

# 최신 AI 연구 동향

Jaekoo Lee<sup>1</sup>

<sup>1</sup> Ph.D., Assistant Professor, School of Software, College of Computer Science

jaekoo@kookmin.ac.kr

Kookmin University, Seoul, Korea

talk @2020 NetSec-KR

07. 17, 2020



# Thank you for your invitation

www.netsec-kr.or.kr

## 2020 NetSec-KR

### Post COVID-19 및 데이터 경제 시대를 위한 정보보호 인텔리전스

07.16<sup>Thu</sup> — 17<sup>Fri</sup> 온라인 컨퍼런스



The 26th  
Network Security  
Conference-Korea

제26회  
정보통신망 정보보호  
컨퍼런스



#### [등록비 및 등록방법 안내]

회원	비회원	학생(전일제)	공무원
500,000원	550,000원	200,000원	200,000원

#### [사전등록]

- 학회 홈페이지(www.kiisc.or.kr)에서 접속할 경우  
학회행사 → 사전등록 바로가기 → 학술행사 선택(NetSec-KR 2020) 등록하기 선택
- 학생의 경우 kiisc@kiisc.or.kr 로 학생증 사본 송부
- 사전등록마감: 2020년 7월 9일(목)
- 계좌번호 : 국민은행 754-01-0008-146 (예금주 : 한국정보보호학회)
- 사전등록 시 등록비는 위의 계좌로 송금하시고, 입금자가 대리일 경우 통보바랍니다.
- 신용카드 결제 시 계산서 발급이 불가합니다. (부가가치세법 시행령 제57조)
- 사전등록 시 (2~3일 이내) 기재해주신 이메일로 청구용 계산서가 발행되오니  
영수증 계산서가 필요하신 경우 미리 학회로 연락바랍니다.
- 학회 특별회원사 임직원은 학회 회원으로 존함합니다.
- 홈페이지(kiisc@kiisc.or.kr) 회원광장 → 특별회원사에서 확인하실 수 있습니다.
- 등록자의 핸드폰 번호로 모바일 상품권(학술대회 기념품)이 발송될 수 있으나,  
반드시 본인 핸드폰 번호를 정확하게 기재하시어 불이익이 없으시길 바랍니다.
- 입금명은 회사명뿐만 아니라 개인이 입금 시 확인이 되지 않습니다.  
행사 및 등록 금액이 경지는 경우가 있으므로 학회 입금 시 입금명은 필수  
[행사명 첫 글자+ 등록자 성명]으로 기재해 주시기 바랍니다.  
예) NetSec-KR 등록 홍길동 + "N홍길동" 기재
- 금번 학술대회는 현장 등록이 없습니다.

주 최 한국인터넷진흥원(KISA)

주 관 한국정보보호학회(KIISC)

후 원 과학기술정보통신부(MSIT), 행정안전부(MOIS)

기관 후원 국가보안기술연구소(NSR), 한국전자통신연구원(ETRI), 금융보안원(FSI),  
한국과학기술정보연구원(KISTI), 한국정보기술연구원(KITRI)  
한국남동발전(KOEN)

기업 후원 Platinum Sponsor 두나무, 메가존클라우드, 코나아이  
Gold Sponsor KT, 네이버, 안랩, 시스메이트, 앳진시큐러스,  
원스, 유비벨록스, 유엔로직스, 시큐브

Silver Sponsor 에스에스엔씨, 엔앤에스피, 지니언스,  
지란지교시큐리티, 한국통신인터넷기술, 루테스

Bronze Sponsor 에스지아이솔루션즈, 팅타시큐리티시스템, SK인포섹,  
이글루시큐리티, 수산아이앤티, ICTK holdings, 삼성SDS,  
라운시큐어, 엔엑스아이씨씨

# Outline

- Introduction
- Background for deep learning
- Research trends in deep learning
- Conclusion

# Introduction

- About me

▶ Jaekoo lee

- Kookmin university
- Assistant professor, School of software, College of computer science
- jaekoo@kookmin.ac.kr



- ▶ Machine intelligence (MI) lab.

- Our research topics

Bio or  
health-care analysis

IoT (e.g. sensor)  
analysis

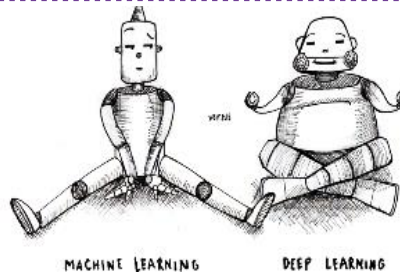
self-driving car  
or drone

## Security

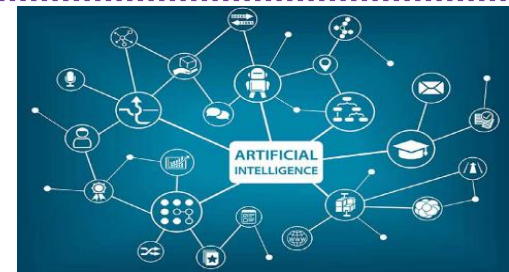
## Apps.



## Artificial intelligence



## Machine (deep) learning



System (Robot) for intelligence

## Fundamentals

# Introduction

- Tutorial objectives:
  - ▶ understand fundamentals of deep learning
  - ▶ review of recent research trends in deep learning
  - ▶ motivate to learn recent breakthroughs in deep learning

*Learning Objectives*



---

## Intelligent Machines

---

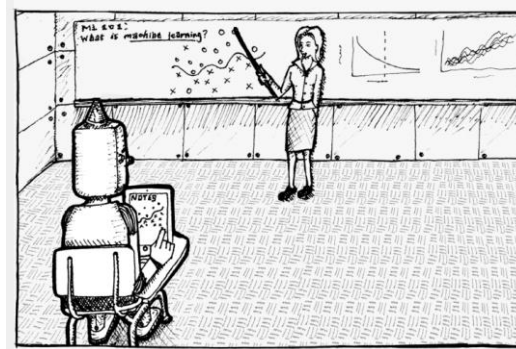
# Nvidia CEO: Software Is Eating the World, but AI Is Going to Eat Software

Jensen Huang predicts that health care and autos are going to be transformed by artificial intelligence.



# Introduction

- Artificial intelligence (AI):
  - ▶ the simulation of human intelligence processes by machines (computer systems)



[from <https://www.euclidean.com/>]

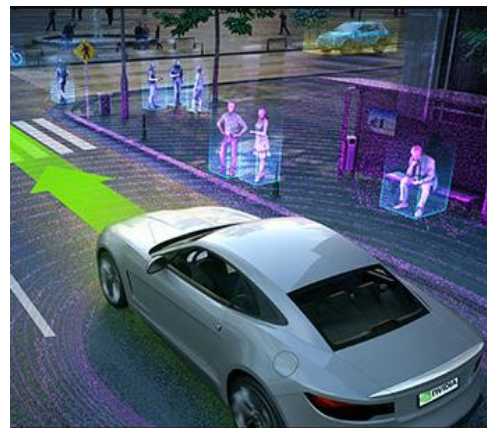
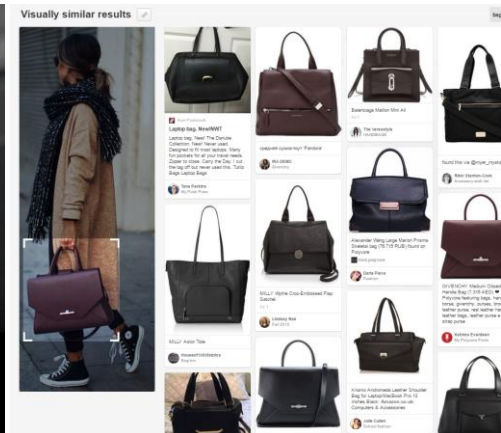
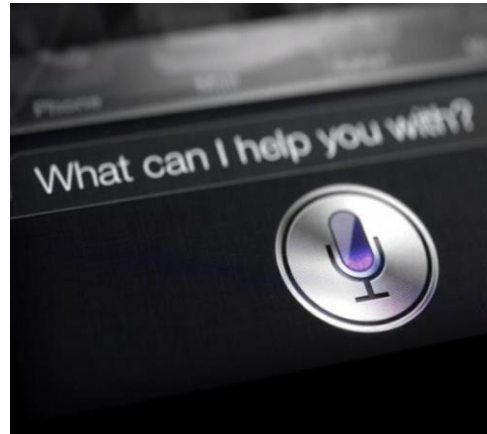
- ▶ include (major components of AI)
  - learning (the acquisition of information and rules for using the information),
  - reasoning (using rules to reach approximate or definite conclusions),
  - knowledge,
  - language understanding, and
  - self-correction
- ▶ Goal:
  - A machine that **thinks or acts like a human**



# Introduction

- AI in production
  - ▶ Speech recognition
  - ▶ Recommender systems
  - ▶ Autonomous driving
  - ▶ Real-time object recognition
  - ▶ Robotics
  - ▶ Real-time language translation
  - ▶ Many more...

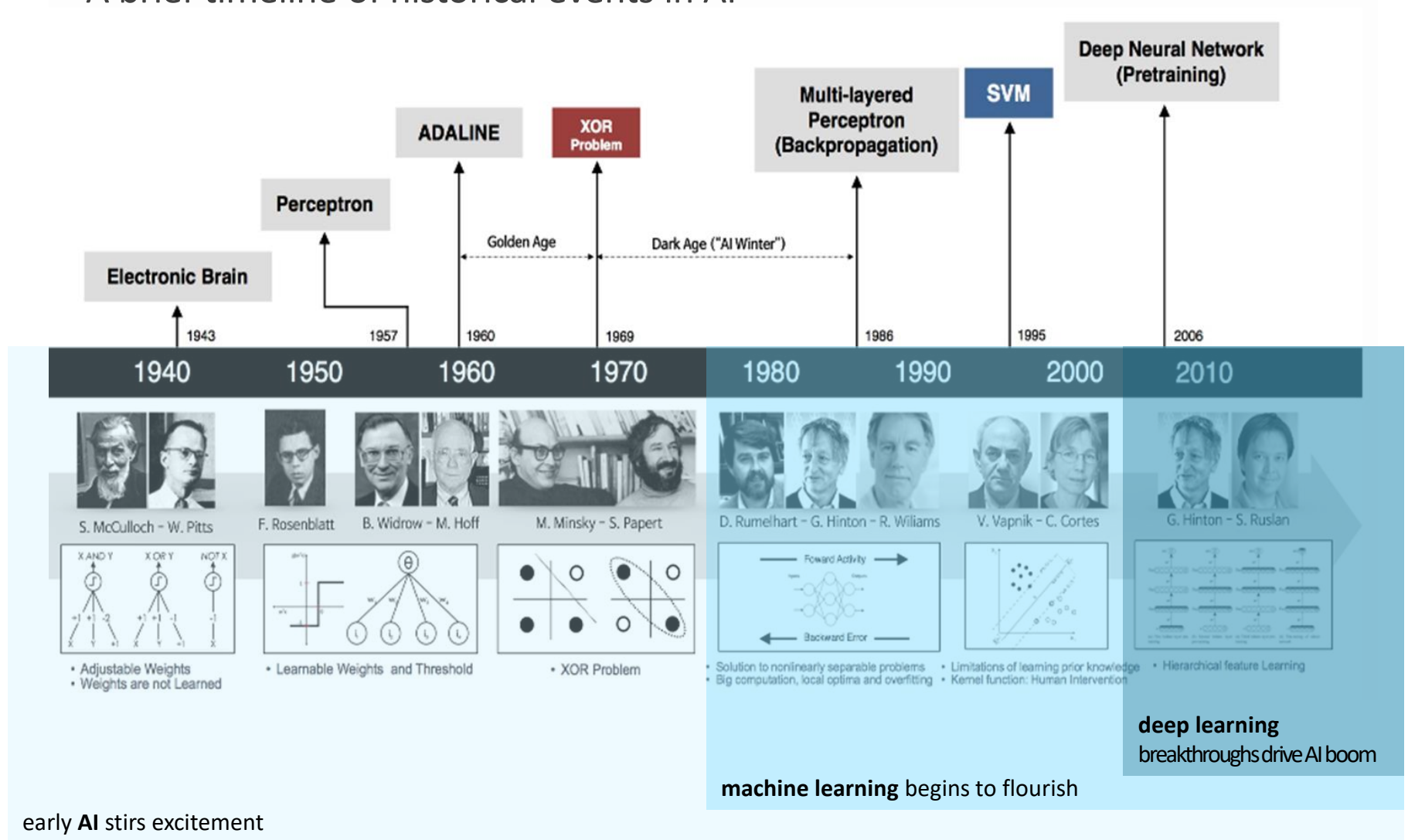
AI systems deployed to billions of users





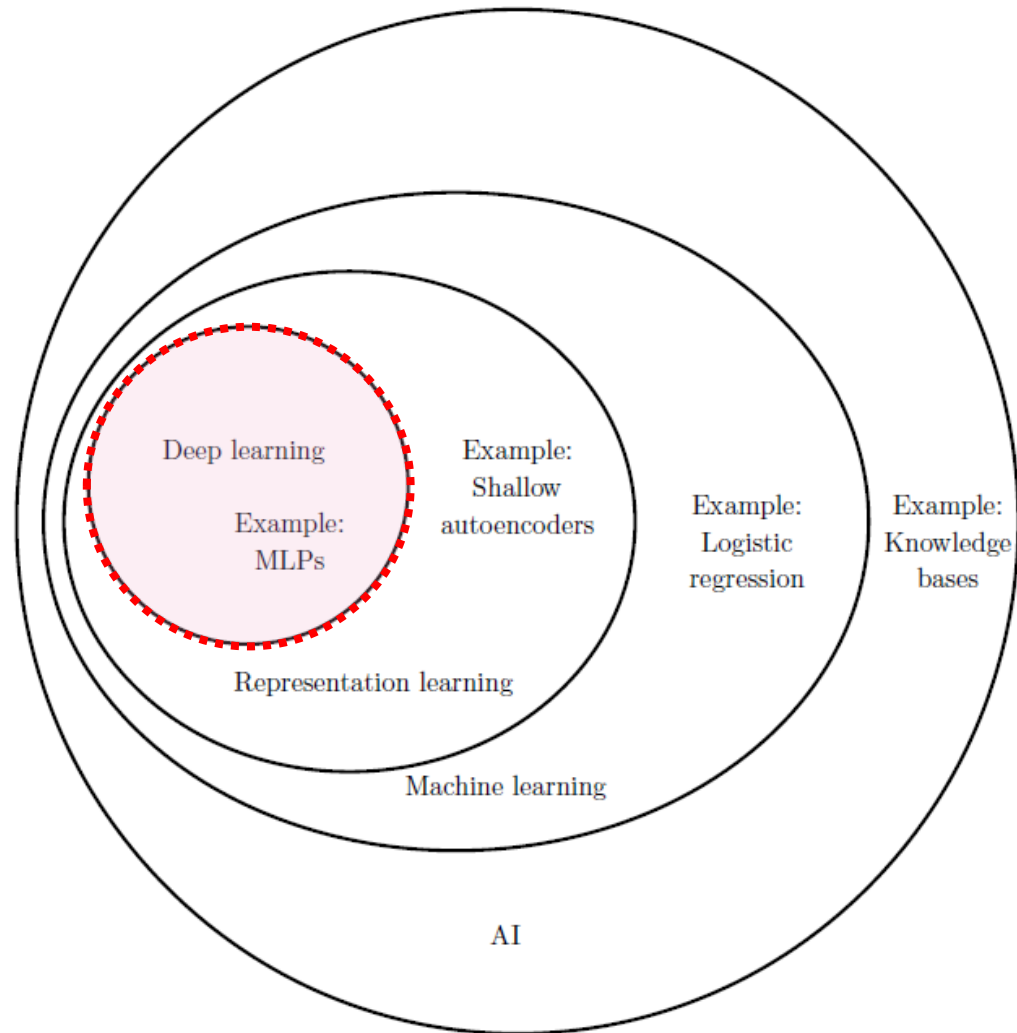
# Introduction

- A brief timeline of historical events in AI



# Background for deep learning

- Field of artificial intelligence

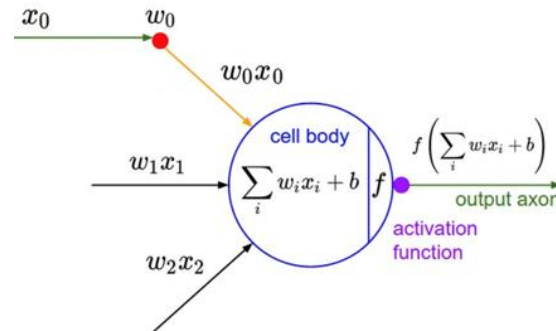


[from book: deep learning @MIT]

# Background for deep learning

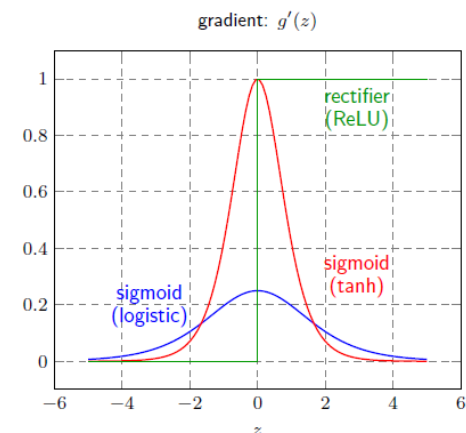
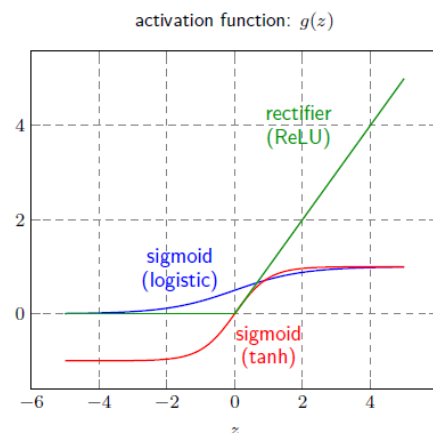
## Basic operation in a node of neural networks

- inner product == linear function



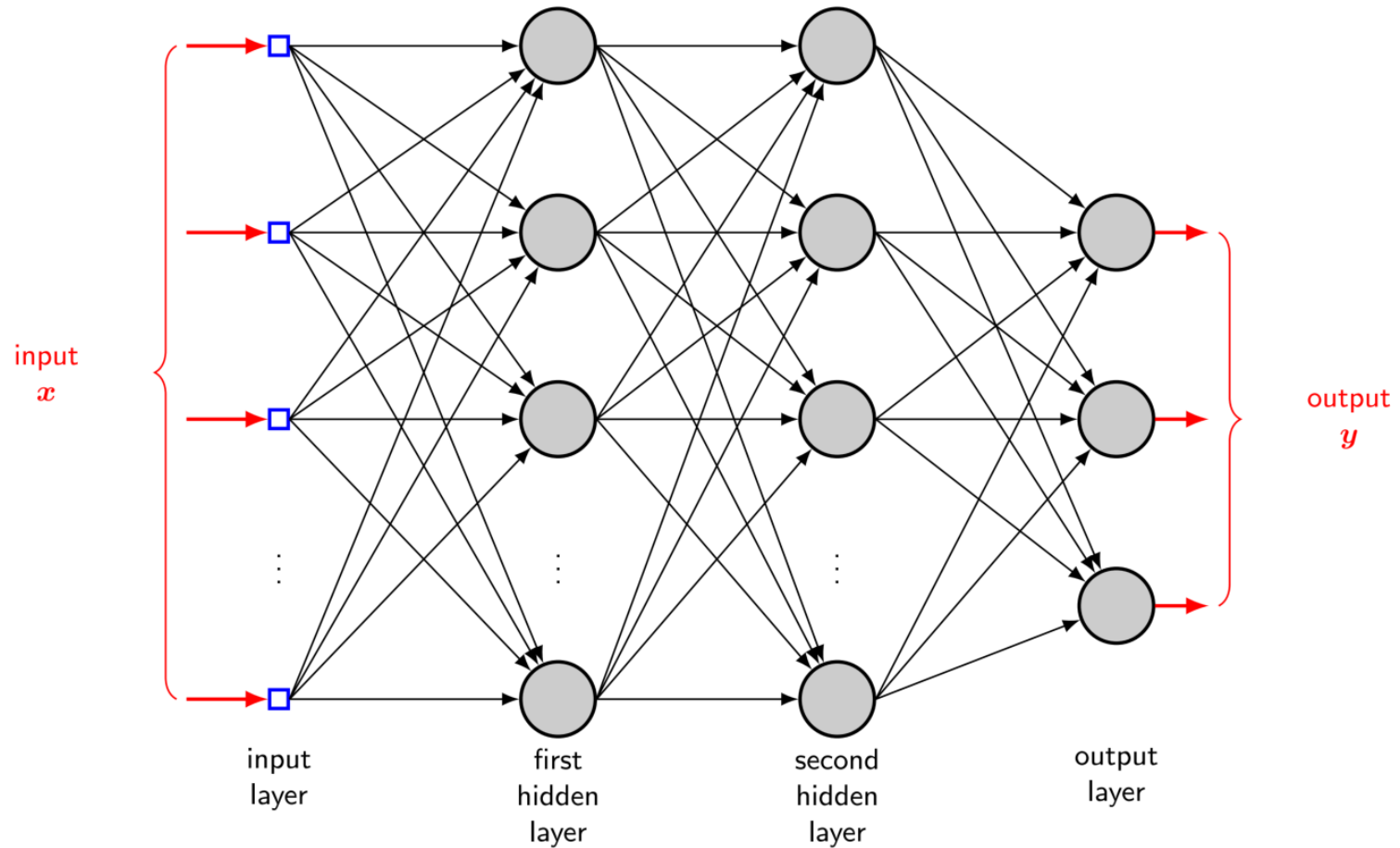
- activation function == non-linear function
  - various activation functions

Linear	$\phi(z) = z$	Adaline, linear regression	
Unit Step (Heaviside Function)	$\phi(z) = \begin{cases} 0 & z < 0 \\ 0.5 & z = 0 \\ 1 & z > 0 \end{cases}$	Perceptron variant	
Sign (signum)	$\phi(z) = \begin{cases} -1 & z < 0 \\ 0 & z = 0 \\ 1 & z > 0 \end{cases}$	Perceptron variant	
Piece-wise Linear	$\phi(z) = \begin{cases} 0 & z \leq -1/2 \\ z + 1/2 & -1/2 \leq z \leq 1/2 \\ 1 & z \geq 1/2 \end{cases}$	Support vector machine	
Logistic (sigmoid)	$\phi(z) = \frac{1}{1 + e^{-z}}$	Logistic regression, Multilayer NN	
Hyperbolic Tangent (tanh)	$\phi(z) = \frac{e^z - e^{-z}}{e^z + e^{-z}}$	Multilayer NN, RNNs	
ReLU	$\phi(z) = \begin{cases} 0 & z < 0 \\ z & z > 0 \end{cases}$	Multilayer NN, CNNs	



# Background for deep learning

- Structure of neural networks (by using connectionism)



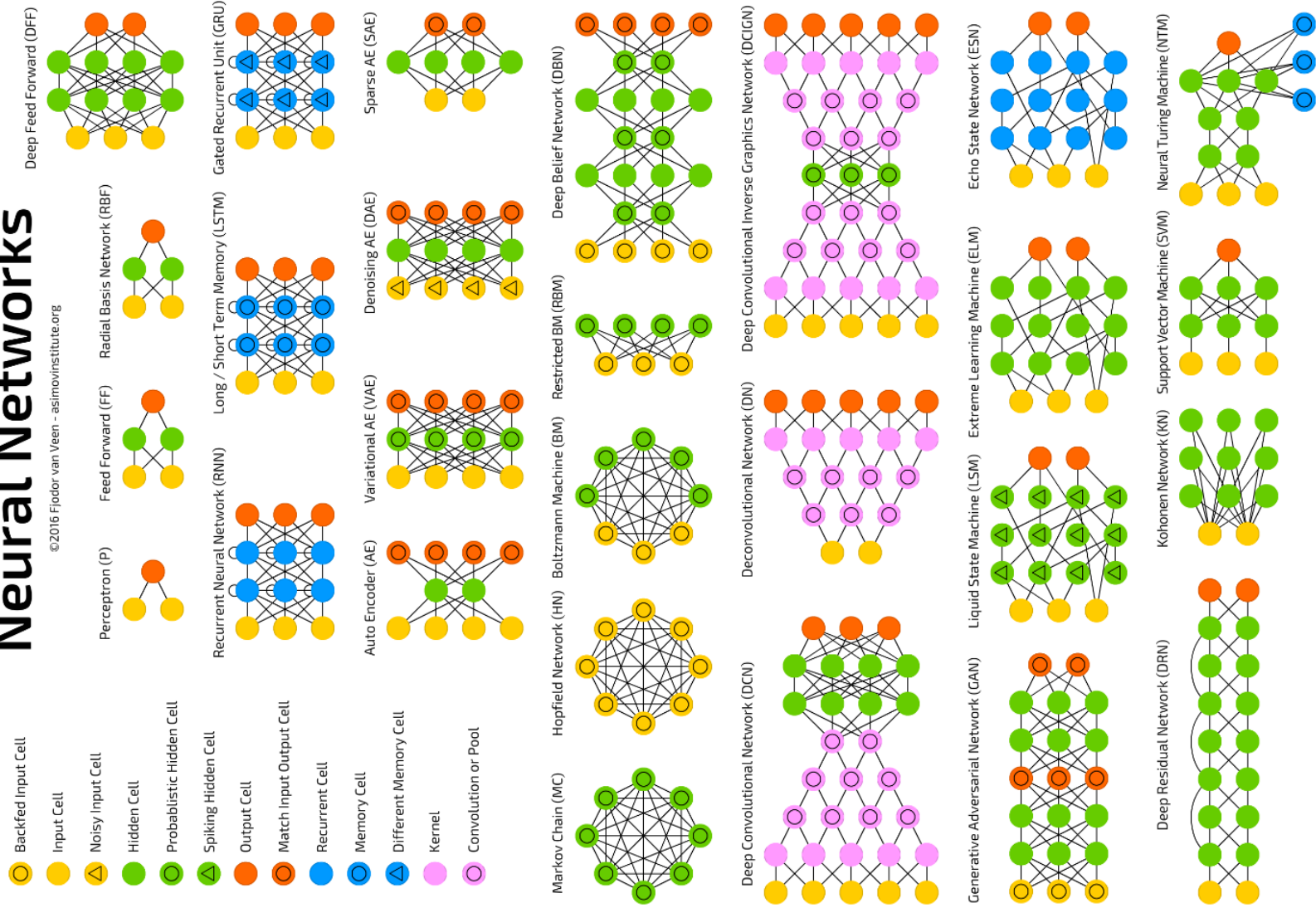
# Background for deep learning

## ● Zoo of neural networks

### Neural Networks

*A mostly complete chart of*

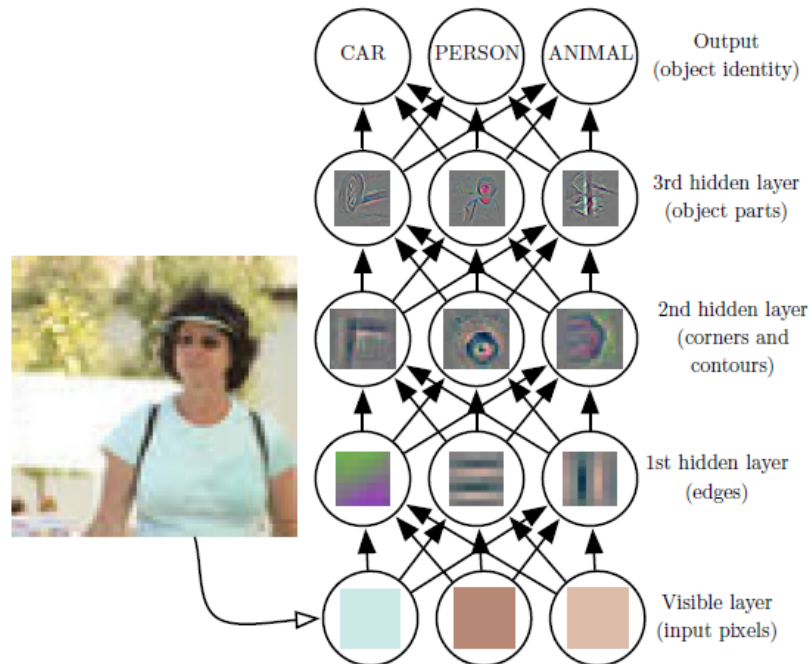
©2016 Fjodor van Veen - asimovinstitute.org



# Background for deep learning

## ● Deep learning

- ▶ deep neural network with multiple levels of linear / non-linear operations
  - introducing representation that are expressed in terms of other (simpler) representations
  - each stage: a kind of trainable feature transform
  - hierarchy of representations with increasing level of abstraction
- ▶ learning representation → data-driven features
- ▶ deep neural network == universal approximator



### Image

pixel → edge → textron → motif  
→ part → object

### Text

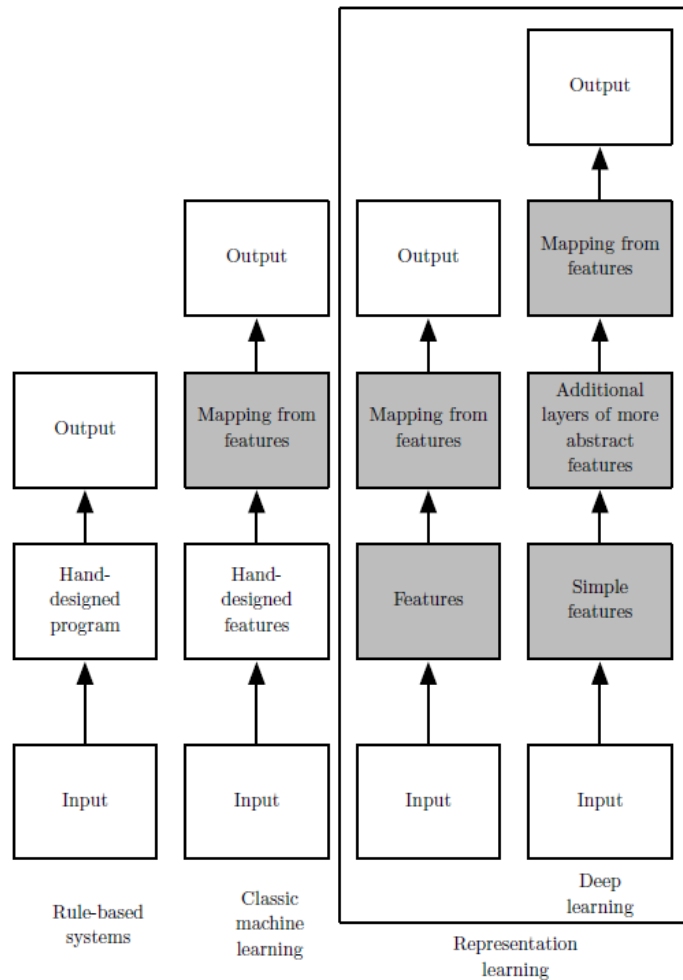
character → word → word group  
→ clause → sentence → story

### Speech

sample → spectral band →  
sound → ... → phone →  
phoneme → word →

# Background for deep learning

- Comparisons between traditional machine learning and deep learning



## Machine Learning



## Deep Learning

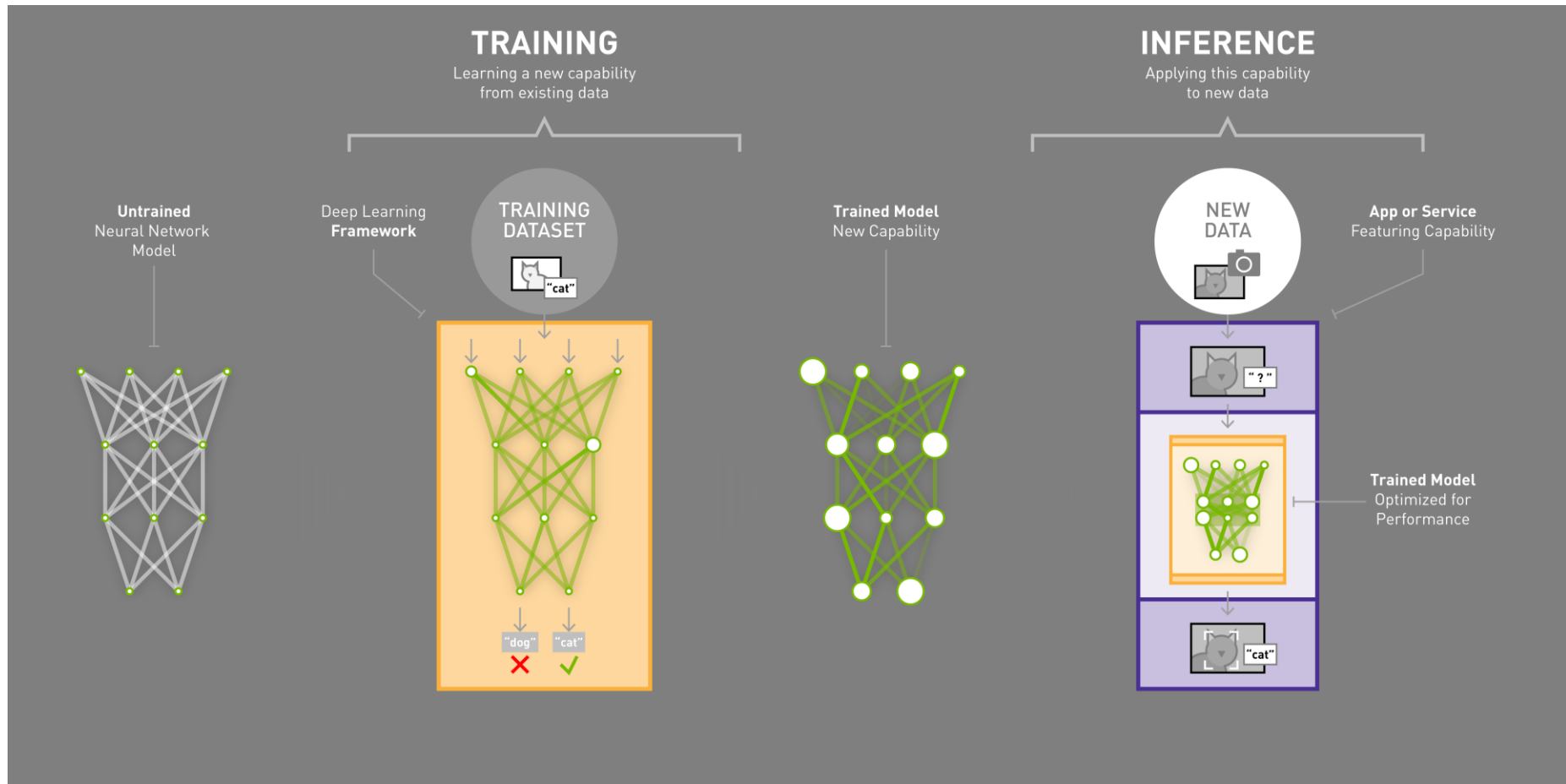


[from <https://verhaert.com>]



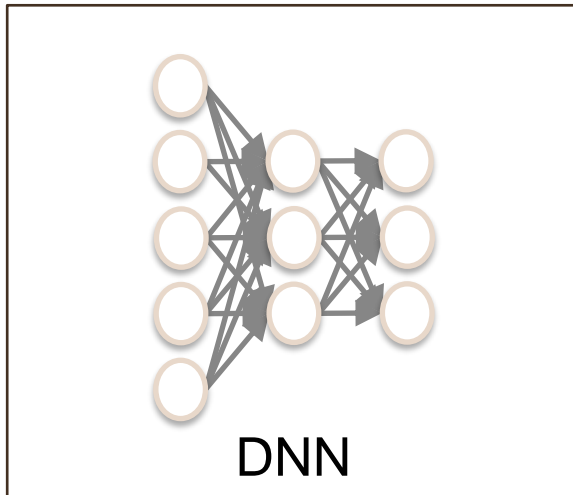
# Background for deep learning

- Training and inference



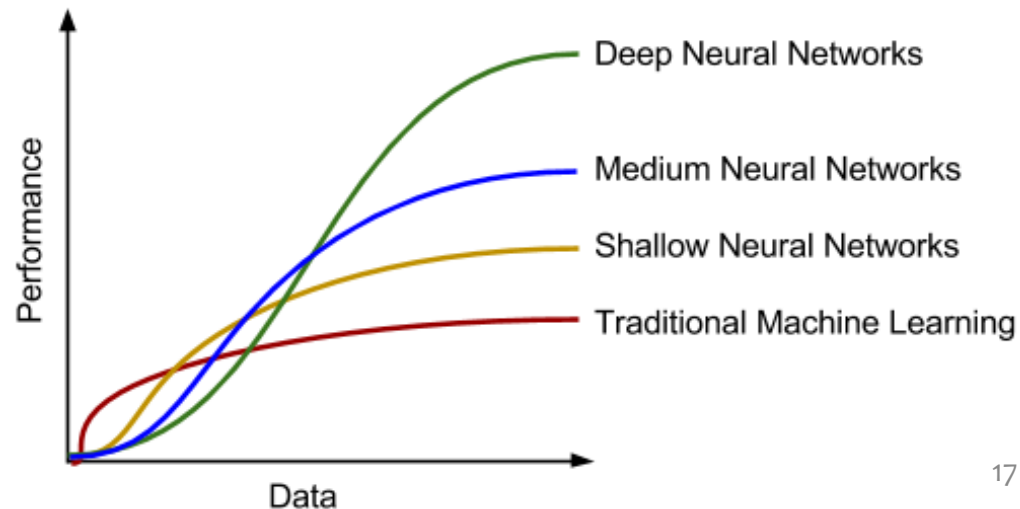
# Background for deep learning

- Reasons for deep learning's success



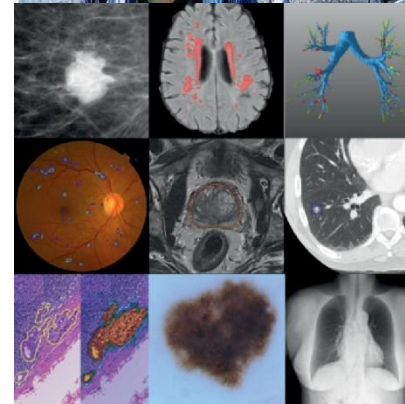
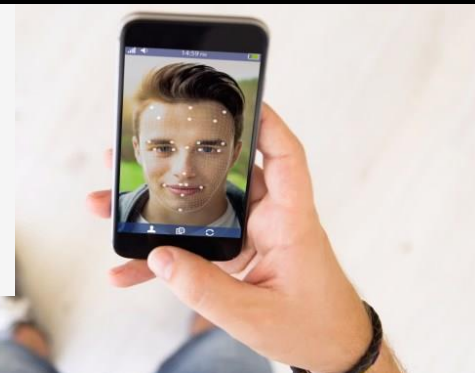
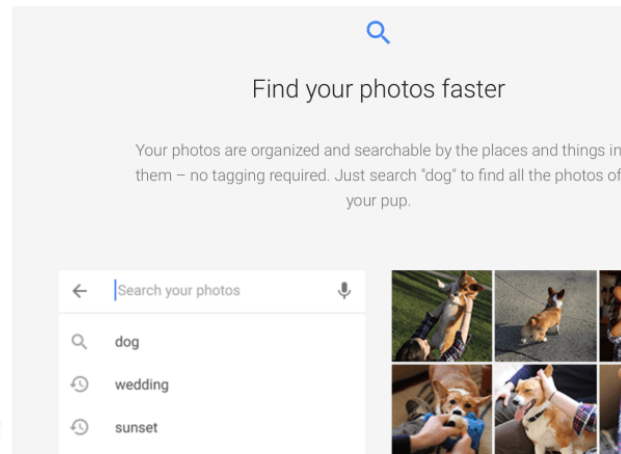
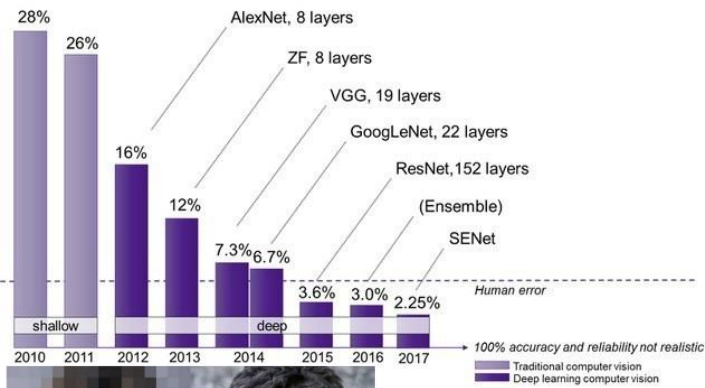
[from <https://www.nvidia.com>]

- Performance on |data|



# Research trends in deep learning

## ● The power of deep learning



Collage of some medical imaging applications in which deep learning has achieved state-of-the-art results.

From top-left to bottom-right:

1. mammographic mass classification
2. segmentation of lesions in the brain,
3. leak detection in airway tree segmentation,
4. diabetic retinopathy classification
5. prostate segmentation,
6. nodule classification,
7. breast cancer metastases detection,
8. skin lesion classification
9. bone suppression

### Leaderboard

SQuAD2.0 tests the ability of a system to not only answer reading comprehension questions, but also abstain when presented with a question that cannot be answered based on the provided paragraph.

Rank	Model	EM	F1
	Human Performance Stanford University (Rajpurkar & Ji et al. '18)	86.831	89.452
1	SA-Net on Albert (ensemble) QIANXIN	90.724	93.011
2	SA-Net-V2 (ensemble) QIANXIN	90.679	92.948
2	Retro-Reader (ensemble) Shanghai Jiao Tong University <a href="http://arxiv.org/abs/2001.09494v2">http://arxiv.org/abs/2001.09494v2</a>	90.578	92.978
3	ELECTRA+ALBERT+EntitySpanFocus (ensemble) SRCB_DMIL	90.442	92.839

### Leaderboard

KorQuAD 1.0의 Test set으로 평가한 Exact Match(EM) 및 F1 score입니다.

Rank	Reg. Date	Model	EM	F1
-	2018.10.17	Human Performance	80.17	91.20
1	2020.01.08	SkERT-Large (single model) Skelter Labs	87.66	95.15

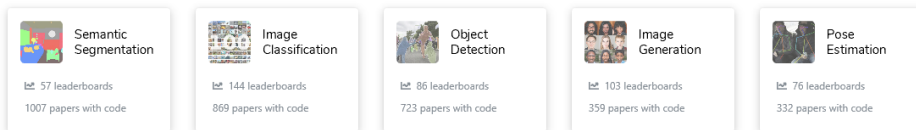


# Research trends in deep learning

- The power of deep learning (SOTA)

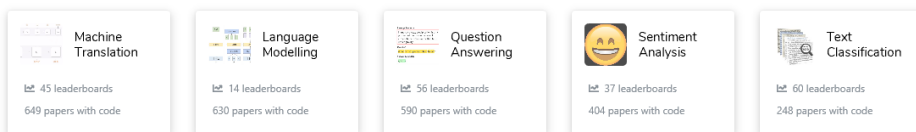
▶ reference from <https://paperswithcode.com/sota>

## Computer Vision



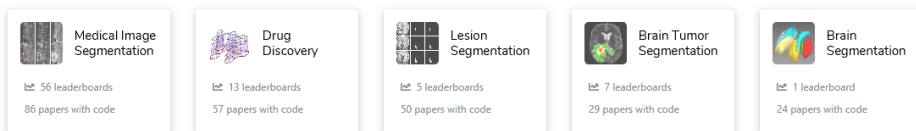
▶ See all 810 tasks

## Natural Language Processing



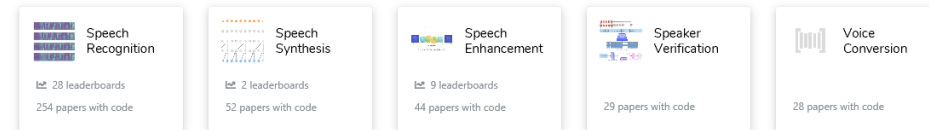
▶ See all 304 tasks

## Medical



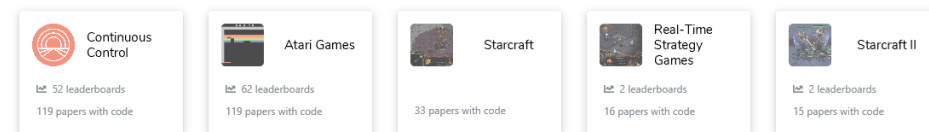
▶ See all 186 tasks

## Speech



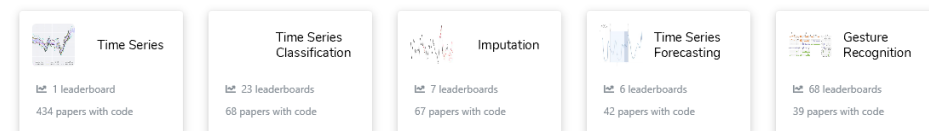
▶ See all 43 tasks

## Playing Games



▶ See all 42 tasks

## Time Series



▶ See all 34 tasks



# Research trends in deep learning

## ● The limits of deep learning

### A Sobering Message About the Future at AI's Biggest Party

Leaders in artificial intelligence warn that progress is slowing, big challenges remain, and simply throwing more computers at a problem isn't sustainable.



WILL KNIGHT BUSINESS 12.04.2019 07:00 AM

### Facebook's Head of AI Says the Field Will Soon 'Hit the Wall'

Jerome Pesenti is encouraged by progress in artificial intelligence, but sees the limits of the current approach to deep learning.



Forbes

Billionaires Innovation Leadership Money Business Small Business Lifestyle

30,436 views | Feb 9, 2020, 08:39pm EST

## Deep Learning Has Limits. But Its Commercial Impact Has Just Begun.



Rob Toews Contributor

AI

*I write about the big picture of artificial intelligence.*



The Economist

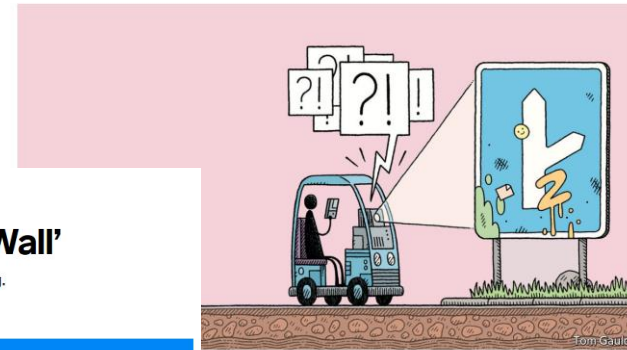
Today

Weekly edition

Menu

Subscribe

Search



Automobiles

Driverless cars show the limits of today's AI

MENU

nature

Subscribe

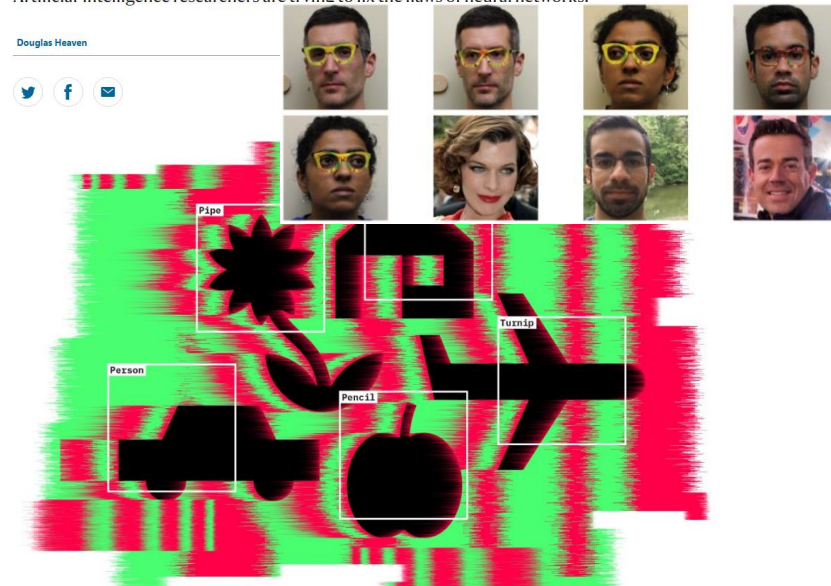


NEWS FEATURE • 09 OCTOBER 2019

## Why deep-learning AIs are so easy to fool

Artificial-intelligence researchers are trying to fix the flaws of neural networks.

Douglas Heaven



# Research trends in deep learning



# Research trends in deep learning

The  
Economist

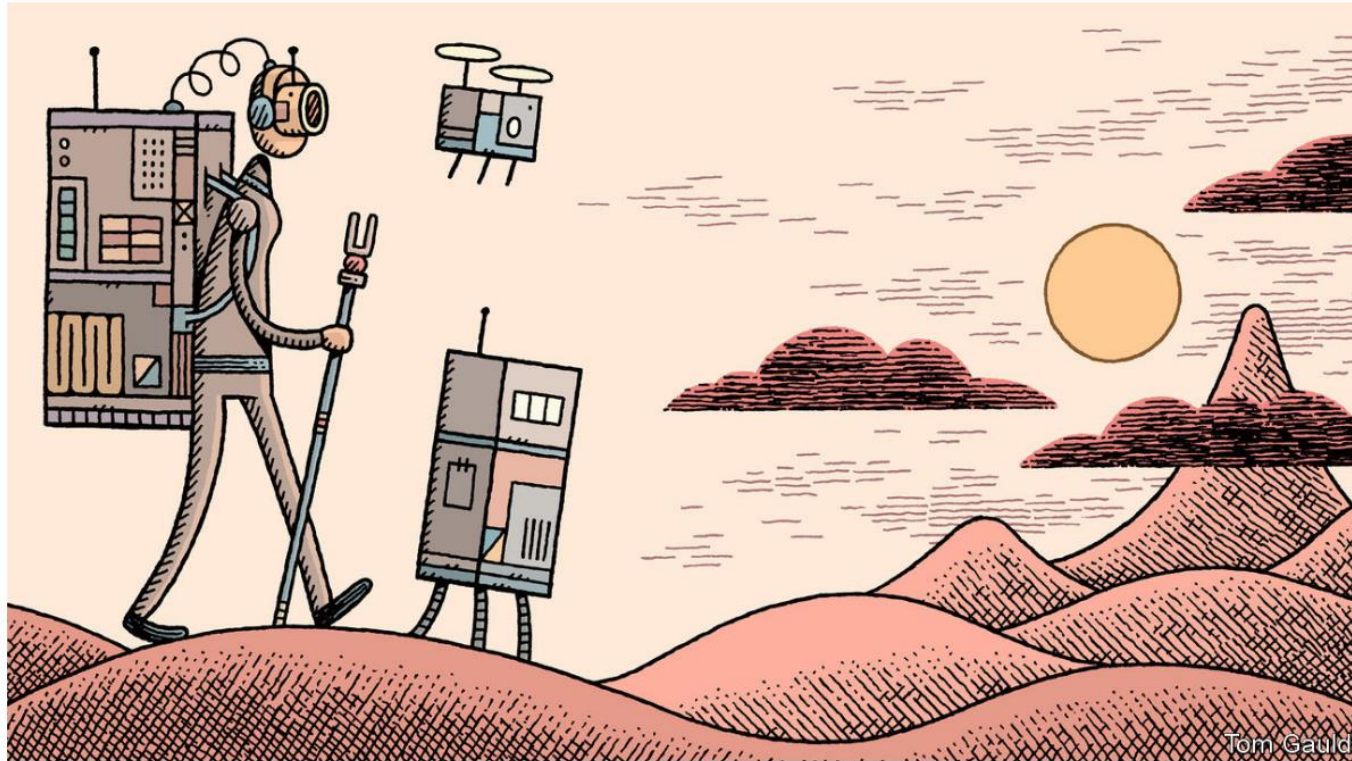
Today

Weekly edition

Menu

Subscribe

Search



Technology Quarterly

Jun 11th 2020 edition >

The future

## Humans will add to AI's limitations

It will slow progress even more, but another AI winter is unlikely



# Conclusion

- Deep (representation) learning have achieved remarkable improvement
  - ▶ e.g., image recognition, voice assistants, security
- Deep change is started by deep learning!
  - ▶ deep neural network == (linear + nonlinear)\*M == universal approximator
  - ▶ change of paradigm → the deep learning revolution
- Deep learning has power and limits
  - ▶ rapidly changing, must stay in tune!!
- AI <sup>enabler</sup> ↔ Security

# Question and Answer

- If you have any comments,  
suggestions or questions then please do let me know!
- For more information, contact me  
*jaekoo@kookmin.ac.kr*



Thank you 😊