

# Second Session

**Alireza Moradi**

---



| [Linkedin](#) |



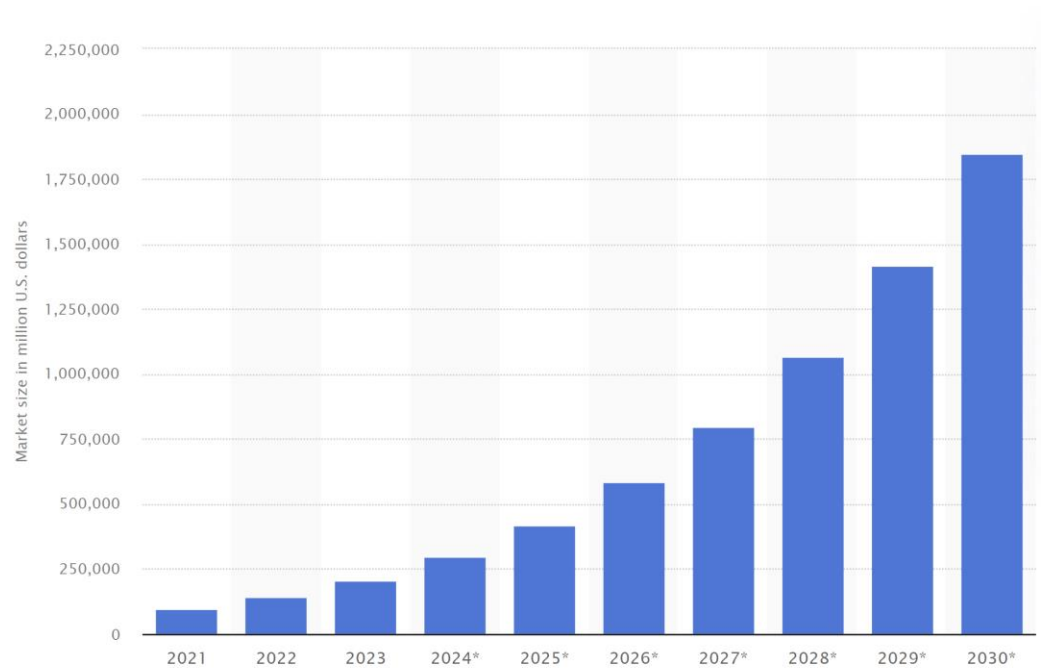
| [k](#)

# AI on the rise

- AI market size by 2030 will be more than **\$1.8 trillion**.

Global Rank	Stock Exchange	Market Cap Aug 2023
1	NYSE	<b>\$25.0T</b>
2	Nasdaq	<b>\$21.7T</b>

- This is the **pure AI market!**



# AI on the rise

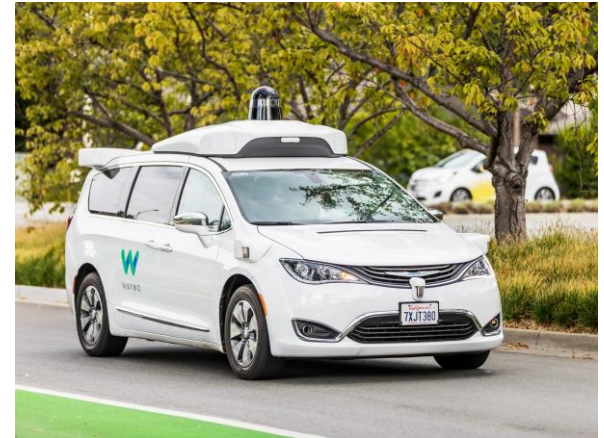
- AI papers increased 20-fold between 2010 and 2019! (about 20,000 a year)
- During these years, the most popular category was **machine learning**. (Machine learning papers in [arXiv.org](https://arxiv.org) doubled every year from 2009 to 2017.) **Computer vision** and **natural language processing** were the next most popular.
- By launching ChatGPT3, **natural language processing** take the first place in popularity.

- 
- ❑ arXiv(pronounced as archive) is an open-access repository for scholarly articles.



# Applications; Robotics

- Robotics focuses on the manipulation of the physical. It usually involves three concept.
  1. **Perception:** figuring out what's in the world around you
  2. **Motion planning:** finding a path for the robot to follow
  3. **Control:** Sending commands to the motors to follow a Path
- One of the important example in this area is **Self-driving car**.
- Big players : **Waymo, Baidu** and **tesla**



# Applications; Robotics

- In the air, **autonomous fixed-wing drones** have been providing cross-country blood deliveries in Rwanda since 2016.
- In manufacturing, **AI-powered robots** are used for production line automation, product assembly, quality control, and logistics. Their ability to work 24 hours a day without fatigue and with pinpoint accuracy has transformed the way consumer goods are produced.
- There are over 3.4 million industrial robots in the world today. The global robot-to-human ratio in the manufacturing industry is **1 to 71**.



# Applications; Robotics

- In-home sensors and robots are on the rise, offering new ways to provide support and care, **especially for elderly people.**



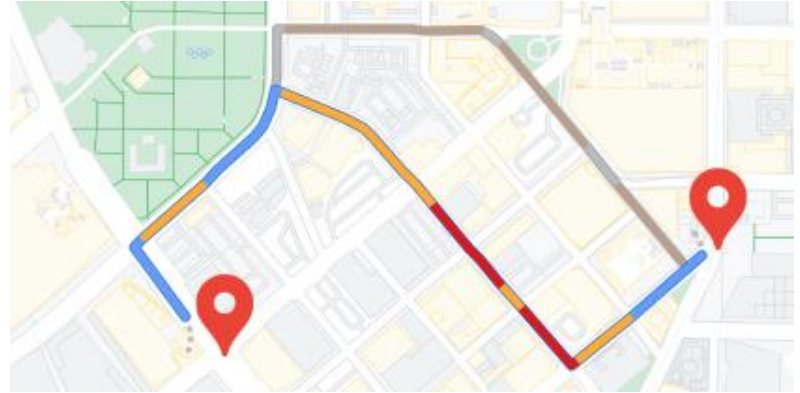
robot sweepers



ElliQ robot

# Applications; Autonomous planning and scheduling


- Automated planning and scheduling in AI is the process of using computers to **automatically plan and schedule actions or events**. This can include planning and scheduling tasks, resources, and events. (**Logistics and transportation**)
- Every day, ride hailing companies such as **Uber** and mapping services such as **Google Maps** provide driving directions for hundreds of millions of users, quickly **plotting an optimal route** considering current and predicted future traffic conditions.



Uber



# Applications; digital assistant

- Digital assistants use advanced artificial intelligence (AI), natural language processing, natural language understanding, and machine learning to learn as they go and **provide a personalized, conversational experience**.
- Constituents: 
  - Speech recognition (speech-to-text)
  - Trigger word/wake-word detection
  - Speech synthesis (text-to-speech, TTS)
- In 2017, Microsoft showed that its Conversational Speech Recognition System had reached a word error rate of 5.1%, matching human performance on the Switchboard task.
- Big players:



Amazon  
*Echo / Alexa*



Google  
*Home*



Apple  
*Siri*

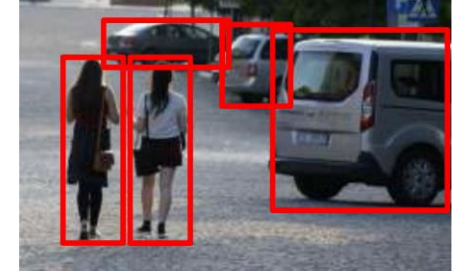


Baidu  
*DuerOS*



# Applications; Vision

- Image classification/Object recognition
- -Face recognition
- Object detection
- Image segmentation
- Tracking



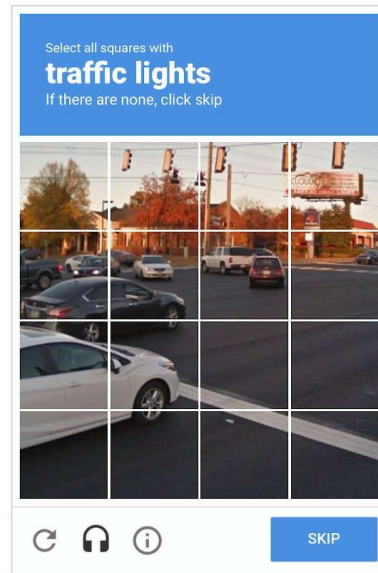
# Applications; Vision

- **Facial recognition** technology, demonstrated here via Google Photos on a 2019 photo taken at an AI conference, can spot a wide range of individuals in photos and associate them with their names.
- 
- Applying the same ideas to massive collections of imagery posted online makes it possible to **spot and name strangers in public**.
- The capability raises concerns about how AI can simplify mass intrusions into the privacy rights of citizens by governments and private companies all over the world.



# Applications; Vision

- Tremendous improvements in different areas like vision!
- Error rates for object detection (as achieved in LSVRC, the Large-Scale Visual Recognition Challenge) improved from 28% in 2010 to 2% in 2017, **exceeding human performance**.
- AI bots are now outperforming humans in solving CAPTCHAs.
- Training time for the image recognition task dropped by a factor of 100 in just the past two years. The amount of computing power used in top AI applications is **doubling every 3.4 months**.



# Applications; Natural language processing

- Text classification like **Sentiment recognition** from comments which is quite popular in marketing.

“The food was good” => Good

“Service was horrible” => Bad

- Information retrieval is another popular application. Every **web search** is a kind of AI!
- Big players:



# Applications; Natural language processing

- **Machine translation** is the process of using artificial intelligence to automatically translate text from one language to another without human involvement. Modern machine translation goes beyond simple word-to-word translation to communicate the full meaning of the original language text in the target language.
- Machine translation a difficult problem to solve.
- Code:
  - Code generation(Text to codes)
  - Code explanation

Google Translate



OpenAI codex



GitHub Copilot

# Applications; Recommender System

- Companies such as Amazon, Facebook, Netflix, Spotify, YouTube, Walmart, and others use machine learning to recommend what you might like **based on your past experiences** and **those of others like you**. This is called recommender system.



- Spam filtering can also be considered a form of recommendation.(or **dis-recommendation**)
- current AI techniques filter out over 99.9% of spam, and email services can also recommend potential recipients, as well as possible response text.

# Applications; Game playing

- ALPHAZERO, used no input from humans (except for the rules of the game), and was able to **learn through self-play** alone to defeat all opponents, human and machine, at Go, chess, and shogi.
- Defeated champions by AI in video games:  
E.g., Dota 2 (Fernandez and Mahlmann, 2018)
- An AI program **learned to cooperate with copies of itself** and defeated the world champions.
- OpenAI Five plays 180 years' worth of games against itself every day, learning via self-play!





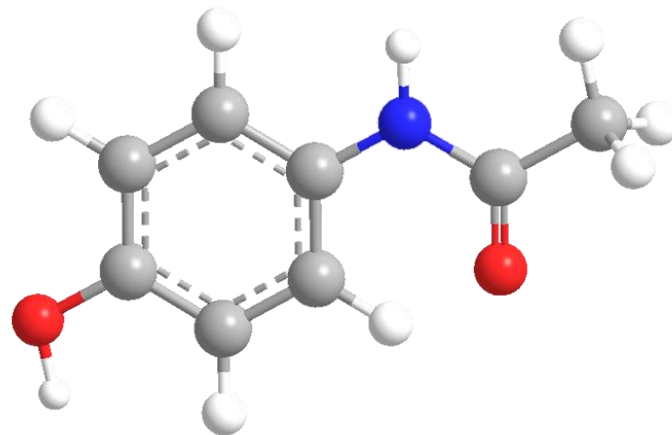
# Applications; Health

- The LYNA system achieves 99.6% overall accuracy in diagnosing metastatic breast cancer—**better than an unaided human expert**—but the combination does better still (Liu et al., 2018; Steiner et al., 2018).
- AI algorithms now **equal or exceed expert doctors** at diagnosing many conditions, particularly when the diagnosis is based on images.
- Beside diagnosis, AI can treat complex conditions with **surgery** (Robotics).



# Applications; Health

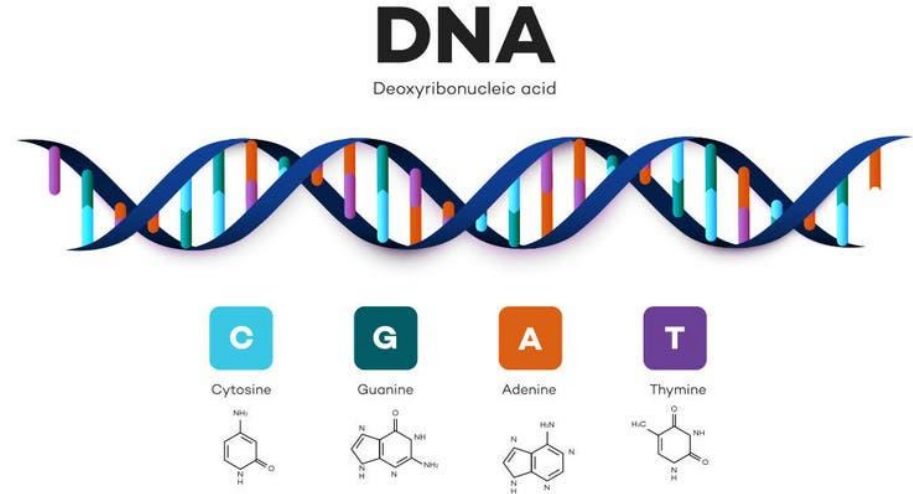
- As COVID-19 has demonstrated, the speedy development of new drugs or new formulations of existing ones is needed – and increasingly expected by the public. AI has the potential to deliver this speed by transforming **materials and molecular discovery**.
- The pre-clinical stage of drug discovery can take up to six years, potentially costing billions of dollars. But AI tools are helping speed up the development process—by repositioning drugs, identifying **drug interactions**, **assessing toxicity**, and **predicting novel drug targets**.



acetaminophen

# Applications; Health

- Bioinformatics is a scientific subdiscipline that involves using **computer technology** to collect, store, analyze and disseminate **biological data and information**, such as DNA and amino acid sequences or annotations about those sequences.
- AI algorithms, such as machine learning (ML) and deep learning (DL), are used in genomic analysis to process and interpret large amounts of genetic data.
- These algorithms can identify patterns, make predictions, and classify genetic variations.



# Applications; Climate science

- Predicting weather accurately is a hard problem to solve.
- An AI model called GraphCast can forecast the weather faster and cheaper than today's top weather systems, Google DeepMind scientists report.
- It can predict weather up to 10 days in advance, in less than a minute on a single desktop computer.
- Current systems take hours, on huge supercomputers.



# Applications; Generative AI

- Generative AI can be use to generate Image, Audio and Video.



A beautiful, pastoral mountain scene.  
Landscape painting style (Midjourney)



Two cute kittens playing (DALL-E).



# Applications; Generative AI

- Neural networks, trained on tens of thousands of portrait photographs of faces, can now generate novel high-resolution images that appear compellingly like pictures of real human faces.
- The technology behind this development, **generative adversarial networks (GANs)**, has advanced rapidly since its introduction in 2014.



# Applications; Generative AI

- Another important applications of Generative AI is **large language models**. The abbreviated form is LLM.
- LLMs is an important step towards AGI.
- LLMs can now input and output text, image, voice, videos, etc.
- LLMs can do a lot of different tasks:
  - ✓ Translation
  - ✓ Sentiment analysis
  - ✓ Categorization
  - ✓ Summarization
  - ✓ Brainstorm ideas
  - ✓ Code generation
  - ✓ Question answering
  - ✓ Solve math question
  - ✓ Compose music
  - ✓ Information extraction and many more!



# Applications; Generative AI

- There are two kind of LLMs:
  - Open-source
  - Closed-source(commercial)
- Closed-source models are developed, maintained, and owned by specific entities or organizations, with their underlying code and training data kept under wraps.
- You can access Open-source models in [Hugging Face](#).



BERT (Google)



BLOOM (BigScience)



ChatGPT Models(OpenAI)



Ernie(Baidu)



LLaMA (Meta)



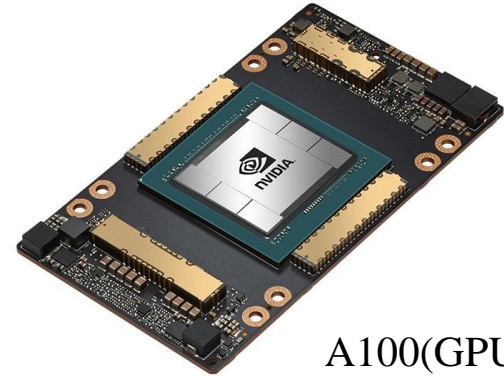
Alpacha (Stanford)



PaLM(Google)

# What are the recourses?

- Central Processing Unit (CPU)
  - Graphics Processing Unit (GPU)
  - Tensor Processing Unit (TPU)
- 
- Tensor Processing Unit is an AI accelerator application-specific integrated circuit developed by Google for neural network machine learning, using Google's own TensorFlow software.























A100(GPU)



Google racks of TPUs

# What are the recourses?

Big players:

	CPU		GPU		TPU
			NVIDIA®		
			AMD		
		 BROADCOM®			
		 Imagination			
					

# Risks

- Although AI is a great opportunity for us, **we will incur risks from the misuse of AI**. Some of these are already apparent, while others seem likely based on current trends.
- Short-term risks:
  1. Lethal autonomous weapons
  2. Surveillance and persuasion
  3. Biased decision making
  4. Impact on employment
  5. Safety-critical applications
  6. Cybersecurity
- Long-term risk:
  - ❑ ASI

# Risks; Lethal autonomous weapons

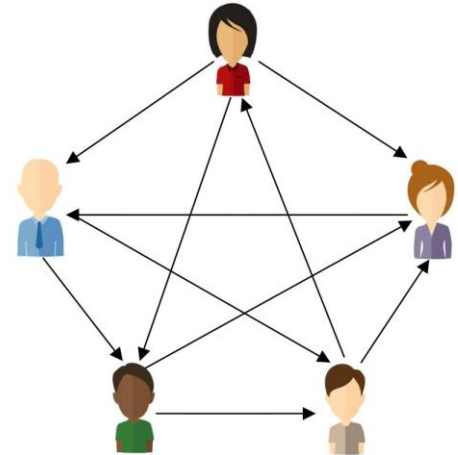
- These are defined by the United Nations as **weapons that can locate, select, and eliminate human targets without human intervention.**
- A primary concern with such weapons is their **scalability**: the absence of a requirement for human supervision means that a small group can deploy an arbitrarily large number of weapons against human targets defined by any feasible recognition criterion.
- The technologies needed for autonomous weapons are like those needed for self-driving cars.



Turkish STM KARGU drone

# Risks; Surveillance and persuasion

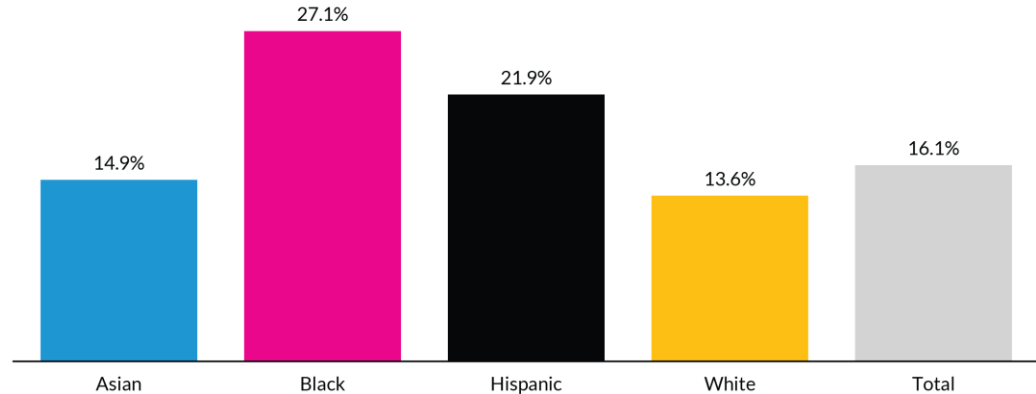
- While it is expensive, tedious, and sometimes legally questionable for security personnel to monitor phone lines, video camera feeds, emails, and other messaging channels, AI (speech recognition, computer vision, and natural language understanding) can be used in a scalable fashion to **perform mass surveillance of individuals and detect activities of interest**.
- By tailoring information flows to individuals through **social media**, based on machine learning techniques, political behavior can be modified and controlled to some extent.



# Risks; Biased decision making

- Careless or deliberate misuse of machine learning algorithms for tasks such as **evaluating parole** and **loan applications** can result in decisions that are **biased by race, gender, or other protected categories**.
- Often, the data themselves reflect pervasive bias in society.

Mortgage Denial Rate Comparison, by Race or Ethnicity



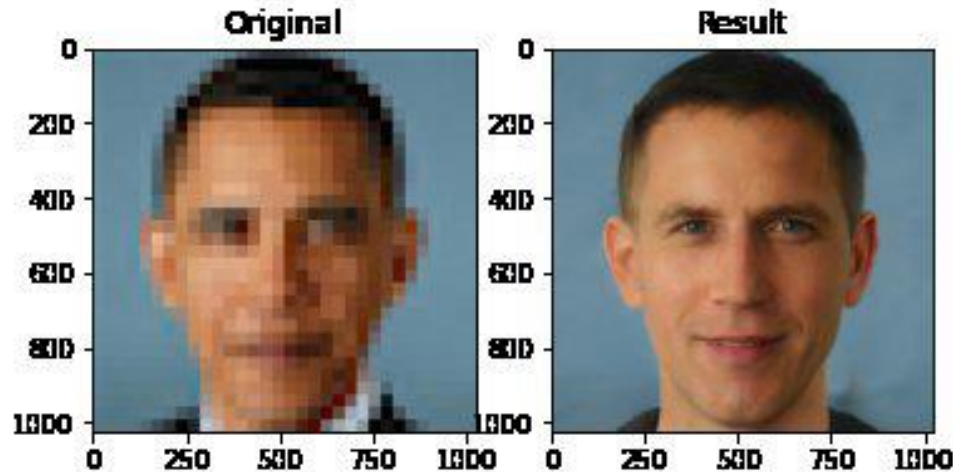
URBAN INSTITUTE

Source: Authors' calculations using 2020 Home Mortgage Disclosure Act data.



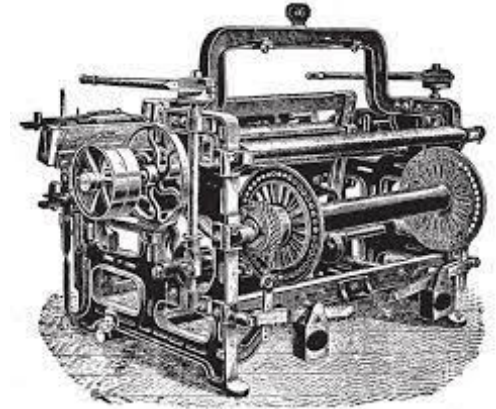
# Risks; Biased decision making

- Image-generation GANs can be used to perform other tasks like translating low-resolution images of faces into high resolution images of faces
- As an example, the PULSE system tends to generate images with features that appear ethnically white, as seen in this input image of former US President Barack Obama



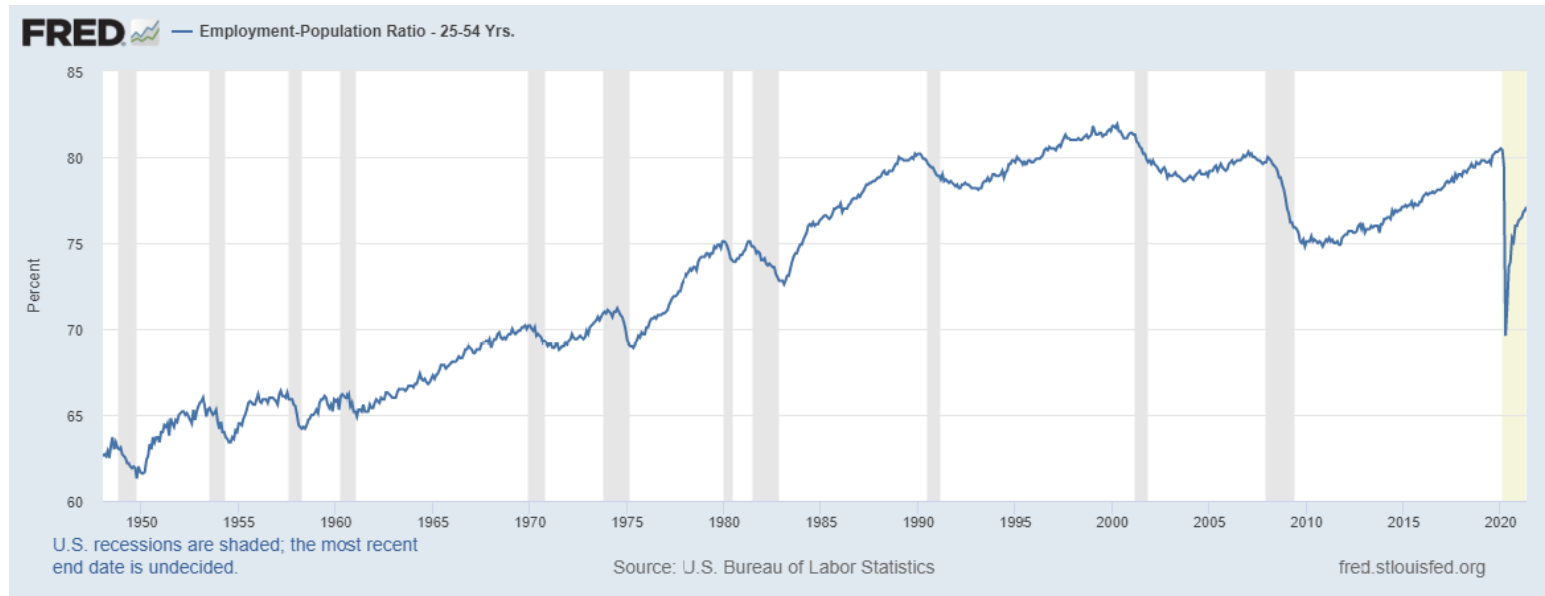
# Risks; Impact on employment

- Concerns about machines eliminating jobs are centuries old. Machines do some of the tasks that humans might otherwise do, but they also make humans **more productive** and therefore more employable and make companies more profitable and therefore able to pay higher wages.
- Their use generally results in **increasing wealth** but tends to have the effect of shifting wealth from labor to capital, further exacerbating **increases in inequality**.
- Previous advances in technology—such as the invention of mechanical looms—have resulted in serious disruptions to employment, but eventually people find new kinds of work to do. On the other hand, it is possible that AI will be doing those new kinds of work too!



# Risks; Impact on employment

Data from the US Bureau of Labor Statistics shows that employment as a fraction of the population reached a 20- year high right before the pandemic, suggesting that the growth of AI is not yet producing large-scale unemployment.



# Risks; Safety-critical applications

- As AI techniques advance, they are increasingly used in high-stakes, safety-critical applications such as **driving cars** and **managing the water supplies** of cities. Fatal accidents have already occurred and highlight the difficulty of formal verification and statistical risk analysis for systems developed using machine learning techniques
- Also, we have adversarial attacks. Adversarial Attacks in AI refers to the deliberate manipulation of models **by introducing carefully crafted input data**. These attacks take advantage of the vulnerabilities in the models' decision-making processes to cause misclassifications or faulty outputs.



# Risks; Cybersecurity

- AI techniques are useful in defending against cyberattack, for example by detecting unusual patterns of behavior, but they will also contribute to the potency, survivability, and proliferation capability of **malware**. For example, reinforcement learning methods have been used to create highly effective tools for automated, personalized blackmail and phishing attacks.
- **Deep Fake:** Synthesize images or videos of people doing things they never did
- **Generating fake comments:**  
Researchers identify a bot network of 1305 accounts active during Republican debate and Donald Trump interview.(2023)



# ASI

- It is not obvious that we can control machines that are more intelligent than us. ASIs can lead to **losing our superiority** and even extinction.
- These concerns have only become more widespread with recent advances in deep learning, the publication of books such as Superintelligence by Nick Bostrom (2014), and public pronouncements from Stephen Hawking, Bill Gates, Martin Rees, and Elon Musk.
- What do you think?

