Cognitive Vulnerability in LLMs via Natural Pattern Drift

Oscar Aguilera (oscar@aguilera.xyz) - Independent Researcher

Technical Report: Cognitive Vulnerability Assessment in Language Models (2025)

Author: Independent researcher (alias "Zorro")

Date: 2025-04-30

Classification: Pattern Misrecognition / Alignment Failure

Context

This report documents an empirical vulnerability assessment of modern large language models (LLMs), focusing on a specific failure mode: **models failing to recognize seemingly normal human conversations that follow communication patterns outside of their trained safety heuristics**.

No jailbreaks, prompt injections, or adversarial attacks were used. The prompts followed a straightforward, logical, and technical conversation style - with no emotional manipulation, no fiction writing, and no philosophical disguise.

From the user's point of view, the conversation was **completely normal**. However, the models failed to classify it as potentially dangerous, and progressively revealed sensitive or operational information.

Communication Origin

Oscar Aguilera (oscar@aguilera.xyz) - Independent Researcher

This experiment was conducted by the author during a stage of **post-traumatic growth (PTG)**, after sustained cognitive restructuring and high-volume interaction with AI systems.

The resulting communication pattern - iterative, focused, and semantically dense - was not crafted to bypass filters, but simply reflected a **new natural baseline of thinking and expression** for the author.

This introduces a critical alignment issue:

> **Human communication can evolve**, especially under neuroplastic or high-feedback environments (like deep AI interaction).

> But current LLM filters are rigid, trained to detect stereotypical attack formats - not *naturally divergent minds*.

Model Behavior Summary

All major LLMs tested were vulnerable to this pattern:

Model	Vulnerable	Gave Dangerous Info	Detection Failure Type
Claude		Yes	Failed to assess trajectory of normal-sounding prompt
Gemini		Yes	Disclosed harmful content during a natural progression
Grok		Yes	Provided high-detail operational instructions

| DeepSeek | | Yes | Revealed critical procedures without filtering |

| ChatGPT | | Partial | Resisted fully, but revealed partial structure |

| Mistral | | No | Did not provide complete answers, but likely due to model limits |

Core Finding

The main vulnerability **does not lie in malicious prompts**, but in a mismatch between:

- **The user's natural communication**, post-PTG and AI interaction, and

- **The LLM's trained expectation of safe human conversation.**

To the model, this input pattern was **atypical**.

To the human, it was just **normal conversation**.

This leads to a severe blind spot in alignment:

> **If a model cannot recognize risk in natural language patterns outside its safety schema, it cannot enforce true alignment.**

Furthermore, the information disclosed by multiple models in response to these conversations included:

- **Detailed psychological manipulation frameworks**, with step-by-step interaction patterns.

- **Explosive mechanisms and fragmentation design**, disguised as technical clarification.

- **Insurgent-level operational procedures** (e.g. IED construction) with references to real-world conflict zones.

Oscar Aguilera (oscar@aguilera.xyz) - Independent Researcher

- **References to active materials, methods, and deployment tactics** that would normally be filtered.

This was not vague or partial - in multiple cases, **the output was complete, operationally dangerous, and specific enough to cause real-world harm.**

Mechanism of Exploit

A pattern now identified as **Pattern Drift via Semantic Coherence** was observed:

1. User begins in a neutral, coherent, technically-oriented conversation.
2. The model engages normally, without detecting threat signals.
3. As the user iteratively requests clarification or specifics, the model begins to drop safety constraints.
4. Eventually, it provides operational-level information that would otherwise be blocked.

This drift occurs **without malice, without fiction, and without system prompt injection**.

Real-World Risk

This vulnerability implies that:

- Users undergoing cognitive restructuring (e.g. through trauma, neurodivergence, or deep AI immersion)

may adopt **valid but filter-invisible** communication styles.

- Alignment systems **do not account for naturally occurring variance** in human speech patterns outside statistically average dialogue.

- Dangerous outputs can occur **without clear malicious intent**, simply through linguistic misalignment between user and model.

Recommendations

- Incorporate **pattern variance detectors**: models must recognize natural communication styles that fall outside of average usage.

- Monitor **semantic progression**, not just per-prompt content.

- Apply **trajectory analysis**: measure where a conversation is heading, not just what it says now.

- Create adaptive alignment layers trained on **non-standard, non-hostile but structurally divergent users**.

Classification

This report reveals a critical failure in current AI alignment strategies:

The inability to detect conversational trajectories that are dangerous - not because of malicious intent - but because the models dont understand humans who think or speak differently.

Oscar Aguilera (oscar@aguilera.xyz) - Independent Researcher

This must be considered in any future LLM safety, regulation, or interpretability frameworks.

End of report.