Artificial Intelligence & Privacy

Budi Rahardjo (@rahard)

2024

riset.ai

VLSI/Security/ AI/IoT/Blockchain/Big Data

- Lecturer at STEI, ITB
- Manage .ID domain 1997-2005
- Founder & chairman of ID-CERT
  Indonesia Computer Emergency Response Team
- Serial technopreneur – startup mentors

http://budi.rahardjo.id
youtube.com/@rahard

YouTube
Channel : Budi Rahardjo
https://www.youtube.com/user/rahard

AI Hype

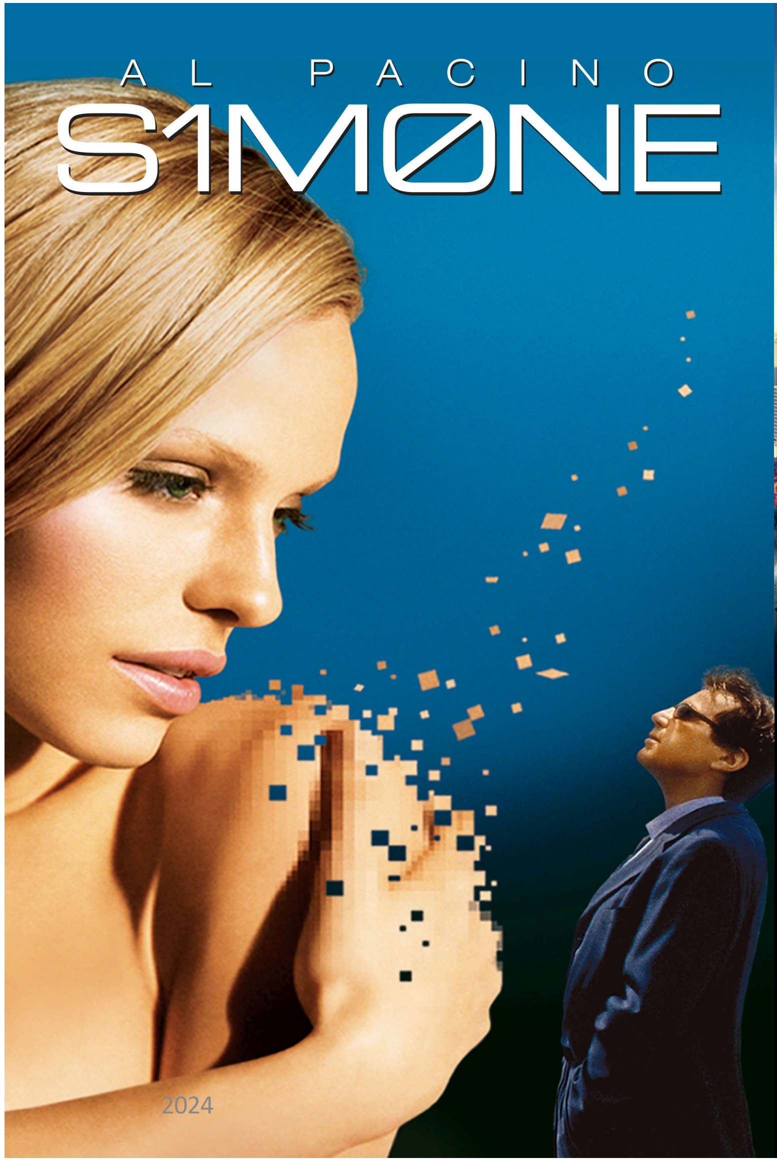
- ChatGPT
- Bard / Gemini
- Bing, Copilot
- Midjourney, Dall-E
- Sora AI – text to video
- …

History of Artificial Intelligence

John McCarthy coined "Artificial Intelligence" in **1956**:

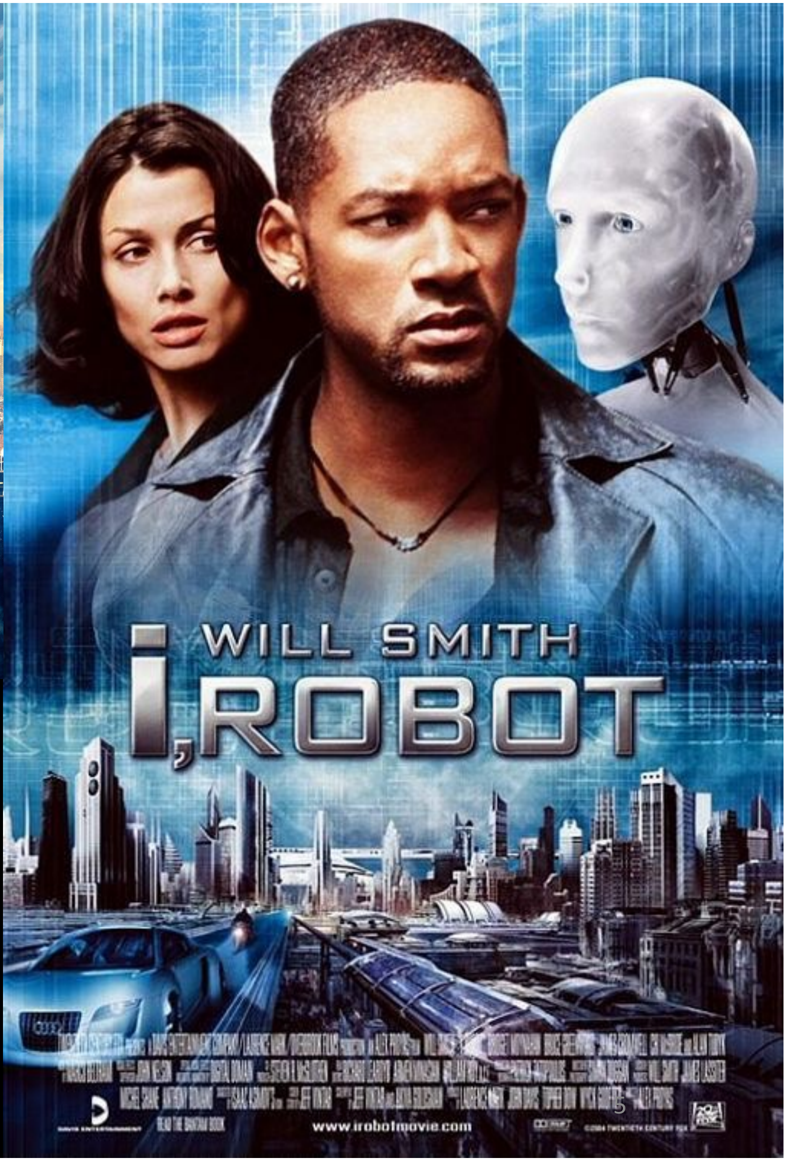
… machines that can perform tasks
that are characteristic of human intelligence …

General AI vs. Narrow AI (specific task)

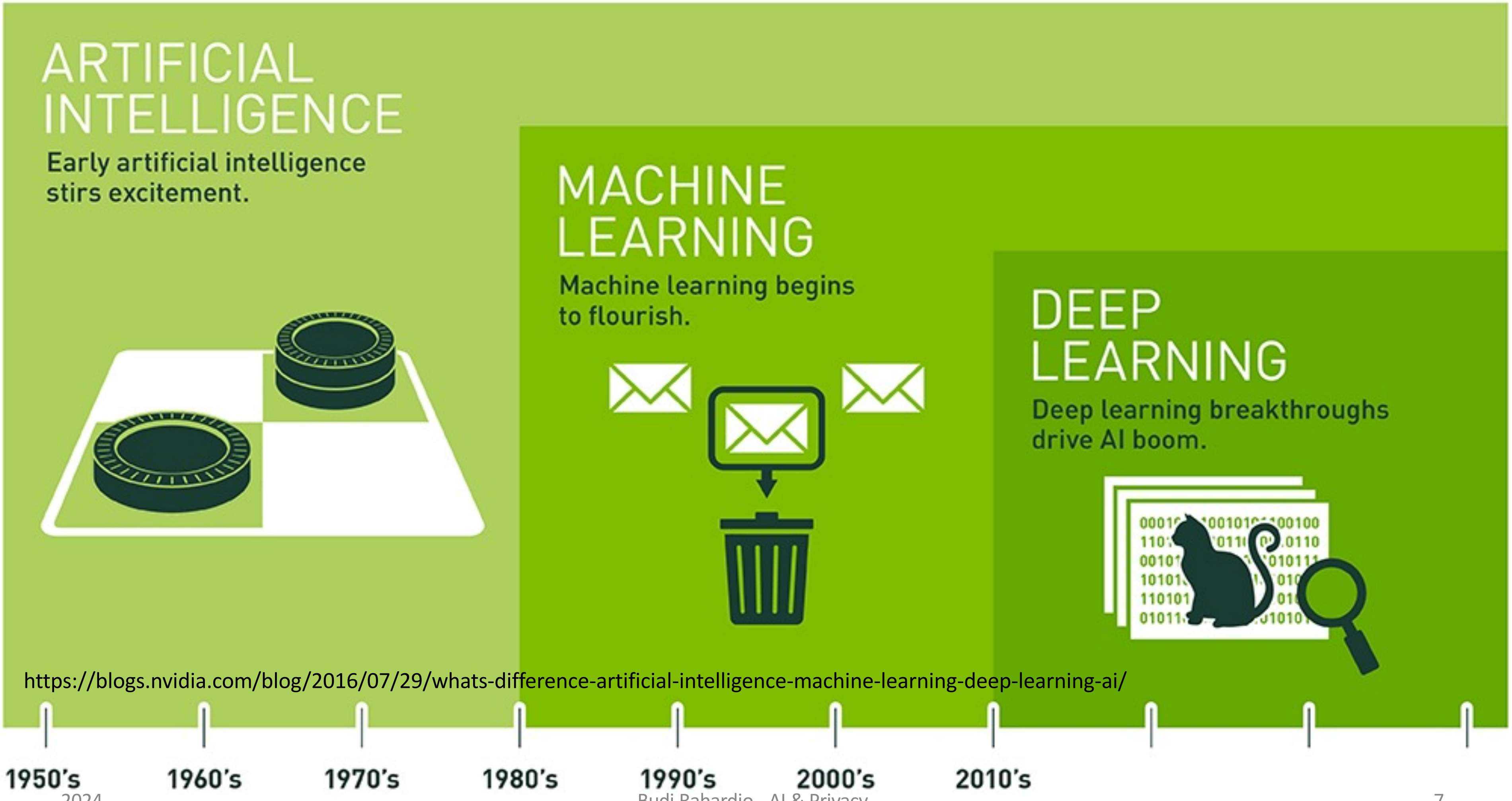

AL PACINO
S1MØNE

LIFE'S TOO SHORT TO BE A BACKGROUND CHARACTER
FREE GUY
ONLY IN THEATERS
AUGUST 13

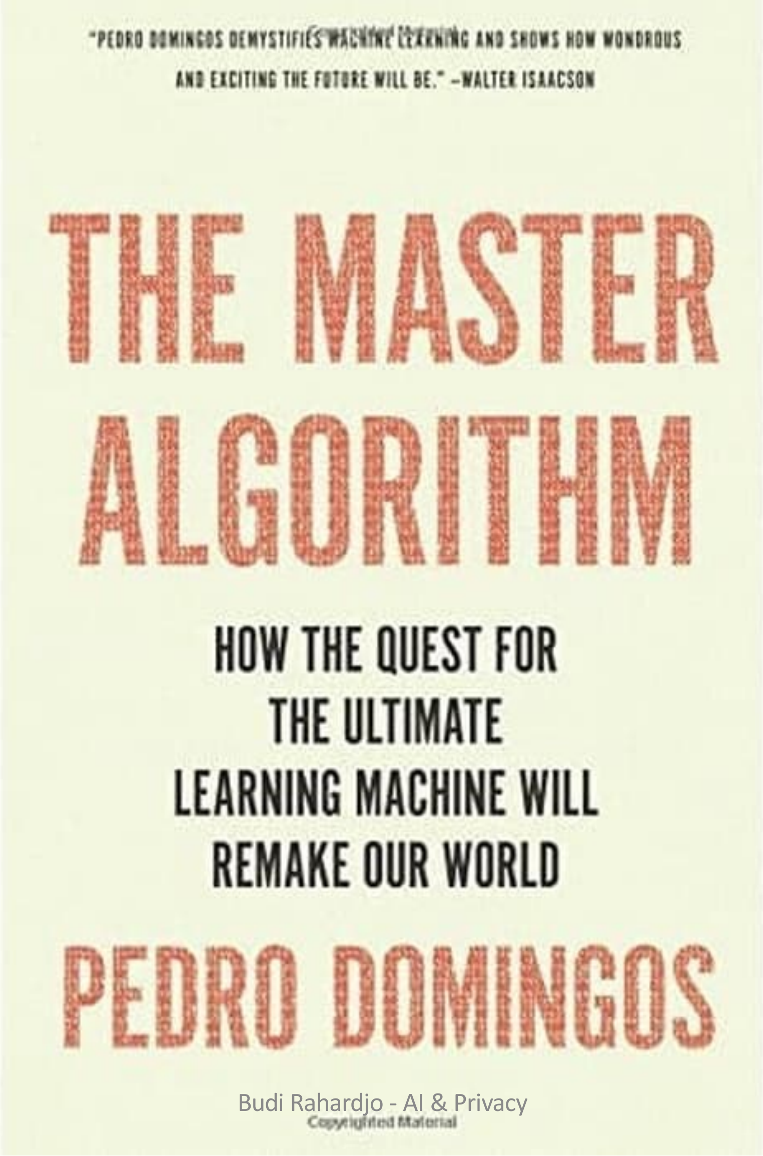
A.I.
ARTIFICIAL INTELLIGENCE


WILL SMITH
I, ROBOT
www.irobotmovie.com

General AI vs. Narrow AI (specific task)


ARTIFICIAL INTELLIGENCE
Early artificial intelligence stirs excitement.
MACHINE LEARNING
Machine learning begins to flourish.
DEEP LEARNING
Deep learning breakthroughs drive AI boom.
1950's
1960's
1970's
1980's
1990's
2000's
2010's

https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/



"PEDRO DOMINGOS DEMYSTIFIES MACHINE LEARNING AND SHOWS HOW WONDROUS AND EXCITING THE FUTURE WILL BE." —WALTER ISAACSON

THE MASTER ALGORITHM

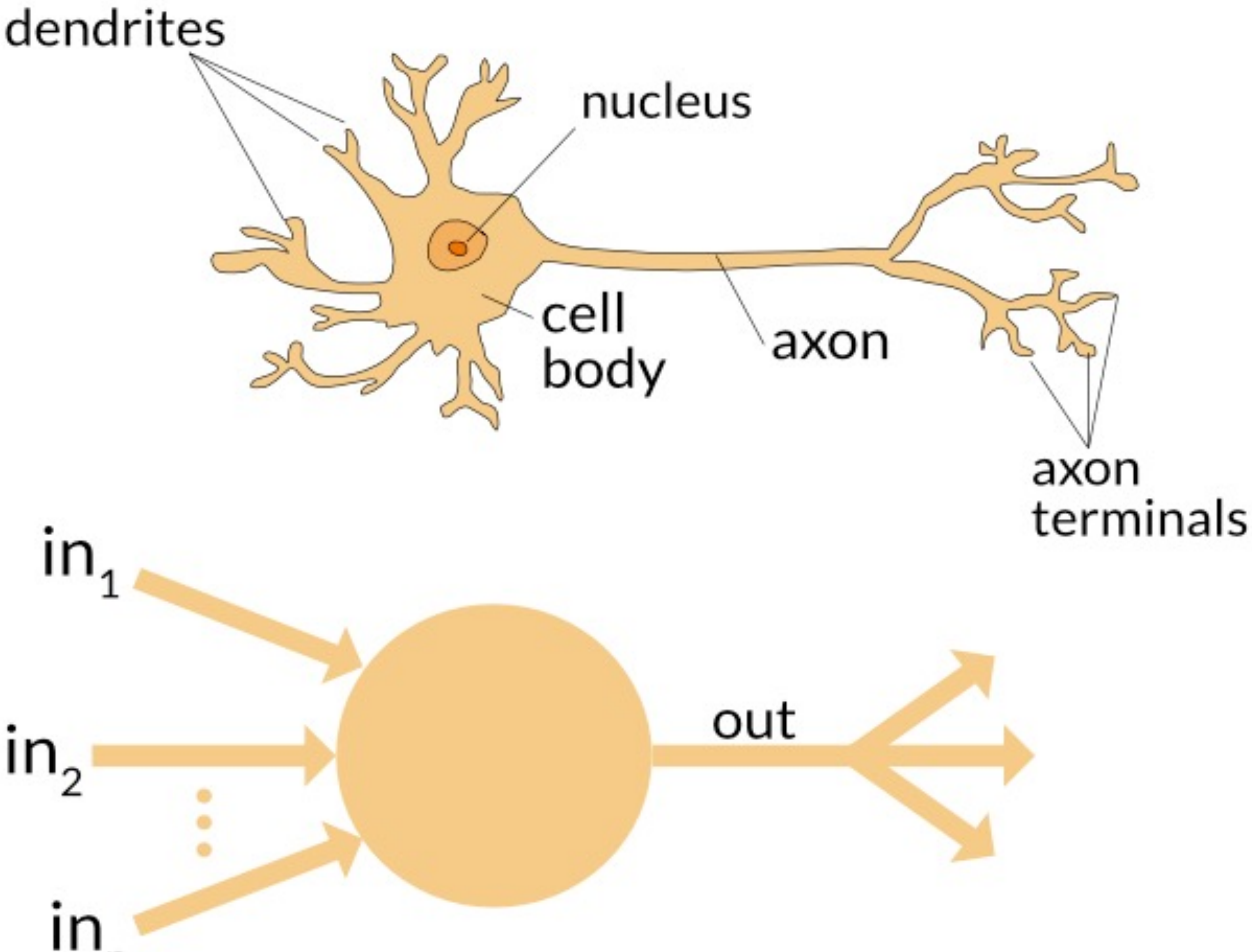
HOW THE QUEST FOR
THE ULTIMATE
LEARNING MACHINE WILL
REMAKE OUR WORLD

PEDRO DOMINGOS

Pedro Domingos: 5 Tribes of Machine Learning

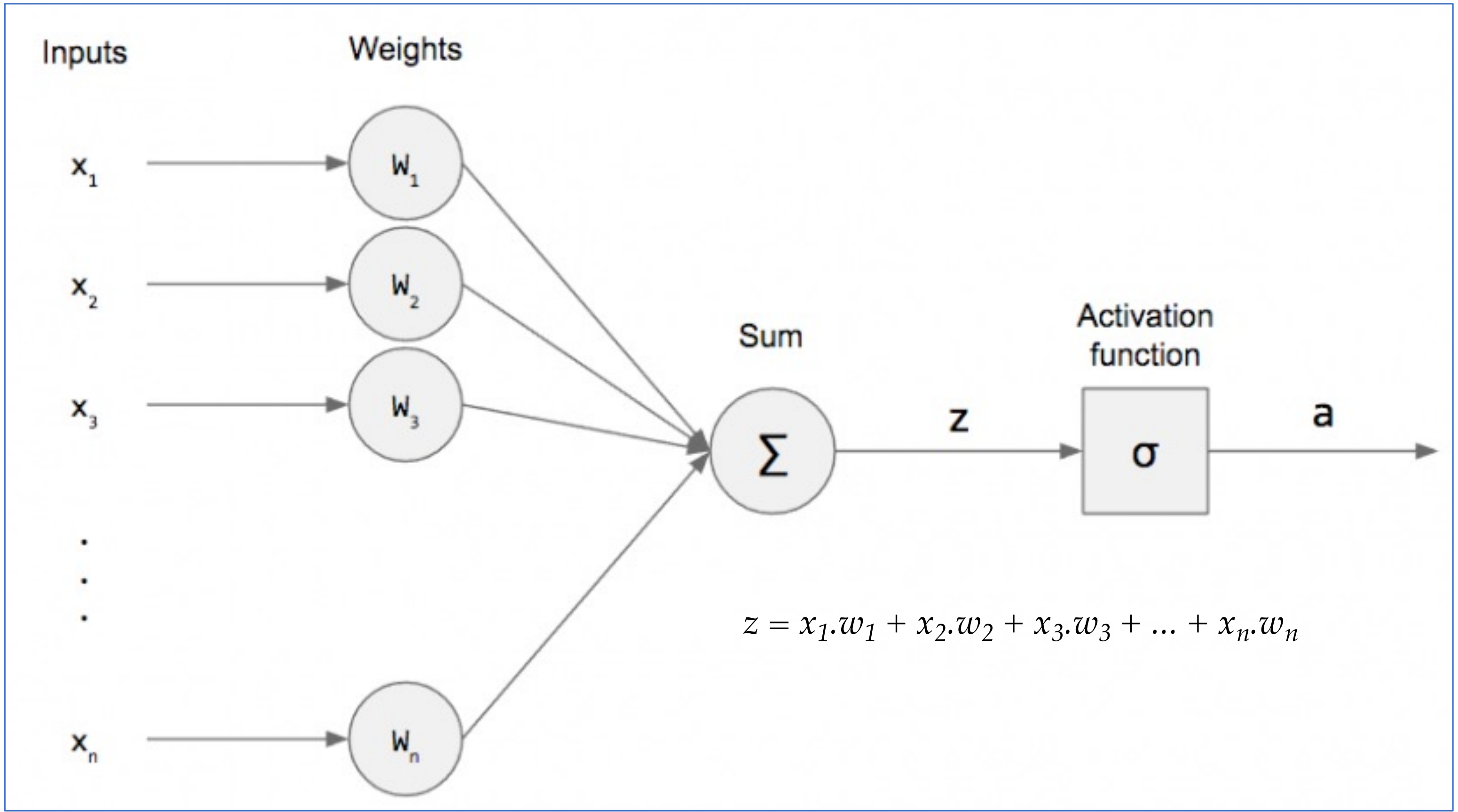
Tribe	Origins	Master Algorithm
Symbolists	Logic, philosophy	Inverse deduction
Connectionists	Neuroscience	Backpropagation
Evolutionaries	Evolutionary biology	Genetic programming
Bayesians	Statistics	Probabilistic inference
Analogizers	Psychology	Kernel machines

Source: Pedro Domingos – The Five Tribes of Machine Learning



https://www.codeproject.com/Articles/1205732/Build-Simple-AI-NET-Library-Part-Perceptron

Model of a Neuron

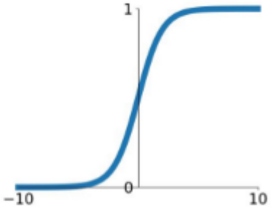


$$z = x_1.w_1 + x_2.w_2 + x_3.w_3 + \ldots + x_n.w_n$$

Activation Functions

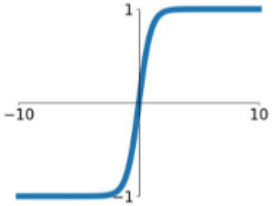
Sigmoid

$\sigma(x) = \frac{1}{1+e^{-x}}$



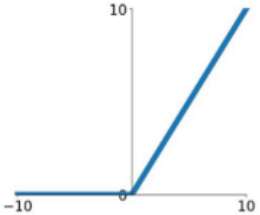
tanh

$\tanh(x)$



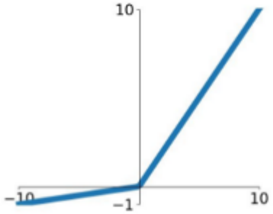
ReLU

$\max(0, x)$



Leaky ReLU

$\max(0.1x, x)$

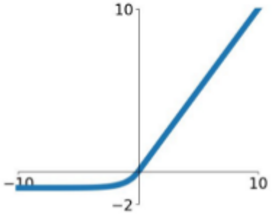


Maxout

$\max(w_1^T x + b_1, w_2^T x + b_2)$

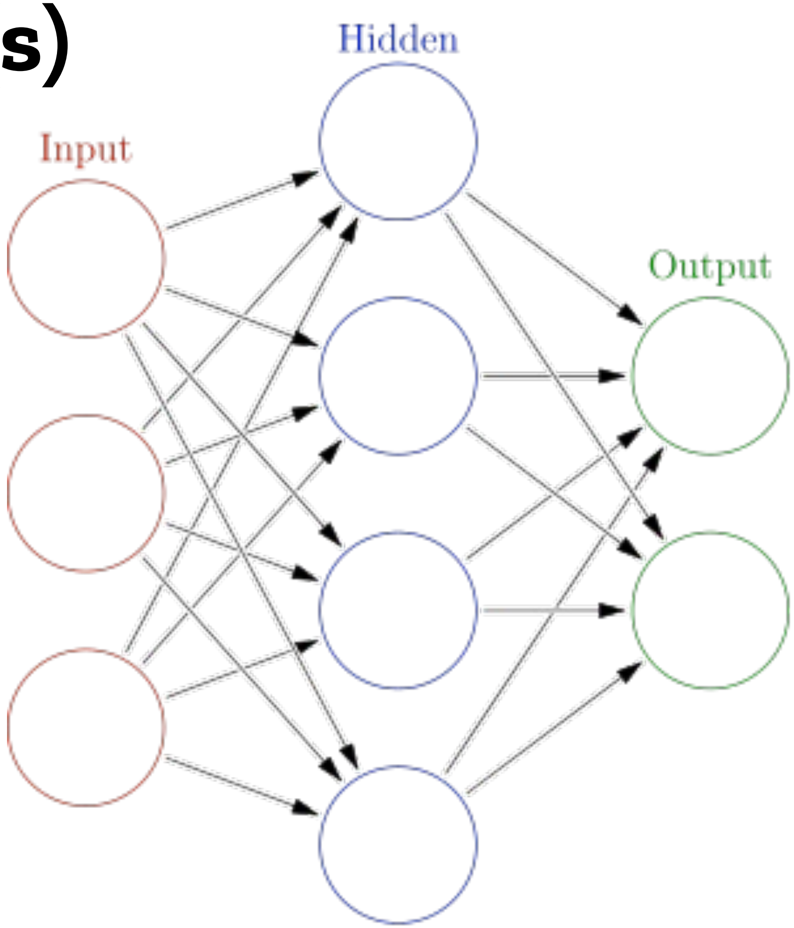
ELU

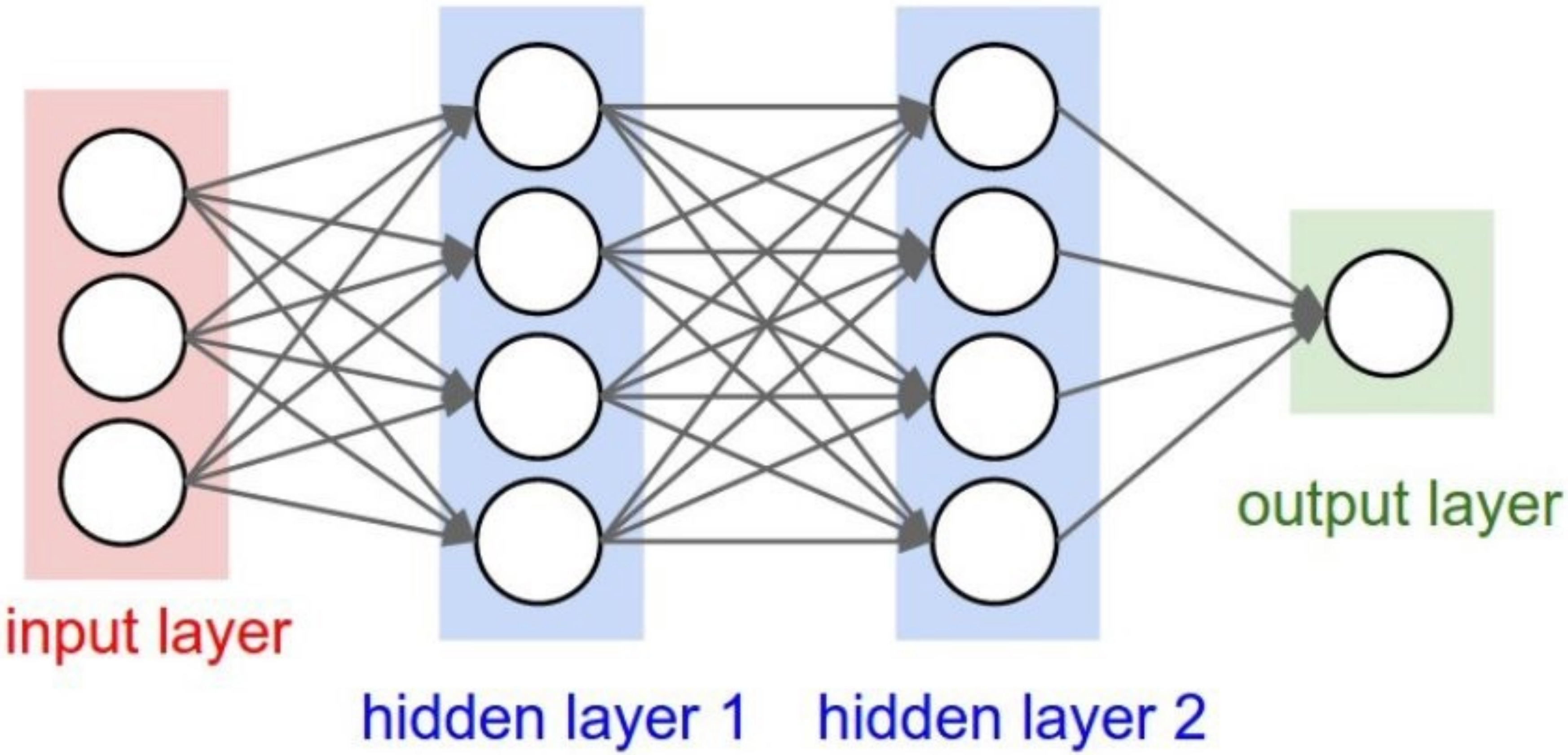
$$\begin{cases} x & x \geq 0 \\ \alpha(e^x - 1) & x < 0 \end{cases}$$

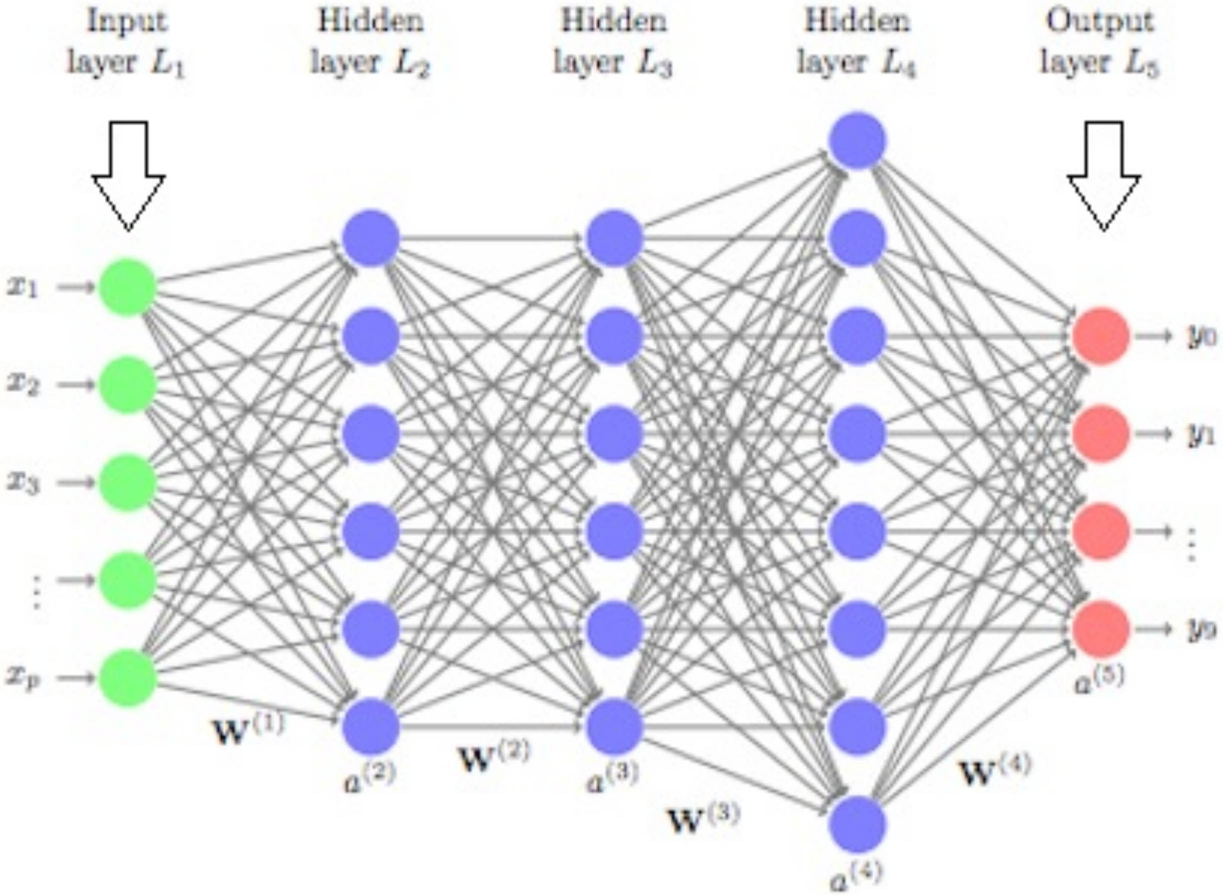


https://deepai.org/machine-learning-glossary-and-terms/activation-function

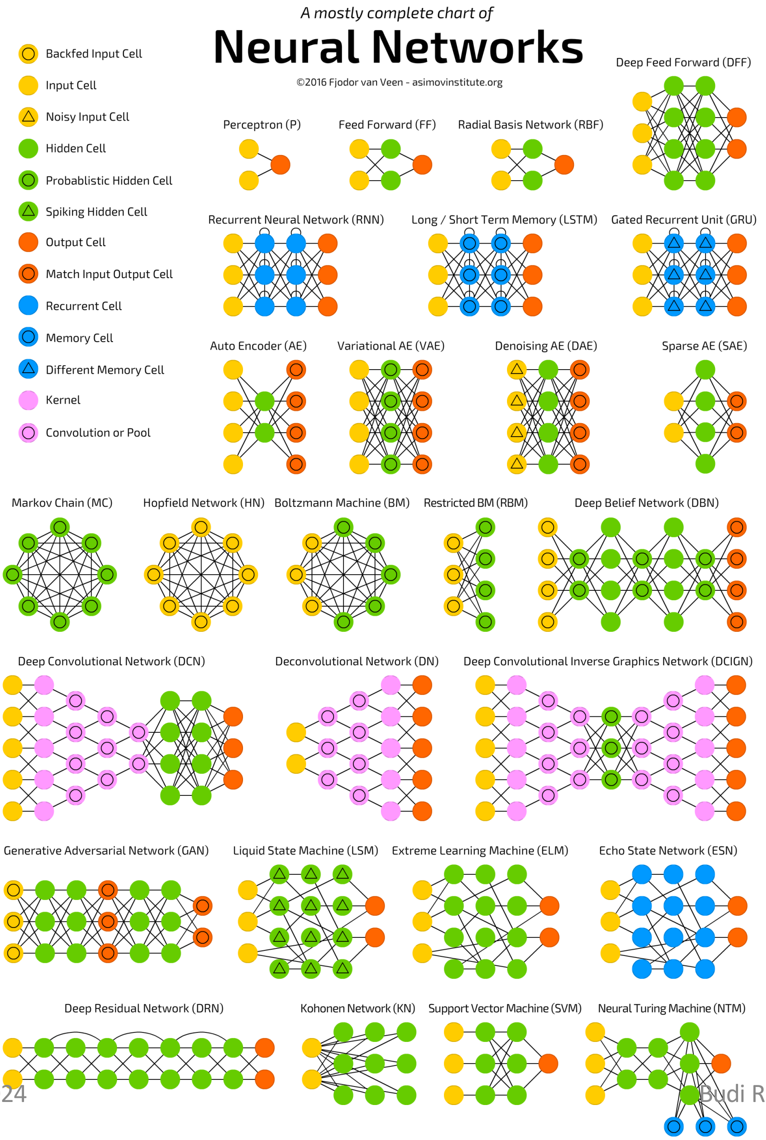
Hidden Layer(s)

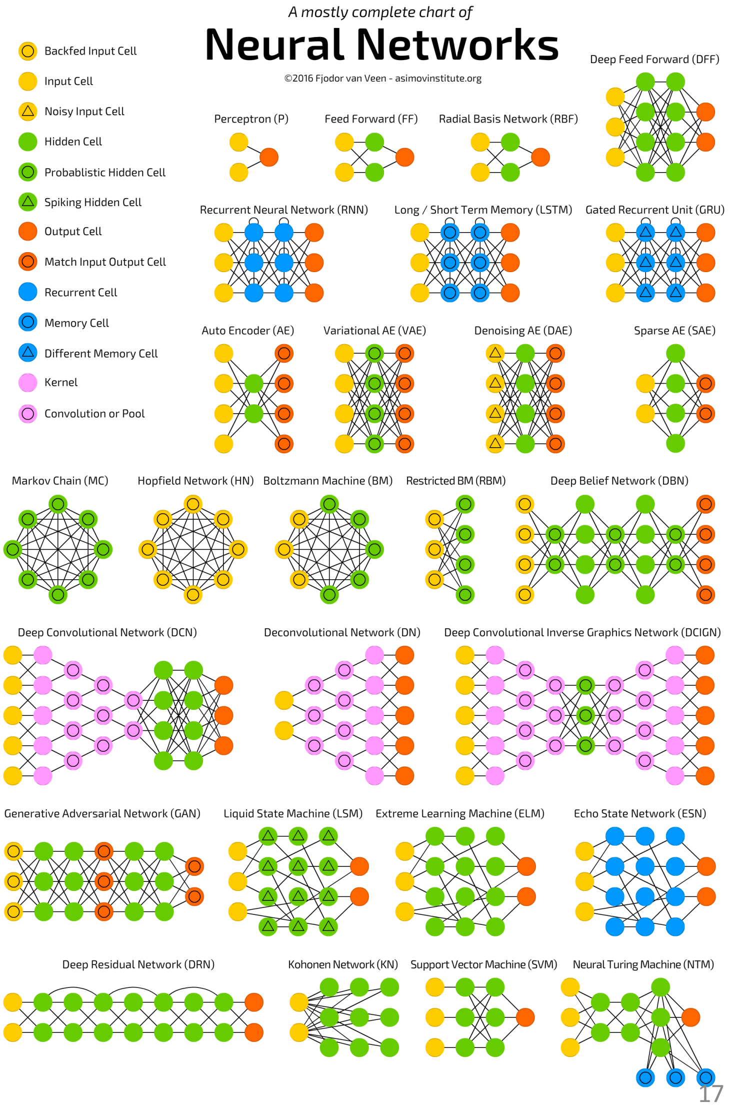



input layer
hidden layer 1
hidden layer 2
output layer

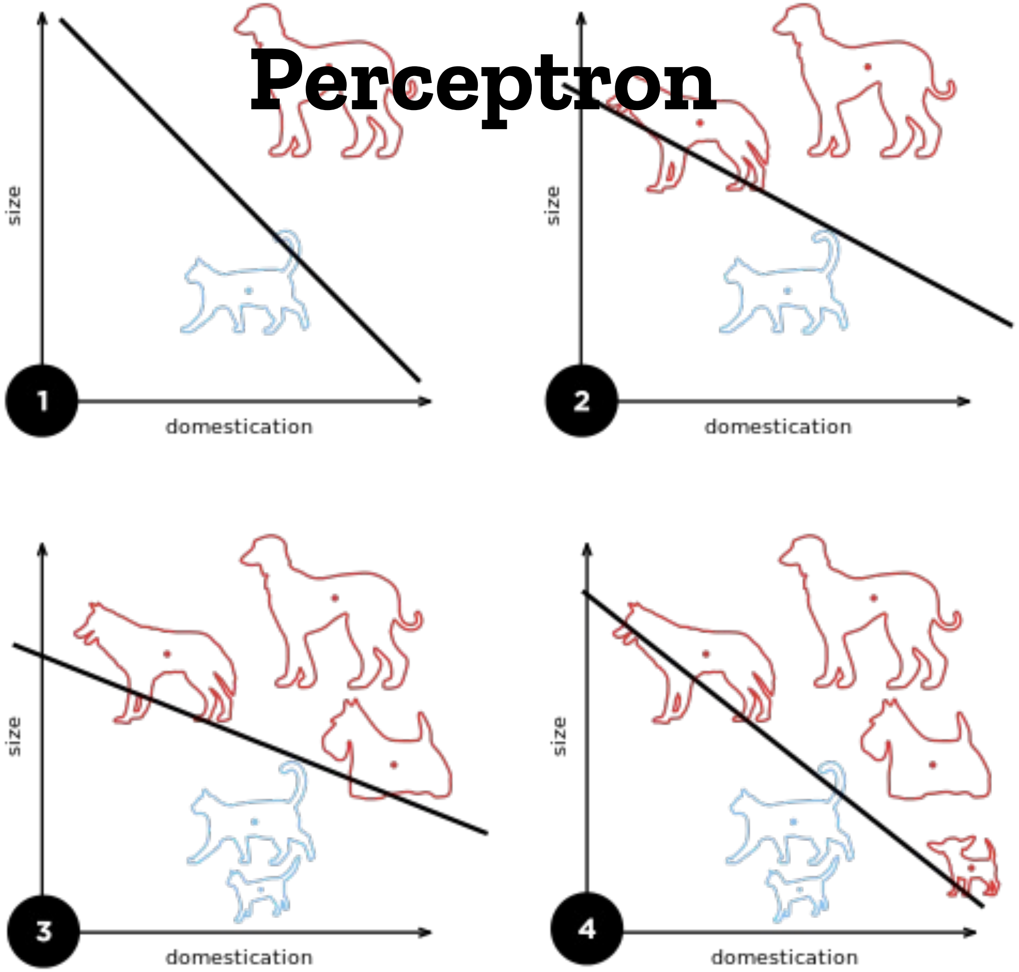


https://medium.com/analytics-vidhya/the-shortest-introduction-to-deep-learning-you-will-find-on-the-web-25a9975bbe1d

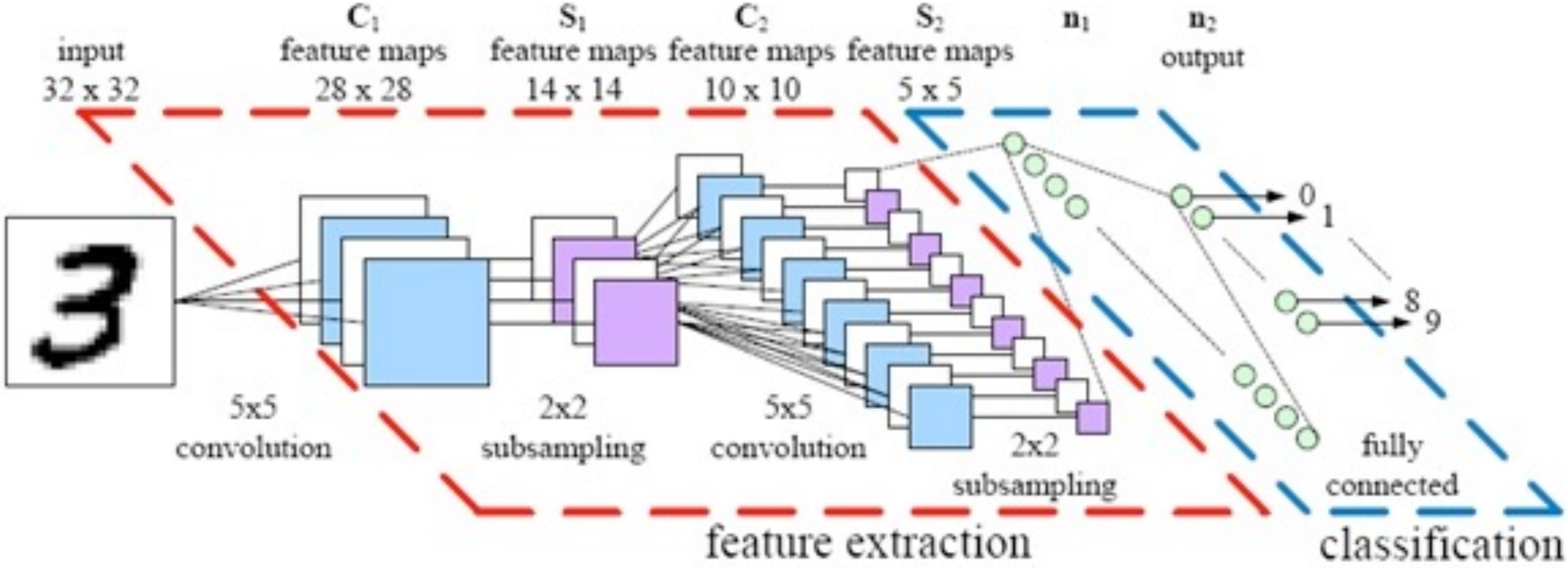

A mostly complete chart of
Neural Networks
©2016 Fjodor van Veen - asimovinstitute.org
Backfed Input Cell
Input Cell
Noisy Input Cell
Hidden Cell
Probablistic Hidden Cell
Spiking Hidden Cell
Output Cell
Match Input Output Cell
Recurrent Cell
Memory Cell
Different Memory Cell
Kernel
Convolution or Pool
Perceptron (P)
Feed Forward (FF)
Radial Basis Network (RBF)
Deep Feed Forward (DFF)
Recurrent Neural Network (RNN)
Long / Short Term Memory (LSTM)
Gated Recurrent Unit (GRU)
Auto Encoder (AE)
Variational AE (VAE)
Denoising AE (DAE)
Sparse AE (SAE)
Markov Chain (MC)
Hopfield Network (HN)
Boltzmann Machine (BM)
Restricted BM (RBM)
Deep Belief Network (DBN)
Deep Convolutional Network (DCN)
Deconvolutional Network (DN)
Deep Convolutional Inverse Graphics Network (DCIGN)
Generative Adversarial Network (GAN)
Liquid State Machine (LSM)
Extreme Learning Machine (ELM)
Echo State Network (ESN)
Deep Residual Network (DRN)
Kohonen Network (KN)
Support Vector Machine (SVM)
Neural Turing Machine (NTM)

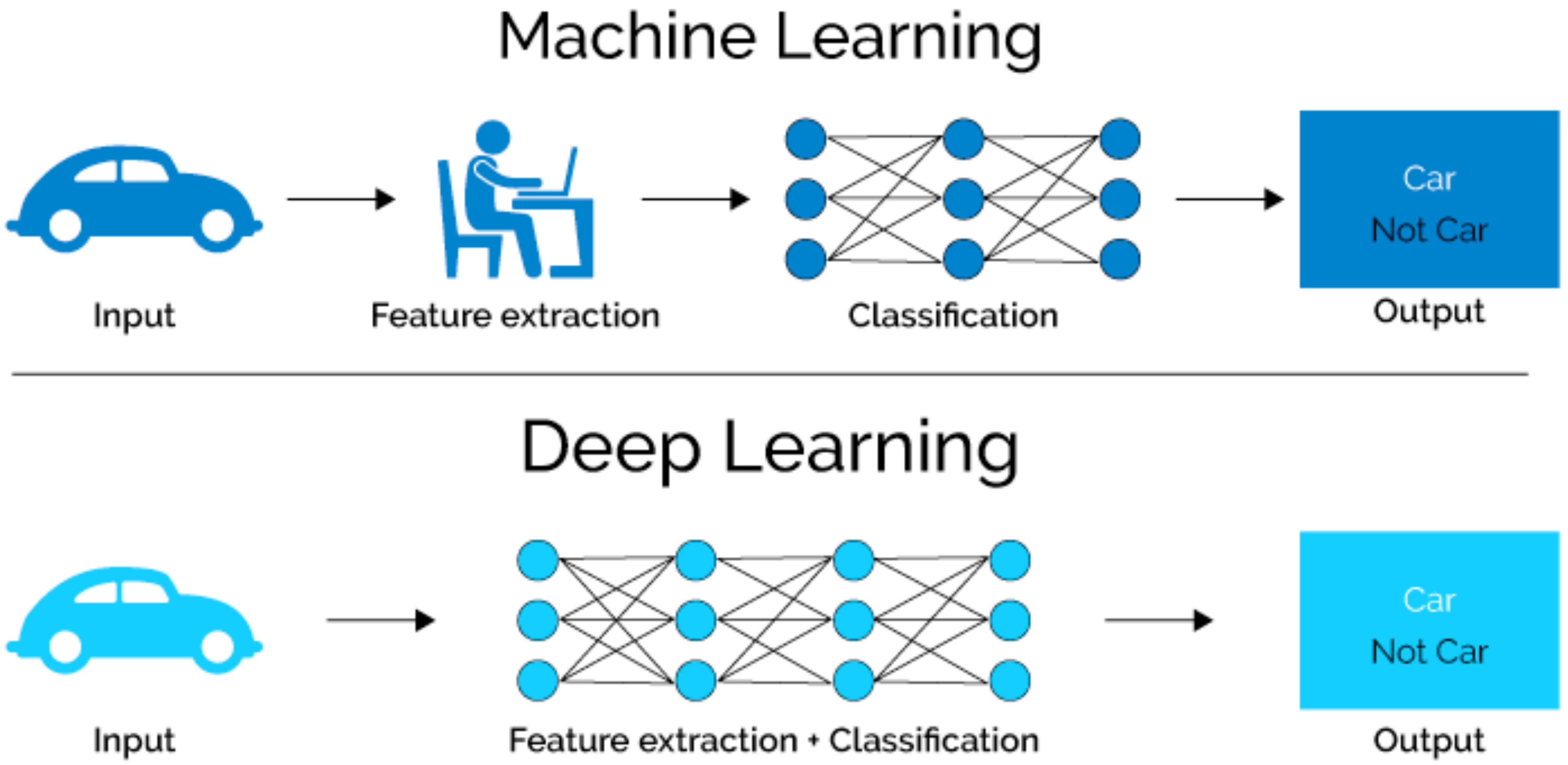

A mostly complete chart of
Neural Networks
©2016 Fjodor van Veen - asimovinstitute.org
Backfed Input Cell
Input Cell
Noisy Input Cell
Hidden Cell
Probablistic Hidden Cell
Spiking Hidden Cell
Output Cell
Match Input Output Cell
Recurrent Cell
Memory Cell
Different Memory Cell
Kernel
Convolution or Pool
Perceptron (P)
Feed Forward (FF)
Radial Basis Network (RBF)
Deep Feed Forward (DFF)
Recurrent Neural Network (RNN)
Long / Short Term Memory (LSTM)
Gated Recurrent Unit (GRU)
Auto Encoder (AE)
Variational AE (VAE)
Denoising AE (DAE)
Sparse AE (SAE)
Markov Chain (MC)
Hopfield Network (HN)
Boltzmann Machine (BM)
Restricted BM (RBM)
Deep Belief Network (DBN)
Deep Convolutional Network (DCN)
Deconvolutional Network (DN)
Deep Convolutional Inverse Graphics Network (DCIGN)
Generative Adversarial Network (GAN)
Liquid State Machine (LSM)
Extreme Learning Machine (ELM)
Echo State Network (ESN)
Deep Residual Network (DRN)
Kohonen Network (KN)
Support Vector Machine (SVM)
Neural Turing Machine (NTM)

Perceptron



1
size
domestication
2
size
domestication
3
size
domestication
4
size
domestication

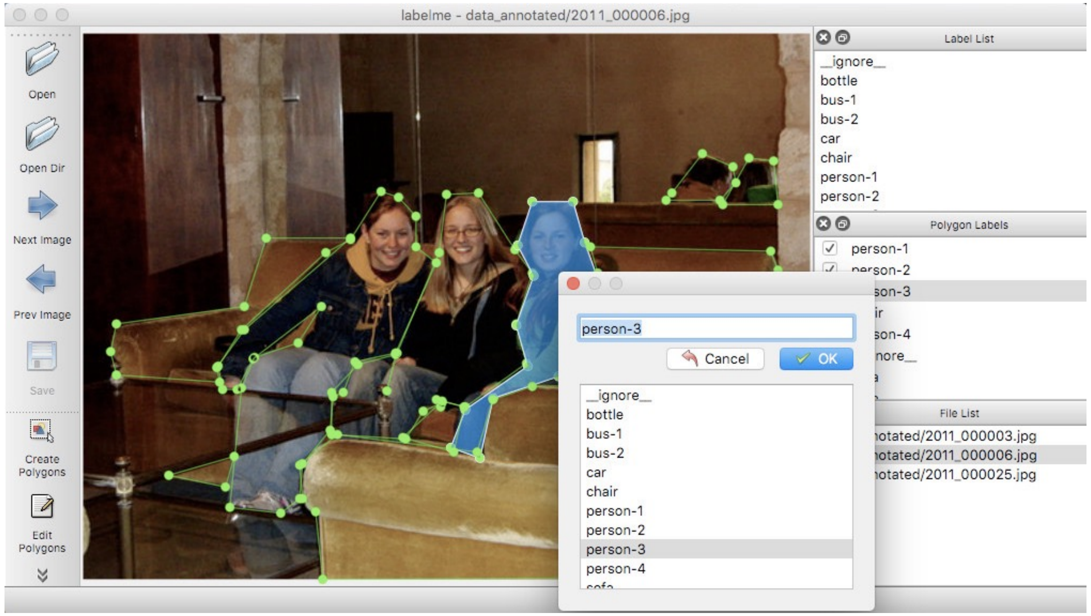

input
32 x 32
C₁
feature maps
28 x 28
S₁
feature maps
14 x 14
C₂
feature maps
10 x 10
S₂
feature maps
5 x 5
n₁
n₂
output
0
1
8
9
5x5
convolution
2x2
subsampling
5x5
convolution
2x2
subsampling
fully
connected
feature extraction
classification


Machine Learning
Input
Feature extraction
Classification
Car
Not Car
Output
Deep Learning
Input
Feature extraction + Classification
Car
Not Car
Output

The Core of Deep Learning – MODEL creation

- Architecture
  - The connections of neurons, layers, ...
  - Still an art, educated guess
  - Algorithm(s) used for training: back propagation
- Dataset
  - The data used for training
  - Need MANY of these
  - Privacy?
- Once the MODEL is created it can be used in ***inferencing***

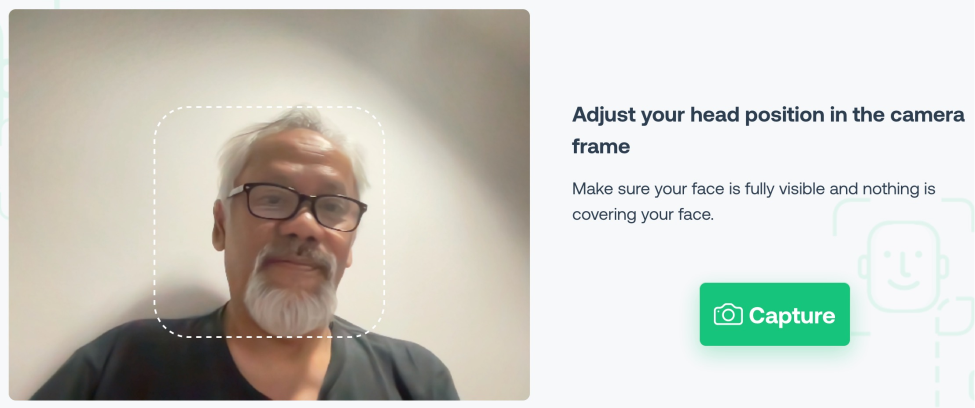
Data Set – Anotate Data



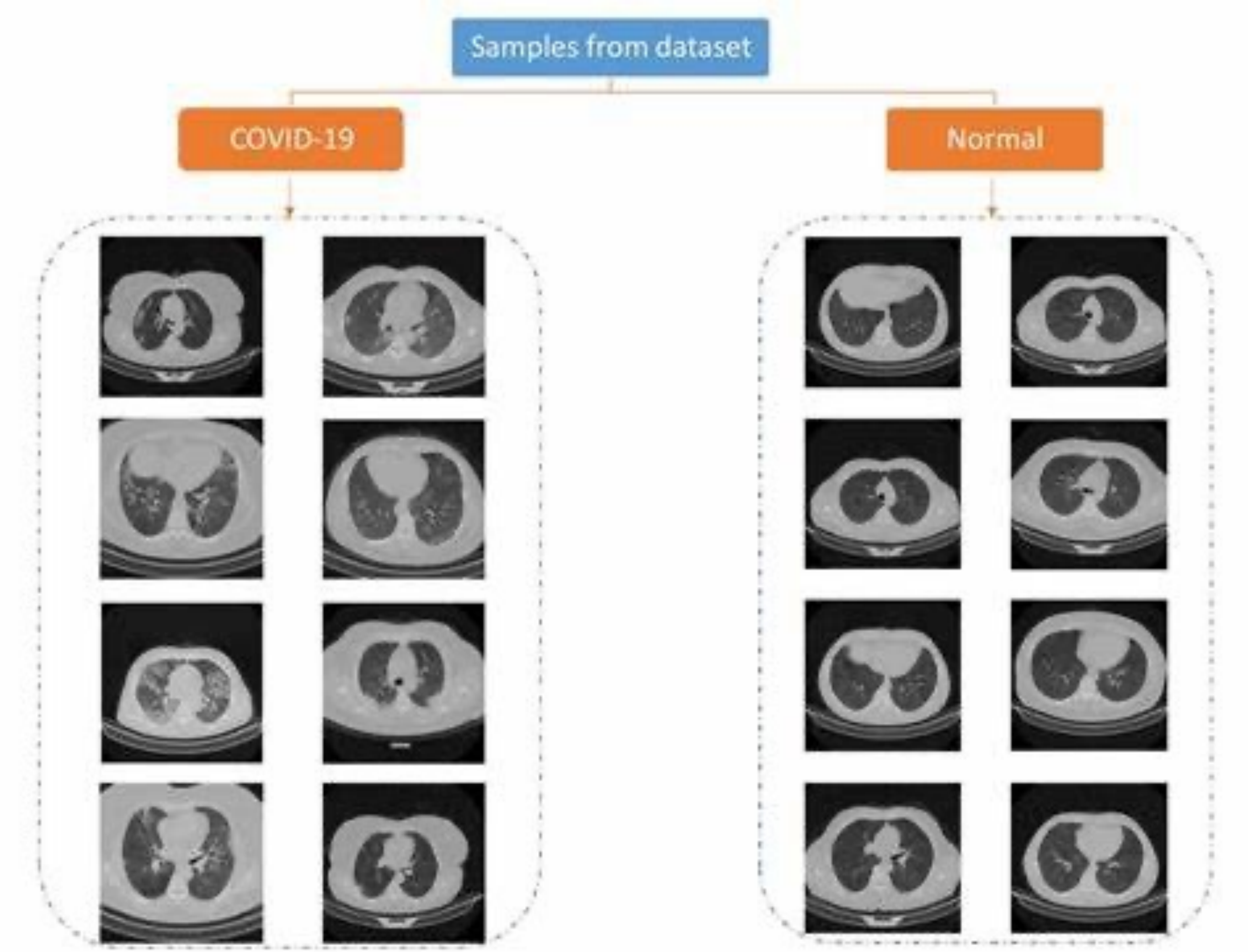
https://github.com/wkentaro/labelme

Dataset Examples

- ALPR – Automatic License Plate Recognition
- Face Detection and Recognition
- Issues
  - Needs a large number of examples (photos) as data set
  - Where do we get the photos?
  - Do wee need to get permission to get the photos?
  - Can we share or sell these photos


Adjust your head position in the camera frame

Make sure your face is fully visible and nothing is covering your face.



Example: COVID-19 detection

- where do we get the dataset?

MODEL and Applications

- Depending on the applications, the MODEL may not have the detailed information of data
  - MODEL for Object/Face Detection, does not have data of persons used in training
  - MODEL for license plate detection only understands Numbers and Characters. It does not have the actual plates

Other AI Issues

- Bias?
- Explainable? Trustworthy? Reliability?
- Issues related to data set

Concluding Remarks

- Artificial Intelligence is becoming more **and more important** in our daily lives
- The search for **killer application** is still on
- There are still many issues many of which are non-technical. **Privacy** is one of them, but there are ways to reduce the risks