Introduction to Artificial Intelligence

Instructor:

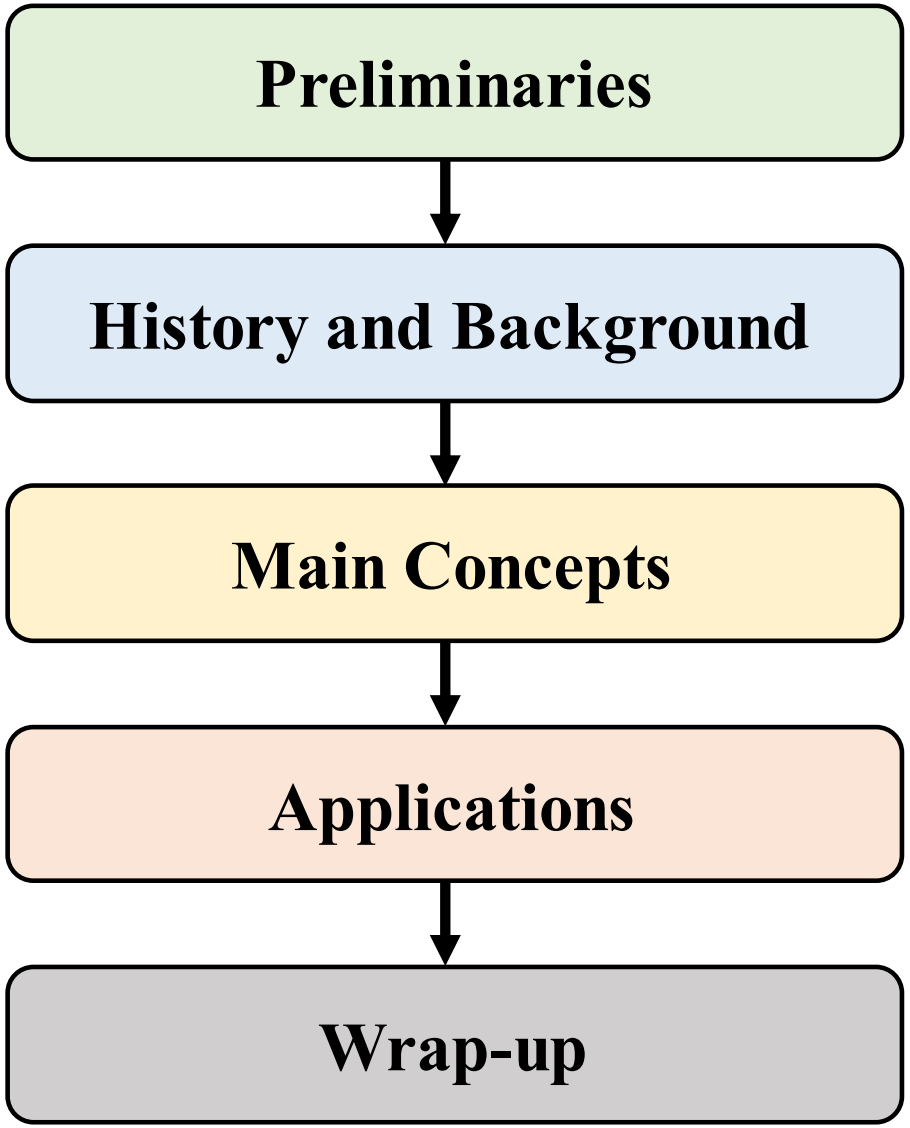
Dr. Navid Asadi

Presenter:

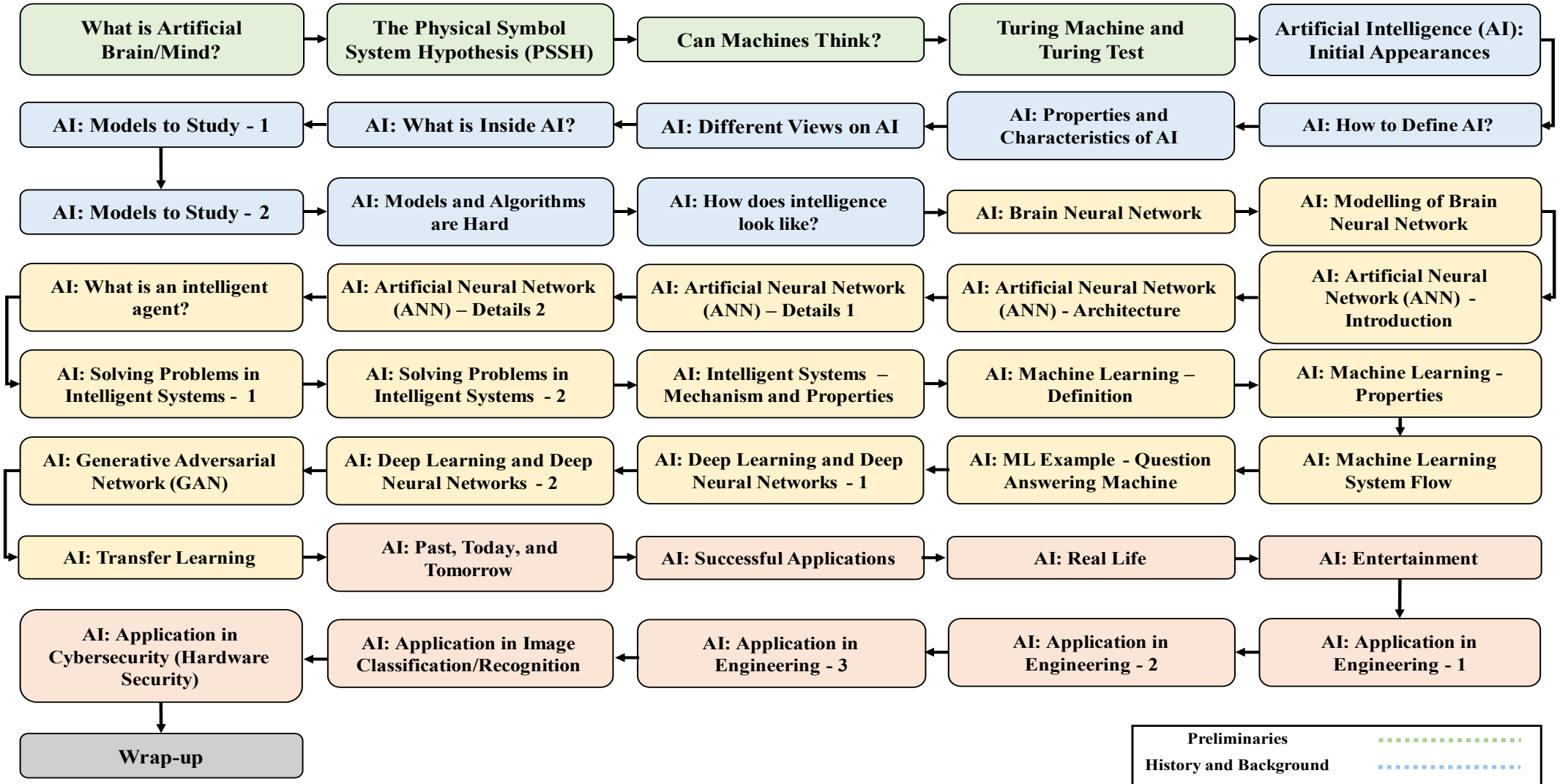
Shayan (Sean) Taheri

Florida Institute for Cybersecurity (FICS) Research
Electrical and Computer Engineering Department
University of Florida (UF)

Lecture Plan



Details of Lecture Plan



What is Artificial Brain/Mind?

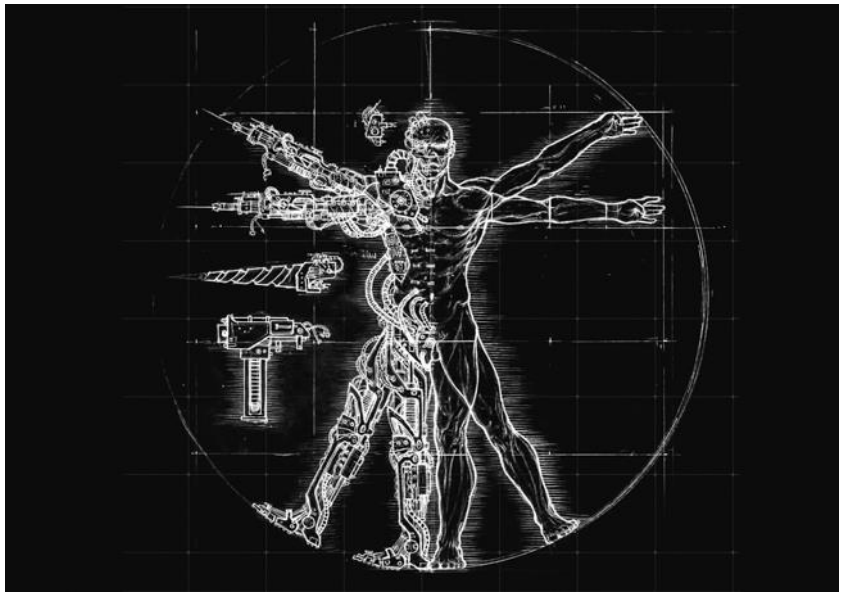
- "You, your joys, and your sorrows, your memories and your ambitions, your sense of personal identity and free will, are in fact no more than the behavior of a vast assembly of nerve cell and their associated molecules."

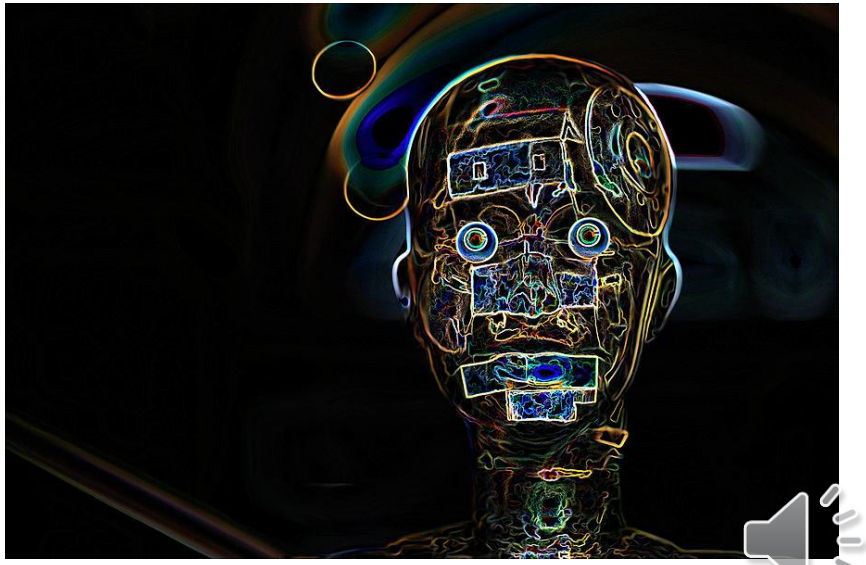
  Francis Crick

- Because we do not understand the brain very well we are constantly tempted to use the latest technology as a model for trying to understand it. In my childhood we were always assured that the brain was a telephone switchboard ('What else could it be?').

  John R. Searle

- **How to theorize the artificial modeling of human feelings, thoughts, and actions?**





The Physical Symbol System Hypothesis (PSSH)

- *Intelligence actions can be modeled by a system manipulating symbols*.
- "A **physical symbol system** consists of a set of entities, called **symbols**, which are physical patterns that can occur as components of another type of entity called an **expression** (or symbol structure).
- A **physical symbol system** has the necessary and sufficient means for performing **intelligent actions**. So, it is a modelling platform. At any instant of time the system will contain a collection of these symbol structures.
- A **symbol structure** is composed of a number of **instances** (or tokens) of symbols related in some physical way (such as one token being next to another).
- Besides these structures, the system also contains a collection of **processes** that operate on expressions to produce other expressions: processes of *creation, modification, reproduction, and destruction*."
- **How to implement the artificial modeling of human feelings, thoughts, and actions?**

Formal Logic/Algebra

Digital Computer

Chess

Can Machines Think?

- "*The new problem has the advantage of drawing a fairly sharp line between the physical and the intellectual capacities of a man.*" (**Turing**, **1950**)

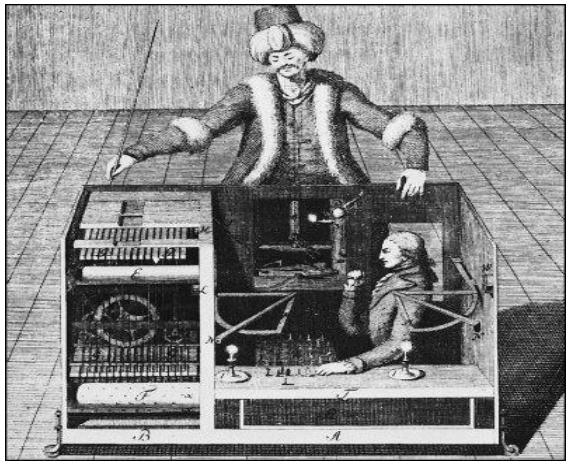
- **Machines with Thinking Abilities:**
  - ✓ A Turing machine is a mathematical model of a physical computing device.
  - ✓ Any given problem for which a Turing machine can provide solution, it can be provided by the physical machine as well.
  - ✓ Formulation: Every function that can be naturally regarded as computable can be computed by a Turing machine.
  - ✓ Can we create intelligence using machines?

Alan Turing depicted on the Loebner Prize Gold Medal.

- **The Arguments about Questioning the Thinking Ability of Machines?** Given that the nervous system is not a discrete-state machine, you cannot mimic the behavior of nervous system with a discrete-state machine (*Continuity in the Nervous System*).

- Machines with thinking capabilities: Ctesibius of Alexandria - Water Clock with a Regulator and Thermostat of Wiener - Controller of the Environment Temperature.

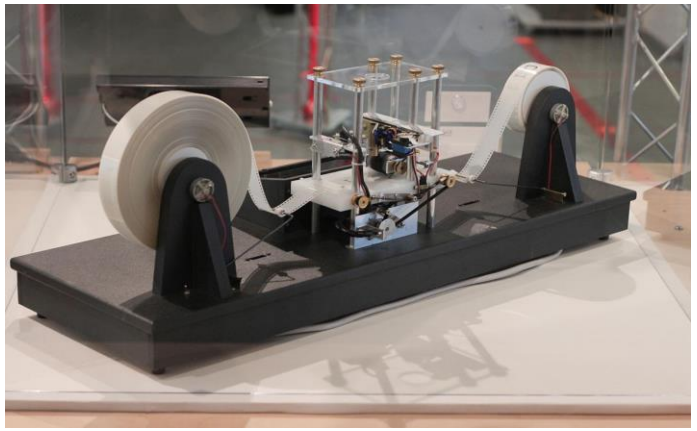
- **How about having a machine capable of having human feelings and thoughts, and performing actions?**



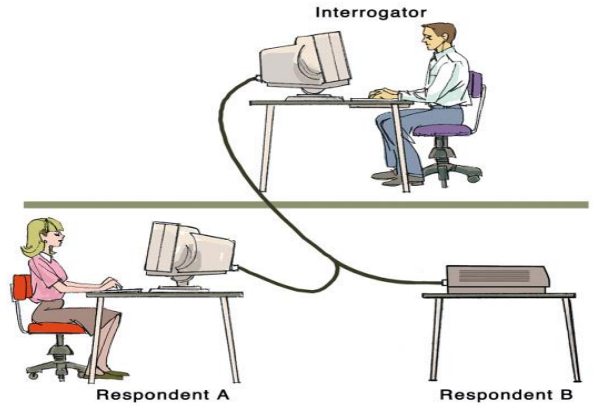
Automated device for playing chess and performing arts .

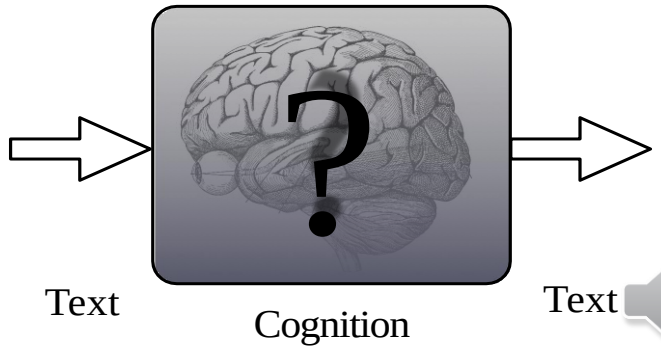
Turing Machine and Turing Test

- **Turing Machine**:
  - ✓ A **finite state machine** with Governing each transition by the input symbol, the current state, and the corresponding entry in the transition table.
  - ✓ The next state is stored into the state register and the output is written to the cell.
  - ✓ Transition Table: A set of entries in the format of
    {<Current State, Input Symbol> → < Next State, Output Symbol, Move>}
  - ✓ *When we do prediction, we use a sort of intelligence*!



- **Turing Test**:
  - ✓ A machine can be described as thinking machine if it passes the **Turing Test**. This test *evaluates the intelligence*.
  - ✓ If a human agent is engaged in two isolated dialogues (connected by teletype), one with a computer, and the other with another human.
  - ✓ The human agent cannot reliably identify which dialogue is with the computer due to its kind of intelligence.
  - ✓ A human communicates with a computer via a teletype. If the human cannot tell he is talking to a computer or another human, it passes the test.





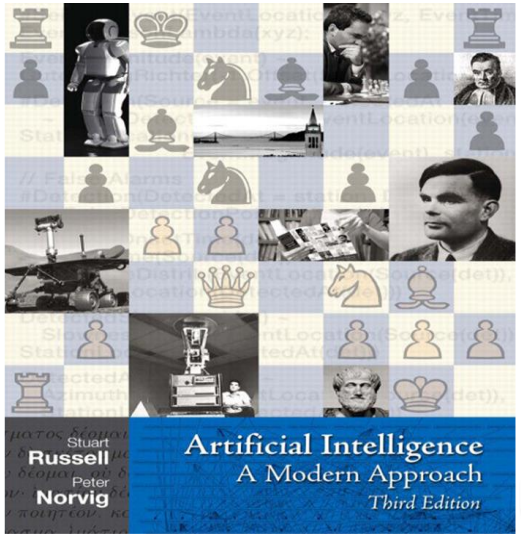
- **How does the machine with thinking ability perform and how to test it?**

Artificial Intelligence (AI): Initial Appearances

- **John McCarthy**: "We propose that a two-month, ten man study of **Artificial Intelligence** carried out during the summer of 1956 […]"
  - ✓ The study is to proceed on the basis of conjecture that every aspect of learning or any other feature of **intelligence** can in principle be *so precisely described* that a machine can be made to simulate it. […]
  - ✓ It may be speculated that a large part of human thought consists of manipulating *words* according to *rules of reasoning* and *rules of conjecture*.

John McCarthy: American Computer Scientist

- **The first generation of AI researchers made these predictions about their work**:
  - ✓ *1958, H. A. Simon and Allen Newell*: "within ten years a digital computer will be the world's chess champion" and "within ten years a digital computer will discover and prove an important new mathematical theorem."
  - ✓ *1965, H. A. Simon*: "machines will be capable, within twenty years, of doing any work a man can do."
  - ✓ *1967, Marvin Minsky*: "Within a generation ... the problem of creating 'artificial intelligence' will substantially be solved."
  - ✓ *1970, Marvin Minsky (in Life Magazine)*: "In from three to eight years we will have a machine with the general intelligence of an average human being."



- **When did the Artificial Intelligence get appeared since the time of the artificial mind theory and later on the Turing Machine idea (1950)?**

AI: How to Define AI?

- The term got coined by **John McCarthy** in **1956** when a group of when scientists began exploring how computers could solve problems on their own..

- **Def. 1 by David Marr**: "AI is the study of complex information processing problems that often have their roots in some aspects of biological information processing. The goal of the subject is to identify solvable and interesting information processing problems, and solve them."

- **Def. 2 by Rodney Brooks**: "The intelligent connection of perception to action."

- **Def. 3 by Alan Turing**: "Actions that are indistinguishable from a human's ones."

- **How to simply define AI?** A machine with the ability to perform cognitive functions such as perceiving, learning, reasoning and solve problems are deemed to hold an artificial intelligence. The benchmark for AI is the human level concerning reasoning, speech, and vision.

- **How to well define AI?** ***We can define intelligence as the computational part of the ability to achieve goals in the world. Varying kinds and degrees of intelligence occur in humans, many animals and some machines. It is the capacity to learn and solve problems in particular tacking novel problems, act rationally, and act like humans***.

- **How to define AI and what properties and characteristics to include in AI?**

AI: Properties and Characteristics of AI

- *Associating AI with certain human behavior*: ***perception, natural language processing, reasoning, planning, and problem solving, learning and adaption, and so forth***.

- The purpose of having AI can be described as <u>better understanding of the human thinking and how to improve it</u>.

- The root of AI is found in Computer Science and Engineering, Philosophy, Mathematics, Cognitive Science and Psychology, Neural Science, and Linguistic.

- **AI Levels**:
  - ✓ ***Narrow AI***: A artificial intelligence is said to be narrow when the machine can perform a specific task better than a human. The current research of AI is here now.
  - ✓ ***General AI***: An artificial intelligence reaches the general state when it can perform any intellectual task with the same accuracy level as a human would.
  - ✓ ***Strong AI***: An AI is strong when it can beat humans in many tasks.

- **Major Goals**:
  - ✓ Understand the principles that make intelligence possible (in humans, animals, and artificial agents).
  - ✓ Developing intelligent machines or agents (no matter whether they operate as humans or not).
  - ✓ Formalizing knowledge and mechanizing reasoning in all areas of human endeavor.
  - ✓ Making the working with computers as easy as working with people.
  - ✓ Developing human-machine systems that exploit the complementariness of human and automated reasoning.

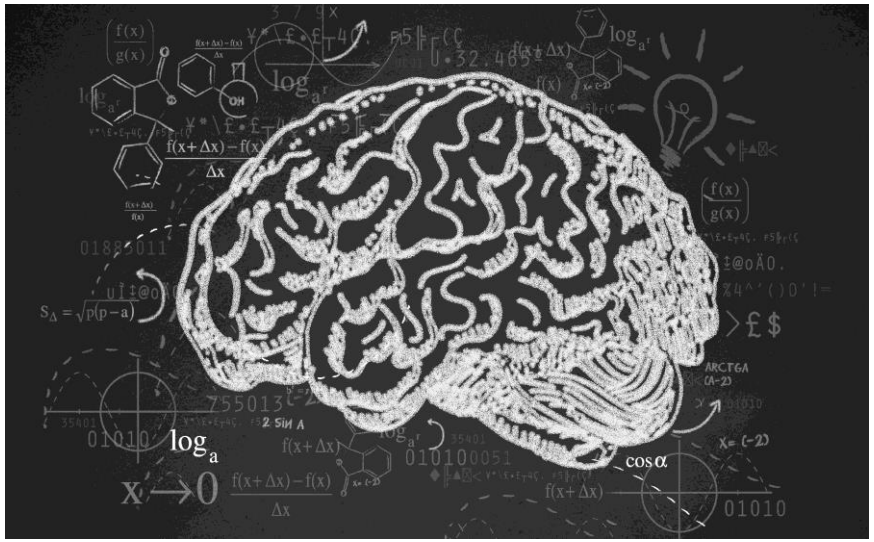
AI: Different Views on AI

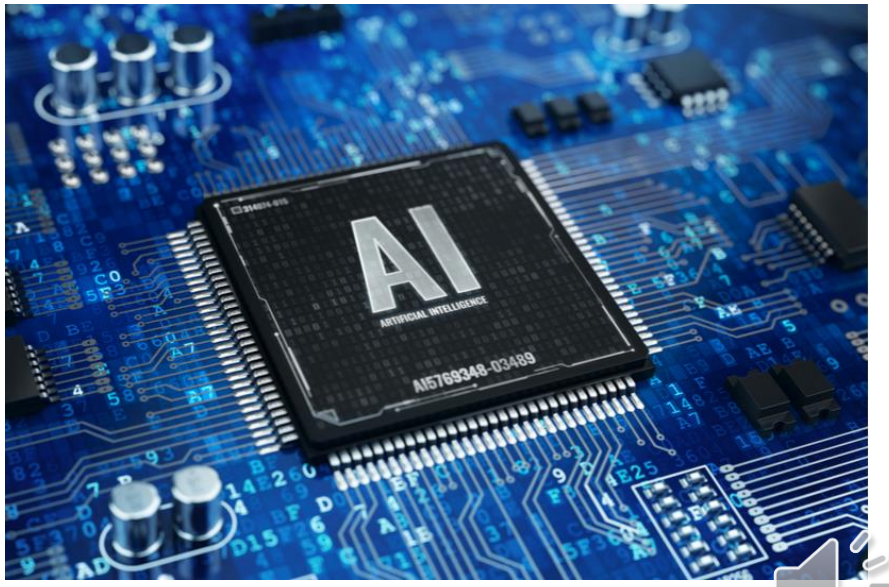
- **Philosophy, Ethics, and Religion**:
  - ✓ What is intelligence?
  - ✓ Is there any formal expression?
  - ✓ How to define mind as a machine with internal operations?

- **Cognitive Science, Neuroscience, Psychology, and Linguistics**:
  - ✓ Understand natural forms of intelligence.
  - ✓ Learn principles of intelligent behavior.

- **Engineering**:
  - ✓ Can we build intelligent devices and systems?
  - ✓ Autonomous and semi-autonomous for replicating human capabilities, improving performance, and so forth.

- **How should scientists from different areas of science view AI and what technical elements (i.e. models, libraries, and etc.) should we have inside AI?**

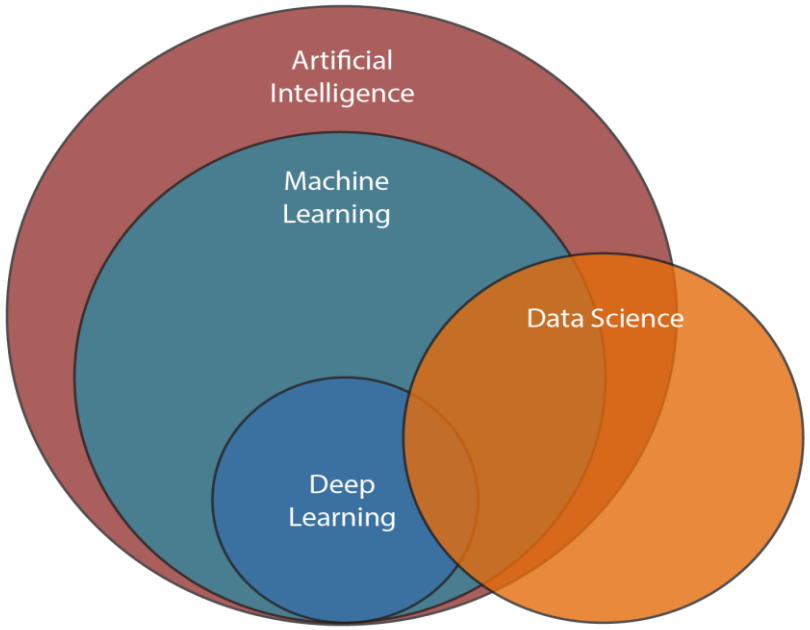




AI: What is Inside AI?

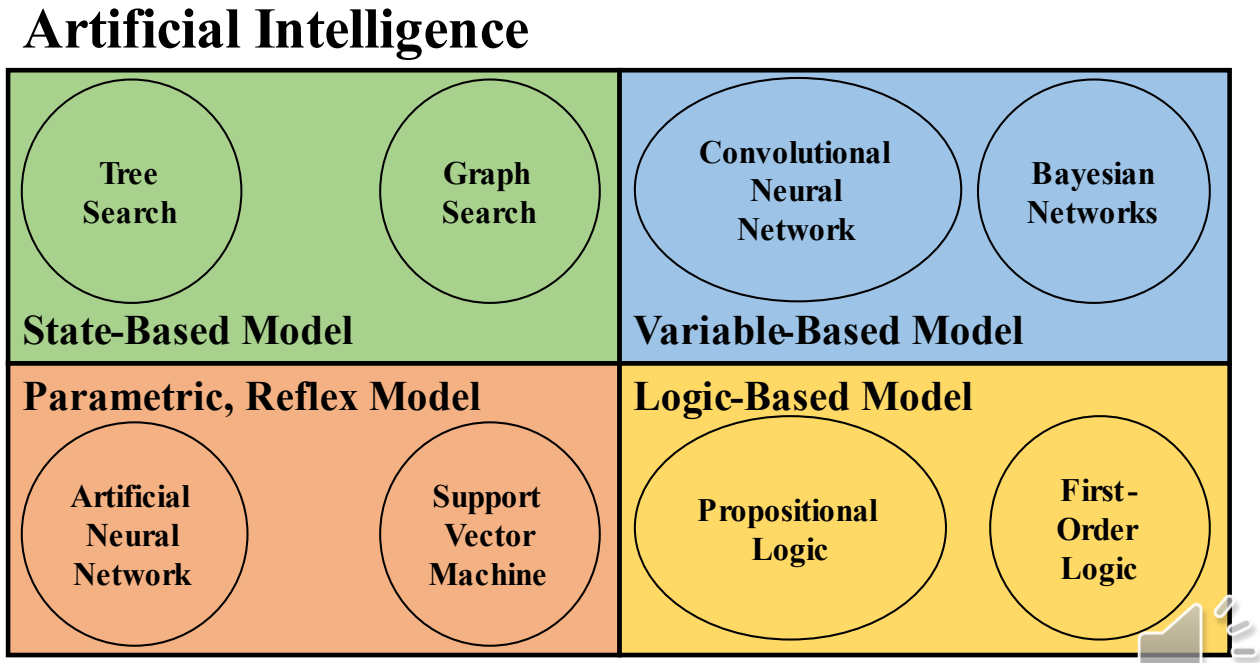
- **Applications**:
  - ✓ Image and Speech Recognition
  - ✓ Natural Language Processing
  - ✓ Autonomous Driving

- **Types of Models**:
  - ✓ Artificial Intelligence
  - ✓ Machine Learning
  - ✓ Deep Learning



- **Software/Hardware**:
  - ✓ Graphical Processing Unit
  - ✓ Parallel Processing Tools (e.g. Spark)
  - ✓ Cloud Data Storage and Computing System

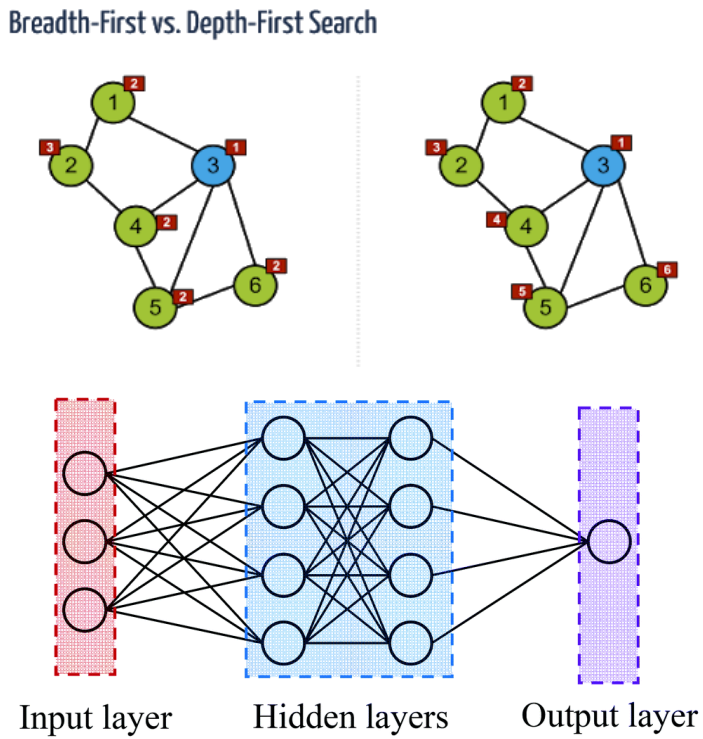
- **Programming Languages and Libraries**:
  - ✓ Python, MATLAB, Java, and C++
  - ✓ TensorFlow, Keras, PyTorch, OpenCV, and Caffe



AI: Models to Study - 1

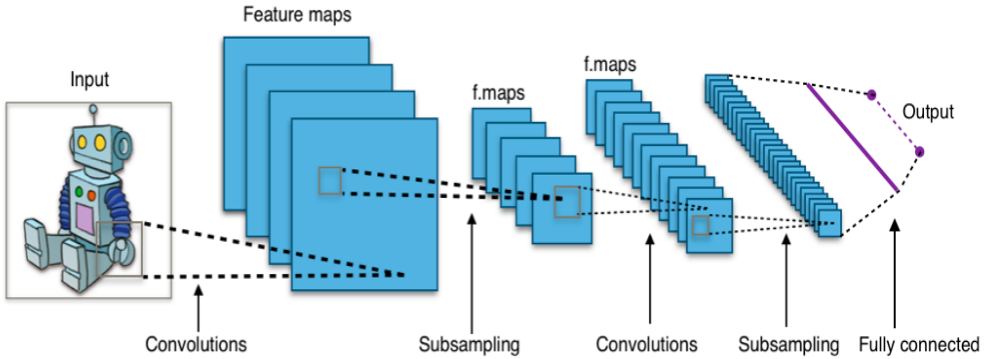
- *The array of problems the businesses face is huge, and the variety of models used to solve these problems is quite wide, as some algorithms are better at dealing with certain types of problems than the others. One needs a clear understanding of what every type of models is good for.*

- **State-Based Models**:
  - ✓ Solutions are defined as a sequence of steps.
  - ✓ Model a task as a graph of states and a solution as a path in the graph.
  - ✓ A state captures all of the relevant information about the past in order to act in the future.
  - ✓ **Apps**: Navigation and Games.
  - ✓ **Options**: Tree Search (Breadth-first search, Depth-first search, and Iterative deepening), Graph search (Dynamic programming)
- **Parametric, Reflex-Based Models**:
  - ✓ Given a set of <Input, Output> pairs of training data, learn a set of parameters that will map input to output for future data.
  - ✓ **Apps**: Classification and Regression.
  - ✓ **Options**: **Artificial Neural Networks (ANN)**, Decision Trees, Support Vector Machines, Regression, Principal Component Analysis, K-Means Clustering, and K-Nearest Neighbor.



AI: Models to Study - 2

- **Variable-Based Models (Uncertainty):**
  - ✓ Solution in an assignment of values for a set of variables.
  - ✓ Apps: Soduko, Speech Recognition, and Face Recognition.
  - ✓ **Options**: **Convolutional Neural Networks**, Constraint Satisfaction, Bayesian Networks, Factor Graphs, Dynamic Ordering, and Hidden Markov Models.



- **Logic-Based Models (Logic)**:
  - ✓ Symbolic representation of classes of objects.
  - ✓ Deductive Reasoning.
  - ✓ **Apps**: Question Answering Systems and Natural Language Understanding.
  - ✓ **Options**: Propositional Logic, First-Order Logic, Knowledge Base.

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

A	B	$A \rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

- **How computationally complex these models are?**
- **How are these models employed in intelligence behavior?**

AI: Models and Algorithms are Hard

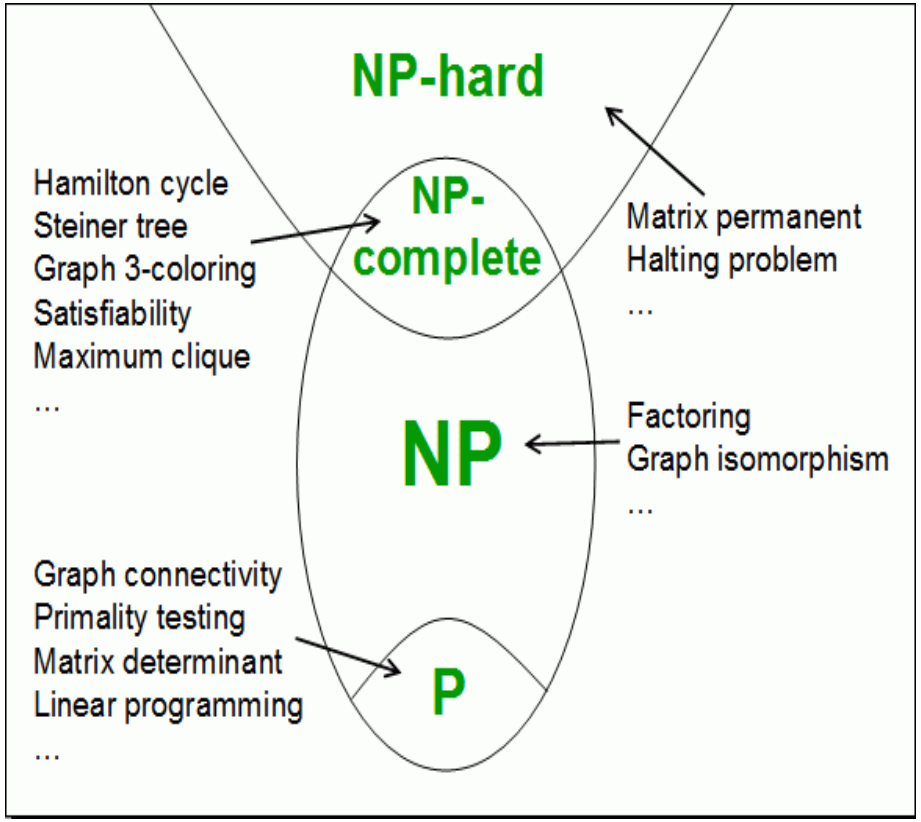
- Mathematics formalizes the three main areas of AI: **Computation**, **Logic**, and **Probability**.

- *AI problems often involve large and complex data*:
  - ✓ Speech, images, natural languages, genomic data, and so forth.
  - ✓ What are the right primitives to use?
  - ✓ Data are often noisy, unstructured, and have missing values.

- **Computationally (NP-) Hard**: A problem is **NP-hard** if an **algorithm** for solving it can be translated into one for solving any **NP**-problem (nondeterministic polynomial time) problem. **NP-hard** therefore means "at least as **hard** as any **NP**-problem," although it might, in fact, be harder.

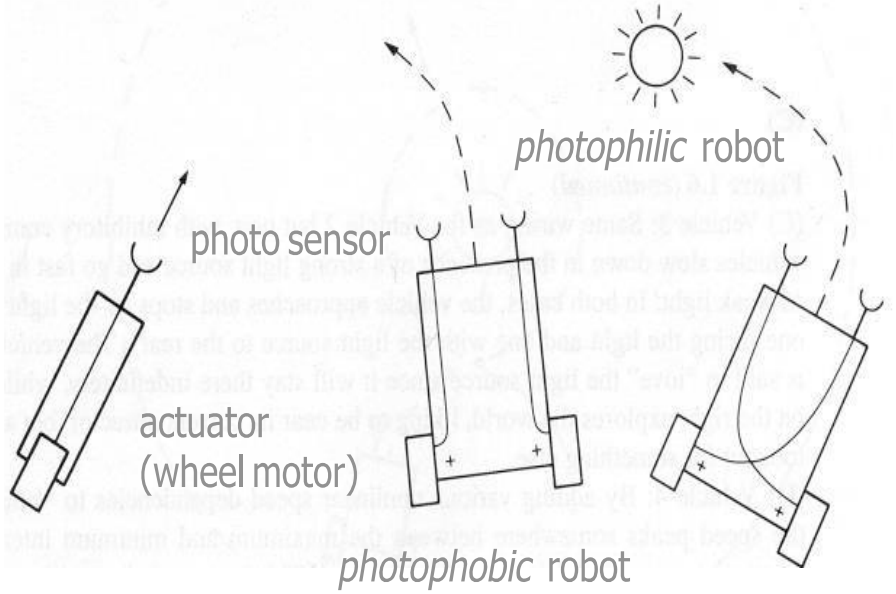
- Very hard to define general, computational "competence theories" for specific tasks that say "what" is computed and why (what to compute)!

- Need algorithms that use *domain-specific knowledge and constraints with incomplete models*, while being time and space constrained, stable, and robust (How to Compute?)

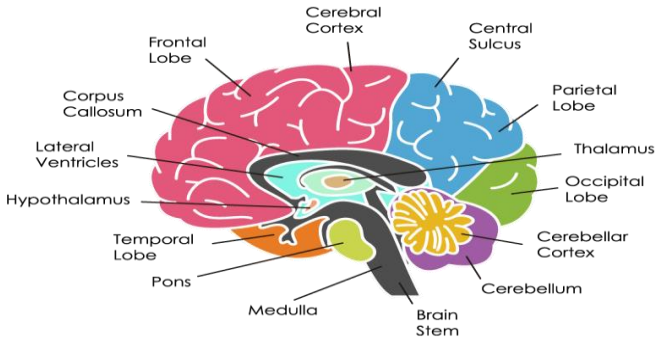


AI: How does intelligence look like?

- **Direct Connection**: These robots by V. Braitenberg have just a reactive behavior, i.e. no 'though in between': Since sensors are directly connected to actuators.
- The resulting behavior is remarkable anyway … ("**intelligence** is in the eye of the beholder").

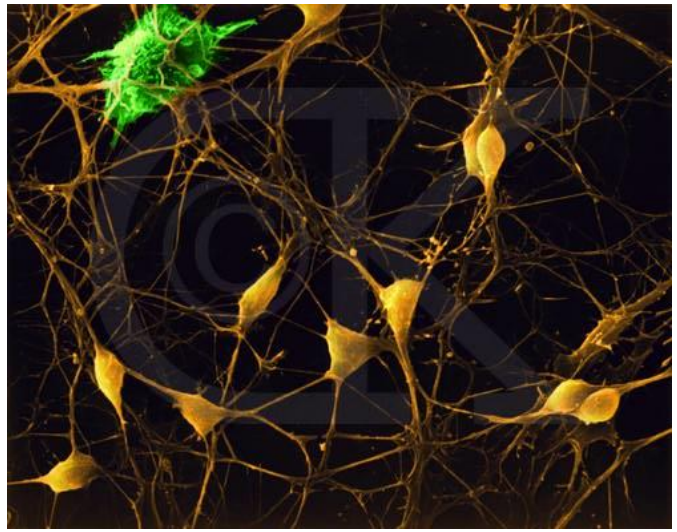


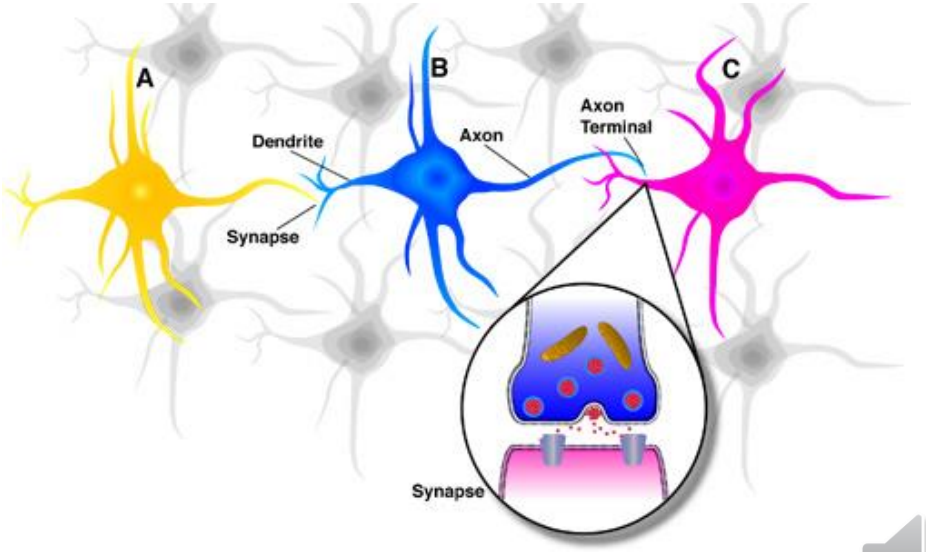
- *What is "intelligence"? Can we emulate intelligent behavior in machines? How far can we take it?*
- **Brain** is made by *neurons and synapses*!
- **Computer** is made by *transistors, crystalline, and electronic components*.
- **How is the intelligence behavior implemented by the Brain Neural Network and the Artificial Neural Network?**



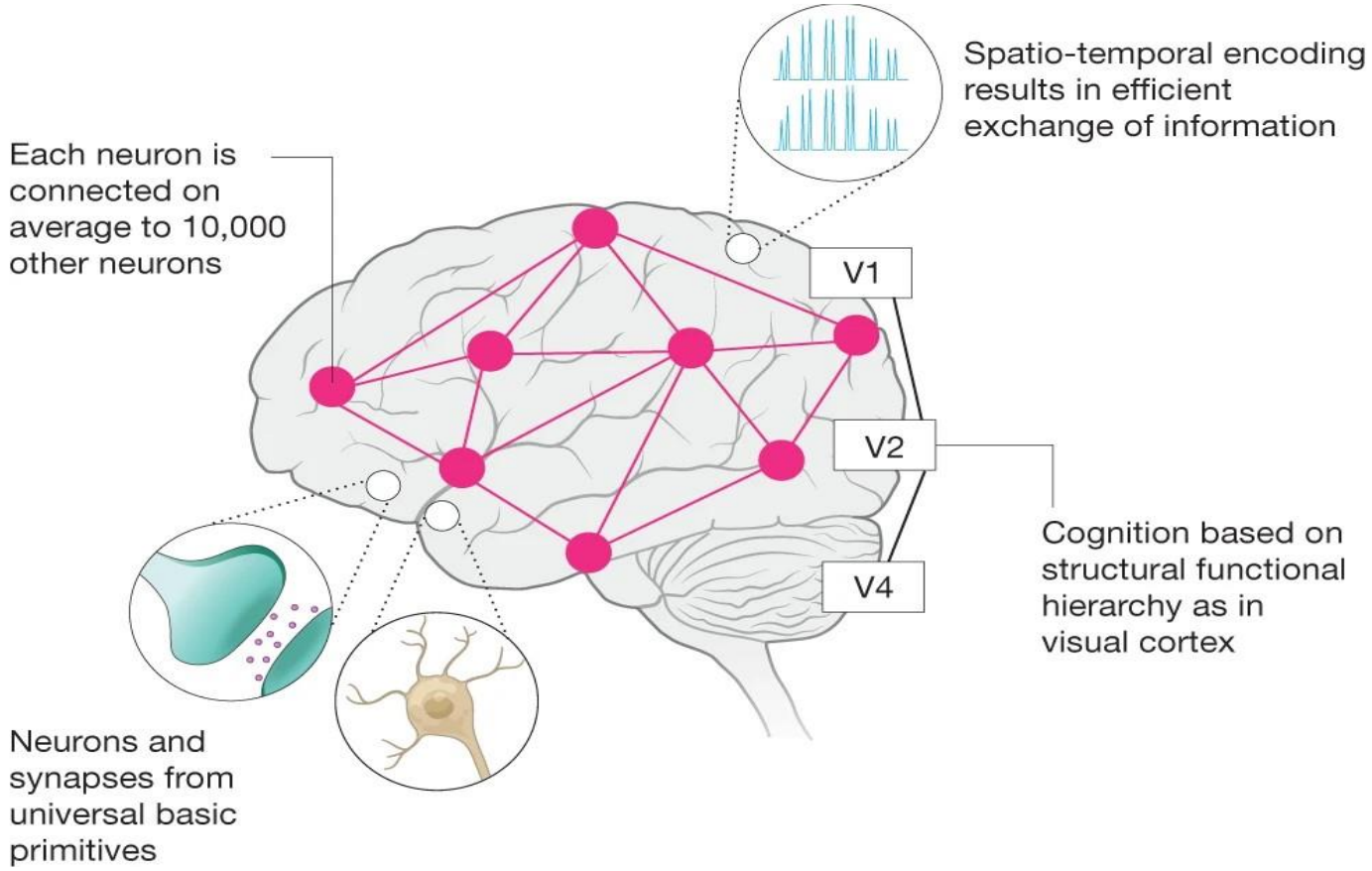
AI: Brain Neural Network

- While *brain* is heterogenous, it is composed of *neurons*.
- A neuron *transmits/receives signal to/from other neurons* (generally thousand) via its connected synapses. The signal is chemically based.
- A neuron can be in either an **Excited** or an **Inhibited** state at any point in time.
- The signal strength is **high** in **Excited** state and is **low** in **Inhibited** state.
- **Inputs** are approximately **summed**.
- When the input exceeds a threshold the neuron sends an electrical spike that travels throughout the body, gets to the axon, and reaches to next neuron(s).
- *How to create a computer neural network based on the brain neural network?*
- As we learn new things, new strong neural pathways (i.e. a series of connected neurons) in our *brain* are formed.



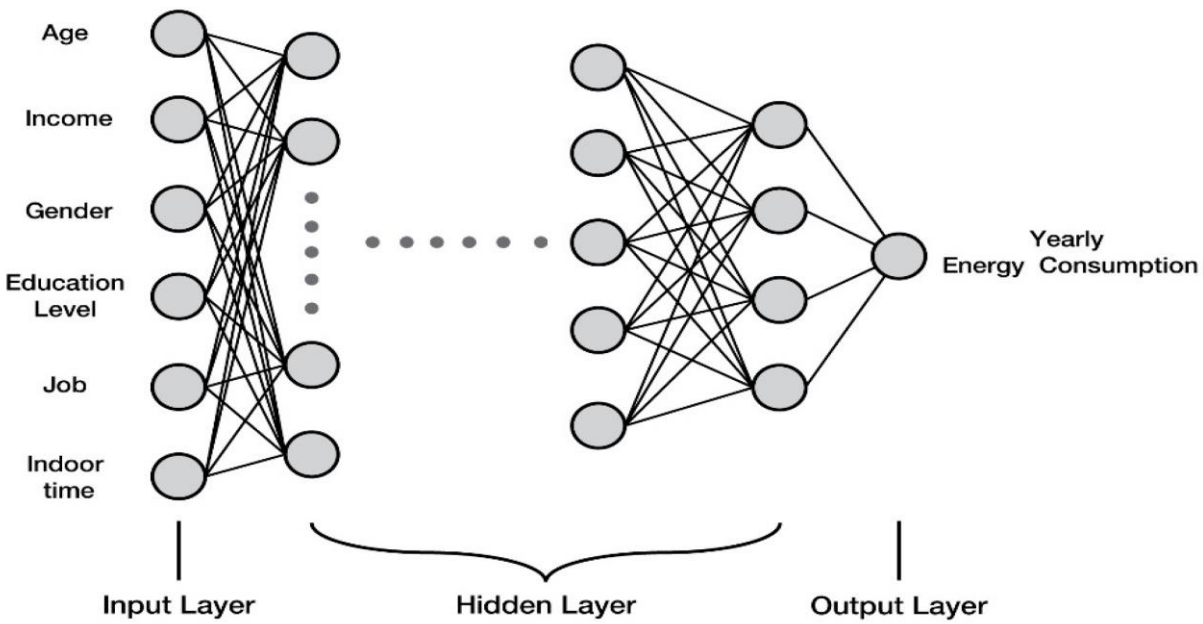


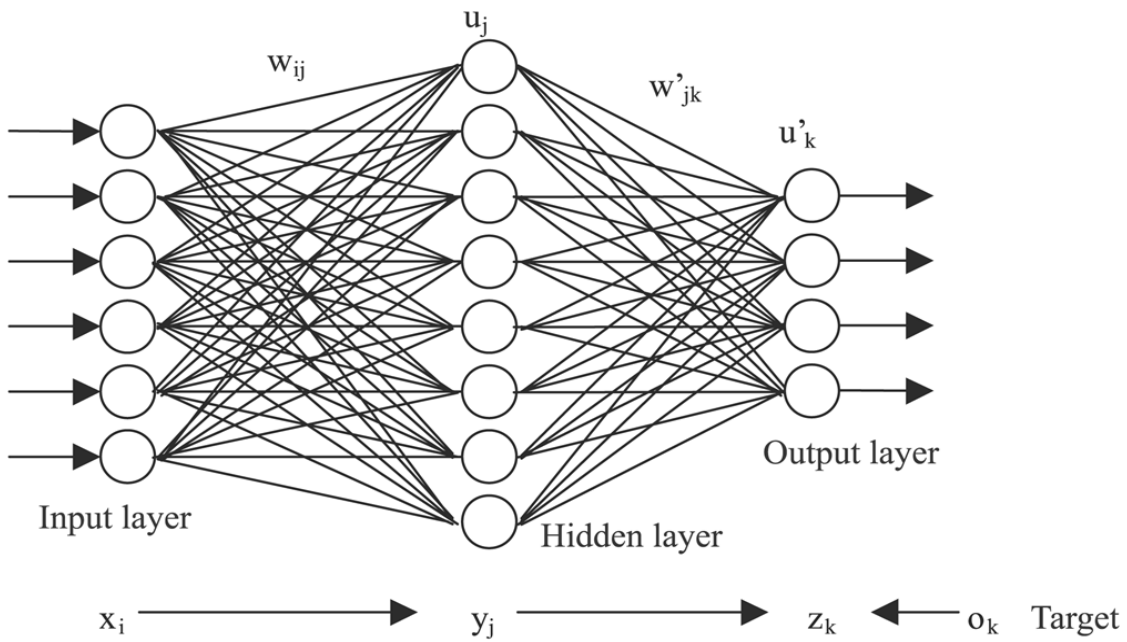
AI: Modelling of Brain Neural Network



- "In our view, people are smarter than today's computers because *the brain employs a basic computational architecture that is more suited to deal with a central aspect of the natural information processing tasks that people are so good at*."
- **Assumption**: *Mental phenomena* can be described *by interconnected networks of simple and often uniform units*.
- ***Can we build a functional brain using computers?***

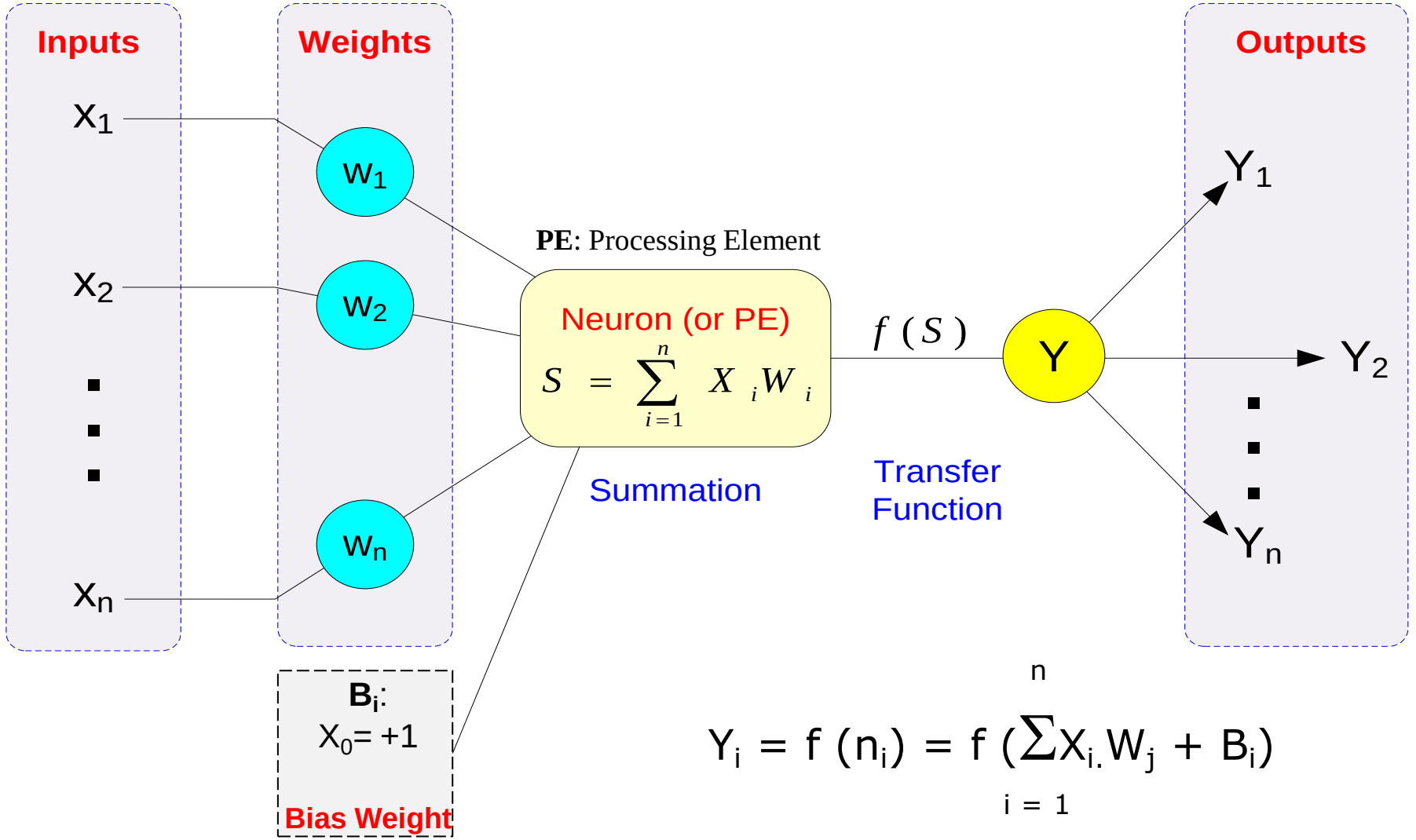
AI: Artificial Neural Network (ANN) - Introduction





- *Computational models* inspired by the *human brain*.
- *Massively parallel*, *distributed system*, and made up of *simple processing units called neurons*.
- Synaptic connection strengths among neurons are used to store the *acquired knowledge*.
- *Knowledge* is acquired by the network from its environment through a learning process.
- A computer representation of knowledge that attempts to mimic the neural networks of the human body.
- **Function Approximation**: *Basically, this is what an artificial neural network does*!
- The ANN resembles the brain in two respects: (**a**) knowledge is acquired by the network from its environment through a learning process; and (**b**) synaptic connection strengths among neurons are used to store the acquired knowledge.
- An ANN may be called ***shallow neural network*** too due to its smaller number of layers in compare to the other type of neural networks.

AI: Artificial Neural Network (ANN) - Architecture



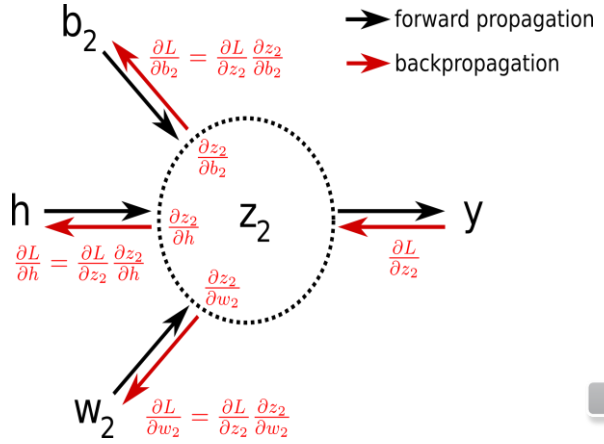
$$Y_i = f(n_i) = f\left(\sum_{i=1}^{n} X_i . W_j + B_i\right)$$

AI: Artificial Neural Network (ANN) – Details 1

- **Descriptions and Properties of ANNs**:
  - ✓ **Descriptions**
    - ✓ A artificial neuron computes the weighted sum of its input (called its net input), adds its bias, and passes this value through an activation function.
    - ✓ The neuron "Fires" that means become active if its output is above zero.
    - ✓ The bias can be incorporated as another weight clamped to a fixed input of +1.0.
    - ✓ The extra free variable or bias makes the neuron more powerful.
    - ✓ The inputs are flexible, with real values, and highly correlated or independent.
    - ✓ Neurons are connected to each other through connection link.
    - ✓ Each link is associated with weights that contain information about the input signal.
    - ✓ Each neuron has an internal state of its own that is a function of the inputs that receives the activation level.
  - ✓ **Properties**
    - ✓ Learning from Data Samples: Labeled or unlabeled.
    - ✓ Adaptivity: Changing the connection strengths to learn things.
    - ✓ Non-Linearity: The non-linear activation functions are essential.
    - ✓ Fault Tolerance: If one of the neurons or connections is damaged, the whole network still works quite well.
    - ✓ Activation Function: Calling it squashing function that limits the output amplitude of neuron. Types of this function are Linear, Threshold, Sigmoid, and etc.
    - ✓ There are **different topologies for ANN**: **single layer feed-forward** (i.e. the input and the output layers), **multi-layer feed-forward** (i.e. the input, the hidden, and the output layers), **recurrent** (i.e. feedback path between the output and the input layers), and so forth.

AI: Artificial Neural Network (ANN) – Details 2

- **Descriptions and Properties of ANNs**:
  - ✓ **Properties**
    - ✓ Network Topology Decision: Based on the number of input nodes, the number of output nodes, the transfer function, and the number of hidden nodes.
    - ✓ Architecture of a neural network is driven by the task it is intended to address: Classification, regression, clustering, general optimization, and association.
    - ✓ Learning: A process by which a neural network learns the underlying relationship between input and outputs, or just among the inputs:
      - ❖ *Supervised Learning*: Usage for prediction type of problems. An example is Backpropagation.
        - The parameters (i.e. weights) are "learnt" from a dataset of inputs and expected outputs pairs.
      - ❖ *Unsupervised Learning*: Usage for clustering type of problems and self organizing. An example is adaptive resonance theory.
    - ✓ Incremental Optimization (a.k.a. Backward Propagation): Weights are progressively corrected to reduce the difference between actual and expected outputs.
      - ✓ *Best Solutions for*:
        - ❖ High dimensionality, noisy, imprecise, or imperfect data.
        - ❖ A lack of a clearly stated mathematical solution or algorithm.

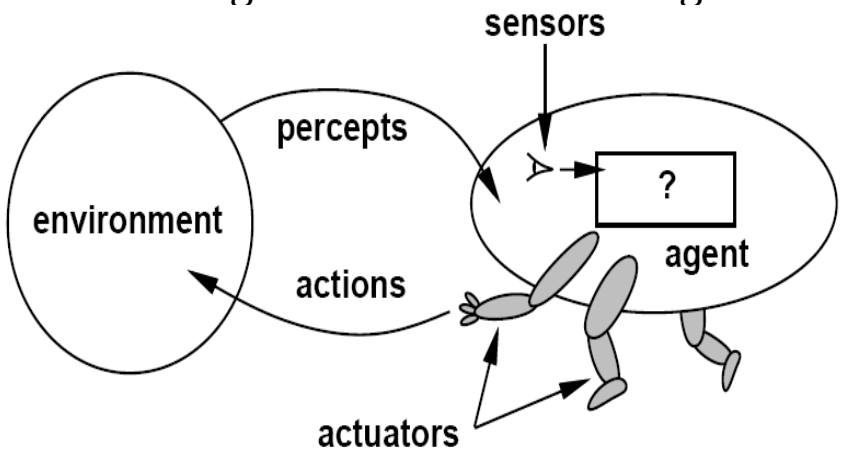


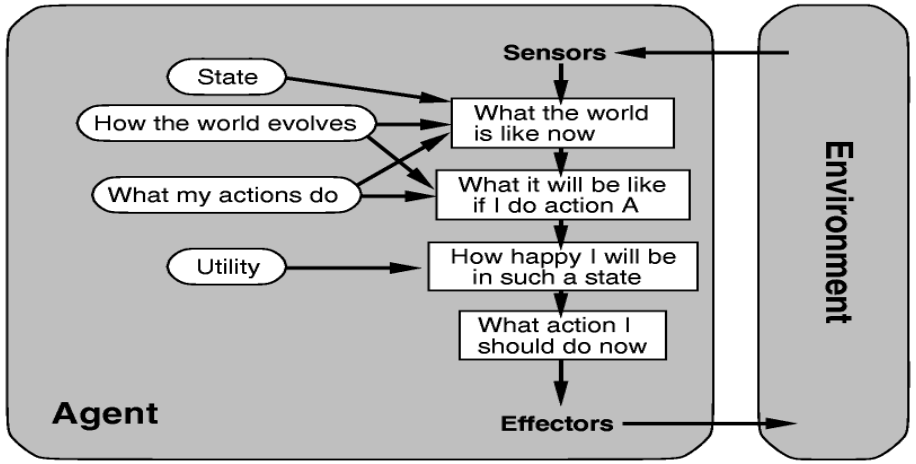
- **How can the AI models like ANNs create intelligent agents and the AI systems?**

AI: What is an intelligent agent?

- An **Intelligent Agent** is a system that:
  - ✓ It is an **AI-based Computing Engine** that includes an **AI Model** and is the core of **Intelligent Systems**.
  - ✓ Perceives its environment (which may be the physical world, a user via a graphical user interface, a collection of other agents, the Internet, or other complex environment).
  - ✓ Reasons to interpret perceptions, draw inferences, solve problems, and determine actions.
  - ✓ Acts upon that environment to realize a set of goals or tasks for which it was designed.

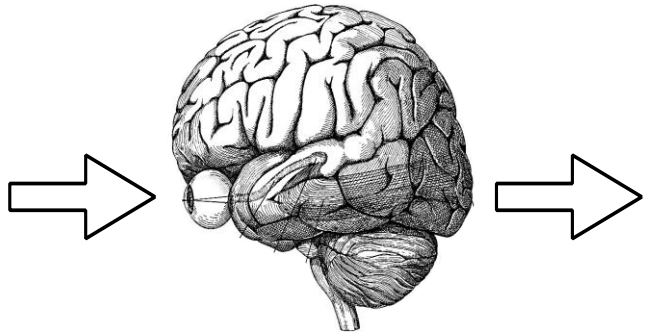
- **Characteristic Features**:
  - ✓ Knowledge Representation and Reasoning.
  - ✓ Transparency and Explanations.
  - ✓ Ability to Communicate.
  - ✓ Use of huge amounts of knowledge.
  - ✓ Exploration of huge search spaces.
  - ✓ Use of heuristics.
  - ✓ Reasoning with incomplete or conflicting data.
  - ✓ Ability to learn and adapt.





AI: Solving Problems in Intelligent Systems - 1

- ***We have certain directions of research and functionalities based on the brain structure***: *Representation, Thinking, Reasoning, Learning, Output, and Search*.



- **Representation**: All AI problems require some form of representation for input data.
  - ✓ The input data can be: chess board, maze, text, object, room, sound, and visual scene.
  - ✓ A major part of AI is representing the problem space so as to allow efficient search for the best solution(s).
  - ✓ Sometimes the representation is the output. An example is discovering patterns.
- **Thinking**: What do you do once you have a representation? This requires a goal and objective.
  - ✓ Rational Behavior: Choosing actions that maximize goal achievements given available information.
  - ✓ The thinking data can be: the best move (for chess board), the shortest path (for maze), the semantic parsing (for text), the recognition (for object, speech, biometric, and etc.), the localization (for room), and the navigation (for visual scene).
  - ✓ What is the strategy for multiple agents?
- **Reasoning**: It can be thought of as constructing an accurate world/real model.
  - ✓ Rational Inference: What can be logically inferred giving available information?
  - ✓ When information is uncertain: Most of the facts are not concrete and are not known with certainty.
  - ✓ Probabilistic Inference: How do we give the proper weight to each observation?

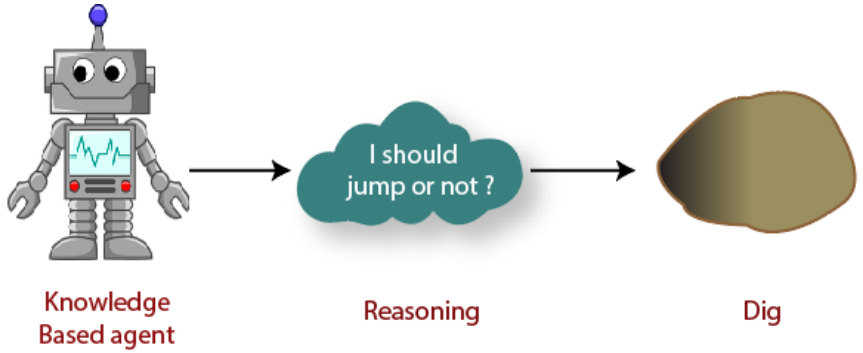
AI: Solving Problems in Intelligent Systems - 2

	Human	Rational
Thought	**Human-like Thinking Systems**	**Rational Thinking Systems**
Behavior	**Human-like Acting Systems**	**Rational Acting Systems**

- **Learning**: What if your world is changing? How do we maintain an accurate model? Requiring a learnable model.
  - ✓ Adapting internal representation so that is as accurate as possible.
  - ✓ Adapting the models of other agents.
- **Output**: The output action can also be complex. The representation and complexity of output data is important.
  - ✓ The output data can be: next move, text, label, actuator, and movement.
  - ✓ Sample output can be from a simple chess move to a motor sequence to grasp an object.
- **Search**: Finding an "*optimal*" sequence of states between initial state and final state. How to find the best model states?
- Humans are not always rational. Rational means doing the right thing. The right thing is defined as expecting to maximizing the goal achievements, given the available information.
- The perception and the motor skills are the most important part of intelligence.

AI: Intelligent Systems – Mechanism and Properties

- **Mechanism**:
  - ✓ The stimulus must be translated into an internal representation.
  - ✓ The representation is manipulated by cognitive processes to derive new internal representations.
  - ✓ These representations in turn are translated into action.
  - ✓ The agent includes different elements, including ***feature extraction***, ***(machine/deep) learning model***, decision making unit, sensors, and actuators.



- **Properties and characteristics of AI-Based (intelligent) systems**:
  - ✓ More powerful and higher usability
  - ✓ Improved interfaces
  - ✓ Solving more complex and emerging problems
  - ✓ Better handling of information
  - ✓ Relieving information overload
  - ✓ Conversion of information into knowledge
  - χ Increased cost
  - χ Difficulty with software development – slow and expensive

- **What is Machine Learning and how its systems look like?**

AI: Machine Learning – Definition

- **Machine Learning (ML) is the domain of AI which is concerned with building adaptive computer systems that are able to improve their competence and/or efficiency through learning from input data or from their own problem solving experience.**

- **What is Learning?**
  - ✓ It denotes *changes in the system that are adaptive in the sense that they enable the system to do the same tasks* or *tasks drawn from the same population more effectively* the next time.
  - ✓ It is about making useful changes in our minds.
  - ✓ We construct or modify representations of what is being experienced.
  - ✓ A computer system **learns** if it *improves its performance at some task through experience*.
  - ✓ *It denotes the way people and computers interact*:
    a. Acquire, discover, and organize knowledge by building, modifying, and organizing internal representations of some external reality.
    b. Acquire skills by gradually improving their motor or cognitive skills through repeated practice, sometimes involving little or no conscious thought.
  - ✓ It results in changes in the agent or mind that improve its competence and/or efficiency:
    - ❖ **Competence**: A system is improving its competence if it learns to solve a broader class of problems, and to make fewer mistakes in problem solving.
    - ❖ **Efficiency**: A system is improving its efficiency, if it learns to solve the problems from its area of competence faster or by using fewer resources.

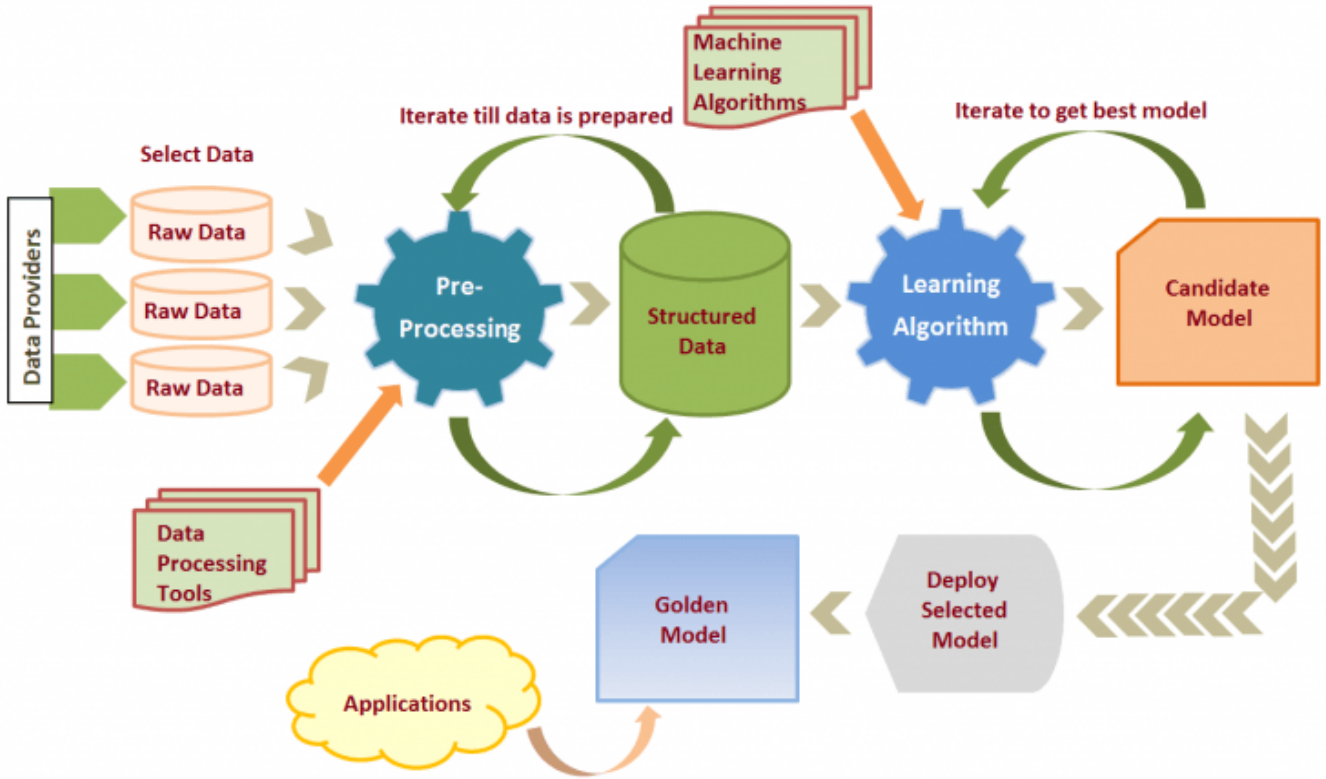
AI: Machine Learning - Properties

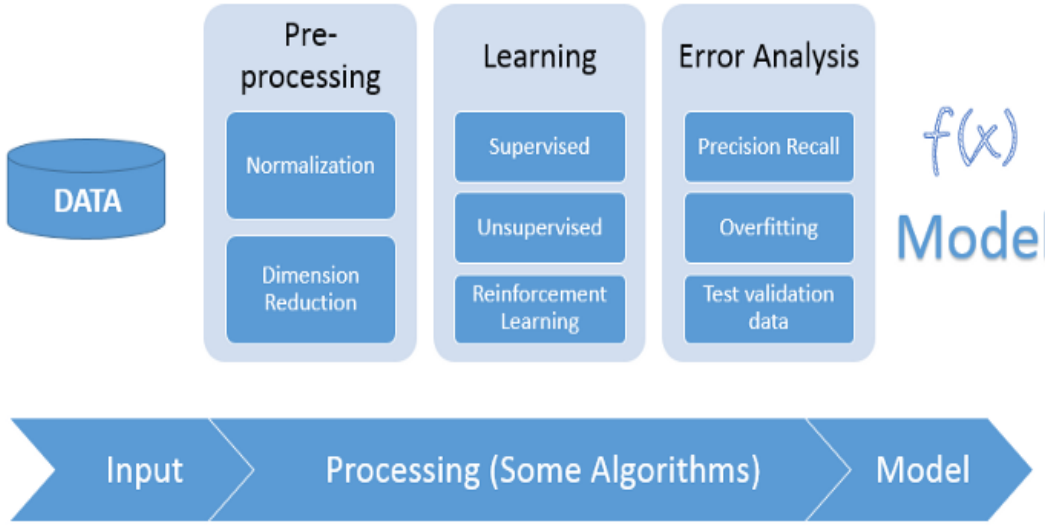
- **Main Research Problems to Study**:
  - ✓ Learning Strategies: Discovery of general principles, methods, and algorithms of learning.
  - ✓ The construction of knowledge-based systems.

- **Learning Strategies**: A basic form of learning characterized by the employment of:
  - ✓ A certain type of inference, such as deduction, induction, and analogy.
  - ✓ A certain type of computational or representational mechanism, such as rules, trees, neural networks, and etc.
  - ✓ A certain type of learning goal, such as learn a concept, discover a formula, acquire new knowledge about an entity, and refine an entity.

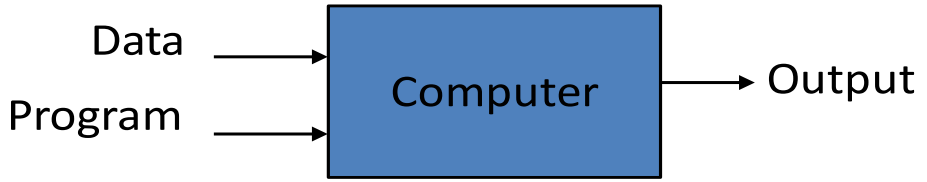
- Options for Machine Learning:
  - ❖ Rote Learning
  - ❖ Learning from Induction
  - ❖ Explanation-Based Learning
  - ❖ Conceptual Clustering
  - ❖ Abductive Learning
  - ❖ Learning by Analogy
  - ❖ Instance-Based Learning
  - ❖ Neural Networks
  - ❖ Genetic Algorithms and Evolutionary Computing
  - ❖ Reinforcement Learning
  - ❖ Bayesian Learning
  - ❖ Multi-strategy Learning

AI: Machine Learning System Flow

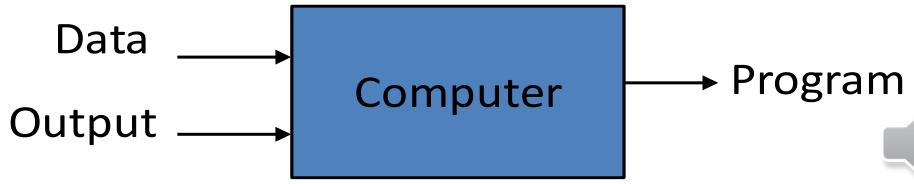




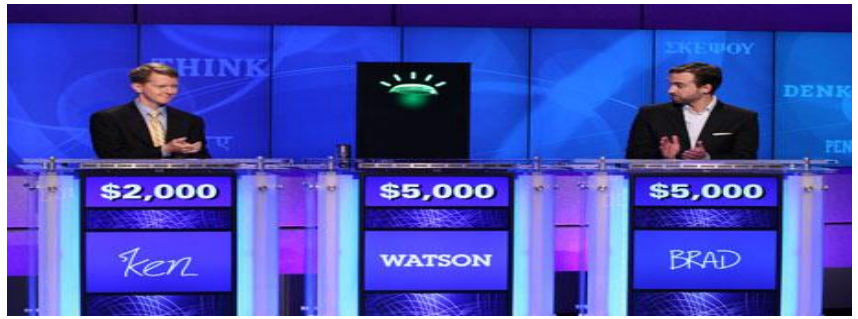
Traditional Programming

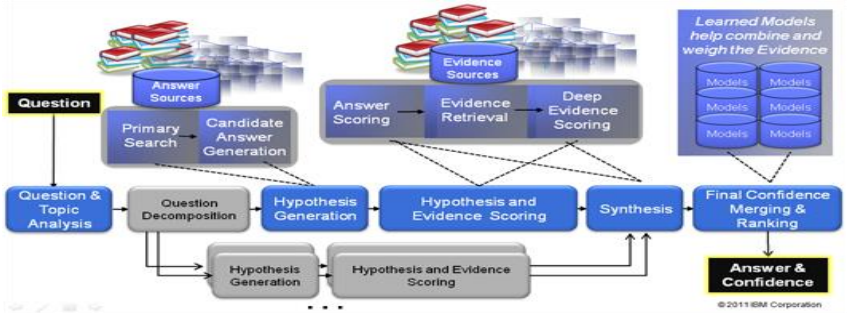


Machine Learning



AI: ML Example - Question Answering Machine





- **DeepQA** (a.k.a. Watson):
  - ✓ Capable of beating humans in many different games.
  - ✓ The questions can be in the format of image, audio, and video but DeepQA only accepts their text version as input.
  - ✓ No connection to the Internet during the game.
  - ✓ Having access to the local memory only.
  - ✓ The Internet can be used during the training. The training is progressive and incremental.
  - ✓ Conventional Hardware but massive parallelism: Having 2880 standard CPUs, Linux SUSE ES 11, Software in Java and C++, with Apache Hadoop, and Apache UIMA.
  - ✓ Several competing streams in parallel with a degree of confidence.

- **After understanding artificial (shallow) neural network and machine learning, how to define deep neural network and deep learning?**

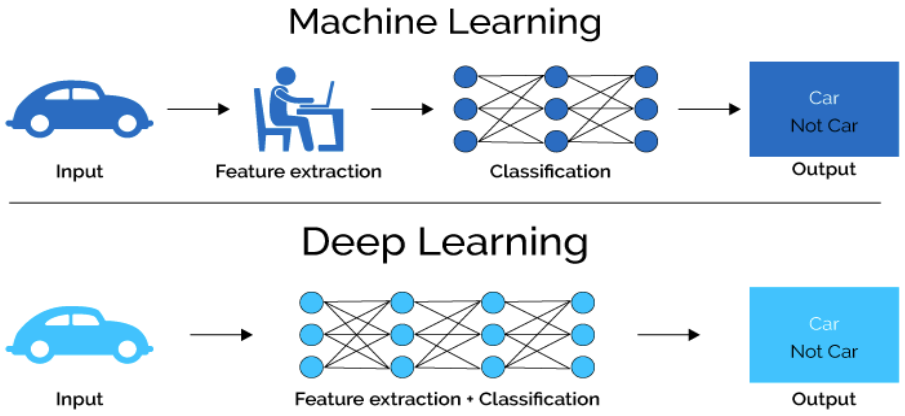
- **What are the important techniques in machine/deep learning for the purpose of improving performance and overcoming possible limitations?**

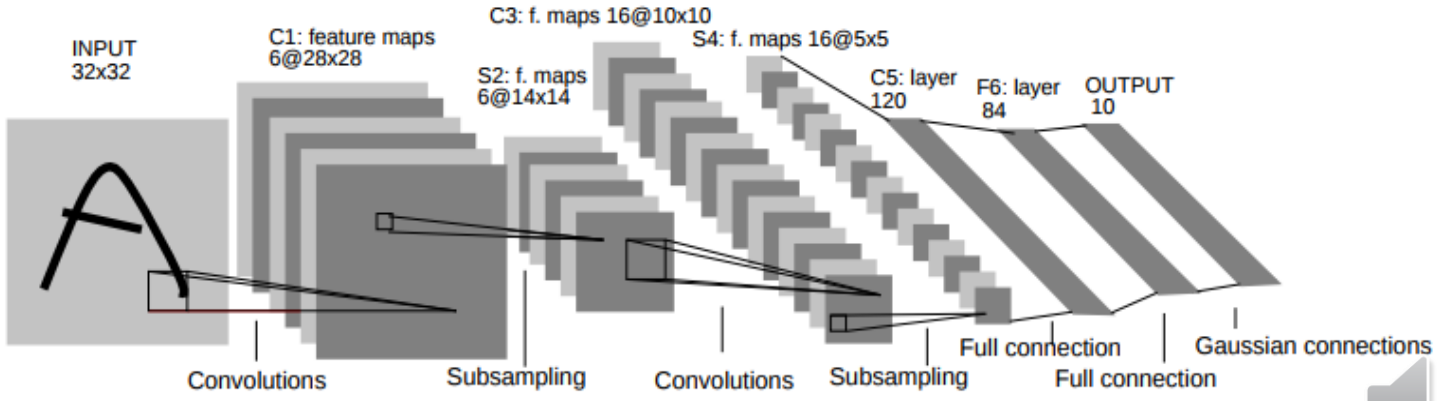
AI: Deep Learning and Deep Neural Networks - 1

- **Deep Neural Network (DNN):** Referring to a feedforward neural network with more than one hidden layer.
  - ✓ DNNs try to learn representation by using a hierarchy of multiple layers.
  - ✓ **Multi-class Classification:** The posterior probability of each class can be estimated using an output softmax layer.
  - ✓ **Pre-Training:** Initializing all the weights especially when the amount of training data is limited and when no constraints are imposed on the weights.
  - ✓ **Restricted Boltzmann Machine (RBM):** Used as a building block for pre-training. All the weights from this block can be used as initialization for one layer.
- **Convolutional Neural Networks (CNNs)**:
  - ✓ Among the oldest deep neural network architectures.
  - ✓ Popular among different applications like handwriting recognition.
  - ✓ A specialized kind of neural network.
  - ✓ Usage for processing data with a known grid-like topology.
    - ❖ Example Data: Time-series data (i.e. a one-dimensional grid with taking samples at intervals) and Image Data (ie.. A two-dimensional grid of pixels).
  - ✓ Utilization of convolution that is a specialized kind of linear operation.
  - ✓ The convolution operation is used in place of general matrix multiplication in at least one layer.
  - ✓ Convolution layer leverages three important ideas to improve the AI system: **Sparse Interactions, Parameter Sharing, and Equivariant Representations**.
  - ✓ Convolution layer allows for working with inputs of variable size.
  - ✓ Making the kernel smaller than the input.

AI: Deep Learning and Deep Neural Networks - 2

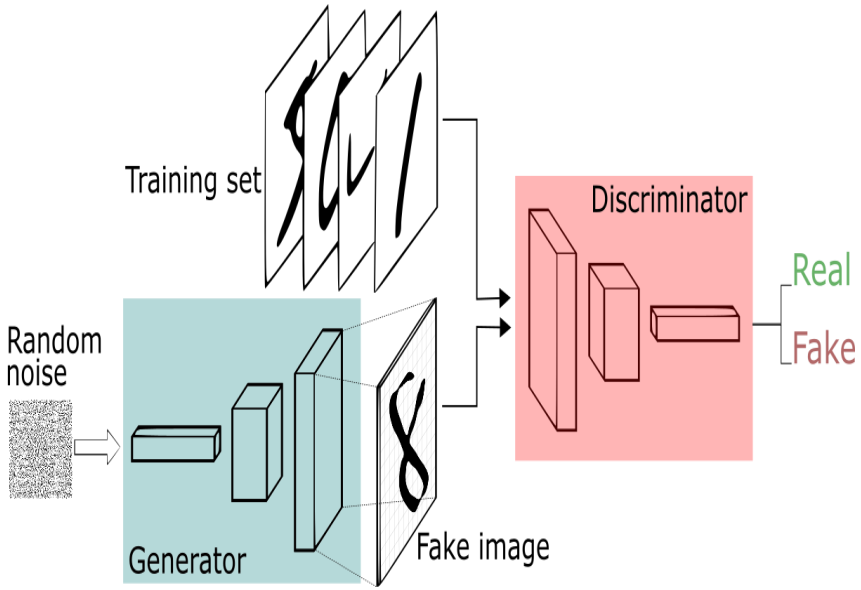
- **Convolutional Neural Networks (CNNs)**:
  - ✓ Organization: An alternating positioning of convolution and pooling layers.
  - ✓ Running a small window over the input image during the training and the testing times.
  - ✓ The entering weights to this window learn from various features of the input data regardless of their absolute position within the input.
  - ✓ The input "*image can loosely be thought of as a spectrogram with static, delta, and delta-delta features serving in the roles of red, green, and blue*".
  - ✓ The locality of data needs to be preserved in both axes of frequency and time.
  - ✓ **Convolution Layer**: Containing a number of filters that performs convolutional operation.
  - ✓ **Pooling Layer**: Subsampling the image pixels leads to fewer parameters to characterize the image. Its maximum version reports the maximum output within a rectangular neighborhood. Its average version reports the average output of a rectangular neighborhood (possibly weighted by the distance from the central pixel).

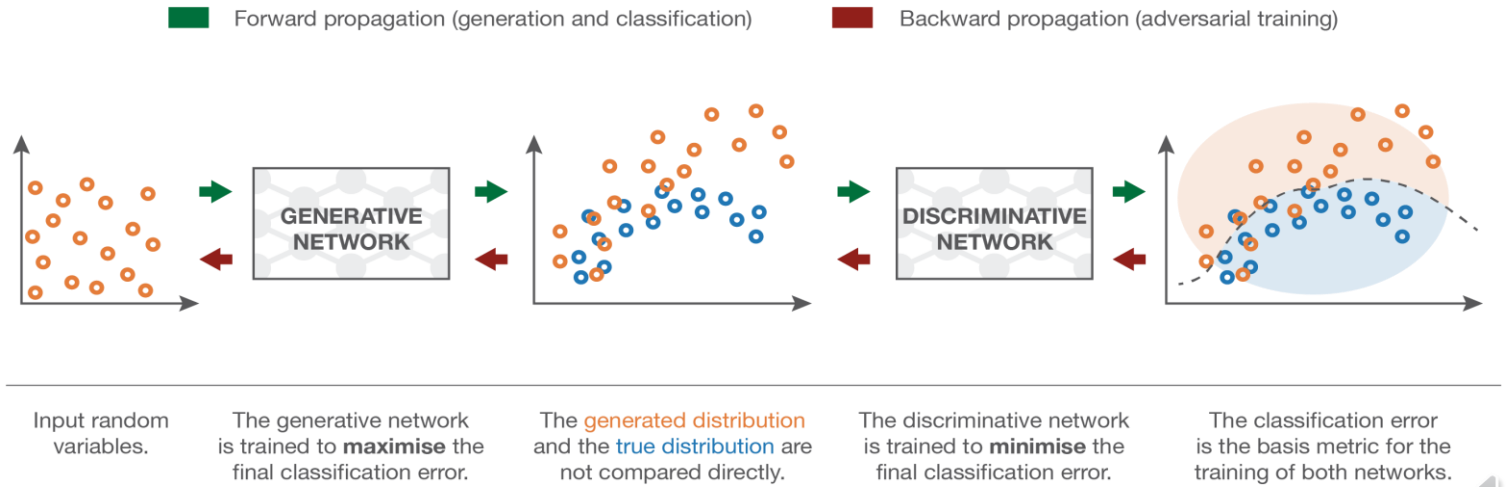




AI: Generative Adversarial Network (GAN)

- **Discriminative Versus Generative Behavior?**
- **Generative Model**: Given a training set drawn from some distribution, it tries to fit a model to greatly represent the data probability. In other words, a network is trained that models a distribution We estimate density using this model and do sample generation.
- **Generative Model Requirement**: Understanding and compressing knowledge; Semi-supervised learning; multi-model outputs; and generating data.
- Possible Models: Naïve Bayes, Variational Autoencoder, and GAN.
- **GAN Players (Elements):** Generator and Discriminator.
- **GAN Generator**: Given a random Z, it outputs an image that looks like a sample from the training set.
- **GAN Discriminator**: Given a sample X, it outputs the probability of X coming from the training set.

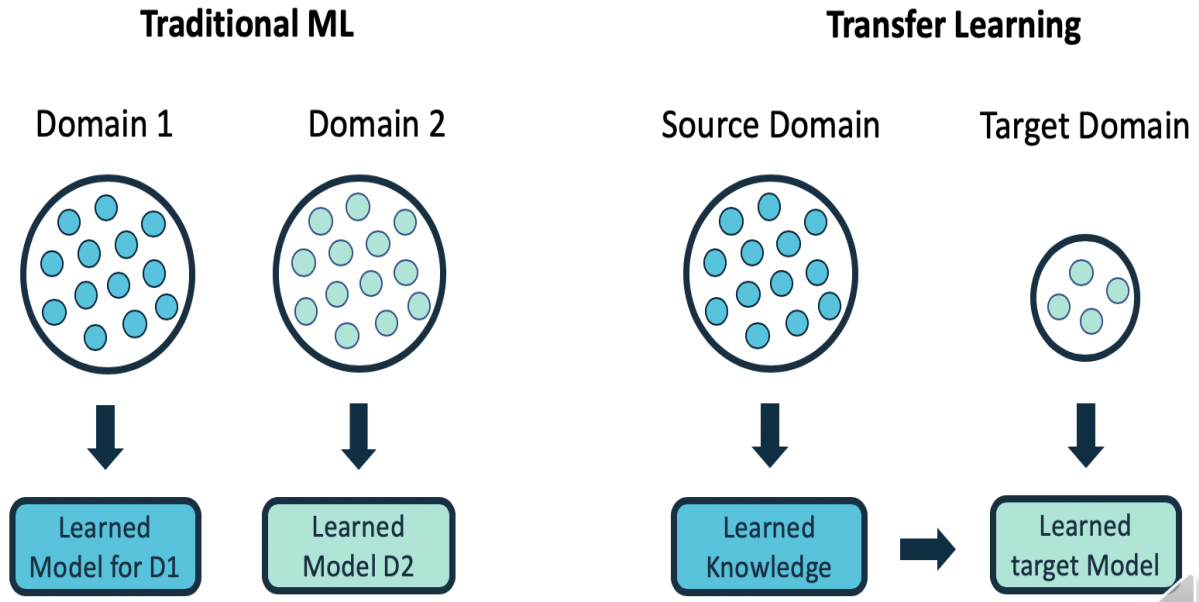




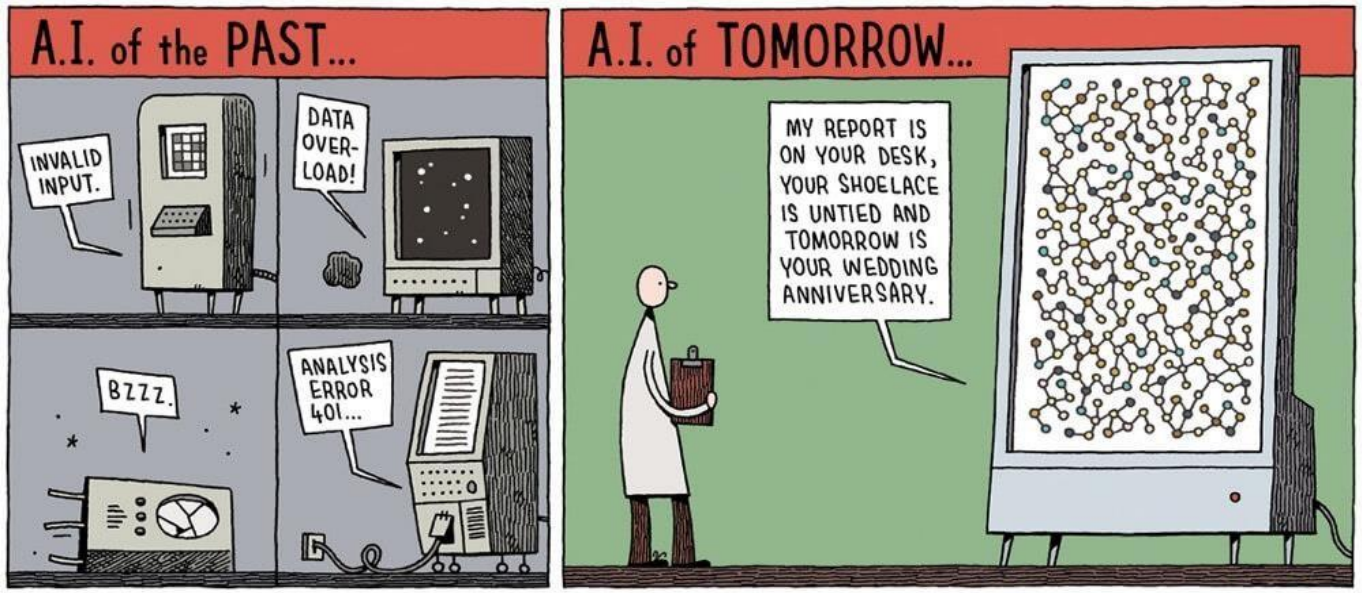
AI: Transfer Learning

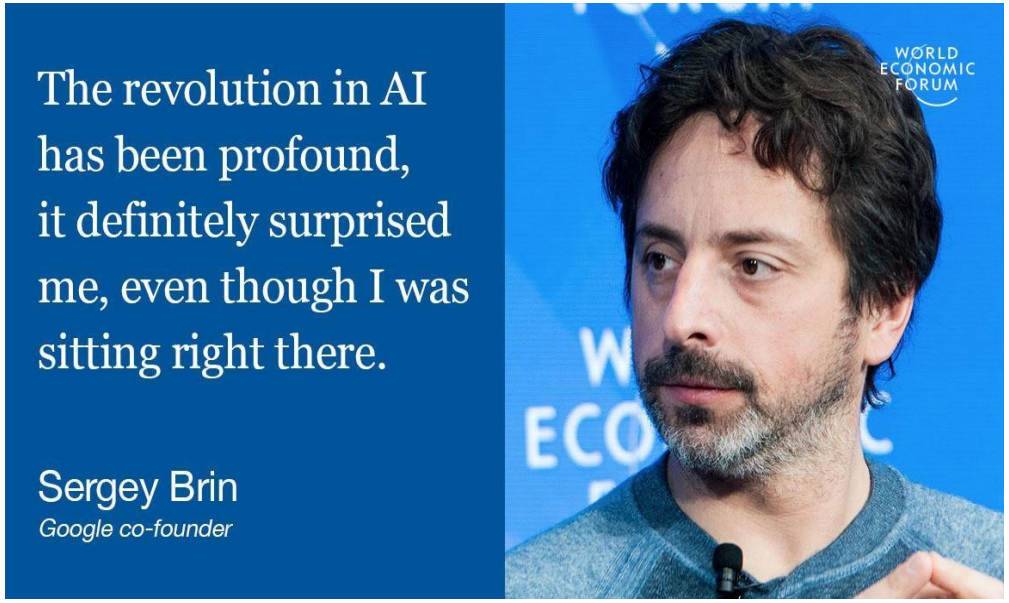
- **Definition**: The ability of a system to recognize and apply knowledge and skills learned in previous tasks to novel tasks (in the new domains) with certain level of commonality.
- **Motivation**: Human learning is the backbone of this concept. Humans transfer knowledge learnt previously to new situations.
- **Why? (a)** labeled data are short supply; **(b)** the calibration effort is very expensive; and **(c)** the learning process is time consuming.
- **Types**: Inductive, Transductive, and Unsupervised.
- **Transfer Question**: Given a target task, how to identify the commonality between the task and previous (source) tasks, and transfer knowledge from the previous tasks to the target one?

Transfer Learning Approaches	Description
Instance Transfer	To re-weight some labeled data in a source domain for use in the target domain.
Feature Representation Transfer	Find a "good" feature representation that reduces difference between a source and a target domain or minimizes error of models.
Model Transfer	Discover shared parameters or priors of models between a source domain and a target domain.
Relational Knowledge Transfer	Build mapping of relational knowledge between a source domain and a target domain.



AI: Past, Today, and Tomorrow

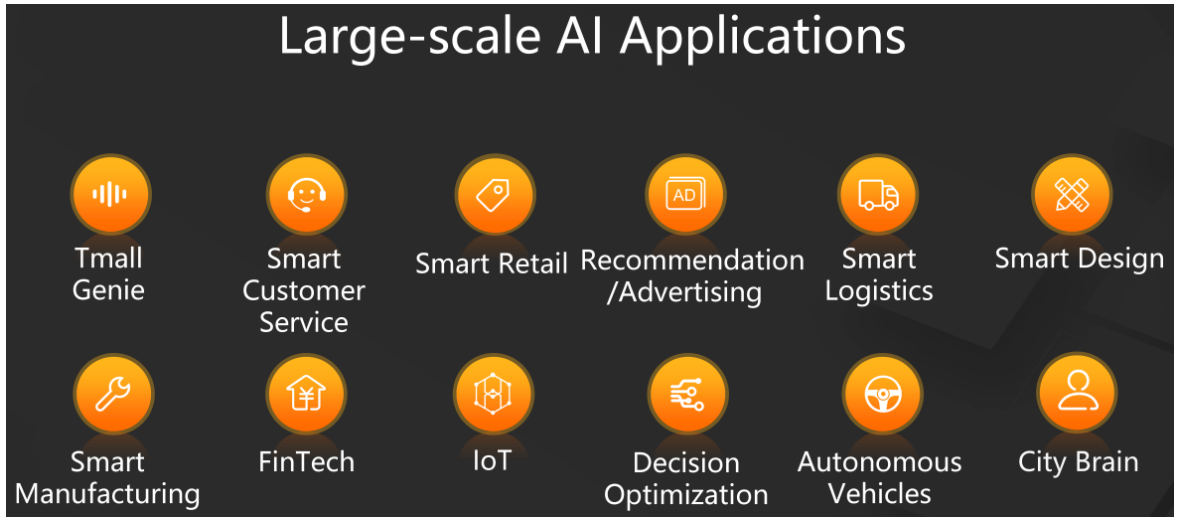




- **Sergey Brin** (Google Co-Founder, January 2017):
  - ✓ "I ***didn't pay attention to it [i.e. Artificial Intelligence]*** at all, to be perfectly honest."
  - ✓ "Having been trained as a computer scientist in the **90s**, ***everybody knew that AI didn't work***. People tried it, they tried neural nets and none of it worked."
- A set of "Tools" for computing a variety of useful classes of model types that represent information extracted from raw input data, and use the associate algorithms to "Solve" specific tasks. **Possible Options**: Neural Networks, Hidden Markov Models, Bayesian Networks, Heuristic Search, and Logic.
- There is no magic in AI. The models (i.e. representation), probability, statistics, optimization, and algorithms provide the desired functions.
- **How successful the AI and its applications were in the past and how they are today?**

AI: Successful Applications

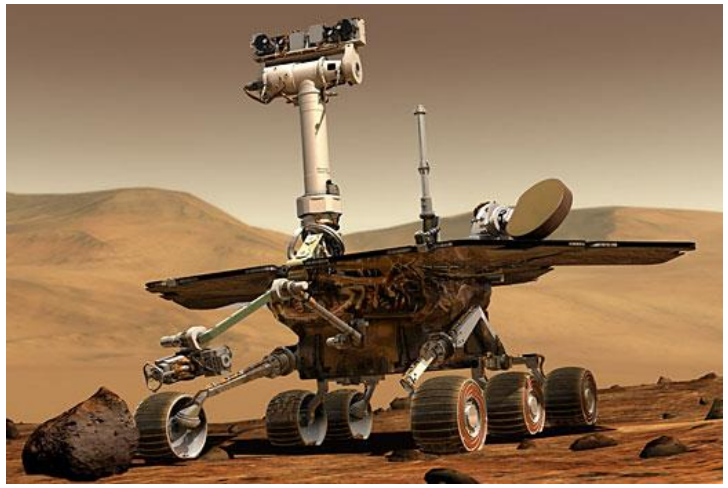
- Language Translation Services (Google)
- Translating Telephone (Skype)
- News Aggregation and Summarization (Google)
- Speech Recognition (Nuance)
- Song Recognition (Shazam)
- Face Recognition (Google)
- **Image Classification/Recognition** (Google)
- Question Answering (Apple Siri, IBM Watson, and etc.)
- Chess Playing (IBM Deep Blue)
- 3D Scene Modeling from Images (Microsoft Photosynth)
- Driverless Cars – Autonomous Driving (Google)
- Traffic Prediction (Inrix)

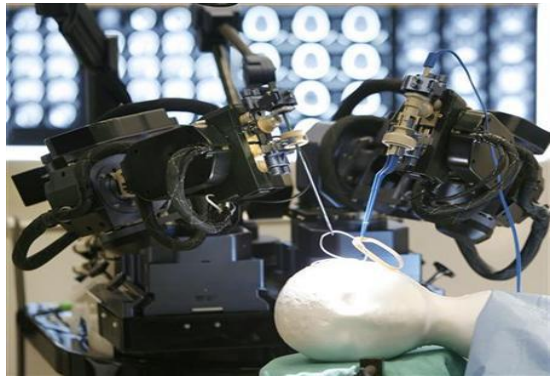


- **Cybersecurity**: Deep vulnerable code analysis, malware detection, intrusion detection, antispam, vulnerability management, normal and malicious data classification, insider attack prediction, adversarial AI (i.e. adversarial inputs, data poisoning, model stealing, and feedback weaponization), malware creation, smart botnets, spear phishing, conditional attacks, classify victims, security incident prediction, threat intelligence, and intelligent network networking.

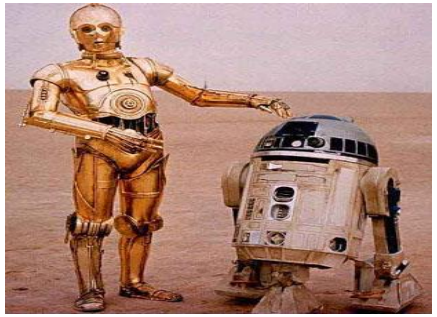
- **Why Image Classification/Recognition and Cybersecurity applications are important for the UF FICS Research and their ongoing projects?**

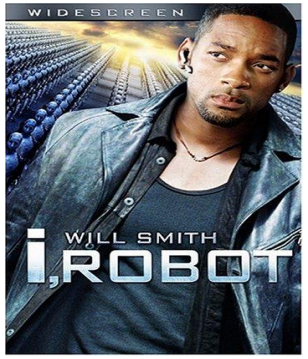
AI: Real Life

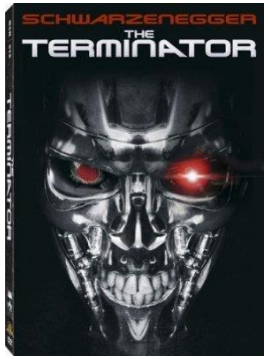




AI: Entertainment

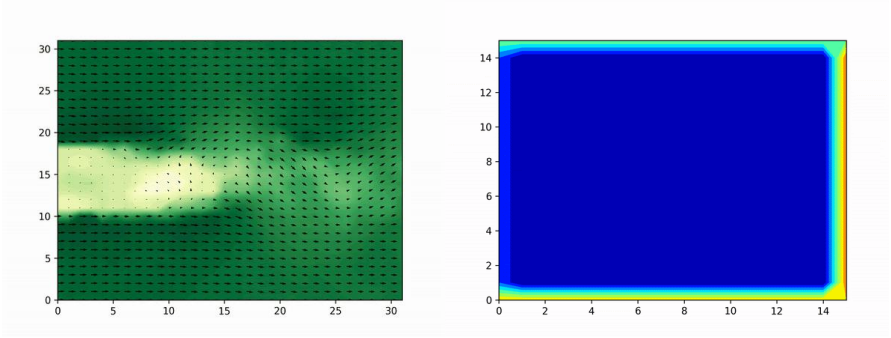






AI: Application in Engineering - 1

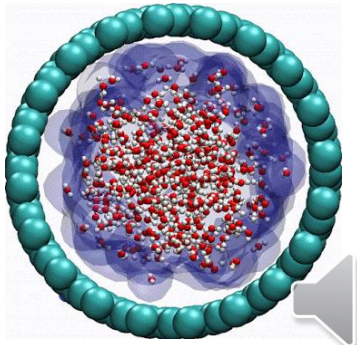
- **AI Physical and Engineering Phenomena:**
  - ✓ Use the state of the art *deep learning and machine learning algorithms* and tools to learn, infer and predict the physical phenomena pertinent to mechanical engineering.
  - ✓ Examples of such phenomena are multi-physics transport, fluid mechanics, and heat transfer. Specifically, with the exponential growth of sensory data and internet of things, data driven modeling of complex physical phenomena is critical in order to engineer the resilient infrastructures.



(L) Deep Leaning Generative model can learn and predict the turbulence wake behind a cylinder with different geometry and shape.

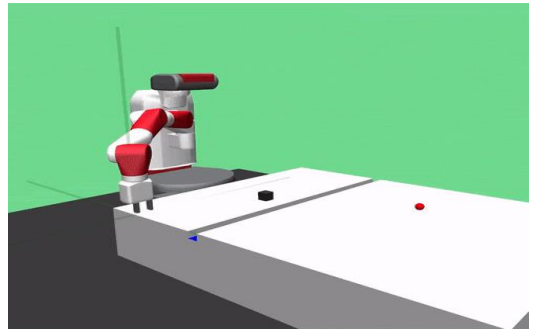
(R) Time-dependent generative models can learn and predict the time-dependent heat diffusion by just giving the boundary condition!

- **AI Material Discovery:**
  - ✓ Accelerate material discovery using ***AI tools***.
  - ✓ Since it is prohibitively expensive to use experimental and computational tools to search for novel material for energy applications, the search process can be greatly accelerated by using *deep learning technology*.
  - ✓ Developing and applying these tools to find optimal materials for energy and health applications.

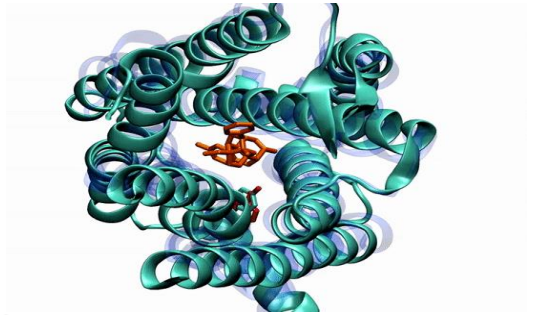


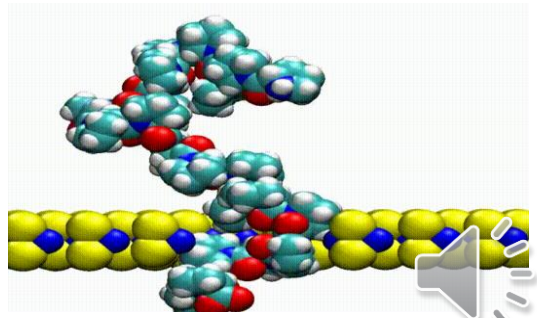
AI: Application in Engineering - 2

- **Artificial Intelligence and Robotics:**
  - ✓ Combining **deep learning** and **reinforcement learning** (RL) together and apply it to the robot intelligence.
  - ✓ Recent observations with deep reinforcement learning shows promises to give robots intelligence and more human like behavior.
  - ✓ Examples of these behaviors can be decision making under constraints, creativity, and persistence.
  - ✓ Applying AI to drones and unmanned aerial vehicles (UAVs).



- **Computational Bio-Engineering and AI:**
  - ✓ Combining *molecular dynamic simulations, machine learning and statistical learning* to <u>understand and predict the properties and interactions of bio-molecules</u>.
  - ✓ Interactions and **recognition** of bio-molecules such as deoxyribonucleic acid (DNA) with synthetic materials using molecular dynamics simulations and statistical learning.





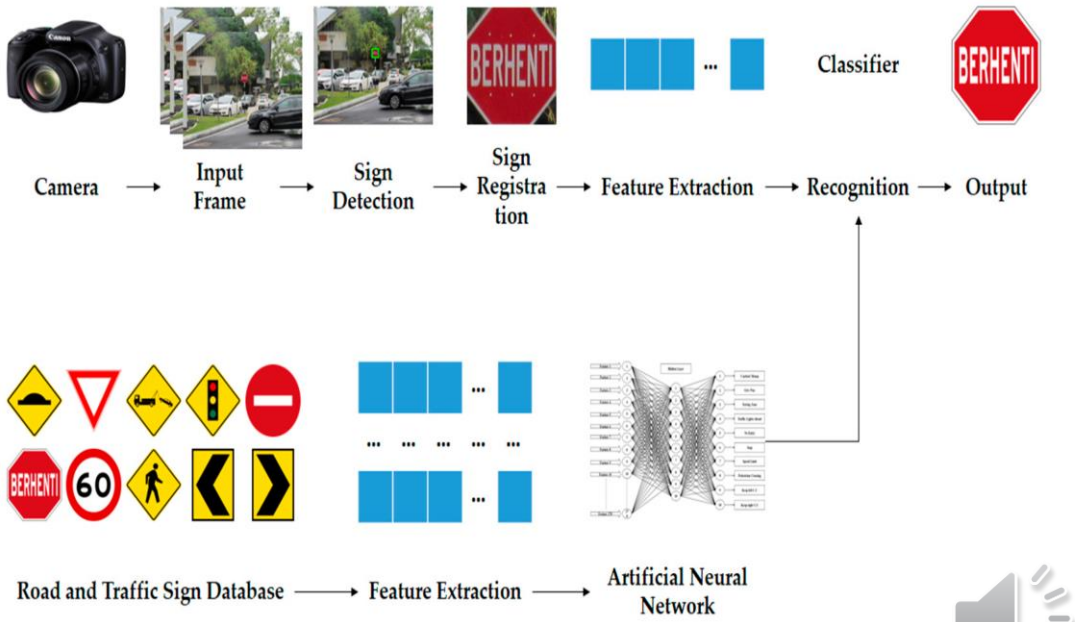
AI: Application in Engineering - 3

- **Artificial Intelligence and Civil Engineering:**
  - ✓ *Intelligent detection and classification* of various types of defects in infrastructure surface images (cracks, deposit, etc.) can largely boost its maintenance efficiency.
  - ✓ Various supervised learning methods have been investigated for this task, including *decision trees* and *support vector machines* in previous studies, and *deep neural networks* more recently.

- **Artificial Intelligence and Drug Discovery:**
  - ✓ AI approaches provide a set of tools that can *improve discovery and decision* making for well-specified questions with abundant, and high-quality data.
  - ✓ The potential for various uses, from initial screening of drug compounds to predicted success rate based on biological factors.
  - ✓ Opportunities to apply AI occur in *all stages of drug discovery*.
  - ✓ Examples include target validation, identification of prognostic biomarkers, and analysis of digital pathology data in clinical trials.

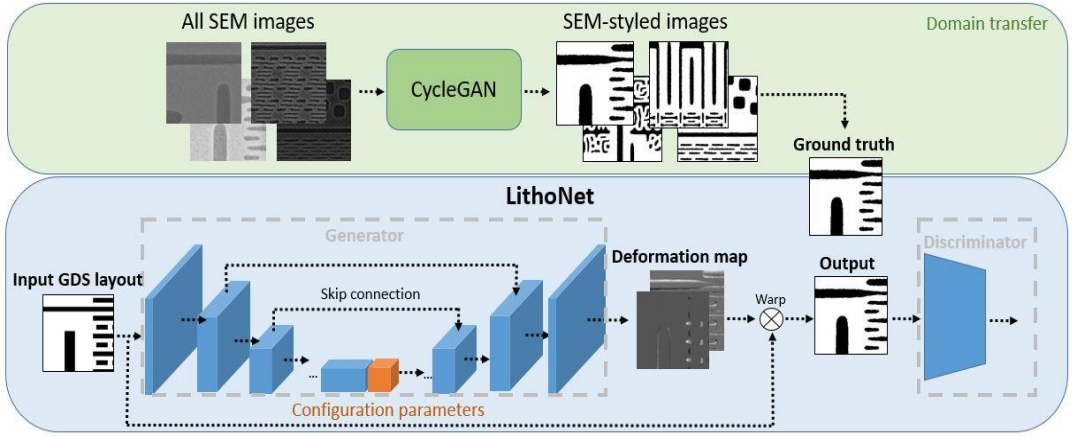
AI: Application in Image Classification/Recognition

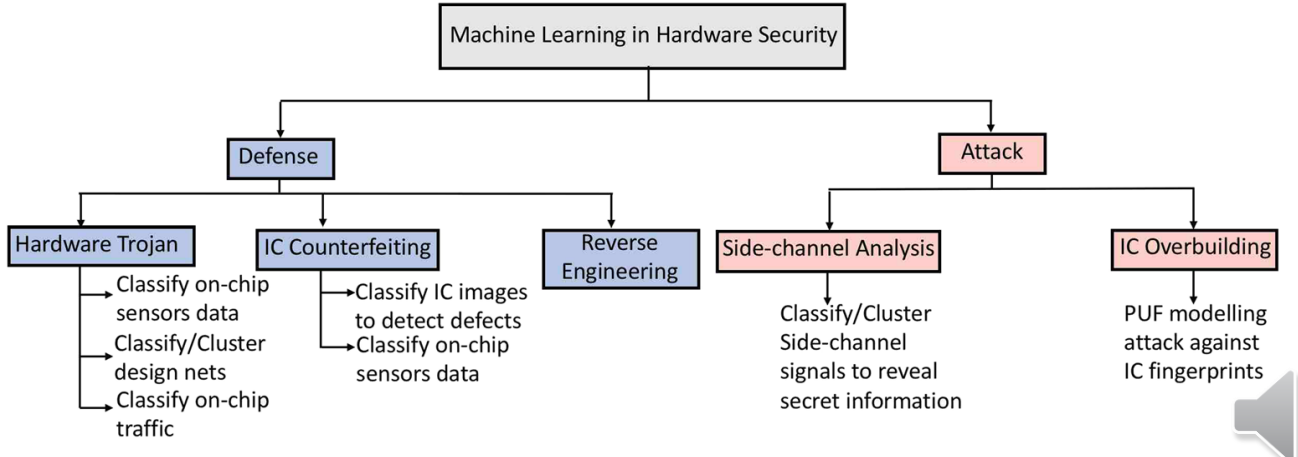
- **Image Processing to Computer Vision Steps**: Acquisition, Representation, Compression, Transmission, Image Enhancement, Edge/Feature Extraction, Pattern Matching, and Image Understanding or Recognition.
- **Definition**: The process of sorting pixels into a finite number of individual classes, or categories of data. Based on their spectral response (i.e. the measured brightness of a pixel across the image bands, as reflected by the pixel's spectral signature).
- The underlying assumption of image classification is that spectral response of a particular feature (i.e. land-cover class) will be relatively consistent throughout the image.
- Supervised Versus Unsupervised Classification:
  - ✓ **Supervised method** uses the image pixels representing regions of known, homogenous surface composition (i.e. training areas) to classify unknown pixels.
  - ✓ **Unsupervised method** identifies groups of pixels that exhibit a similar spectral response.
- Performing image classification through deep convolutional neural network.
- For a hundred thousand full resolution images, with complex and multiple textual annotation and a hierarchy of 1000 object classes along several dimensions, how deep the neural network should be?



AI: Application in Cybersecurity (Hardware Security)

- **AI Meets Hardware Security:**
  - ✓ AI techniques are applied to various hardware security problems.
  - ✓ They can be incorporated both for attack and defense mechanisms.
  - ✓ Possible defense candidate are Hardware Trojan Detection.
  - ✓ Possible attack candidates are: (a) side-channel analysis; and (b) launching modeling attacks on physically unclonable functions.
  - ✓ **Circuit Recognition**: A deep learning framework using CNNs for recognizing circuit functionalities based on a new circuit representation suitable for network computing processes.
  - ✓ **Physical Inspection of Electronics**: Developing a CNN-based approach that learns the parametric model of physical and chemical phenomena of a fabrication process directly from a training dataset containing pairs of Integrated Circuit (IC) layouts and their corresponding scanning electron microscope (SEM) images. Based on the learned CNN model, we can predict a fabricated circuit shape and structure more accurately and efficiently than traditional methods along with evaluating the trustiness of the ICs.





Wrap-up

- In **AI problems**, we want to take an advantage of drawing a fairly sharp line between the physical and the intellectual capacities of a man.
- A **knowledge-based agent steps**: **(1)** The stimulus must be translated into an internal representation; **(2)** The representation is manipulated by cognitive processes to derive new internal representations; and **(3)** These is turn translated into action.
- Artificial neural network is **computerized model** of brain neural network.
- **Processes in AI Systems**: **(a)** representation; **(b)** thinking; **(c)** reasoning; **(d)** learning; **(e)** searching; and **(f)** output.
- **AI systems** can think and act like humans and also do them rationally.
- The **intelligence** as the computational part of the ability to achieve goals in the world.
- The **intelligence** is described as the capacity to learn and solve problems in particular tacking novel problems, act rationally, and act like humans.
- **Machines and computer programs** are capable of problem solving and learning like a human brain.
- **Artificial Neural Network** is described as computational models inspired by the human brain. It is **massively parallel**, **distributed system**, and **made up of simple processing units called neurons**.
- **Convolutional neural network** is a deep neural network with application for processing data with a known grid-like topology.
- **AI techniques** are applied to various hardware security problems.
- **Using AI** for learning the parametric model of **integrated circuit layouts and their corresponding SEM images** for predicting circuit shape and structure more accurately and efficiently along with evaluating the trustiness of the ICs.