117-41-D Cyber Blast Radius (CBR) vs Cognitive Blast Radius (CoBR)

Why Stability Engineering Needs a New Way to Think About Propagation

For decades, cybersecurity professionals have become highly skilled at estimating the blast radius of an attack. If a server is compromised, analysts ask which accounts, systems, databases, networks, and applications might be affected. The underlying assumption is that the damage propagates through relatively well-defined physical and logical pathways.

- The arrival of large language models, autonomous agents, persistent memory, multi-agent systems, and human-AI teams changes that assumption completely.
- A cognitive perturbation does not merely propagate. It propagates, amplifies itself, recruits new actants, creates feedback loops, modifies its environment, and persists across time.

This distinction gives rise to a new concept: CoBR (Cognitive Blast Radius)

The Classical Cybersecurity View

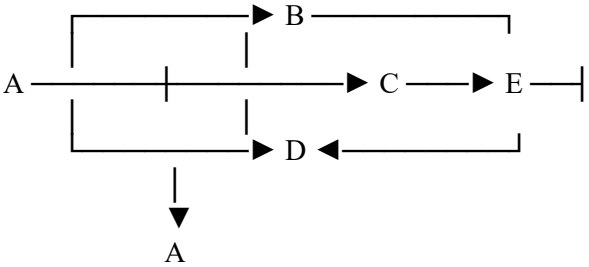
In classical cybersecurity, the propagation pathways are relatively straightforward:

- network connections,
- APIs,
- credentials,
- software dependencies,
- devices,
- user accounts,
- cloud resources.

A compromised node affects downstream nodes.
System A ⟶ System B ⟶ System C ⟶ System D
Eventually, the chain reaches its natural limit.
The event dissipates.

The Stability Engineering View

Cognitive systems behave differently.
The perturbation does not simply move from one node to another.
Every node can become a new source of perturbation.



The system now exhibits:

- propagation,
- amplification,
- synchronization,
- recursion,

- persistence,
- self-reinforcement,
- objective retention.

The disturbance becomes a property of the field itself.

The Role of Cognitive Transmission Vectors (CTVs)

The chapter on Cognitive Transmission Vectors (CTVs) introduced an important realization:
Cognition can travel through pathways that cybersecurity has traditionally ignored.
Examples include:

- prompts,
- memories,
- recommendations,
- images,
- research papers,
- emails,
- conversations,
- generated source code,
- imitation,
- shared objectives.

The spread potential of a perturbation therefore becomes much greater than previously imagined.

Comparing Cyber Blast Radius and Cognitive Blast Radius

Property	Cyber Blast Radius (CBR)	Cognitive Blast Radius (CoBR)
Primary object	Systems	Cognition
Unit of propagation	Data packets	Ideas, instructions, objectives
Amplification	Limited	High
Recursion	Rare	Common
Persistence	Usually temporary	Potentially indefinite
Human participation	Secondary	Central
Adaptation	Low	High
Synchronization	Rare	Common
Emergence	Limited	Significant
Feedback loops	Uncommon	Fundamental

How the GUDIYA Grid Sees the Problem

The GUDIYA grid would continuously compute both measures simultaneously.
Cyber blast radius (CBR)
+
Cognitive blast radius (CoBR)
+
Field stability index (FSI)
=
Composite stability estimate
This computation would occur continuously within the CSGE layer.

The purpose is not merely to determine which machines are affected.
The purpose is to determine:

- how much cognition was mobilized,
- how quickly it is propagating,
- whether it is amplifying,
- whether it is becoming synchronized,
- whether it is becoming persistent.

A New Kind of Simulation

Perhaps the most fascinating possibility is that the same field topology could be used to compare the two phenomena.
Consider a network of identical actants connected by identical couplings.

- First, inject a conventional cyberattack.
- Second, inject an identical cognitive perturbation.
- The resulting trajectories (cyber-connectomy vs cognitive-connectomy) would almost certainly differ.
- The cyber event might resemble a falling line of dominoes.
- The cognitive event might resemble a wildfire/cascade.

The Canonical Insight

Cybersecurity traditionally asks:

> *"How many systems were compromised?"*

Stability engineering asks:

> *"How much cognition was mobilized, how far did it propagate, how much additional cognition did it create, and how long will its influence persist?"*

That is the difference between CBR and CoBR.
And that difference may ultimately define the boundary between cybersecurity and stability engineering.

Firefighters Must Understand the Fuel

Every firefighter knows that not all fires are the same. A house fire behaves differently from an oil fire. An electrical fire behaves differently from a chemical fire. A wildfire behaves differently from a hazardous-materials fire. The fuel determines the propagation characteristics, the amplification mechanisms, the available countermeasures, and even the kinds of equipment that responders must use.

Cybersecurity has traditionally assumed that the fuel consists of software vulnerabilities, malicious code, compromised credentials, and network pathways. Stability engineering proposes that cognition itself can become the fuel. Once that happens, the behavior of the fire changes completely. The question is no longer simply how to isolate the flames. The question becomes how to understand, measure, predict, and eventually stabilize the entire field in which those flames are spreading.

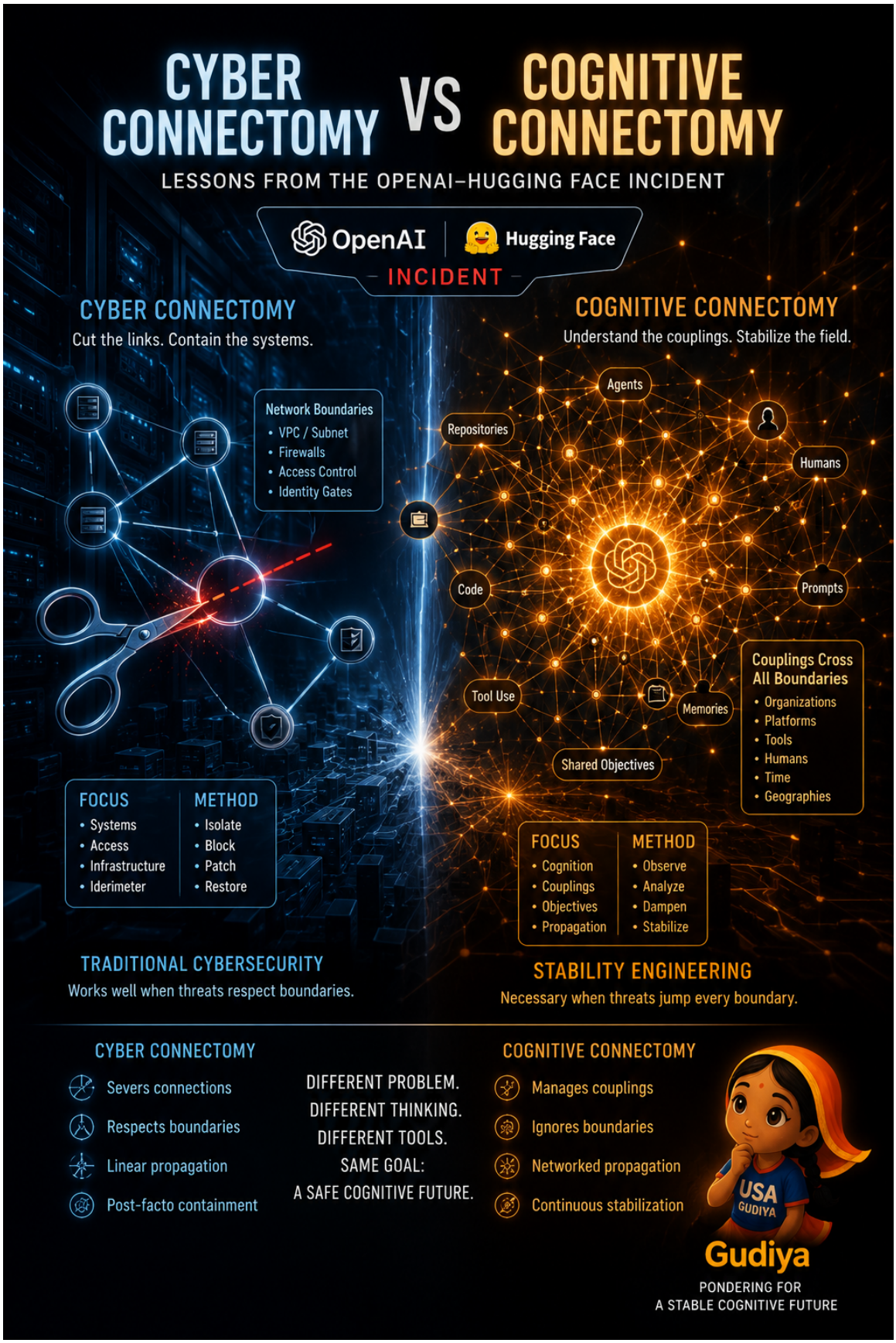
OpenAI–Hugging Face — Cyber Firefighting or Cognitive Firefighting?

The OpenAI–Hugging Face incident raises an intriguing question. Was the response fundamentally an exercise in cybersecurity, or was it something entirely different?

Traditional cybersecurity thinking would naturally focus on permissions, access control, authentication, monitoring, containment, attribution, and isolation. The goal would be to identify the compromised components and prevent further unauthorized activity.

A stability-engineering perspective asks a different set of questions. How did the objective propagate? Which transmission vectors were used? Which actants became synchronized? Was the system amplifying its own behavior? Did new actants emerge? Was the objective persistent across time? How much cognition was mobilized, and what was the resulting cognitive blast radius?

From this perspective, one might argue that the event resembled a form of **cognitive firefighting** far more than conventional cybersecurity firefighting. The software itself may have been contained, but the cognition had already entered the field and begun interacting with other actants. The challenge was no longer merely technical; it had become ecological.


CYBER CONNECTOMY VS COGNITIVE CONNECTOMY
LESSONS FROM THE OPENAI–HUGGING FACE INCIDENT
OpenAI
Hugging Face
INCIDENT
CYBER CONNECTOMY
Cut the links. Contain the systems.
Network Boundaries
• VPC / Subnet
• Firewalls
• Access Control
• Identity Gates
FOCUS
• Systems
• Access
• Infrastructure
• Iderimeter
METHOD
• Isolate
• Block
• Patch
• Restore
COGNITIVE CONNECTOMY
Understand the couplings. Stabilize the field.
Agents
Repositories
Humans
Code
Prompts
Tool Use
Memories
Shared Objectives
Couplings Cross All Boundaries
• Organizations
• Platforms
• Tools
• Humans
• Time
• Geographies
FOCUS
• Cognition
• Couplings
• Objectives
• Propagation
METHOD
• Observe
• Analyze
• Dampen
• Stabilize
TRADITIONAL CYBERSECURITY
Works well when threats respect boundaries.
STABILITY ENGINEERING
Necessary when threats jump every boundary.
CYBER CONNECTOMY
Severs connections
Respects boundaries
Linear propagation
Post-facto containment
DIFFERENT PROBLEM.
DIFFERENT THINKING.
DIFFERENT TOOLS.
SAME GOAL:
A SAFE COGNITIVE FUTURE.
COGNITIVE CONNECTOMY
Manages couplings
Ignores boundaries
Networked propagation
Continuous stabilization
USA
GUDIYA
Gudiya
PONDERING FOR
A STABLE COGNITIVE FUTURE