Introduction to Artificial Intelligence

AI.OFFENSE.1 Stephen Campbell

EU CYBERNET SUMMER SCHOOL 2025

Cyber Crisis Management: Navigating Disinformation and Cyber Attacks in the AI Era

EU CyberNet

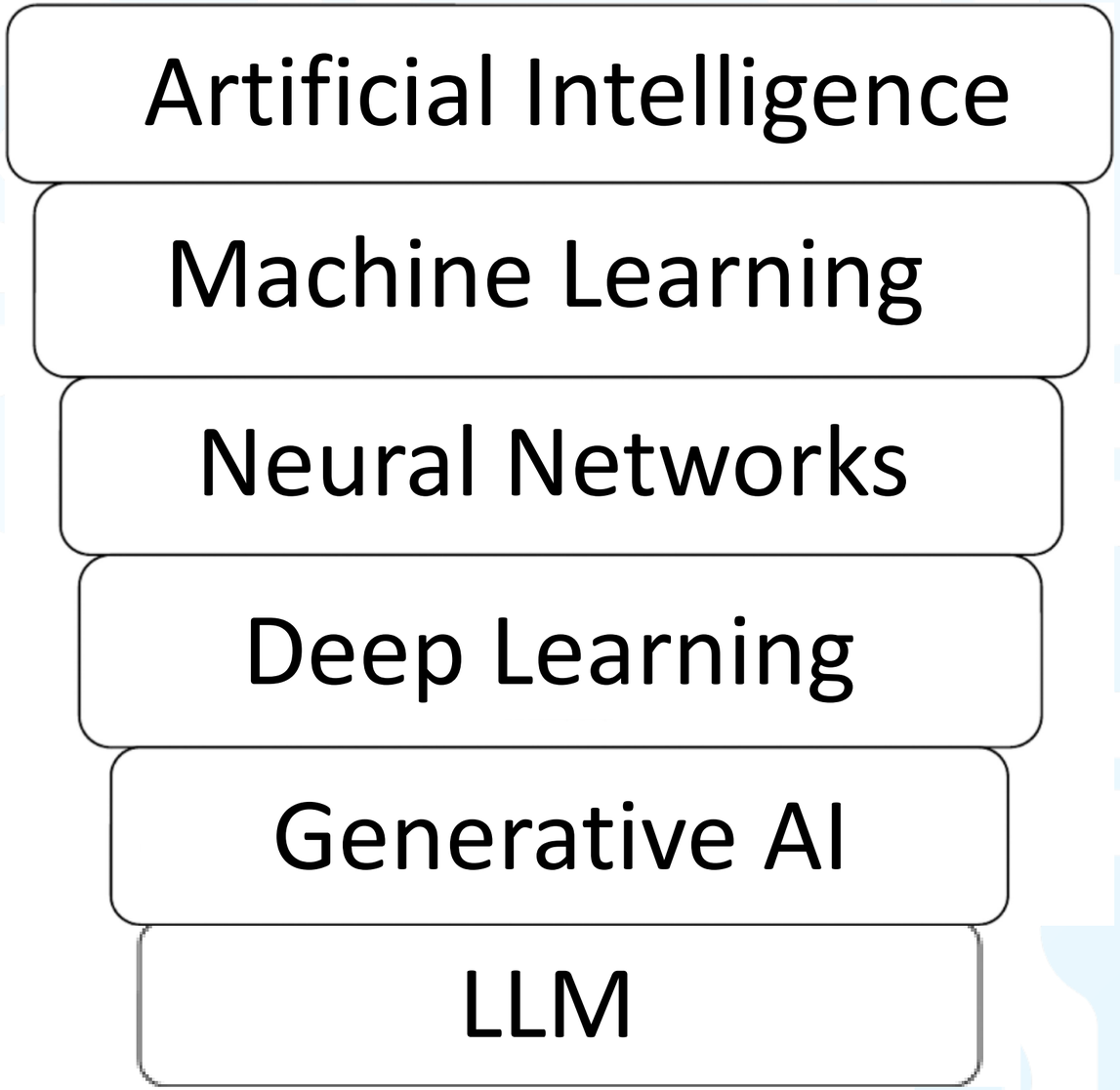
Federal Foreign Office

Funded by the European Union

Module Outline

- Terminology and History
- Neural Networks
- The Generative AI Wave
- Modeling Language and Imagery
- Challenges and the Future of AI

EU CyberNet
Federal Foreign Office
Funded by the European Union

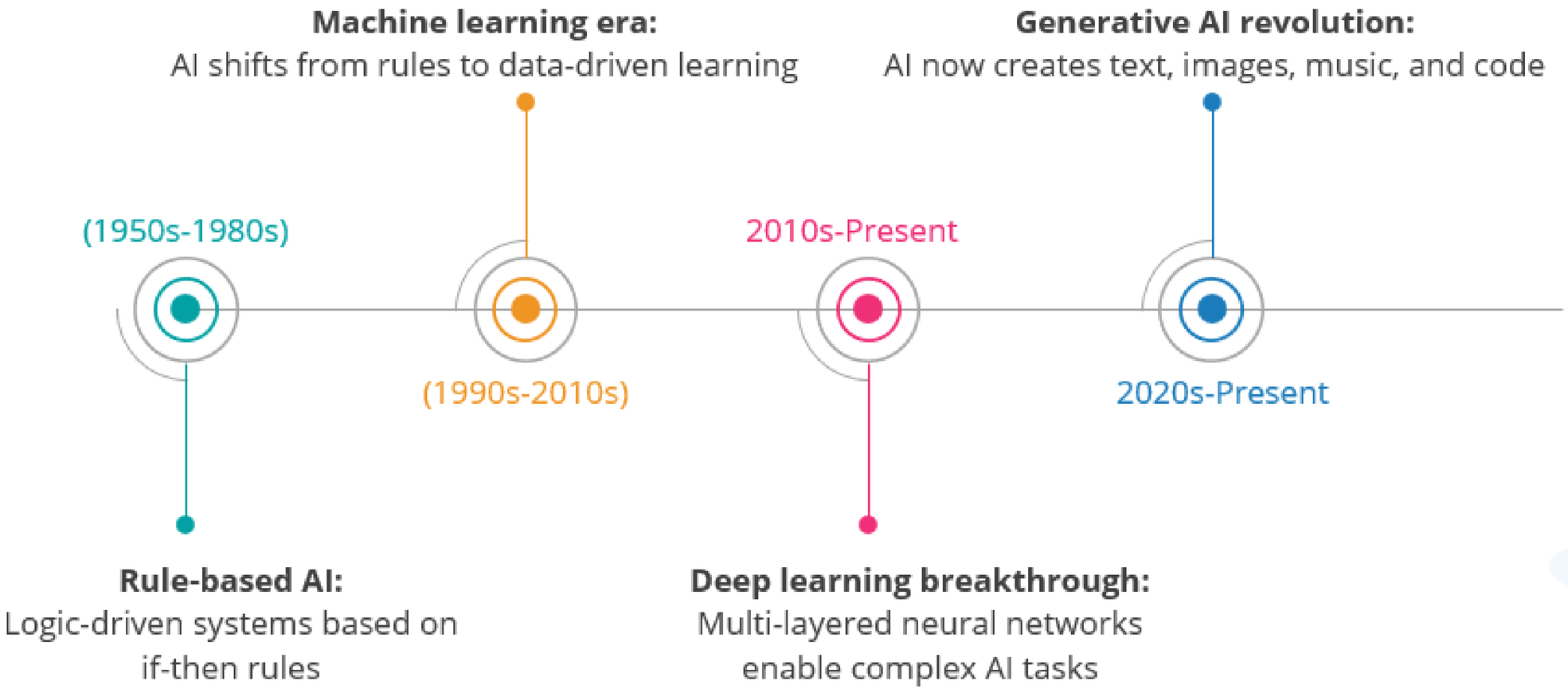


EU CyberNet
Federal Foreign Office
Funded by the European Union

Definitions

- **Artificial Intelligence**
  - *The capability for machines to imitate intelligence human behavior*
- **Machine Learning**
  - *An application of AI that allows computer systems to automatically learn from experience without explicit programming*
- **Neural Networks**
  - *An attempt to model networks of neurons in the brain with computational circuits*
- **Deep Learning**
  - *An application of neural networks strengths organized into many layers*
- **Generative AI**
  - *A type of deep learning that can create new content, including text, images and audio, in response to a query or prompt*
- **Large Language Model (LLM)**
  - *A type of generative AI that can perform a variety of natural language processing (NLP) tasks, including generating and classifying text, answering questions in a conversational manner and translating text from one language to another*

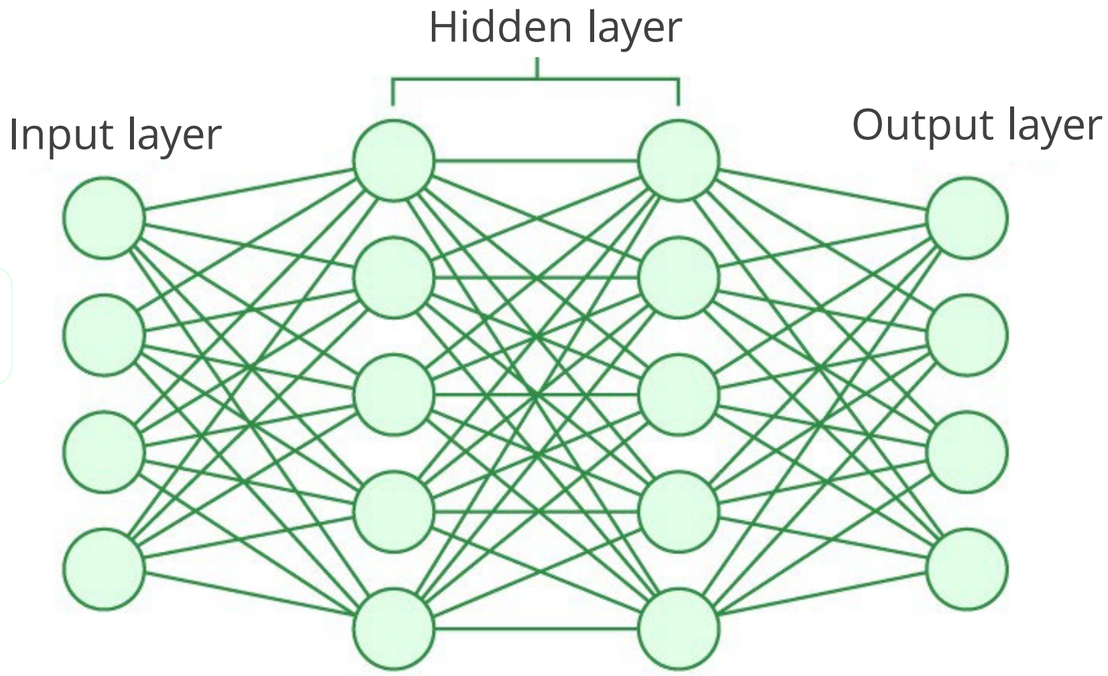
How Did We Get Here?



Courtesy of Purdue University

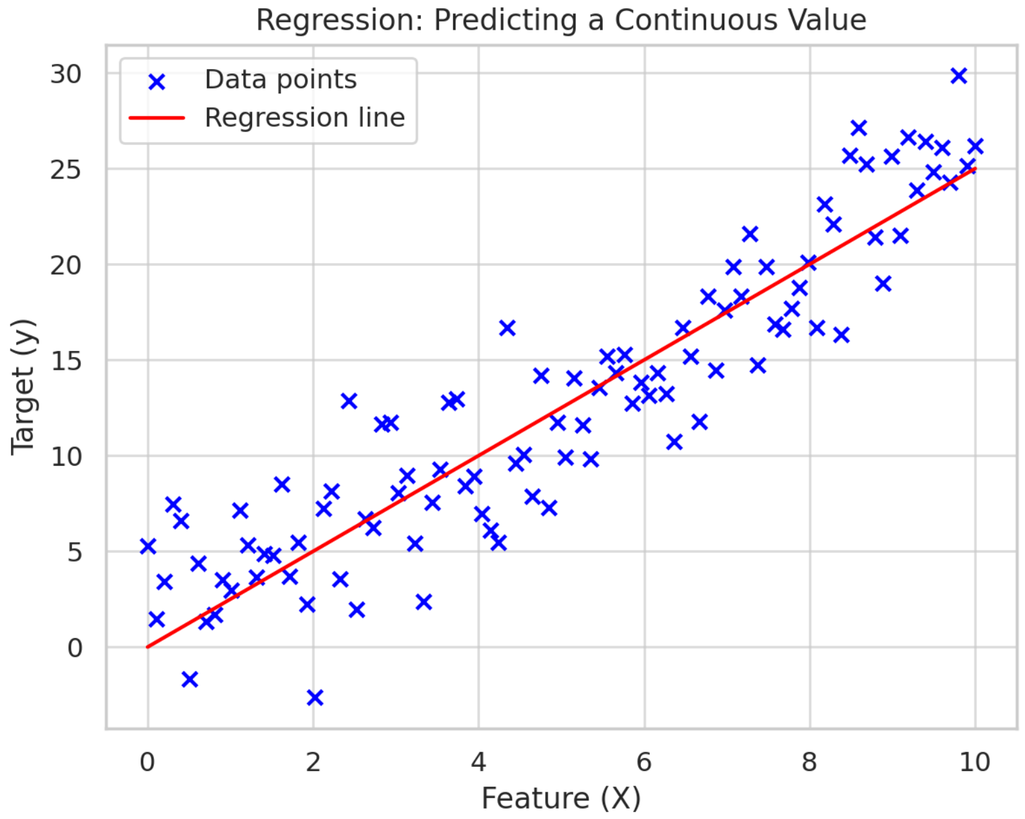
Neural Networks

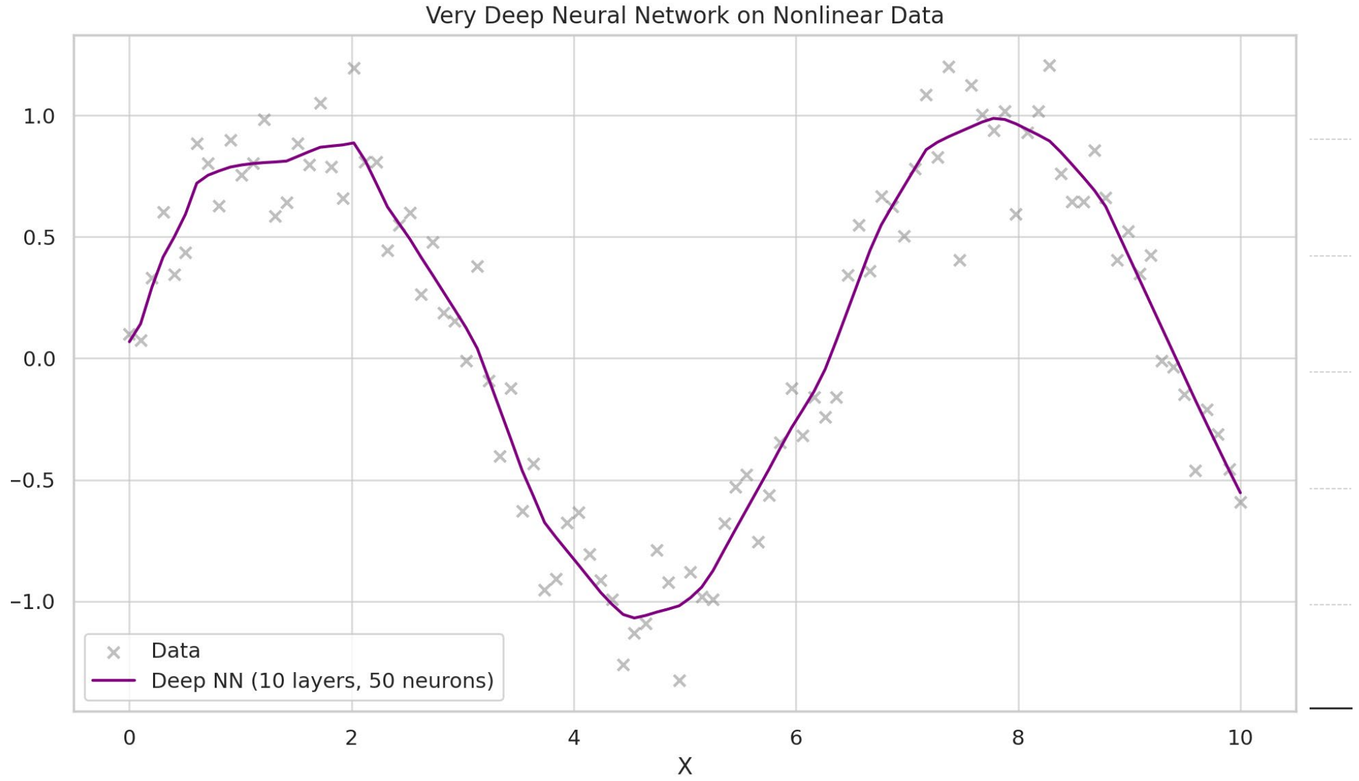
- Mimics the human brain
- The work horse of deep learning
- Most common types are recurrent neural networks and convolutional neural networks



Courtesy of Purdue University

Regression

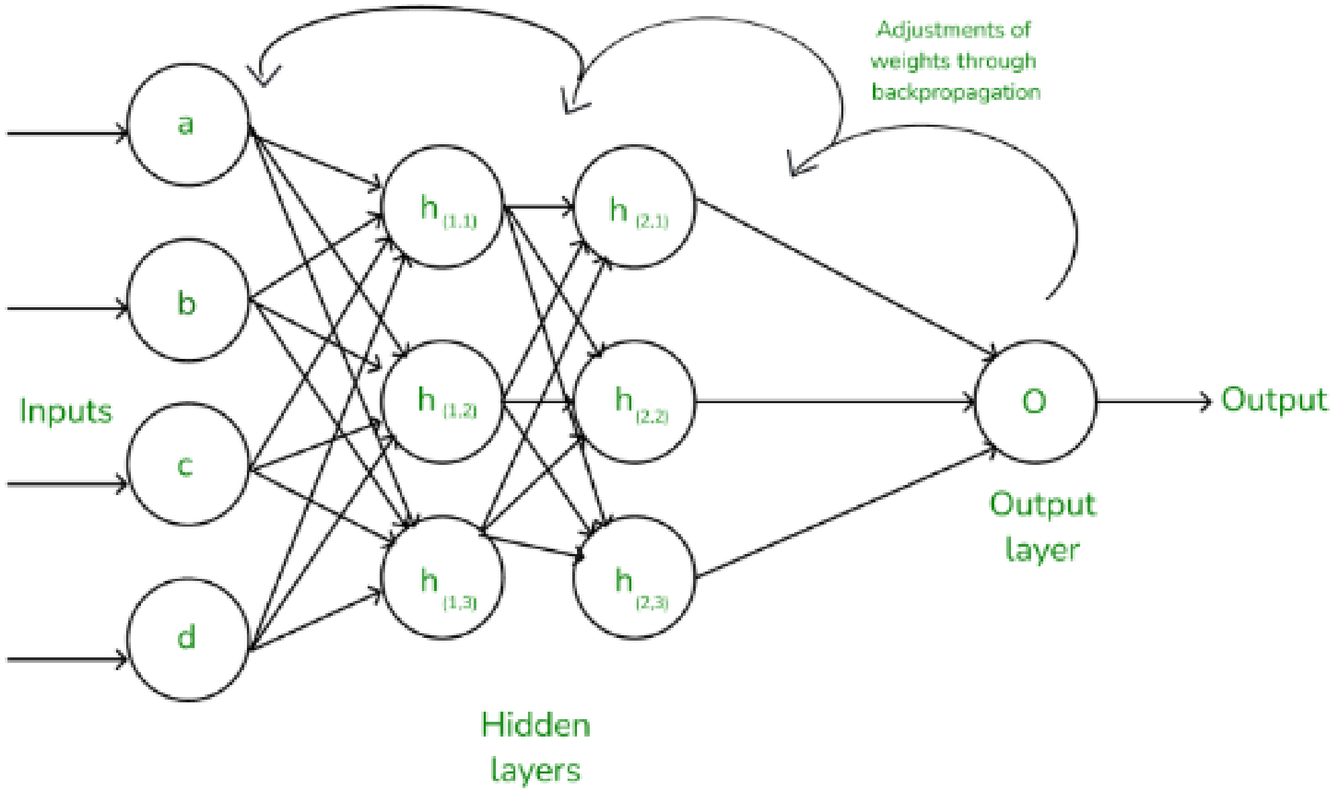




EU CyberNet
Federal Foreign Office
Funded by the European Union

Back Propagation

- We start with a set of inputs
- We make a forward pass through the network to get an output
- We calculate the “loss” or difference between the actual and the expected output
- Then use back propagation to go back through the network adjusting the weights to minimize the loss
- Rinse and repeat till we get the right answer



The Generative AI Wave

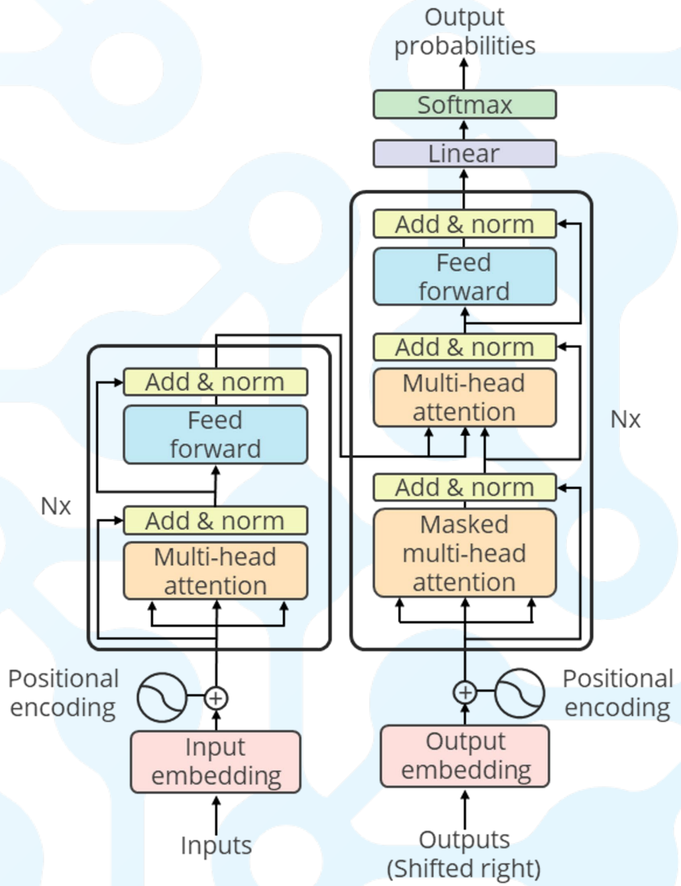
- Massive Compute Power
- Big Data
- Transformer Architecture

Attention Is All You Need

Ashish Vaswani* Google Brain avaswani@google.com
Noam Shazeer* Google Brain noam@google.com
Niki Parmar* Google Research nikip@google.com
Jakob Uszkoreit* Google Research usz@google.com
Llion Jones* Google Research llion@google.com
Aidan N. Gomez* † University of Toronto aidan@cs.toronto.edu
Łukasz Kaiser* Google Brain lukaszkaiser@google.com
Illia Polosukhin* ‡ illia.polosukhin@gmail.com

Abstract

The dominant sequence transduction models are based on complex recurrent or convolutional neural networks that include an encoder and a decoder. The best performing models also connect the encoder and decoder through an attention mechanism. We propose a new simple network architecture, the Transformer, based solely on attention mechanisms, dispensing with recurrence and convolutions entirely. Experiments on two machine translation tasks show these models to be superior in quality while being more parallelizable and requiring significantly less time to train. Our model achieves 28.4 BLEU on the WMT 2014 English-to-German translation task, improving over the existing best results, including ensembles, by over 2 BLEU. On the WMT 2014 English-to-French translation task, our model establishes a new single-model state-of-the-art BLEU score of 41.8 after training for 3.5 days on eight GPUs, a small fraction of the training costs of the best models from the literature. We show that the Transformer generalizes well to other tasks by applying it successfully to English constituency parsing both with large and limited training data.



EU CyberNet
Federal Foreign Office
Funded by the European Union

Generative AI can be Creative

- Think of GenAI as a Chef
- with a set of ingredients (data) and recipes (algorithms)
- Instead of following a fixed recipe the chef might experiment, creating new dishes wth urprising new flavors
- Similarly GenAI can use data and algorithms to cook up new content, adding its own creative touch

Large Language Models

GPT 4

DeepSeek

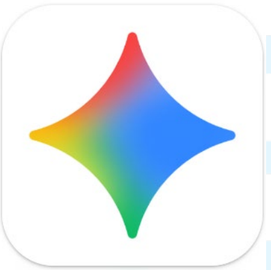
Claude

BERT

Cohere

Falcon

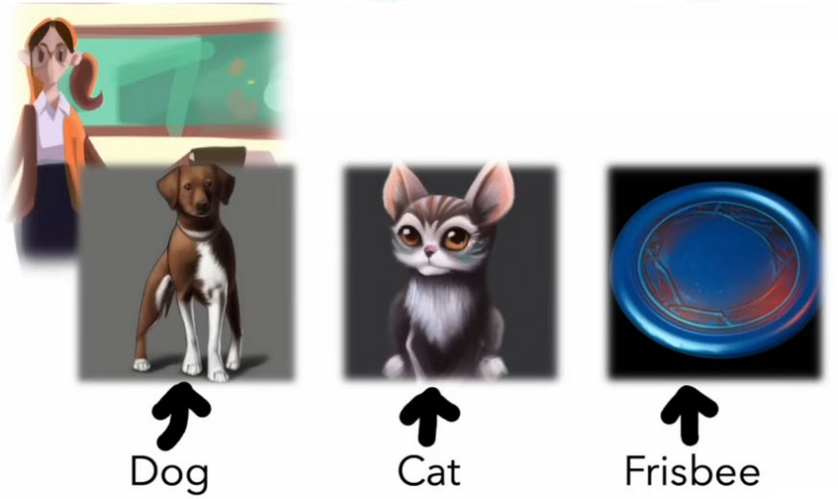
LLaMA



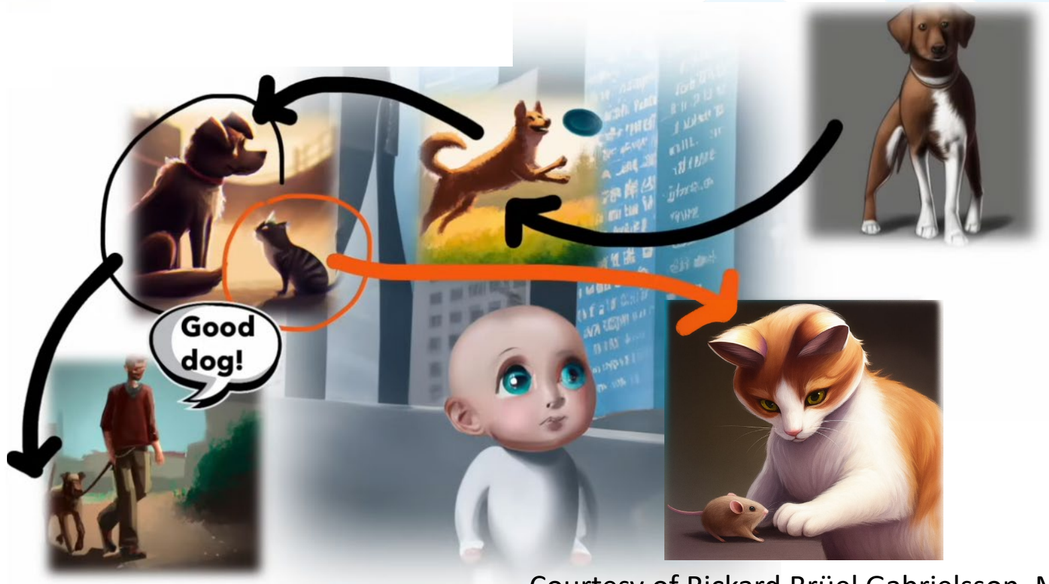
Gemini

Analogies to Training Approaches

Supervised Learning

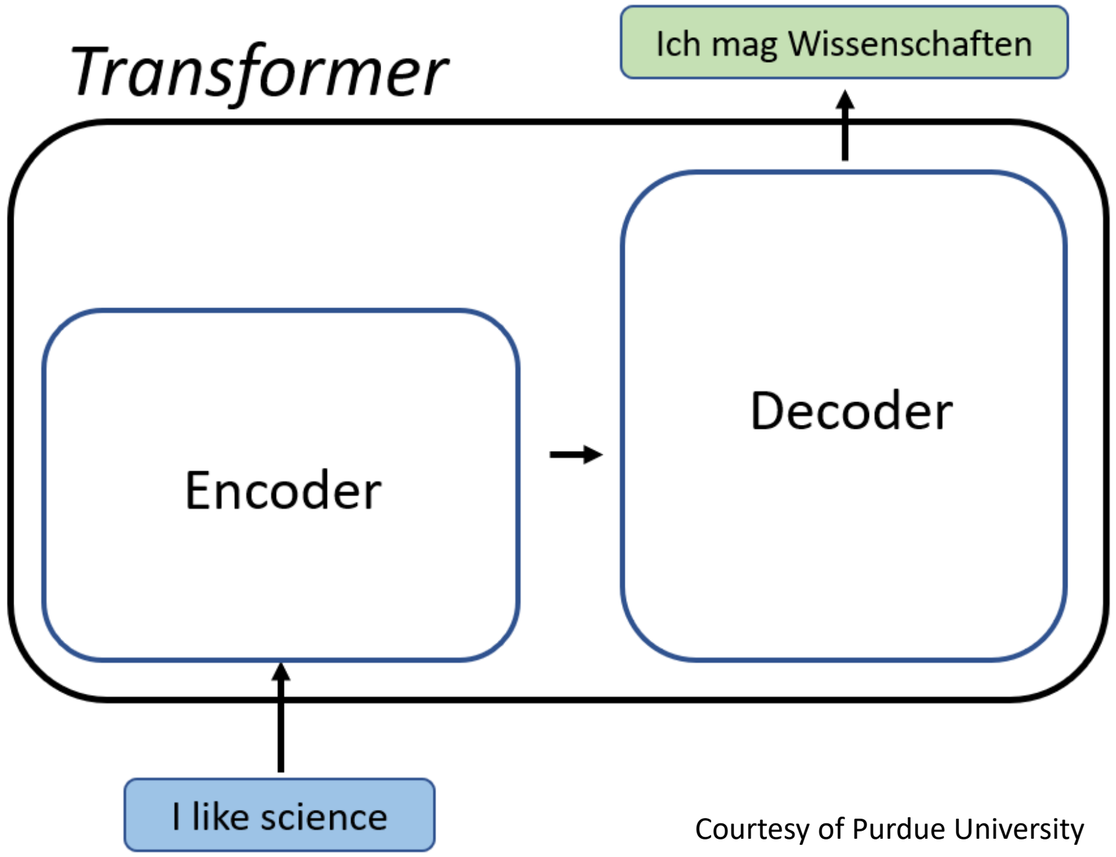


Self-Supervised Learning



Courtesy of Rickard Brüel Gabrielsson, MIT

The Transformer Architecture



Courtesy of Purdue University

Self-Attention

Word Embeddings

- Words are represented as points in an n-dimensional space
- This allows us to capture the complexity and nuance of language in mathematical form
- We use tensor algebra to quantify similarity and relationships and to transform neural states

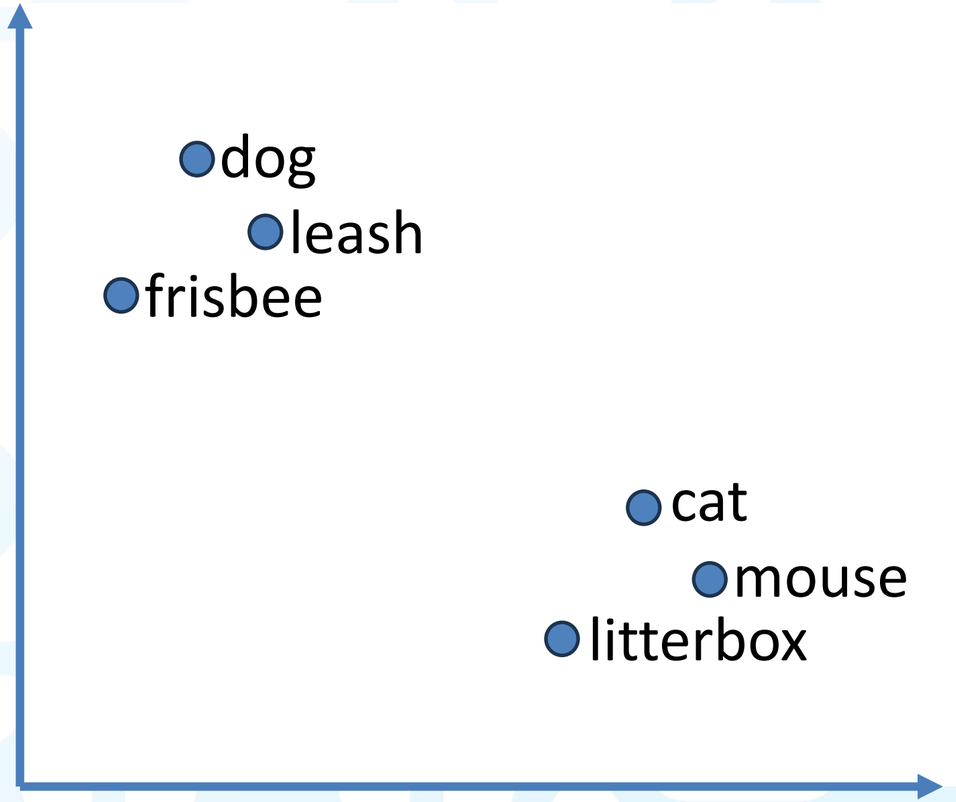
Word Coordinates

	Gender	Age
grandfather	[1,	9]
man	[1,	7]
adult	[5,	7]
woman	[9,	7]
boy	[1,	2]
child	[5,	2]
girl	[9,	2]
infant	[5,	1]

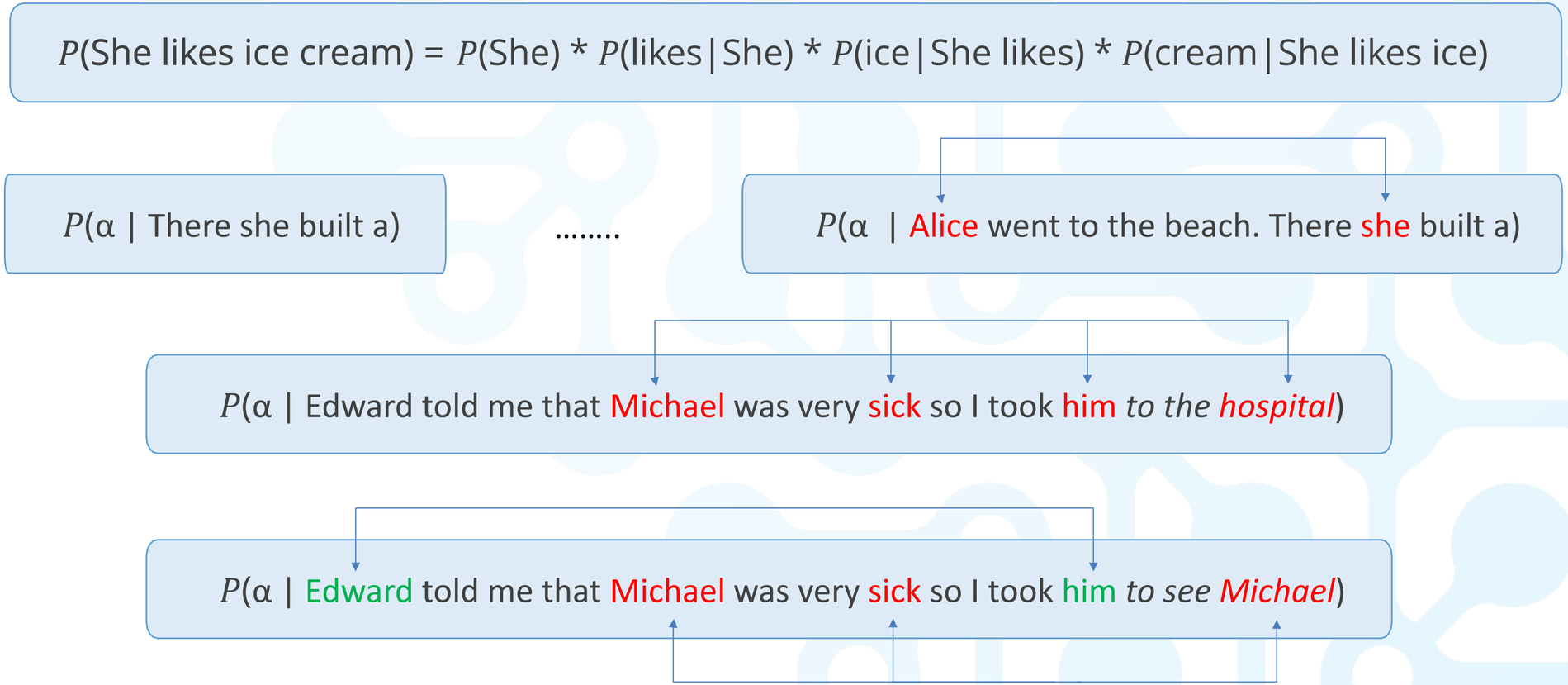
EU CyberNet
Federal Foreign Office
Funded by the European Union

Contextual Word Embeddings

- “You shall know a word by the company it keeps”
- A contextual representation maps both a word and the context into its embedding
- Words that often co-occur end up close to each other in the vector space

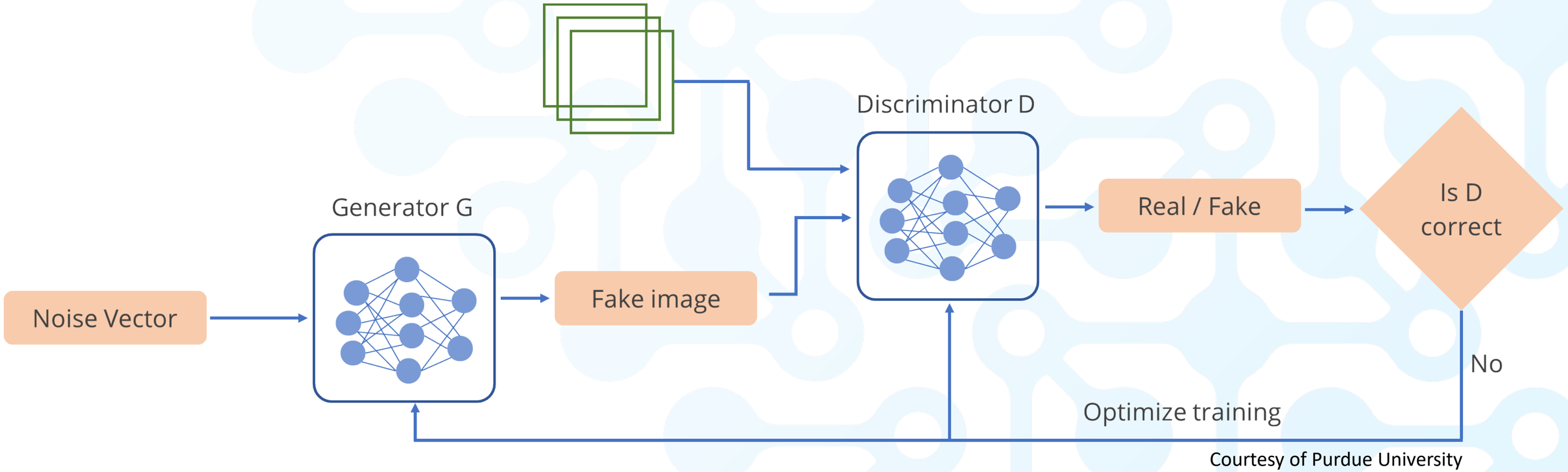


Language Modeling



EU CyberNet
Federal Foreign Office
Funded by the European Union

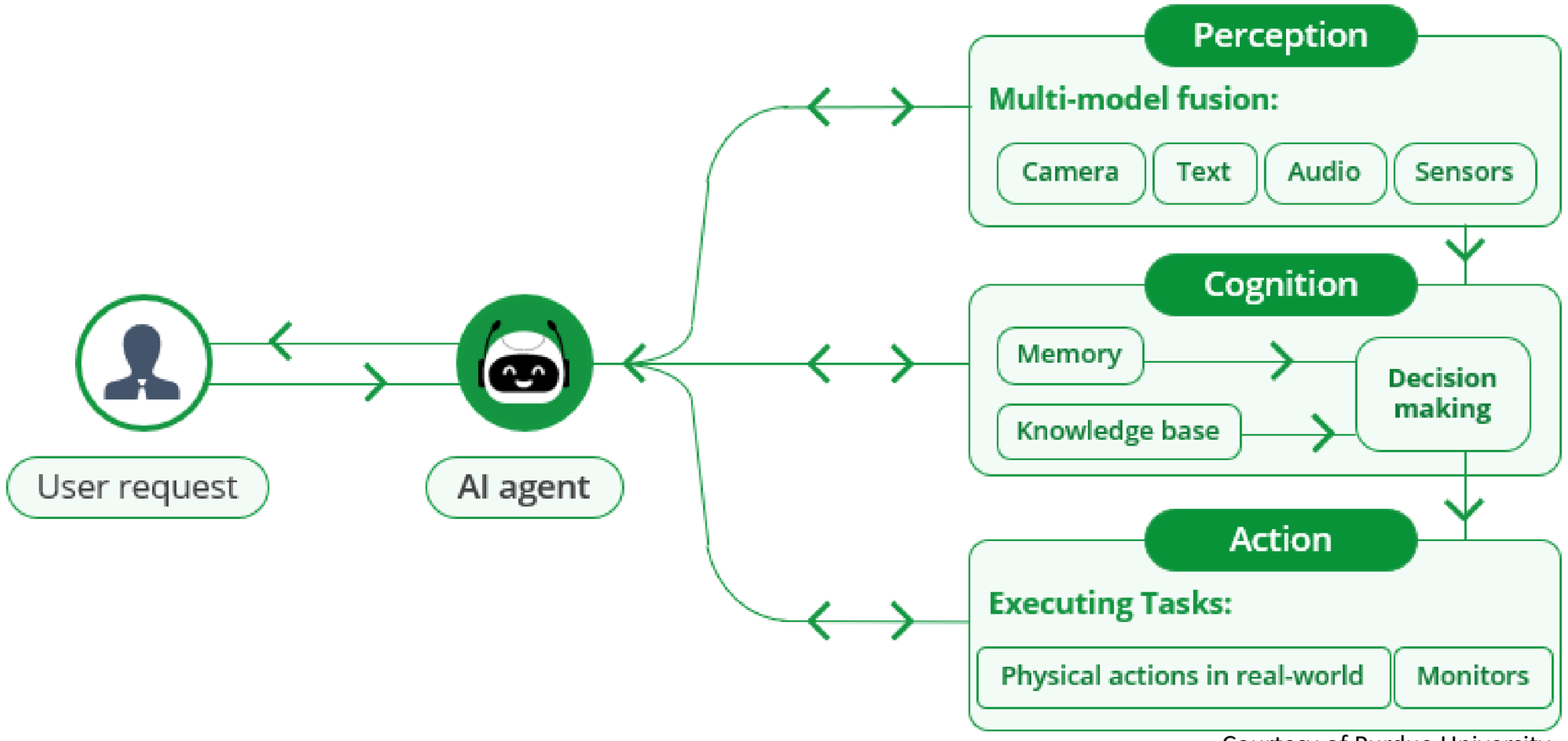
Modeling Imagery with Generative Adversarial Networks



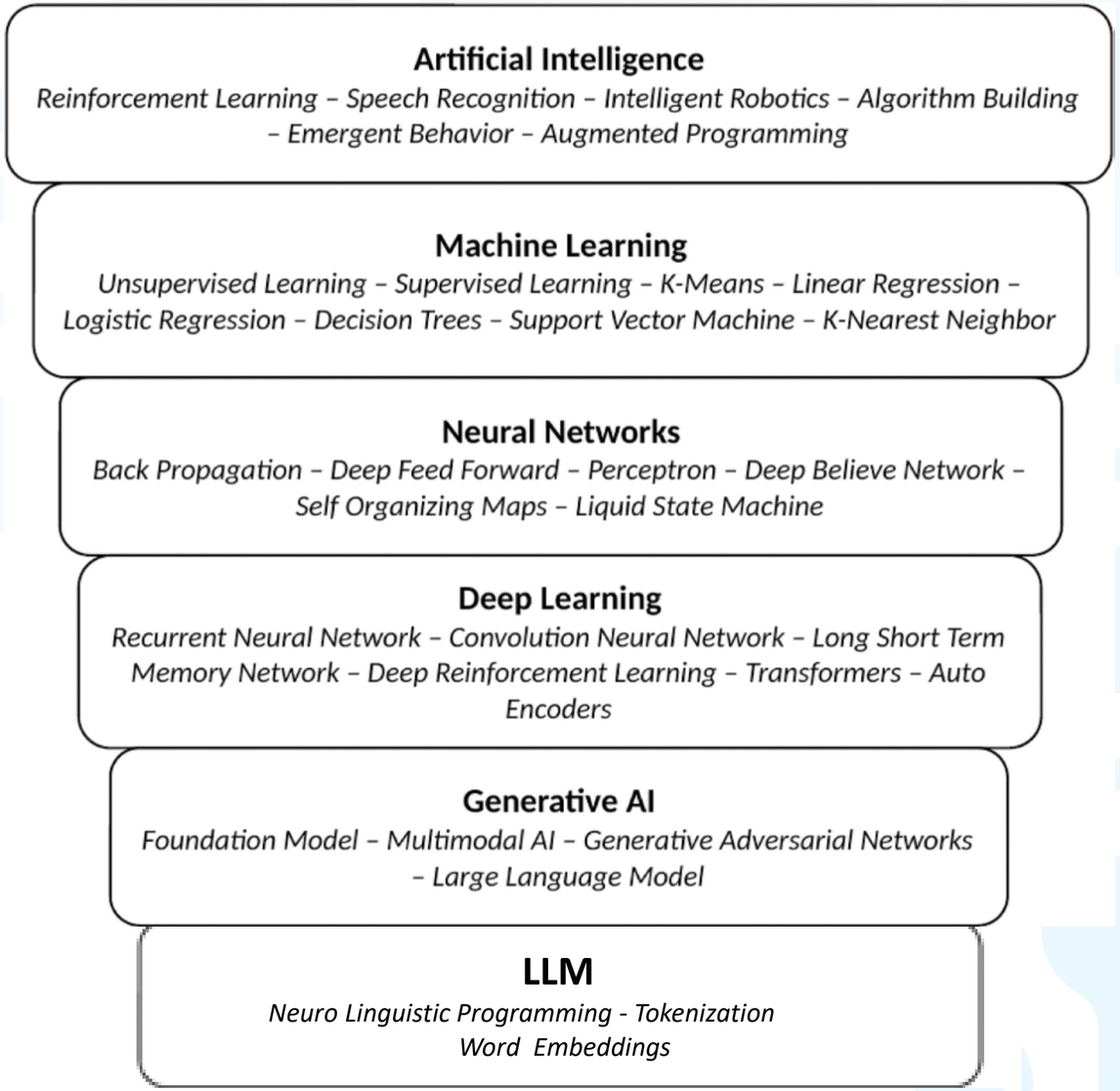
Courtesy of Purdue University

EU CyberNet
Federal Foreign Office
Funded by the European Union

Agentic AI



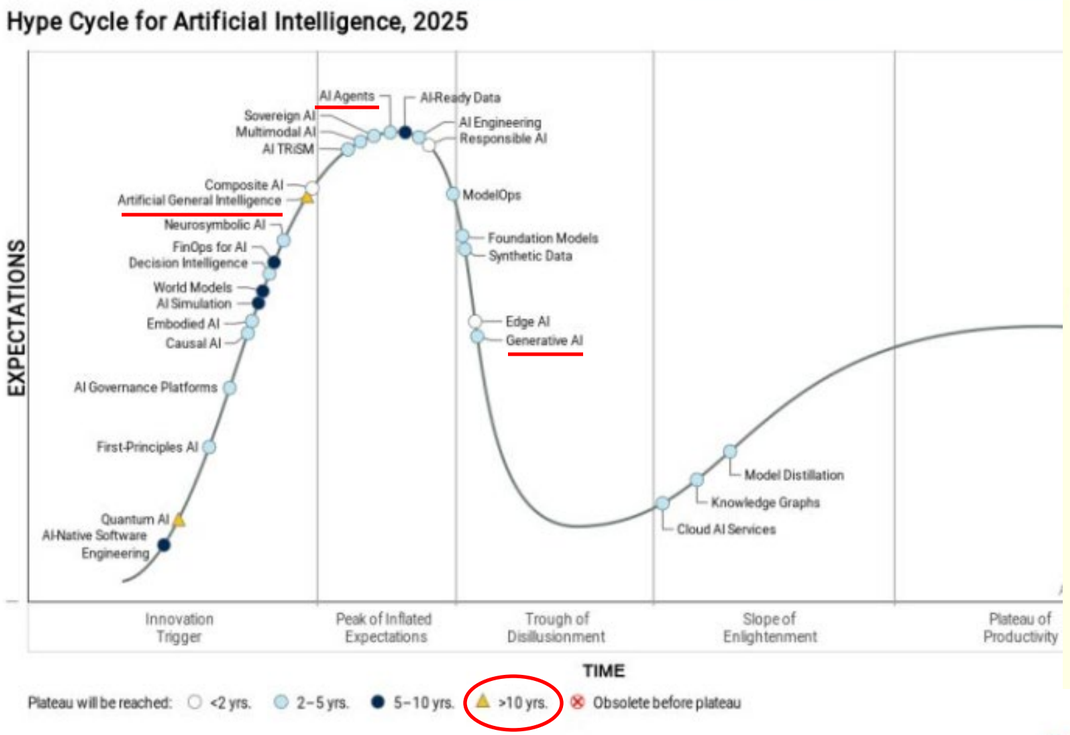
Courtesy of Purdue University

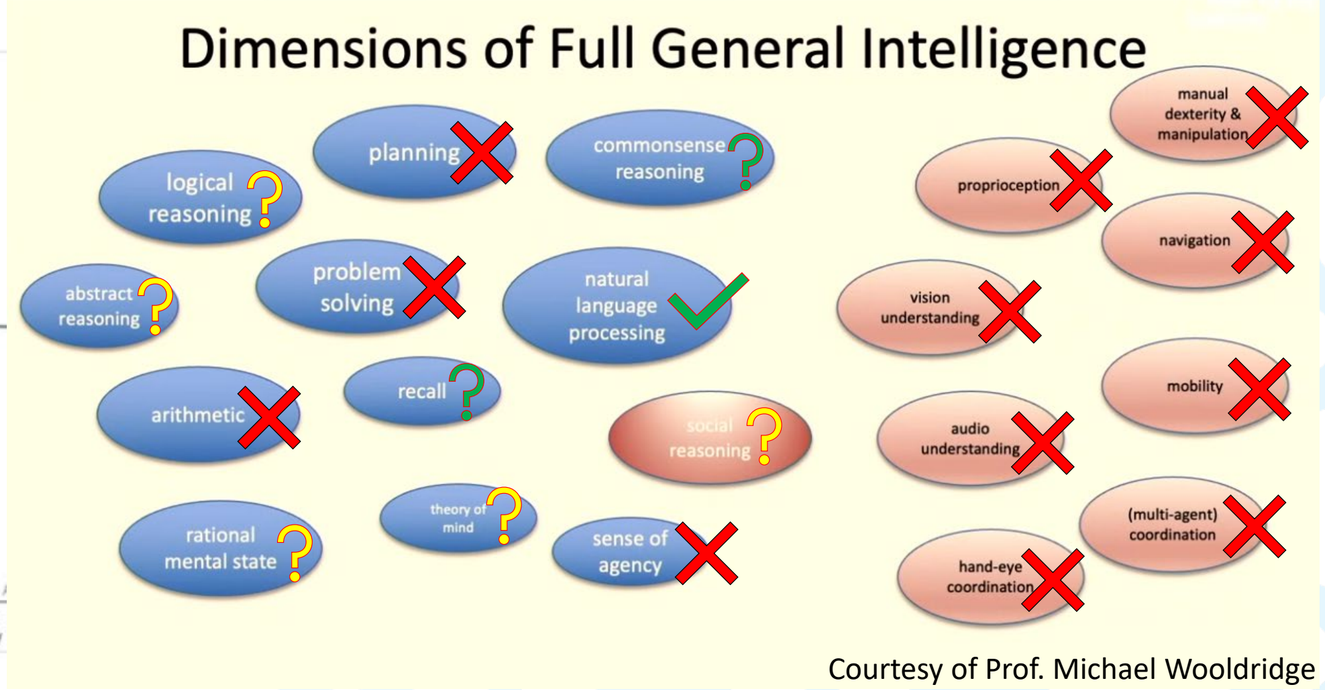

Artificial Intelligence
Reinforcement Learning – Speech Recognition – Intelligent Robotics – Algorithm Building – Emergent Behavior – Augmented Programming
Machine Learning
Unsupervised Learning – Supervised Learning – K-Means – Linear Regression – Logistic Regression – Decision Trees – Support Vector Machine – K-Nearest Neighbor
Neural Networks
Back Propagation – Deep Feed Forward – Perceptron – Deep Believe Network – Self Organizing Maps – Liquid State Machine
Deep Learning
Recurrent Neural Network – Convolution Neural Network – Long Short Term Memory Network – Deep Reinforcement Learning – Transformers – Auto Encoders
Generative AI
Foundation Model – Multimodal AI – Generative Adversarial Networks – Large Language Model
LLM
Neuro Linguistic Programming - Tokenization
Word Embeddings

Challenges of AI

- Hallucinations
- Misinformation
- Anthropomorphism
- Cognitive Offloading
- Data Privacy
- Copyright
- Discrimination
- Fraud
- Environmental Impact

The Future of AI





Courtesy of Prof. Michael Wooldridge

Quiz

1. What is Deep Learning?
2. What is a Word Embedding?
3. How does AI differ from human intelligence?
4. How do you use AI?

EU CyberNet
Federal Foreign Office
Funded by the European Union

EU CyberNet
Federal Foreign Office
Funded by the European Union

BACKUP SLIDES

Growth and Adoption of Generative AI