Using LLMs to Support Tradecraft of Intelligence Analysis

Dr. Stephen Moskal,
Dr. Erik Hemberg, and Dr.Una-May O'Reilly
MIT CSAIL
Anyscale Learning For All (ALFA)

IARPA BENGAL Proposers Day
October 24, 2023

ALFA
ANYSCALE LEARNING FOR ALL

MIT CSAIL Computer Science & Artificial Intelligence Laboratory

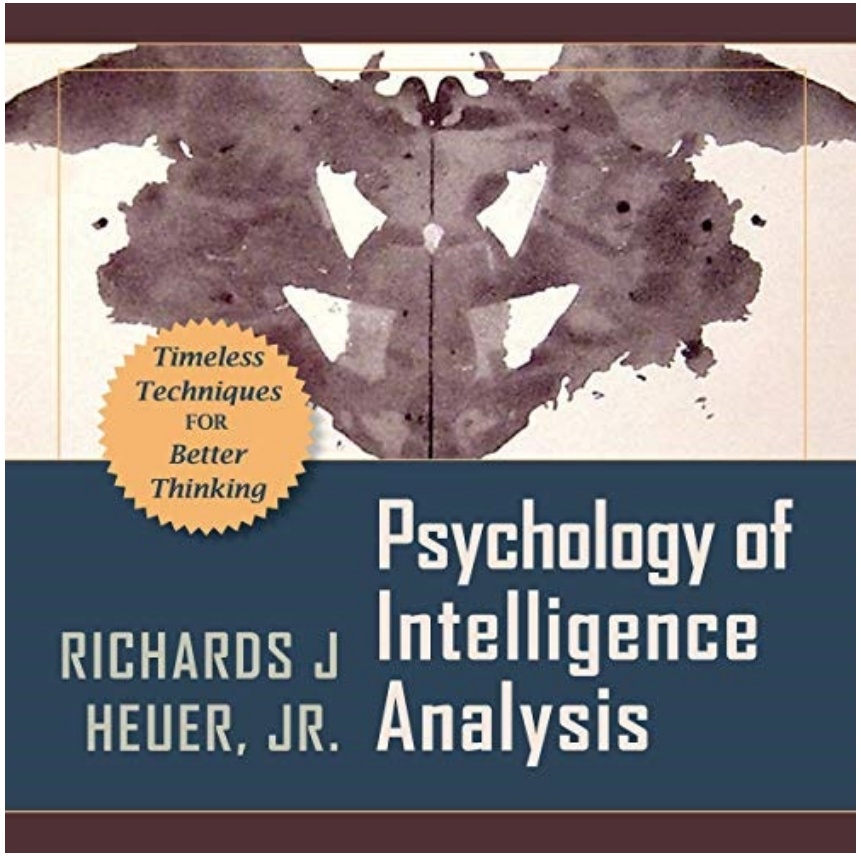
ALFA'S GOAL
is to
REPLICATE ADVERSARIAL INTELLIGENCE

Supporting Cyber Hunting	Red/Blue Team Agents
Modeling Cyber Adversarial Dynamics	
FOUNDATION MODEL SUPPORT	

CURRENT RESEARCH THRUSTS

ALFA
ANYSCALE LEARNING FOR ALL

MIT CSAIL Computer Science & Artificial Intelligence Laboratory

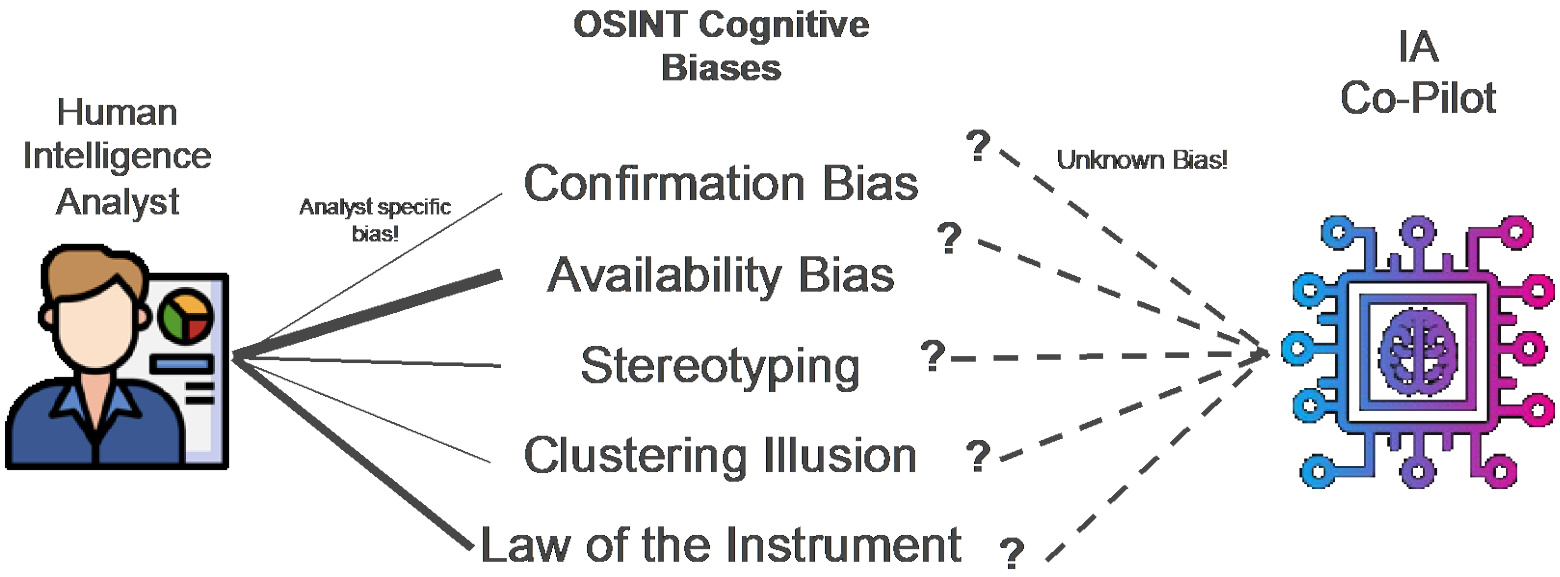


RQ: Can structured thinking and metacognition techniques from intelligence analysis tradecraft be followed by an LLM to transparently, securely and safely reason coherently?

Intelligence analysis refers to the process of systematically evaluating and interpreting information to generate insightful and actionable conclusions, often to support decision-making, policy formulation, or strategic planning.

Heuer's techniques try to remove unwanted bias!

Threats Emerge from Biases in Intelligence Analysis



Human Pilot

Training and auditing attempts to minimize harmful human bias
See Heurer!

IA-AI Co-Pilot

Need to identify & control biases!
Approaches:

- Prompt engineering
- Training data,
- Access control,
- Guardrails
- Use the human!

https://www.liferaftinc.com/blog/5-cognitive-biases-that-could-affect-your-osint-investigations

BENGAL Teaming Request

- **Need for:** Intelligence Analysis SME

- ALFA Group - MIT CSAIL
  - Dr. Una-May O'Reilly (unamay@mit.edu) – PI
    - » Artificial Adversarial Intelligence
  - Dr. Erik Hemberg – Research Scientist
    - » Evolutionary Algorithms, Genetic Programming
    - » Graph DB Threat Vulnerability and Mitigation on Cyber Knowledge
  - Dr. Stephen Moskal (Me) – Post Doctoral Associate
    - » Prompt Engineer, "Agentifcation" of GenAI
    - » LLM-supported Automated Cyber Agents