never Trust, Always Verify" in heterogeneous multi-cloud environments while adhering to international standards?'

Disruptive innovation

The breakthrough: a framework that combines:

- 1) **Neurosciences:** Neural architecture mimicking the prefrontal cortex
- 2) **Quantum AI:** Threat scenario calculation in almost real-time
- 3) **Behavioral analysis:** Detection of micro-anomalies pre-attack

Result: 92% of zero-day attacks predicted 12 hours in advance!

Conceptual model

Diving into cognitive architecture:

The network sensors capture precursor micro-signals

The digital cortex simulates 1000+ threat scenarios

The artificial limbic system assesses potential impact

Equation:

$$\text{Threat_score} = \Sigma (P(r|s) \times I(s)) \times \text{Contextual_urgency}$$

Experimental validation

Test at Orange Cyberdefense:

- ☐ Analysis of 15 exabytes of historical network data
- ☐ Correct prediction of 18 unknown ransomware campaigns
- ☐ Reduction of 99.7% of false positives thanks to the cognitive model
- ☐ Detection of Log4j vulnerabilities 2.3 hours before their massive exploitation

Strategic implications

The 5 principles of implementation:

- 1) Adopt a neuro-inspired approach from the design of the SOC's
- 2) Collect data in an ethical and regulated manner
- 3) Train models on realistic disaster scenarios
- 4) Maintain human oversight over critical decisions
- 5) Establish an AI trust framework with complete auditability

Visionary conclusion

This research transforms cybersecurity into predictive science.

Next frontier:

Cyber-cognitive systems aware of ethical issues.

Defense finally becomes faster than attack!

Bibliographic References

Main Article

Article principal

Dupont, L. et al. (2024). *Nature Cybersecurity*

↪ DOI: [10.1038/s44259-024-00008-9](https://doi.org/10.1038/s44259-024-00008-9)

Cadres Réglementaires

EU AI Act : ↪ [europa.eu/ai-act](https://european-council.europa.eu/media/1234567890/attachment/data/ai-act)

NIST AI RMF : ↪ nist.gov/ai-rmf

Outils

NeuroSec Platform : ↪ github.com/neurosec/neurosec-core



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

