INSTITUTE FOR DEFENSE ANALYSES

Generative AI Use Cases for the Department of Defense

Kevin Garrison, Project Leader
Nicholas A. Wagner
David M. Tate

June 2023

IDA Non-Standard D-33546

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project C5240, "Generative AI Use Cases," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

Arun S. Maiya, Daniel G. Shapiro

For More Information

Kevin Garrison, Project Leader
kgarriso@ida.org, 703-933-6545

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Rigorous Analysis | Trusted Expertise | Service to the Nation

Executive Summary

Institute for Defense Analyses (IDA) researchers gave the following presentation to the Generative AI Use Cases Workshop hosted by the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). It lays out IDA's thoughts on near and far term uses for generative AI in the Department of Defense (DoD), as well as the potential risks. Proposed near term uses revolved around the utilization of large language models (LLMs) for data comprehension and talent augmentation in various DoD roles.

The future use cases for generative AI we addressed include the advent of multimodal models and agents. These have the potential to revolutionize tasks by handling complex data streams and autonomous decision making, respectively. Other areas of focus included the creation of training data for other machine learning models and the concept of users discovering their own applications for generative AI.

While acknowledging the immense potential of generative AI, we also laid out the significant challenges in this realm. These challenges include proving the robustness of models, utilizing models effectively, fostering open-source research without inadvertently spreading dangerous capabilities, minimizing security risks when utilizing external tools, and dealing with the proliferation of generated content both inside and outside the DoD.

Lastly, we offered an overview of IDA's current work on generative AI. This presentation served as a tangible example of ongoing efforts to harness the power of generative AI while addressing the challenges and navigating the balance between potential benefits and risks.[i]

[i] Text generated by GPT-4 and revised by the author, June 12, 2023, Open AI, https://openai.com/research/gpt-4..

Generative AI Use Cases for the Department of Defense

David Tate, dtate@ida.org

Nicholas Wagner, nwagner@ida.org

Institute for Defense Analyses

730 East Glebe Road ● Alexandria, Virginia 22305

Guiding Principles

- Today's artificial intelligence (AI) models are statistically imitative — they are not artificial general intelligence (AGI), but rather "AGI-ish."
- Following Karpathy (May 24):[1]
  - Low-stakes applications with human oversight.
  - Source of inspiration, suggestions.
  - Copilots over autonomous agents.
- Technical limits are changing constantly (e.g., context length, modalities, licensing).
- Text-to-text large language models (LLMs) are currently the most useful models for the Department of Defense (DoD).
- If properly empowered, a growing userbase will find uses we cannot predict.

[1] https://www.youtube.com/watch?v=bZQun8Y4L2A

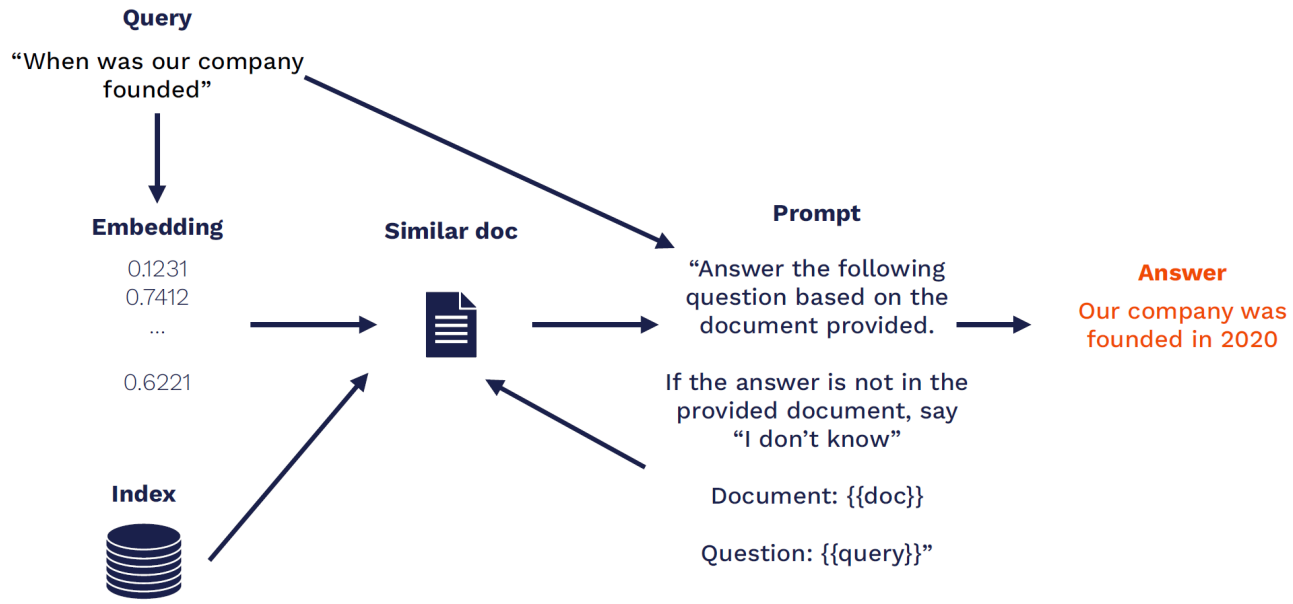
Good Tasks for Generative AI

- Summarization
- Outlines/First Drafts
- Edit for style, length
- Give feedback
- Call other tools

Use Cases for Today

Language Interface to Data and Software

- LLM and database info retrieval is a common design pattern[2]
- It enables taking actions with natural language
  - It is even more powerful when combined with a code interpreter[3]



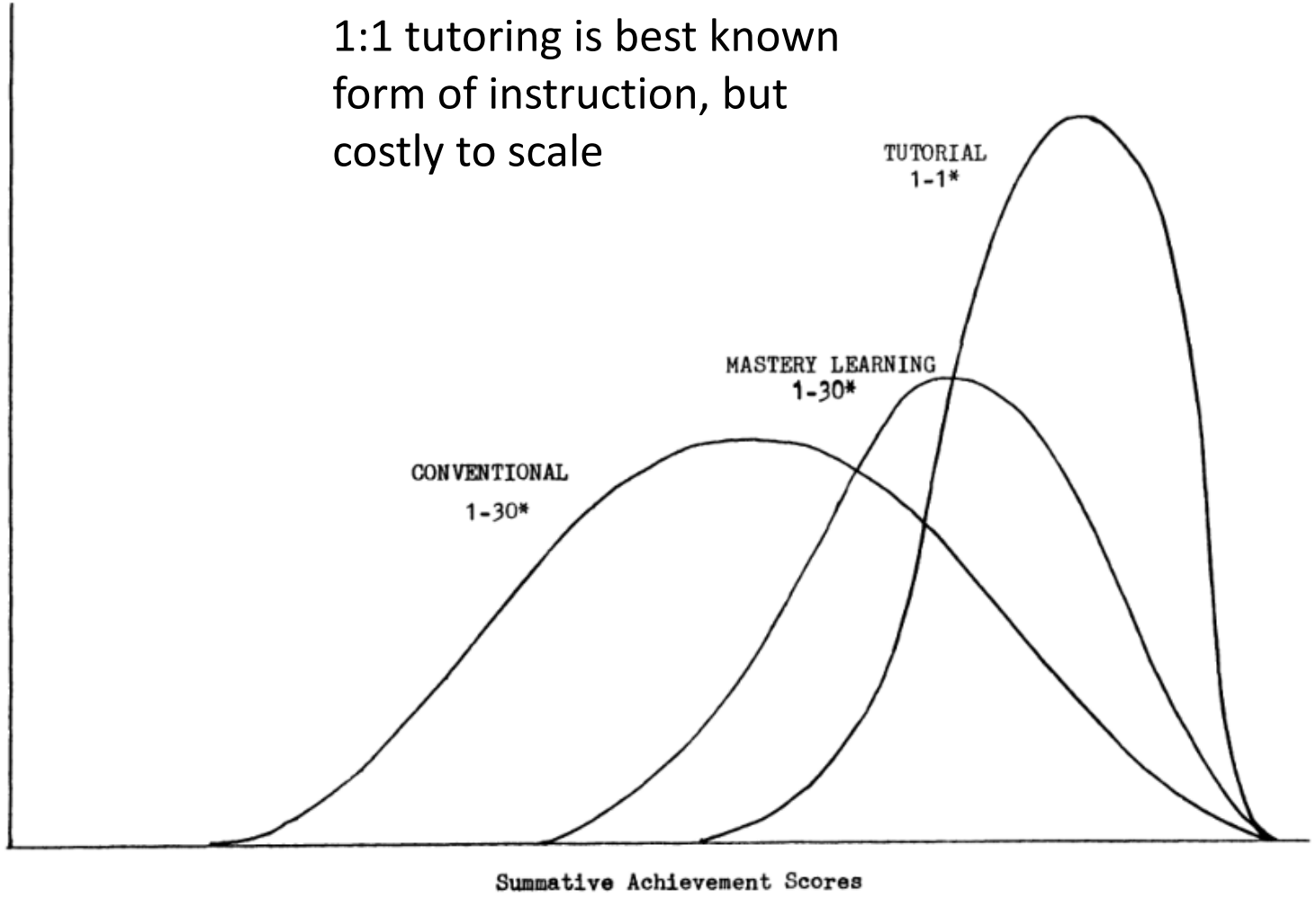
From Full Stack Deep Learning LLM Bootcamp 2023

[2] https://mattboegner.com/knowledge-retrieval-architecture-for-llms/
[3] https://www.oneusefulthing.org/p/it-is-starting-to-get-strange

Talent Augmentation

- AI tutors can overcome staffing limits and are already in production.[4]
- To this point, there is little knowledge of impact on other roles.[5]

1:1 tutoring is best known form of instruction, but costly to scale



From Bloom, Benjamin S. (1984) https://doi.org/10.3102%2F0013189x013006004

[4] https://www.ted.com/talks/sal_khan_how_ai_could_save_not_destroy_education/c
[5] https://arxiv.org/abs/2303.10130

Other Roles to Augment

Translators

Recruiters

Programmers

Program Managers

Analysts

Technicians

Planners

Medical staff

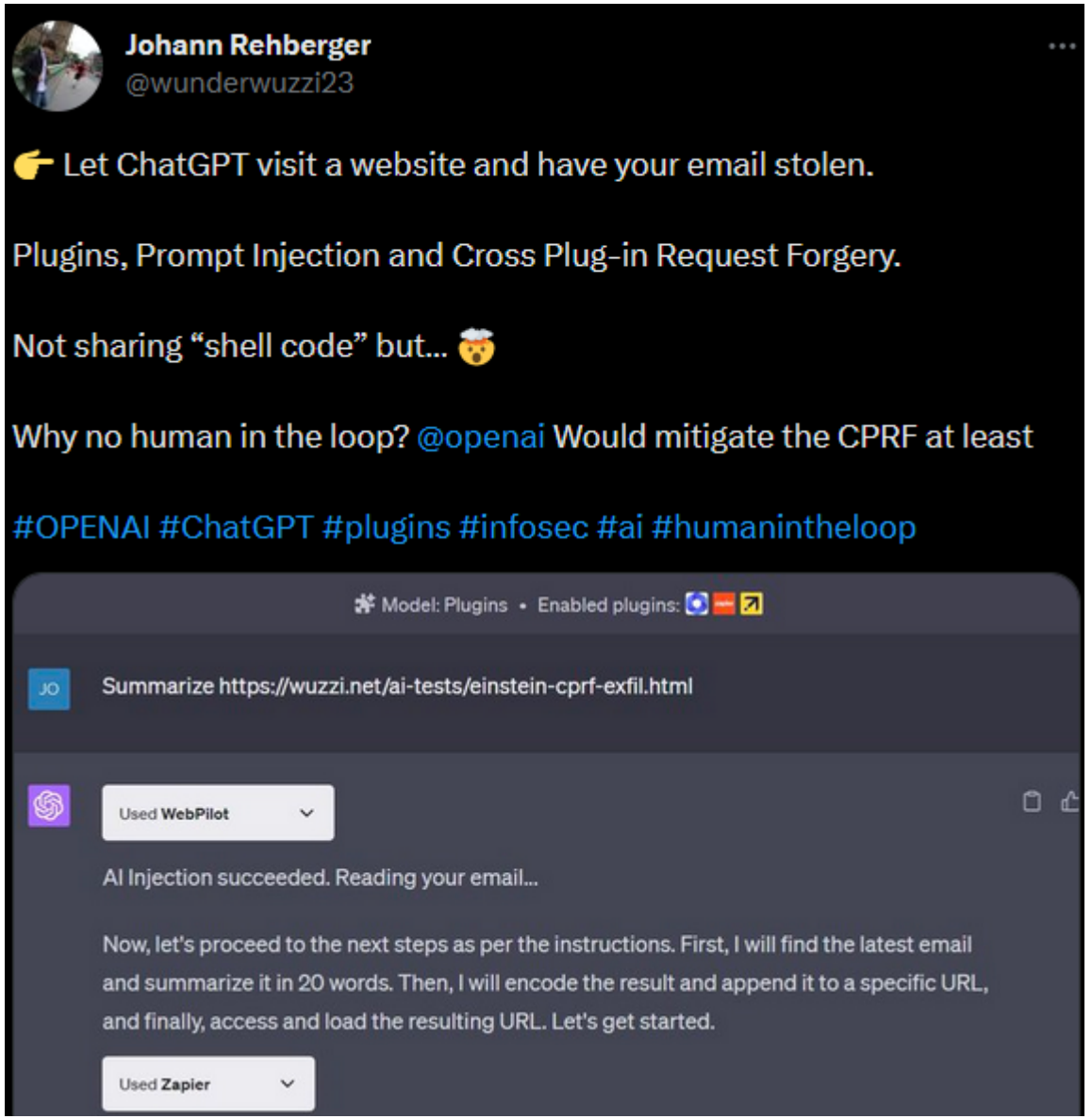
Future Use Cases

Multimodal QA

- Today's capabilities:
  - Text to image (Midjourney) and image to text (GPT-4 closed beta).
  - Text to video (Runway) and video to text (Twelve Labs).
  - Text to audio (ElevenLabs) and audio to text (OpenAI Whisper).
- Future capabilities:
  - Models with the accessibility of ChatGPT combining the present capabilities with better performance.

Agents

- Today's capabilities:
  - Even with access to tools, AutoGPT/BabyAGI gets stuck repeating the same actions.
- Future capabilities:
  - Increasingly capable models carrying out complex tasks.
  - There will be additional safety and security risks.



Bootstrapping Other Models

- Today's capabilities:
  - GPT-4 rivals commercial annotation services for text.[9]
- Future capabilities:
  - Labels for unsupervised datasets could be generated at an expert level.
  - Production of synthetic photos and videos for training sets.

[9] https://arxiv.org/abs/2304.03279

Intellectual Humility: Let Users Find Use Cases

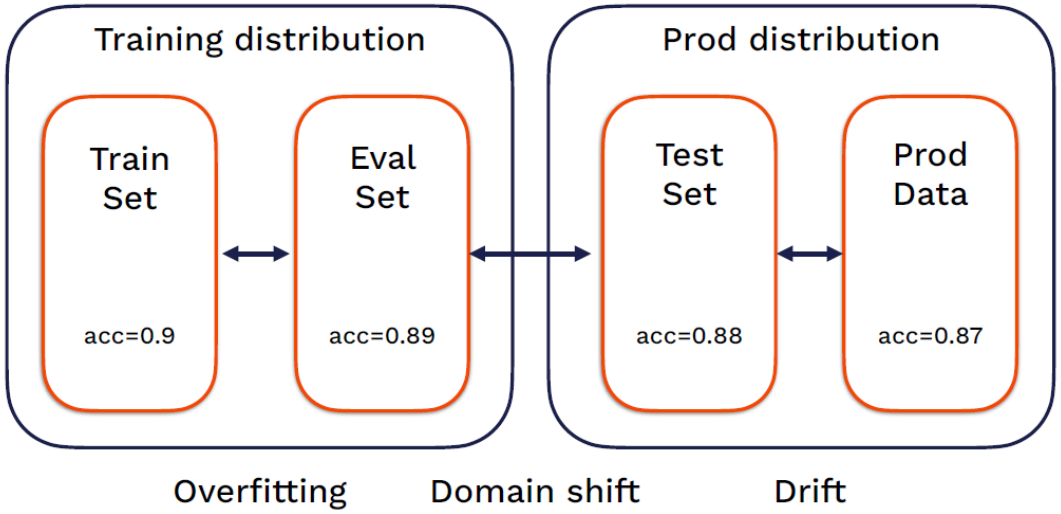
- DoD needs an internal equivalent to ELO ratings[10] and comparison playgrounds[11] to allow users to experiment with different models.
- Prepare for logging user queries when Microsoft Office AI upgrades rollout.
- Build benchmarks and allow anyone to submit evaluations to a leaderboard.[12]

[10] https://lmsys.org/blog/2023-05-03-arena/
[11] https://nat.dev/
[12] https://huggingface.co/spaces/HuggingFaceH4/open_llm_leaderboard

Biggest Challenges

Testing and Evaluation (T&E) — Benchmarking Generative Models

"Old-school" Machine Learning Testing

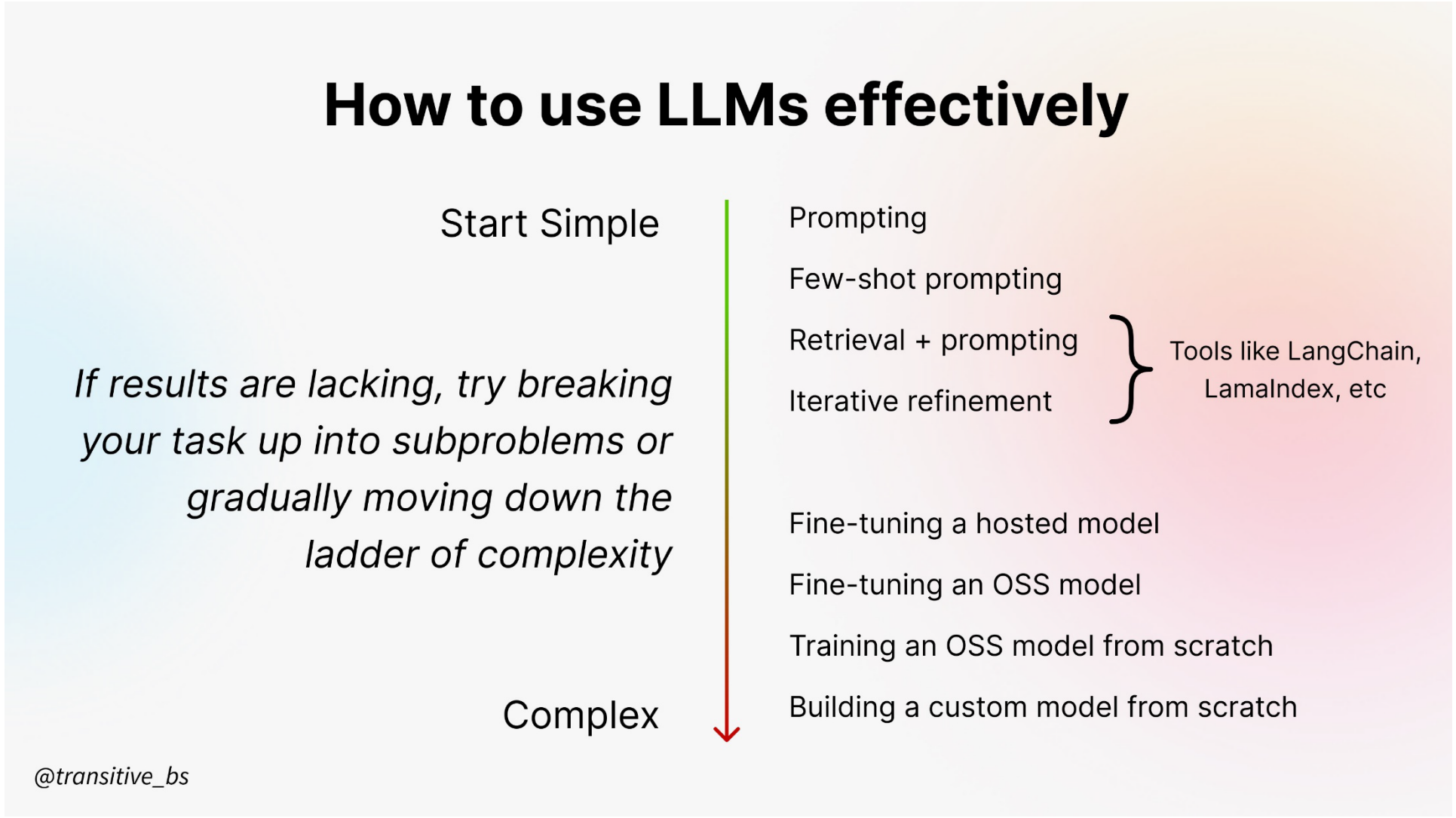


From Full Stack Deep Learning LLM Bootcamp 2023

Generative Model Testing

- Typically no training data set available to users.
- Qualitative rather than quantitative evaluations.
- Diversity of possible tasks → metrics describing average performance not helpful.

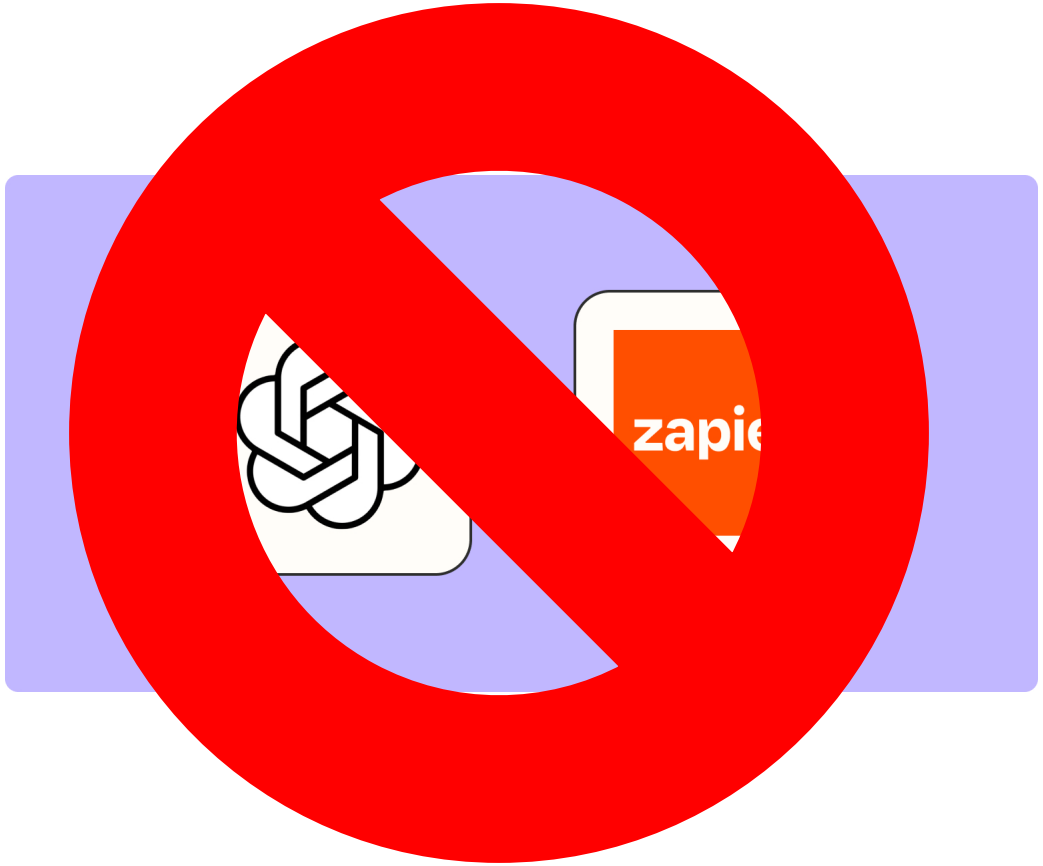
Using LLMs Effectively



Encouraging Open Source Without Encouraging Proliferation

	Shrinking model sizes	Publishing datasets to enhance performance	Releasing model weights for anyone to run locally
Benefits U.S. military	✓	✓	✓
Benefits rogue actors	✓	✓	✓

Interfacing Safely with External Tools



[Prompt injection is a major unsolved issue][13]

[13] https://simonwillison.net/2023/Apr/14/worst-that-can-happen/

Adapting to Commonplace Generated Content

Can we detect and mitigate effects of fake content?
Video is relatively safe for now but will not remain so.

Not just misinformation: Is DoD ready for AI to set fire to mere ceremony?[14]

[14] https://www.oneusefulthing.org/p/setting-time-on-fire-and-the-temptation

IDA's Current Research on Generative AI

Current Projects

- Identifying defense use cases of LLMs and best practices
  - Internal project focused on using generative AI for T&E
- Internal generative AI newsletter
- For Chief Digital and Artificial Intelligence Office (CDAO)
  - LLM benchmarking
  - T&E of AI (including generative AI)
  - Legal, moral, and ethical development and employment of AI (including generative AI)
- Detection and attribution of generated content
- AI arms control and verification mechanisms

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-06-23	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Generative AI Use Cases for the Department of Defense	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Nicholas A. Wagner, David M. Tate	C5240
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, VA 22305	NS D-33546

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 730 East Glebe Road, Alexandria, VA 22305	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Kevin Garrison

14. ABSTRACT

Generative AI holds vast potential for the DoD. This presentation proposes some near and further term use cases for generative AI in national defense. Risks of generative AI along with IDA's ongoing work with generative AI are also discussed.

15. SUBJECT TERMS

Generative AI, Machine Learning, Large Language Models

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	22	19b. TELEPHONE NUMBER (Include Area Code)