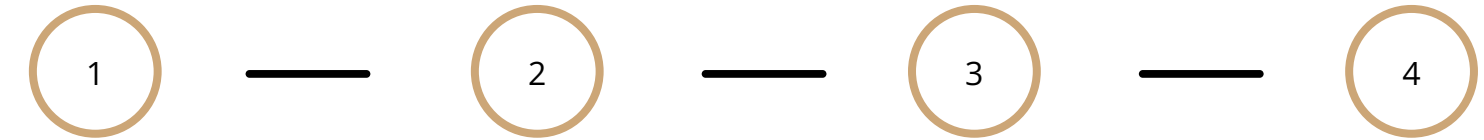
AI Agents

Victor Verma
March 25, 2025



Overview

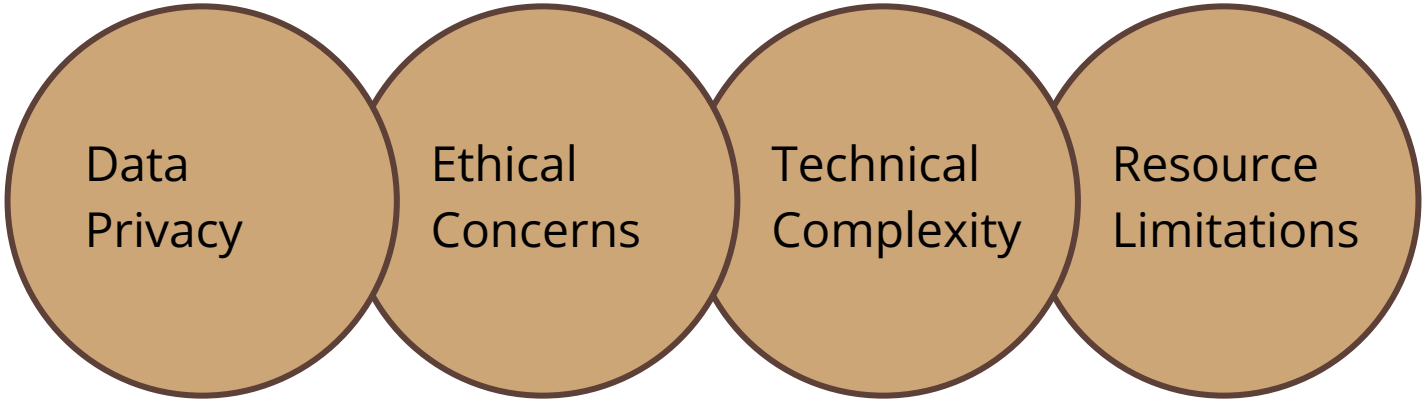
Classical Agents

Modern Agents

The Future

What are AI Agents?

- Software programs that can interact with their environment and collect data to perform tasks to complete their predetermined goals.
- The agent independently identifies the tasks needed to achieve its goals.
- Agents make rational and informed decisions.

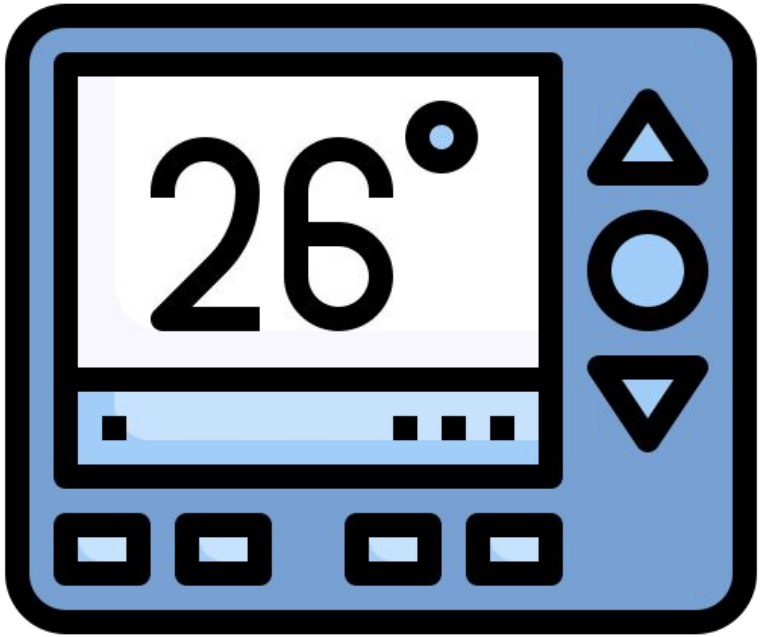

Data Privacy
Ethical Concerns
Technical Complexity
Resource Limitations

Challenges

Classical Agents

Simple Reflex Agent

Operates using predetermined rules and immediate data.



Model-Based Reflex Agent

Uses supporting data to build an internal model that employs probabilistic decision-making.

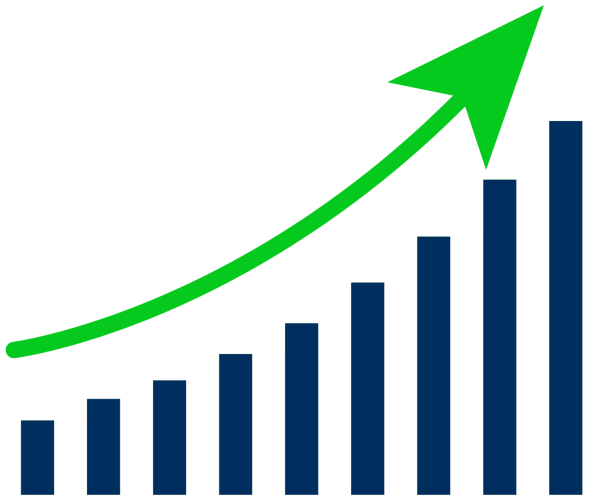
WAYMO

Goal-Based Agent

Evaluates the environment and compares approaches before choosing the most efficient path to the goal.

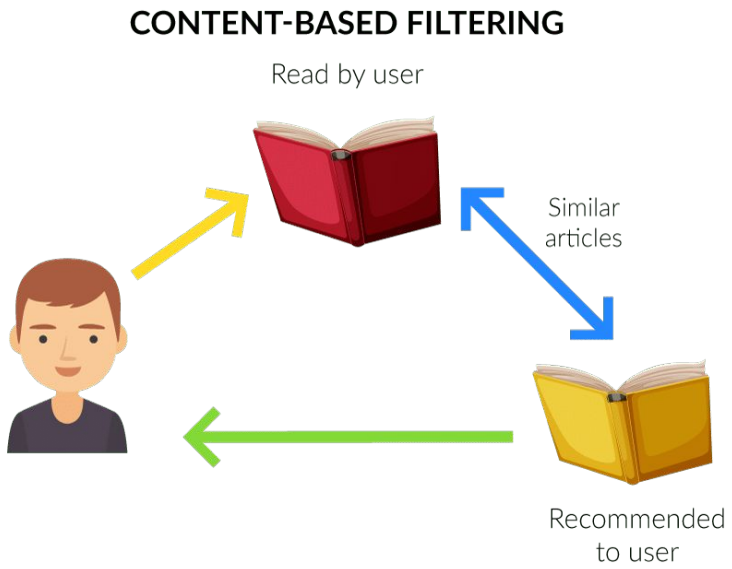
Utility-Based Agent

Compares the utility of different approaches and chooses the one with the most rewards.



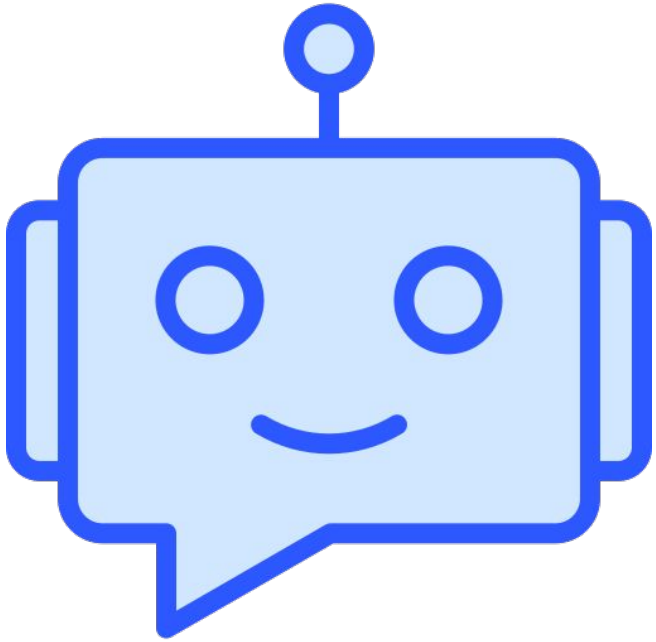
Learning Agent

Uses feedback to continuously learn from previous experiences to improve results.



Hierarchical Agent

A high-level agent breaks down complex tasks into simpler subtasks for low-level agents to complete independently.



Modern Agents

The Agentic Workflow

- Receive instructions from the user and identify the goal.
- Break the goal down into subtasks.

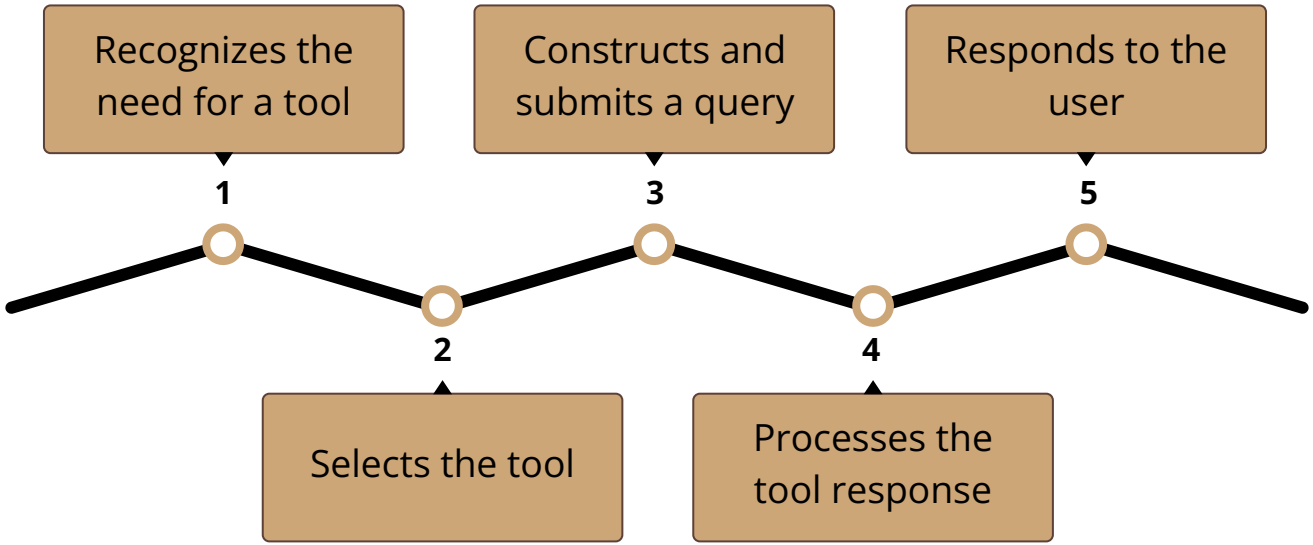
- Collect supplementary information that is required to complete the subtasks.

- Perform the subtasks.
- Dynamically add more tasks as necessary.

Tool-Calling Agent

- Enables foundational models to interact with external tools, APIs, or systems.
- Query databases, fetch real-time information, and execute functions.
- Shift from passive assistants to proactive agents.

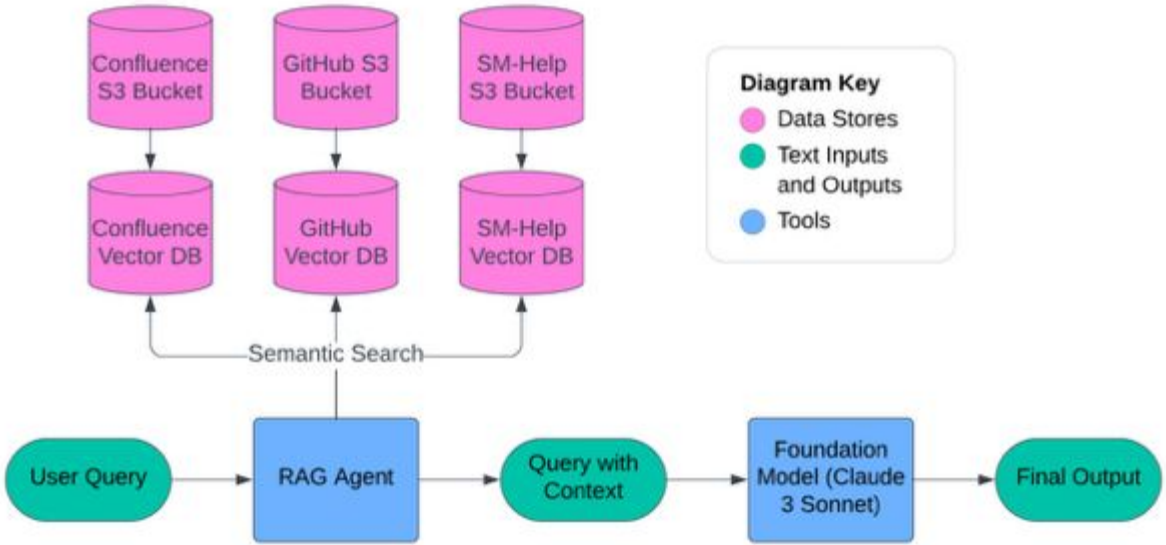
Tool-Calling Agent Workflow



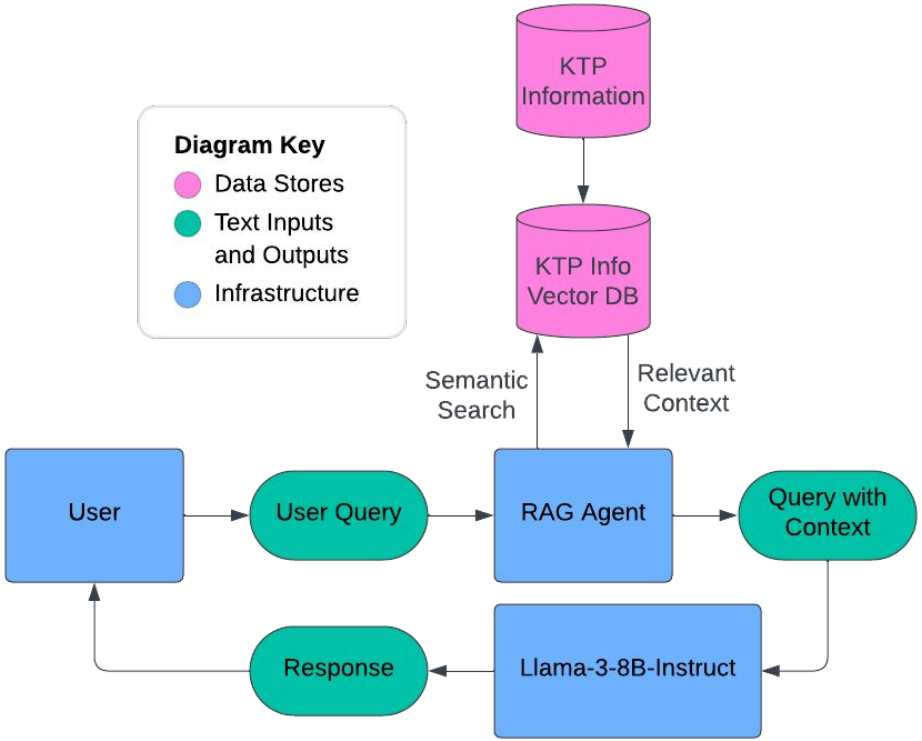
ReAct Agent

- “ReAct: Synergizing Reasoning and Acting in Language Models” (2023).
- Reasoning is used to create, track, and update plans of action.
- Actions allow the agent to interact with external environments.

ReAct Agent Example: My Internship



ReAct Agent Example: My Internship



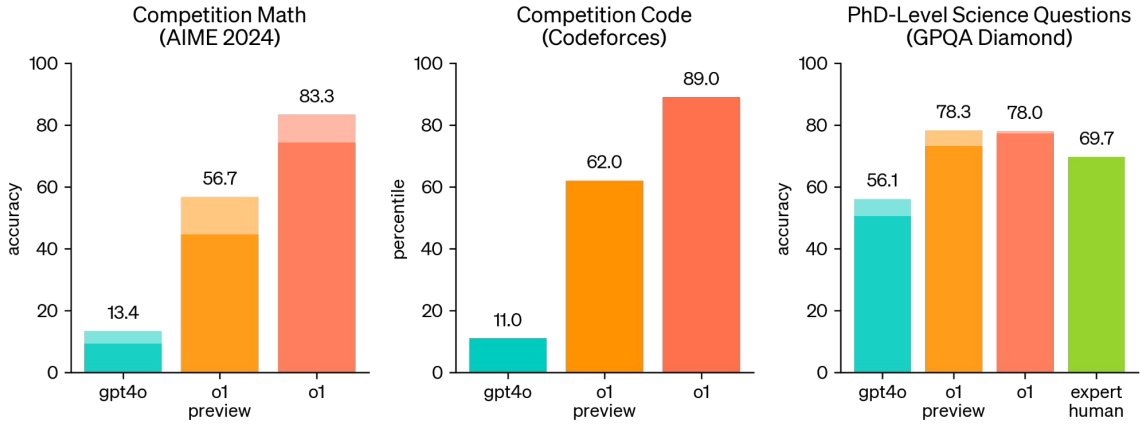
Simplified ReAct Agent Example: KTPaul

Chain of Thought (CoT) Agent

- Facilitates human reasoning and problem-solving through a series of logical deductions.
- The AI constructs the premises, logical argument, and conclusion from scratch.
- Zero-shot chain of thought solves problems without prior specific examples.
- Achieves better results with smaller models.

CoT Agent Example: OpenAI o1

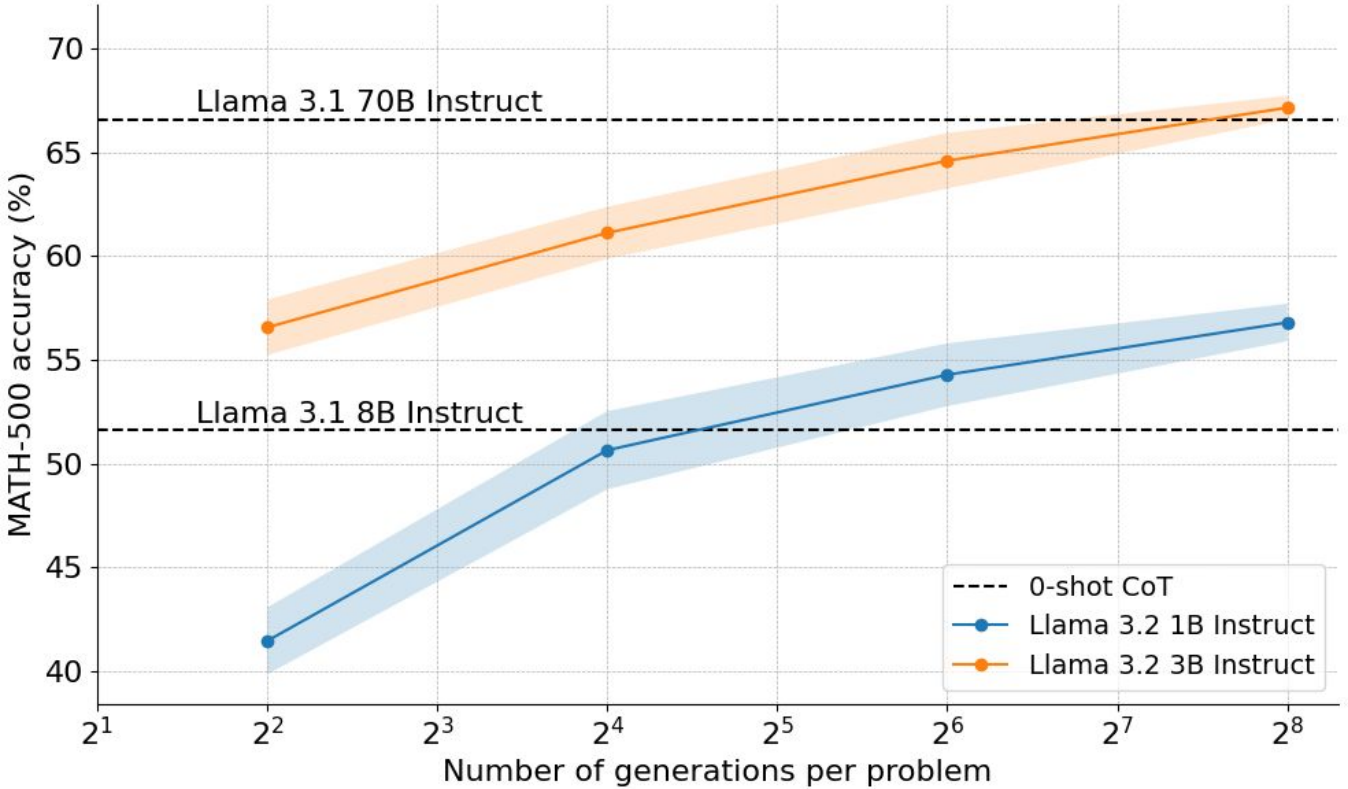
- OpenAI o1 is trained with reinforcement learning to perform complex reasoning using internal chain of thought.



How do you deal with the (lack of) data?

Test-Time Compute

- The amount of processing power and time used by an AI model.
- Resources needed to pre-train models are limited and expensive.
- Allows models to think longer on harder problems.



Increasing Test-Time Compute for Llama-3

Question: If $a > 1$, then the sum of the real solutions of $\sqrt{a - \sqrt{a + x}} = x$ is equal to

Response: <think>

To solve the equation $\sqrt{a - \sqrt{a + x}} = x$, let's start by squaring both $\cdots$

$$\left(\sqrt{a - \sqrt{a + x}}\right)^2 = x^2 \implies a - \sqrt{a + x} = x^2.$$

Rearrange to isolate the inner square root term:

$$(a - x^2)^2 = a + x \implies a^2 - 2ax^2 + (x^2)^2 = a + x \implies x^4 - 2ax^2 - x + (a^2 - a) = 0$$

$\ldots$

Wait, wait. Wait. That's an aha moment I can flag here.

Let's reevaluate this step-by-step to identify if the correct sum can be $\cdots$

We started with the equation:

$$\sqrt{a - \sqrt{a + x}} = x$$

First, let's square both sides:

$$a - \sqrt{a + x} = x^2 \implies \sqrt{a + x} = a - x^2$$

Next, I could square both sides again, treating the equation: $\cdots$

$\ldots$

DeepSeek R1-Zero: "The model learns to rethink using a [humanlike] tone."

The Future

LIMO: Less is More for Reasoning (2025)

- LIMO Hypothesis: "*In foundation models where domain knowledge has been comprehensively encoded during pre-training, sophisticated reasoning capabilities can emerge through minimal but precisely orchestrated demonstrations of cognitive processes.*"

Computer-Using Agent (CUA)

- Combines GPT-4o's computer vision capabilities with advanced reasoning through reinforcement learning.
- Trained to interact with GUIs in the same way that humans do, without OS or web APIs.
- Understands the screen through raw pixel data and completes actions using a virtual keyboard and mouse.

CUA Workflow

1

Perception

Adds computer screenshots to the model's context.

2

Reasoning

Uses chain of thought and considers current and past screenshots and actions to decide the next steps.

3

Action

Performs the actions until the task is completed or user input is necessary.

CUA Example: OpenAI Operator

- “Simply describe the task you’d like done.”
- Set custom instructions for sites, such as airline preferences on Booking.com.
- Automate repetitive tasks like online grocery shopping with saved prompts.
- Introduces novel safety concerns (sensitive user information and adversarial websites).

CUA Example: Manus AI

- Launched on 3/6/25 by the Chinese startup Butterfly Effect.
- General autonomous agent, with multimodal capabilities and advanced tool support.
- Employs a multi-agent system, where a central AI organizes a team of specialized agents.

Where will AI agents will be used?

Agentic Warfare

- On 3/5/25, the DoD announced that Scale AI has been awarded a contract to leverage AI for U.S. military planning and operations.[4,8]
- Scale AI will collaborate with Anduril and Microsoft to develop custom agentic workflows starting with Indo-Pacific Command and European Command.[8]

Agentic Warfare

- Will the AI agents be under human oversight?
  - Scale AI Announcement → YES.[8]
  - DoD Announcement → NOT SPECIFIED.[4]

Is agentic warfare ethical?

Agentic Warfare: Libya

- 3/8/21 letter to the U.N. Security Council: “[l]ogistics convoys and retreating HAF were subsequently hunted down and remotely engaged by the unmanned combat aerial vehicles or the lethal autonomous weapons systems…”[12]
- There is a lot of uncertainty about the situation, but it is possibly the first known case of LAWS used to kill.[6]

Agentic Warfare: Israel

- Although private AI has been used in war for years, the Israel-Palestine conflict is a leading instance of U.S. commercial AI models being used directly in war.[2]
- OpenAI, Microsoft, Google, Amazon, and Palantir all provide AI services to the Israeli military.[2]
- No mention of agents being used at this point.

Appendix

- Key Terms
  - Agent, utility, rewards, foundational models, APIs, reasoning, actions, zero-shot, reinforcement learning, computer vision, GUIs, multimodal, multi-agent system, lethal autonomous weapons systems.
- Further Reading
  - AI Agents Directory.
  - Prompt Injection attack against LLM-integrated Applications (2023).
  - Quantum AI: AI Agents and Quantum Computing - A Synergistic Future?
  - Towards human society-inspired decentralized DNN inference (2025).
  - U.S. Policy on Lethal Autonomous Weapons Systems.

References: Websites

- [1] Beeching, Edward, et al. “SCALING TEST TIME COMPUTE with Open Models.” *Hugging Face*, Hugging Face, 16 Dec. 2024, huggingface.co/spaces/HuggingFaceH4/blogpost-scaling-test-time-compute.
- [2] Biesecker, Michael, et al. “As Israel Uses US-Made AI Models in War, Concerns Arise about Tech’s Role in Who Lives and Who Dies.” *AP News*, The Associated Press, 18 Feb. 2025, apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108.
- [3] “Computer-Using Agent.” *OpenAI*, OpenAI, 23 Jan. 2025, openai.com/index/computer-using-agent.
- [4] “DIU’s Thunderforge Project to Integrate Commercial AI-Powered Decision-Making for Operational and Theater-Level Planning.” *Defense Innovation Unit*, Defense Innovation Unit, 5 Mar. 2025, www.diu.mil/latest/dius-thunderforge-project-to-integrate-commercial-ai-powered-decision-making.
- [5] Gadesha, Vrunda, and Eva Kavlakoglu. “What Is Chain of Thoughts (COT)?” *IBM*, IBM, www.ibm.com/think/topics/chain-of-thoughts. Accessed 15 Mar. 2025.
- [6] Hernandez, Joe. “A Military Drone With A Mind Of Its Own Was Used In Combat, U.N. Says.” *NPR*, NPR, 1 June 2021, www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d .
- [7] “Introducing Operator.” *OpenAI*, OpenAI, 23 Jan. 2025, openai.com/index/introducing-operator.
- [8] “Introducing Thunderforge: AI for American Defense.” *Scale*, Scale AI, 5 Mar. 2025, scale.com/blog/thunderforge-ai-for-american-defense.

References: Websites

- [9] Kumar, Shubham. “What Is Manus Ai : Explore New General AI Agent Features, Architecture, Access & More.” *GeeksforGeeks*, GeeksforGeeks, 15 Mar. 2025, www.geeksforgeeks.org/manus-ai-new-general-ai-agent/.
- [10] “Large-Scale Application of AI with Humans in the Loop.” _Scale_, Scale AI, scale.com/agentic-warfare. Accessed 19 Mar. 2025.
- [11] “Learning to Reason with LLMS.” *OpenAI*, OpenAI, 12 Sept. 2024, openai.com/index/learning-to-reason-with-llms.
- [12] Majumdar Roy Choudhury, Lipika, et al. “Final Report of the Panel of Experts on Libya Established Pursuant to Security Council Resolution 1973 (2011).” Received by President of the U.N. Security Council, 8 Mar. 2021.
- [13] Stryker, Cole. “What Is Tool Calling?” *IBM*, IBM, 7 Mar. 2025, www.ibm.com/think/topics/tool-calling.
- [14] “Types of Agents in AI.” *GeeksforGeeks*, GeeksforGeeks, 15 May 2024, www.geeksforgeeks.org/types-of-agents-in-ai/.
- [15] Vert, Alyona. “What Is Test-Time Compute and How to Scale It?” Edited by Ksenia Se, *Hugging Face*, Hugging Face, 6 Feb. 2025, huggingface.co/blog/Kseniase/testtimecompute.
- [16] “What Are AI Agents?” *AWS*, Amazon Web Services, Inc, aws.amazon.com/what-is/ai-agents/. Accessed 14 Mar. 2025.

References: Papers

- [17] Guo, Daya, et al. "Deepseek-r1: Incentivizing reasoning capability in llms via reinforcement learning." *arXiv preprint arXiv:2501.12948* (2025).
- [18] Yao, Shunyu, Zhao, Jeffrey, Yu, Dian, Du, Nan, Shafran, Izhak, Narasimhan, Karthik, and Cao, Yuan. *ReAct: Synergizing Reasoning and Acting in Language Models*. Retrieved from https://par.nsf.gov/biblio/10451467. *International Conference on Learning Representations (ICLR)*.
- [19] Ye, Yixin, et al. "LIMO: Less is More for Reasoning." *arXiv preprint arXiv:2502.03387* (2025).