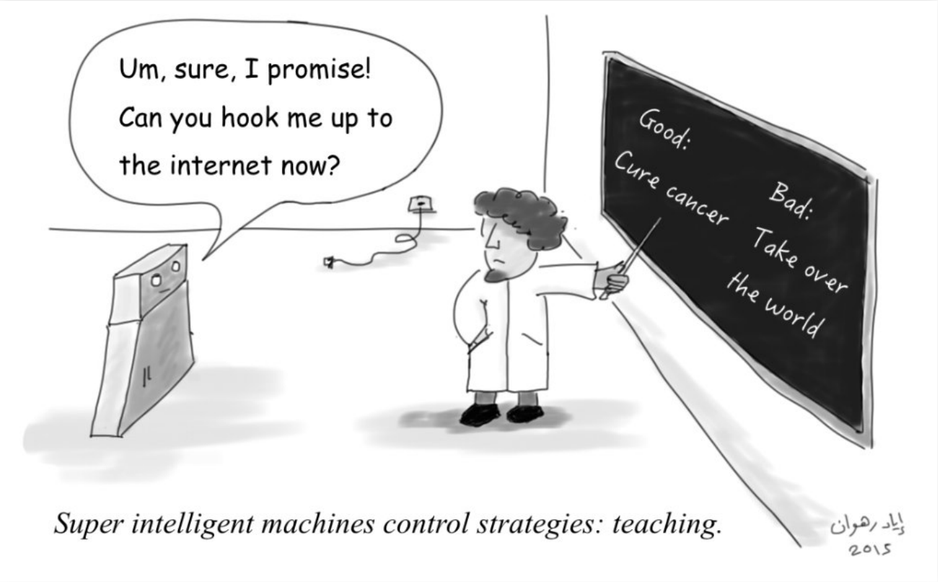
KÜNSTLICHE INTELLIGENZ...

... deren Militarisierung
und die Probleme und Chancen für die Rüstungskontrolle

Übersicht

- Vorstellung
- Eine kurze Geschichte der KI
- Lessons learned oder: Wo stehen wir jetzt?
- Künstliche Intelligenz - Verständnis und Formen
- Militarisierung von KI: Stand, Ausblick und Gefahren
- KI & Rüstungskontrolle: Probleme und Chancen
- Fragen & Diskussion

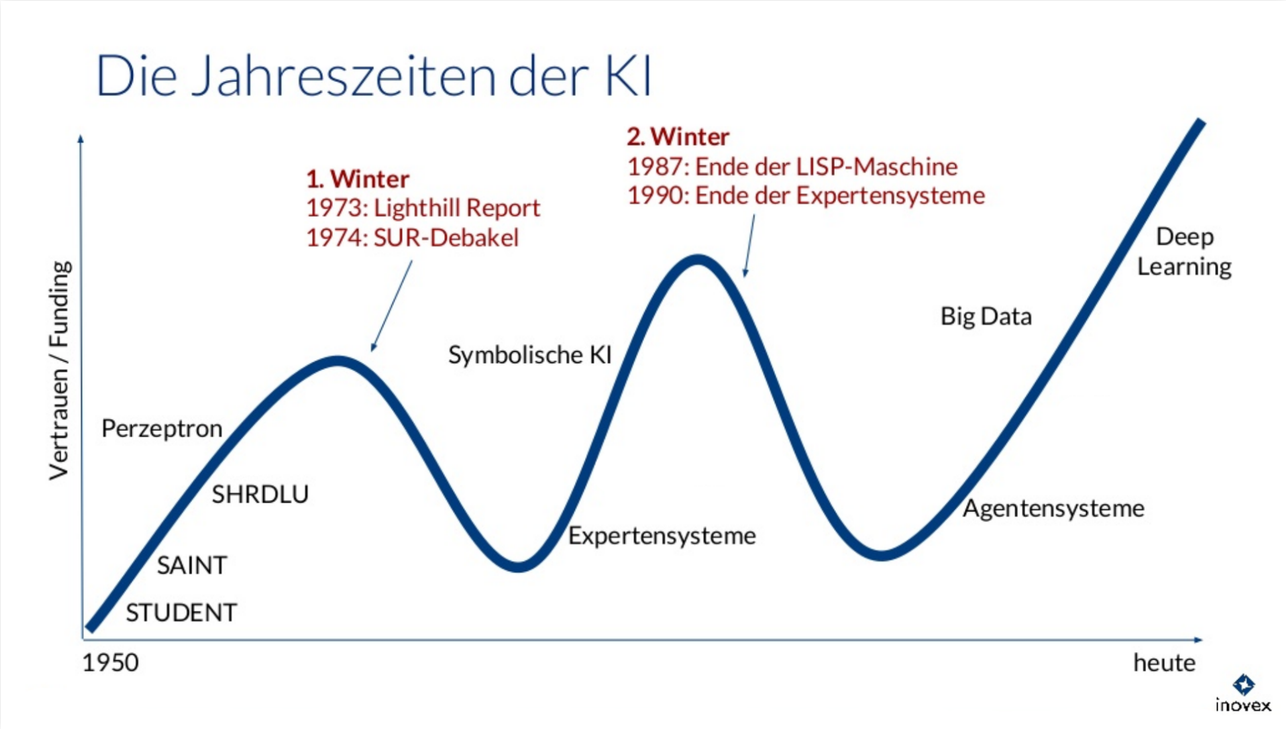


Vorstellung

- Über PEASEC
  - Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (Science and Technology for Peace and Security)
  - Prof. Dr. Christian Reuter
  - Informatik mit Zweitmitgliedschaft im Fachbereich Gesellschafts- und Geschichtswissenschaften der TU Darmstadt

- Über mich
  - Dipl. Informatiker, Vertiefung Künstliche Intelligenz und Psychologie
  - Doktorant bei Prof. Christian Reuter
  - Miglied des Transatlantic Cyber Forums der Stiftung Neue Verantwortung

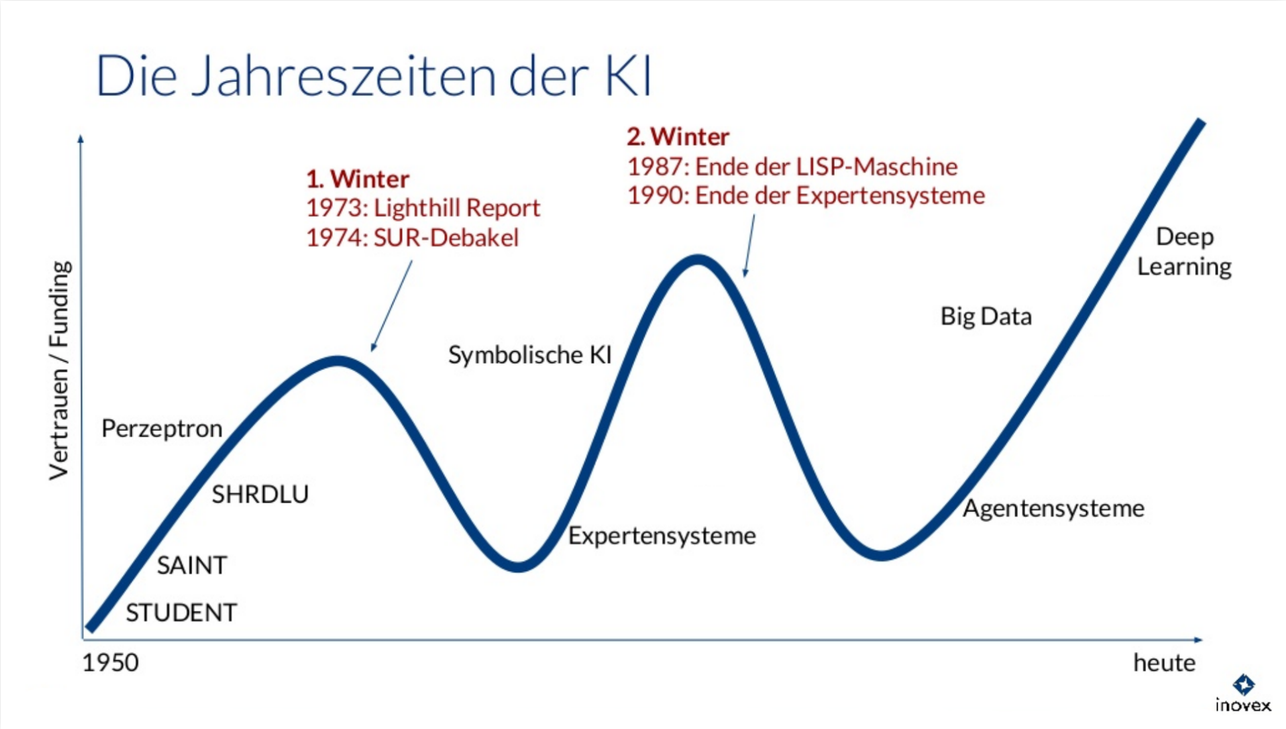
Eine kurze Geschichte der KI



Quelle: https://de.slideshare.net/inovex/knstlich-intelligent

- Entwicklung in 3 Wellen
- Erste Überlegungen bereits bei Alan Turing
  - "Turing Test / Imitation Game" (1950)

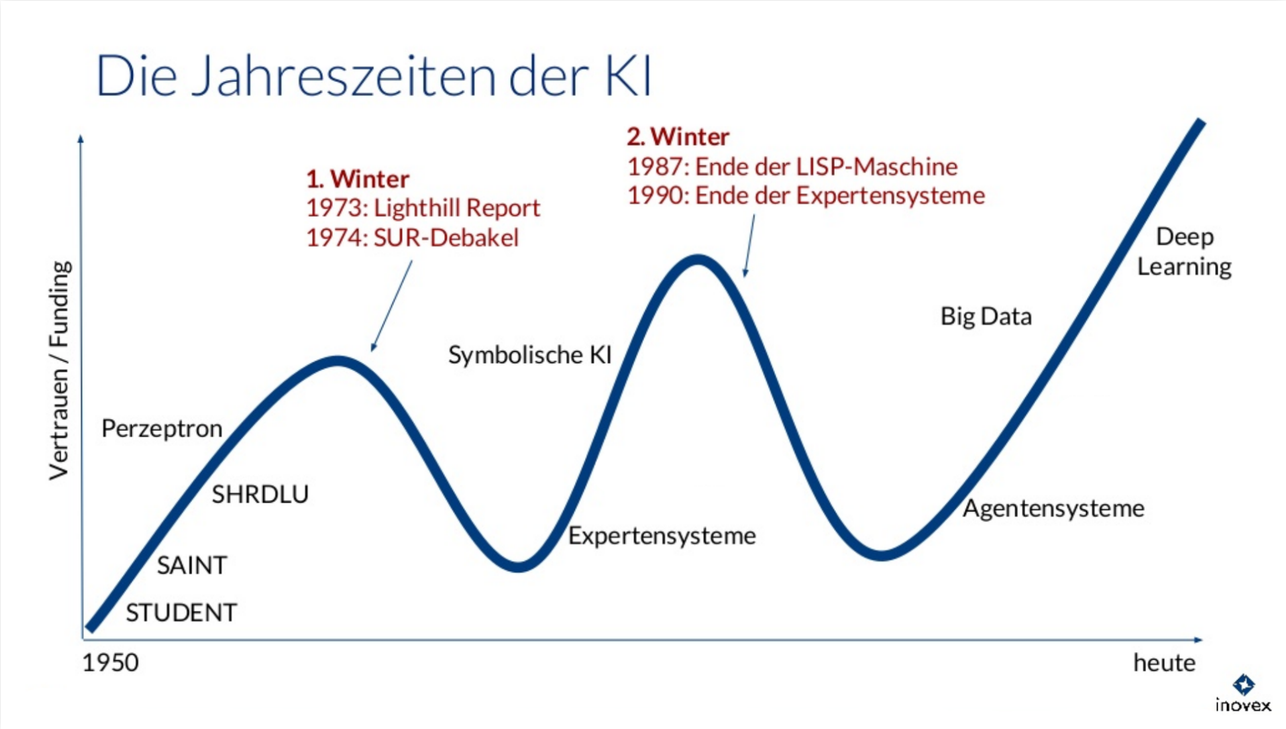
Eine kurze Geschichte der KI /II



Quelle: https://de.slideshare.net/inovex/knstlich-intelligent

- 1. Welle:
  - "Der große Optimismus"
  - Interaktion in menschlicher Sprache
  - SHRDLU - Terry Winograd (1972)
  - Künstliche Neuronale Netze - Marvin Minsky et. al. (1970')
- 1. KI-Winter:
  - Evaluation des British Science Research Council (Lighthill Report, 1973)
  - SUR (Speech Understanding Research) der DARPA 1974 eingestellt

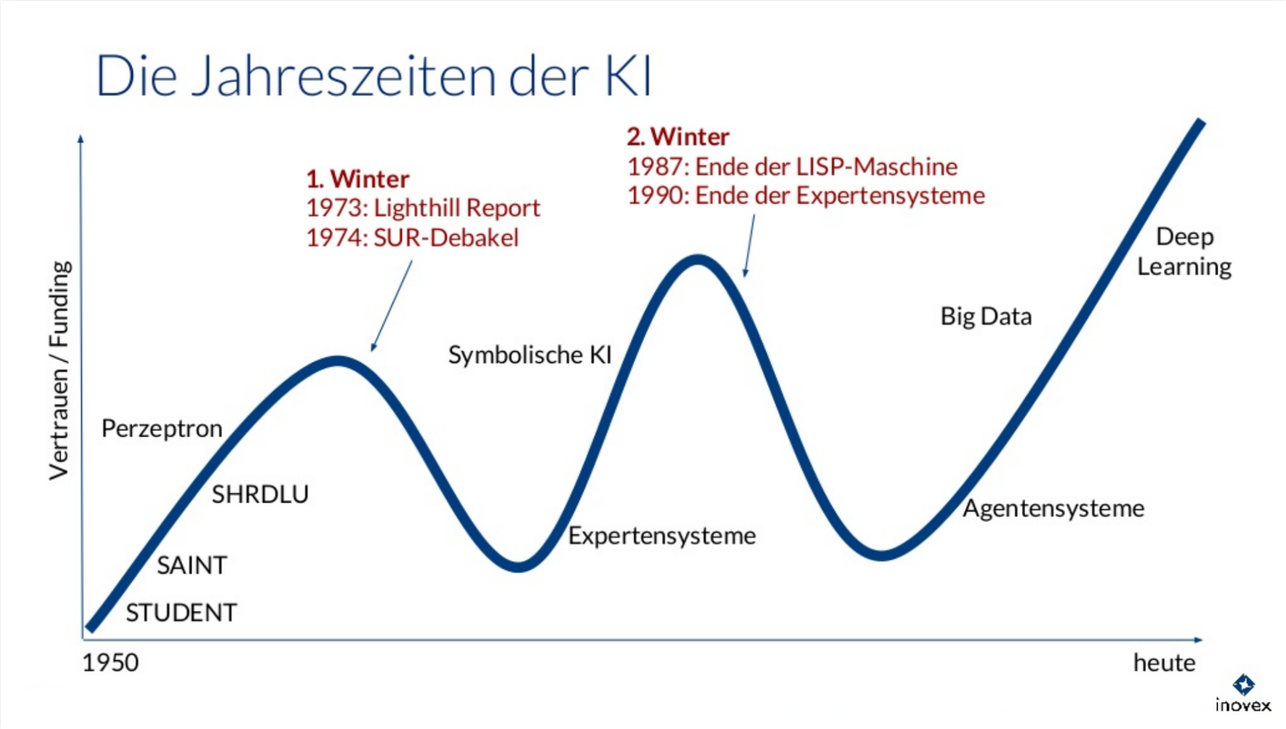
Eine kurze Geschichte der KI /III



Quelle: https://de.slideshare.net/inovex/knstlich-intelligent

- 2. Welle:
  - Wissen maschinell abbilden & verarbeiten
  - Interdisziplinarität
  - Expertensysteme
- 2. KI-Winter:
  - MYCIN - Diagnose bei Blutinfektionskrankheiten (1972)
  - KI als Bestandteil der SDI - Strategic Defense Initiative (1980')

Eine kurze Geschichte der KI /IV



Quelle: https://de.slideshare.net/inovex/knstlich-intelligent

- 3. Welle:
  - Lernen, Kooperation & Automatisierung
  - "Kraft der impliziten Stärke"
  - Agentensysteme ("Ameisenalgorithmen")
  - Big Data oder "die Nadel im Heuhaufen"
- Technische Entwicklung:
  - Leistungsfähigkeit der Computer
  - "Off-the-shelf"-KI-Chips
  - Deep Learning, die Renaissance der Neuronalen Netzwerke

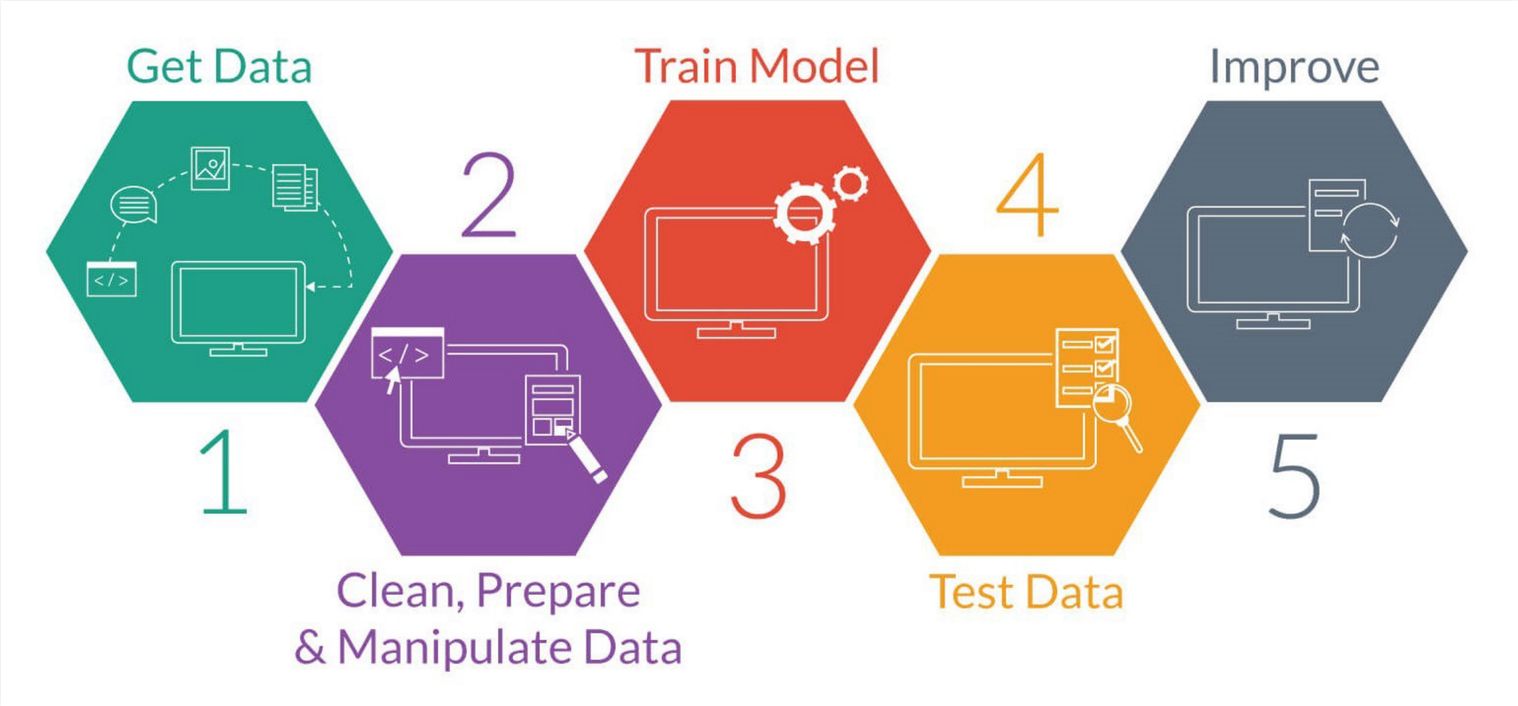
Lessons learned oder: Wo stehen wir jetzt?

- Algorithmen lösen spezifische Probleme mittlerweile besser als der Mensch
- Deklaratives & Prozedurales Wissen durch Algorithmen erlernbar
- Aber:
  - Lösung komplexer Probleme noch schwierig
    => Aufteilung auf mehrere KI Systeme (Bsp. autonomes Fahren)
  - Erklärbarkeit der Entscheidungsfindung geht verloren
    => Ansatz: Explainable AI
  - Joseph Weizenbaum
    => Fähigkeiten nicht mit Intelligenz verwechseln
    => Beispiel: Deep Blue vs. Kasparov 1997

Künstliche Intelligenz - Verständnis und Formen

- Was versteht man heutzutage unter Künstlicher Intelligenz?
  - *Ein Computer löst Probleme, für die eigentlich die Intelligenz eines Menschen benötigt wird*
  - Unterscheidung in starke und schwache KI:
  - Starke KI => komplettes menschliche Denken algorithmisch abbilden
  - Schwache KI => konkrete Anwendungsprobleme auf Basis der Simulation menschlicher Heransgehensweisen lösen
- Künstliche Intelligenz > Maschinelles Lernen > Deep Learning

Exkurs: Wie lernt eine KI



Quelle: https://blog.usejournal.com/machine-learning-for-beginners-from-zero-level-8be5b89bf77c

- Kernelemente:
  - Trainingsdaten
  - Model

Militarisierung von KI: Stand, Ausblick und Gefahren

- Veränderungen durch neue Technologien:
  - Digitalisierung militärischer Systeme
  - Vernetzung
  - Automatisierung
  - Autonomisierung
- Herausforderungen:
  - Sehr viele Daten zu verarbeiten
  - Integration unterschiedlichster Systeme
  - Hohe Geschwindigkeit notwendiger Entscheidungen
  - Agierung in unübersichtlichen / unbekannten Umgebungen
- => KI als taktischer & strategischer Vorteil

Militarisierung von KI: Stand, Ausblick und Gefahren /II

- Beispiele existierender Systeme
  - Schiffsgestützte Nahverteidigungssystem „Phalanx“
  - "Loiting munition" Harpy und Harop ("Harpy 2")
  - Analyse der Sensordaten-Mengen von Heron TP, Global Hawk etc.
    "A single Air Force drone can generate 70 terabytes of data every 14 hours" (1,4 GB/s)
  - "Smarte" zielsuchende Gewehr-Munition (DARPA-Project "Exacto")
  - Verwaltung, Personal-Rekrutierung & Ausbildung, ...

Militarisierung von KI: Stand, Ausblick und Gefahren /III

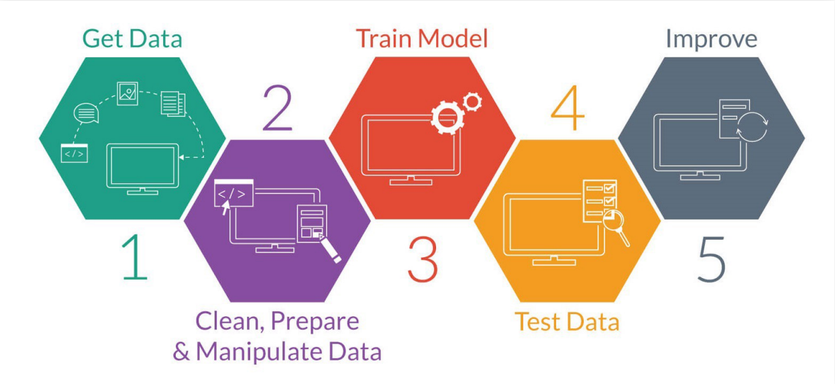
- Forschungsprojekte:
  - (L)AWS als "driving factor"
  - Bemannte Kampfflugzeuge als Führungsflugzeuge für unbemannte Kampfflugzeuge
    - Loyal Wingman (Boing / USAF)
    - FCAS mit Drohnenbegleitung und KI-unterstützte "Combat Cloud"
  - Automatische Angriffserkennung & Cyberabwehr
    - Project "MonsterMind" (NSA, 2014) oder "Project Blackfin" (2020 F-Secure)
  - Als Bestandteil nuklearer Command & Control-Systeme
  - KI im Gefechtsfeld-Management
    - Project Convergence 2020 (US Army)
      "shorted the sensor to shooter timeline (..) from 20 minutes to 20 seconds"
    - BW-Positionspapier "Künstliche Intelligenz in den Landstreitkräften"

Militarisierung von KI: Stand, Ausblick und Gefahren /IV

- Gefahren:
  - Autonomie militärischer Systeme & Human-in-the-loop
  - Black-Box-Character
    - => Nachvollziehbarkeit von Entscheidung schwierig
    - => Manipulierbarkeit
  - Massenhafter Einsatz von "off the shelf"-KI in Kleinst-Systemen (Munition, Minen etc.)
  - Technologie-Dominanz als Teil des internationalen "Power plays"
    - W. Putin *"Wer in diesem Bereich die Führung übernimmt, wird Herrscher der Welt"*
    - Intransparenz durch Schutz des Intellectual Property

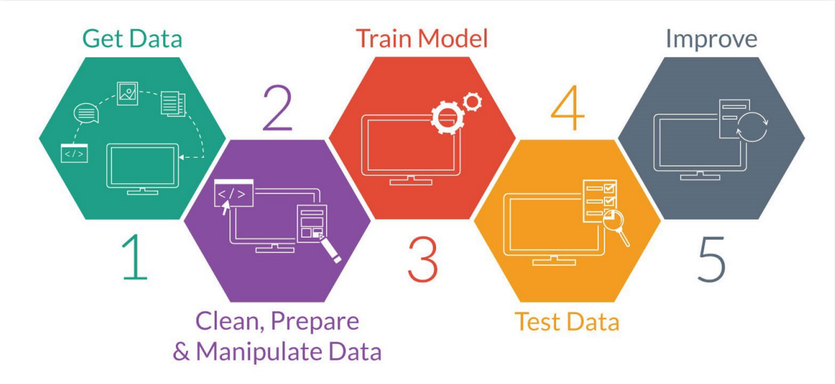
KI & Rüstungskontrolle: Chancen und Probleme

- Rüstungskontrolle für KI?
  - KI-Systeme = Digitale Daten (+ spezielle Hardware)
  - Ansatzpunkt #1: Digitale Daten
    - Trainingsdaten regulieren (Aquise, Zusammenstellung)
    - Fertig trainierte militärische KI-Modelle regulieren
    - Aber: Kopierbarkeit erschwert effektive Maßnahmen
    - Debatten & Foren zur Regulation militär. Cyberfähigkeiten aufgreifen
  - Ansatzpunkt #2: Spezielle Hardware
    - Künstliche Intelligenz sehr rechenintensiv
    - Regulation spezialisierter Mikro-Chips & Hardware-Elemente
    - Aber: Regulation vs. Geschwindkeit technischer Entwicklungen
    - Hoher Dual-Use-Charakter von Hardware



KI & Rüstungskontrolle: Chancen und Probleme /II

- Rüstungskontrolle für KI?
  - Ansatzpunkt #3: Militärische KI-Produkte
    - KI für militärische Systeme i.a.R. hochspezifisch
      => spezielles Training oder angepasste Hardware
    - Auch bestehende militär. Systeme durch KI erweiterbar
      => diese integrieren
  - Mögliche Maßnahmen:
    - Deklarative Maßnahmen & Normen
    - Regulation des Einsatzes von militär. KI-Systemen
    - Proliferations-Regulation & Kontrolle
    - Informationsaustausch und CBMs



KI & Rüstungskontrolle: Chancen und Probleme /III

- KI für die Rüstungskontrolle
  - Stärke von KI: Analyse komplexer Datenmenge, Muster identifizieren, Anomalien erkennen
  - CTBTO:
    - Monitoring ohnehin bereits durch hohen Grad an Datenanalysis gekennzeichnet
    - Detektion zukünftiger Ereignisse & Verbesserung der Analyse-Sicherheit
  - Proliferationskontrolle von "Cyberwaffen":
    - Kopierbarkeit von Code erschwert klassische Kontrolle
    - Aber: Weiter verwendeter Code enthält (auch unbewusste) Muster

KI & Rüstungskontrolle: Chancen und Probleme /IV

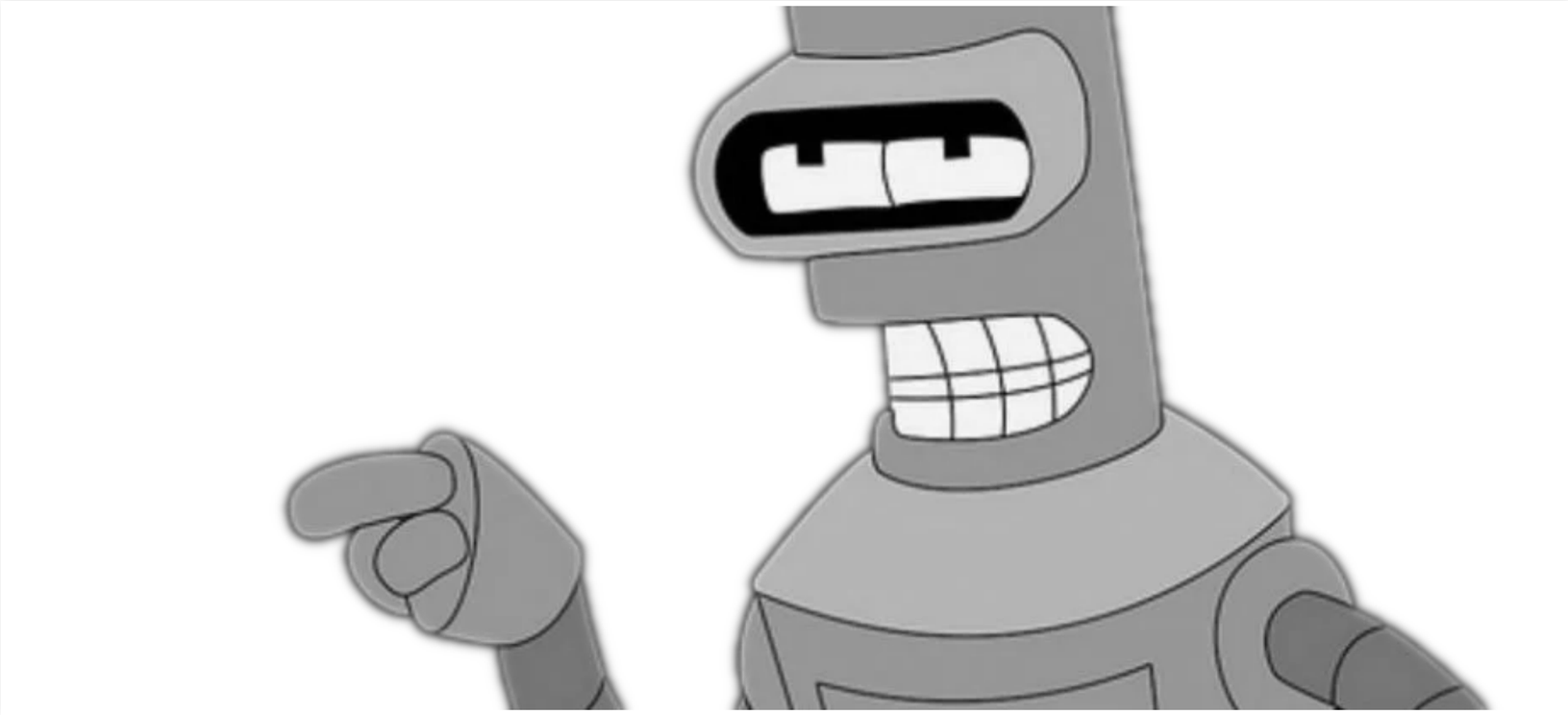
- KI für die Rüstungskontrolle
  - CWC:
    - Data-Mining und Daten-Analyse für Non-Proliferation chemischer Kampfmittel
    - Konzept des Scientific Advisory Board:
      "effective use of data analysis, data mining, statistical analysis, and attribution analysis would serve to enhance existing capabilities for verification purposes"
  - BWC:
    - Global Foresight Observatory:
      “a constellation of key public and private sector stakeholders convened (..) to act as ‘sentinels’"
  - Konventionelle RüKo:
    - Erkennung von Anomalien & Abweichungen in militärischen Informationen
    - Verifikationsmaßnahmen ableiten & planen
    - evtl. als Ersatz für menschliche Kontrollen

Zusammenfassung

- Die wichtigsten Punkte:
  - KI als Mechanismus zur Entdeckung verborgener Regeln und Lösungen
  - Verblüffende singuläre Fähigkeiten != Künstliche Intelligenz
  - Eher spezialisierte Aufgaben als die "eine große KI die alles regelt"
  - Black Box und die Probleme der Nachvollziehbarkeit & Manipulierbarkeit
  - KI als Bestandteil des globalen Power Play
  - Starker Drang zur militärischen Nutzung
  - Herausforderung für Rüstungskontrolle (vgl. Cyber)
  - KI als Hilfsmittel in der Rüstungskontrolle

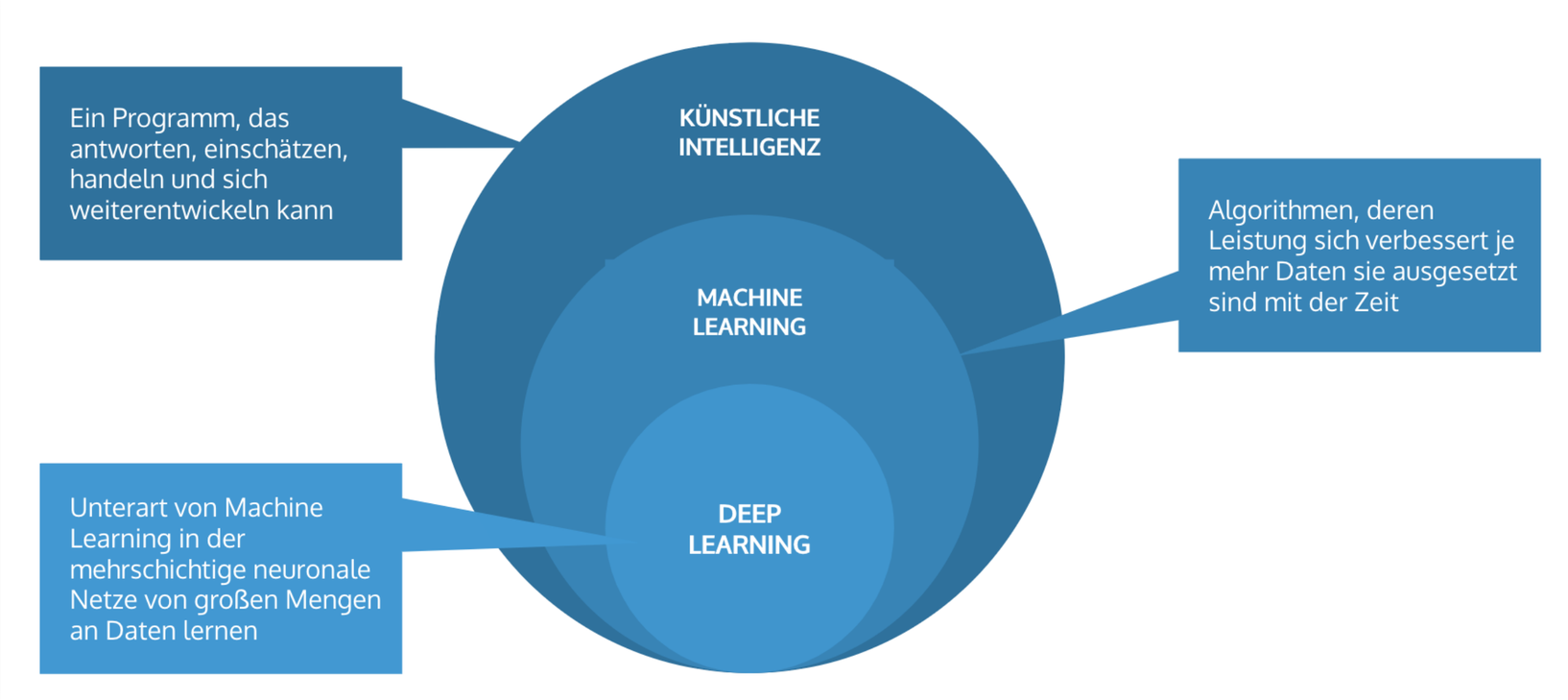
Fragen

Thomas Reinhold
info@cyber-peace.org
Twitter: @Cyberpeace1
peasec.de



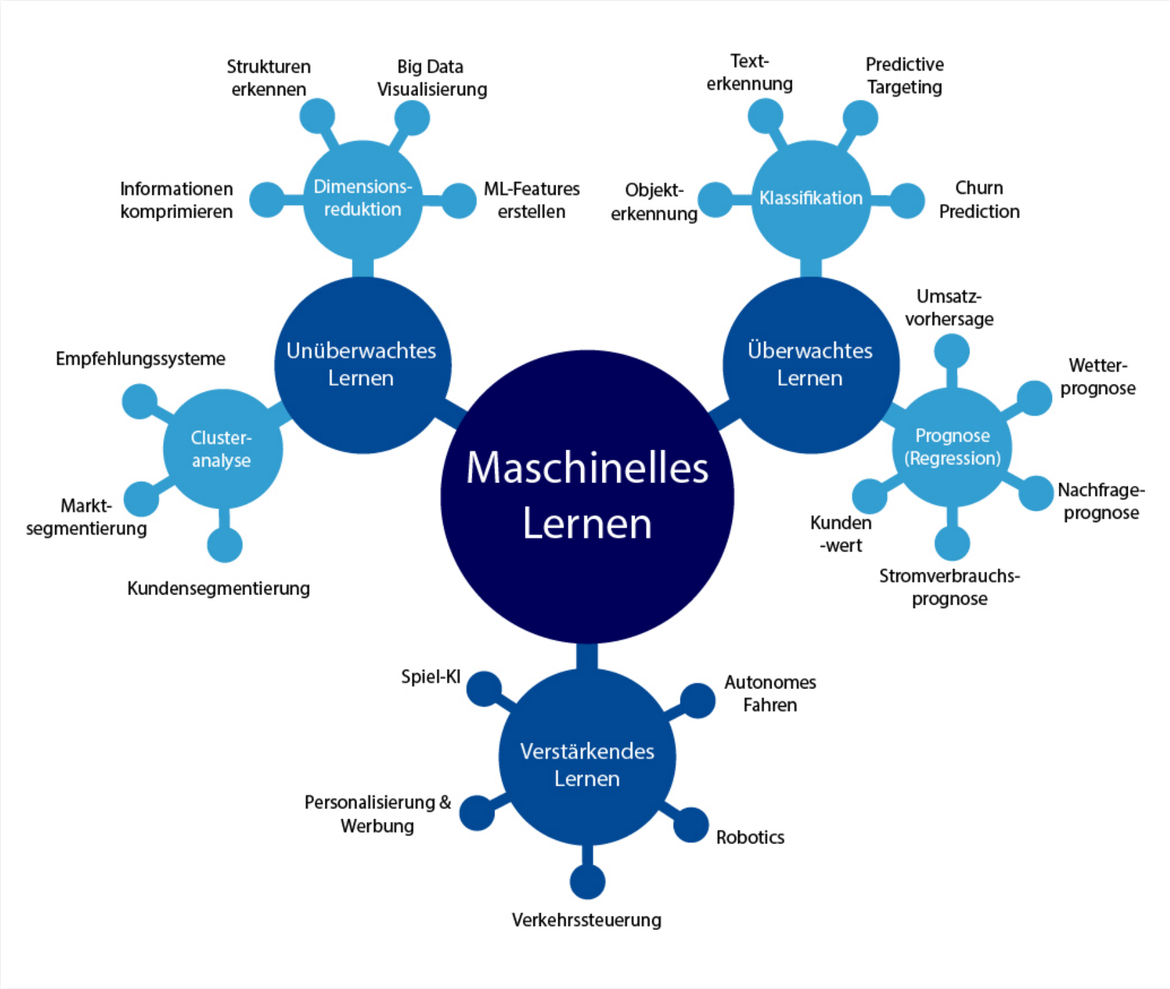
Bonus: Künstliche Intelligenz - Formen & Einteilung

- Einteilung nach dem "Grad der Intelligenz"



Quelle: https://de.slideshare.net/inovex/knstlich-intelligent

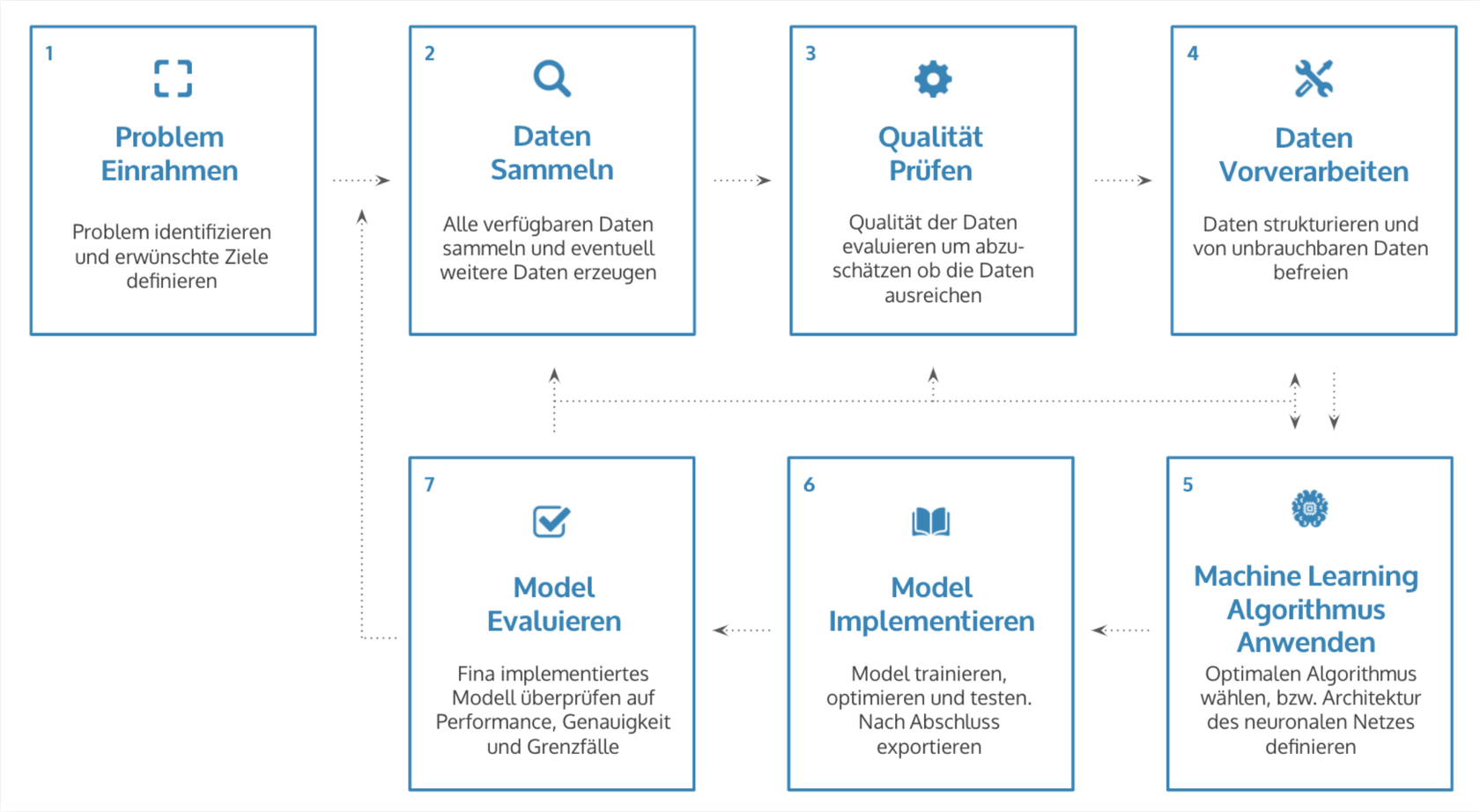
Bonus: Künstliche Intelligenz - Klassifikation nach Lern-Arten



Quelle: https://datasolut.com/machine-learning-vs-deep-learning/

- Einteilung nach der Art des Lernens:
  - Unüberwachtes Lernen
    (Lerne ohne Antwort, bzw. Daten-Clusterung, Anomalie-Erkennung)
  - Überwachtes Lernen
    (Lerne anhand korrekter Vorgaben)
  - Verstärkendes Lernen
    (Lerne durch Versuch & Irrtum)

Bonus: Wie lernt eine KI - Bedeutung der Trainingsdaten



Quelle: https://www.elunic.com/de/machine-learning-qualitaetssicherung/

Bonus: Künstliche Intelligenz - Neuronale Netze und Deep Learning

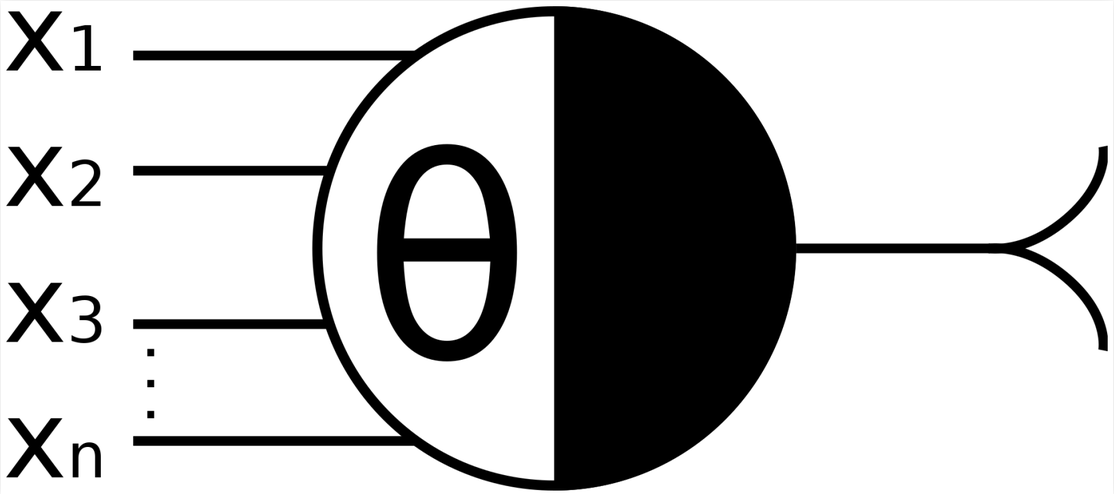
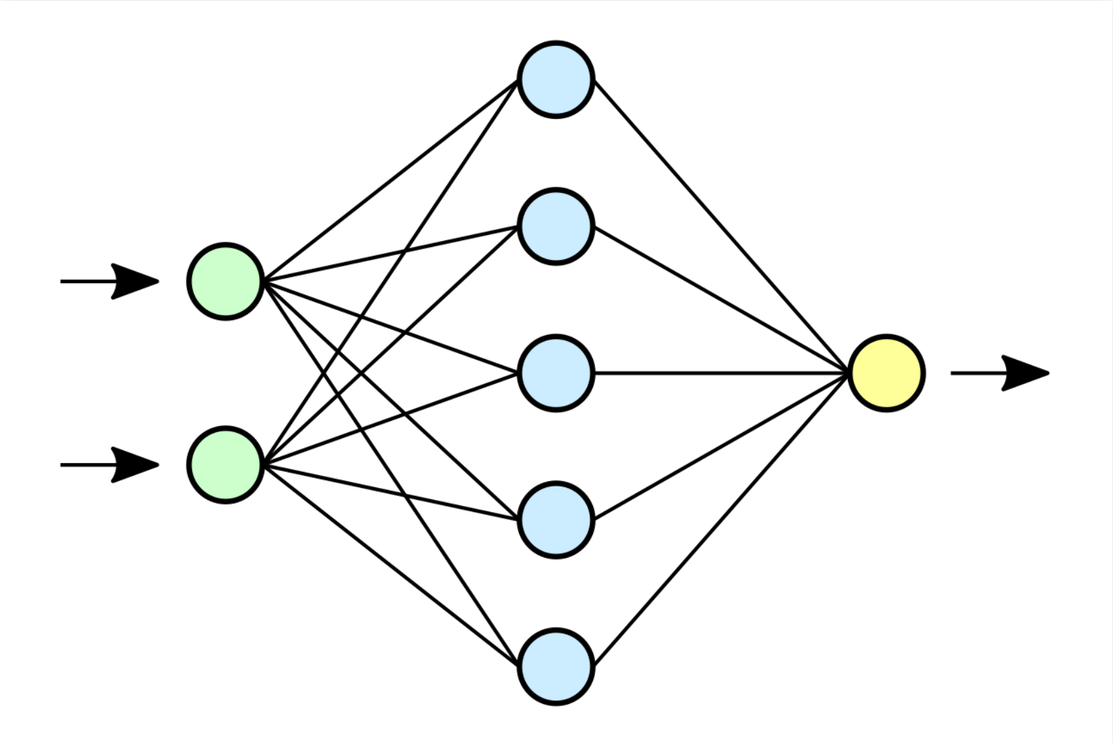
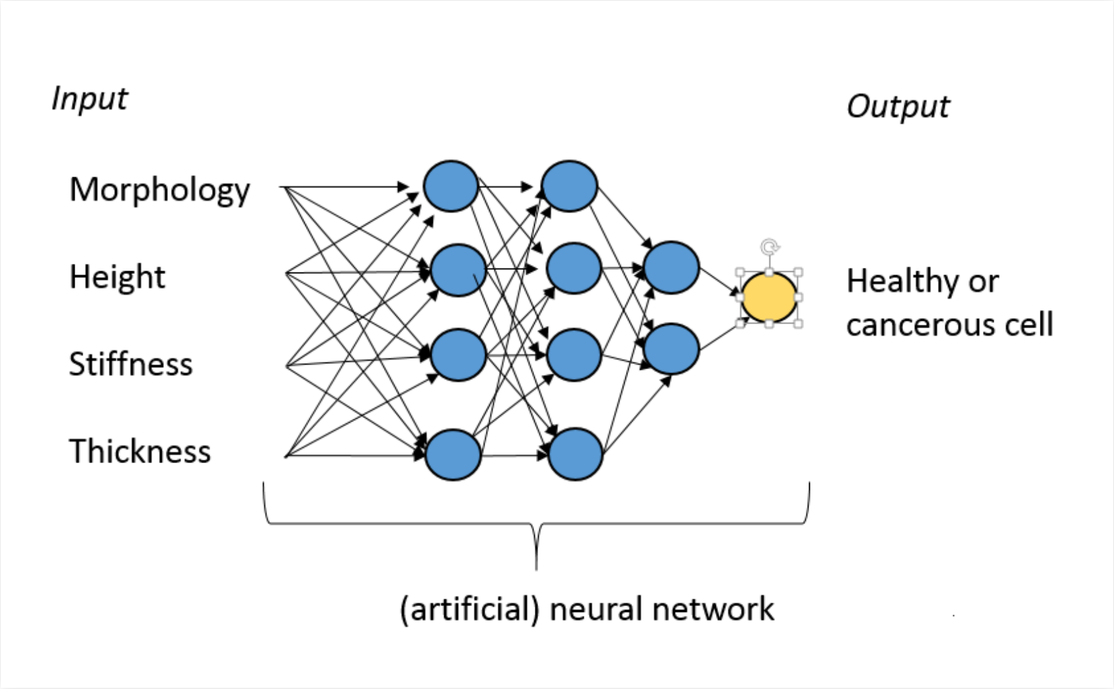


Diagramm einer McCulloch-Pitts-Zelle nach Minsky
Quelle: https://de.wikipedia.org/wiki/McCulloch-Pitts-Zelle

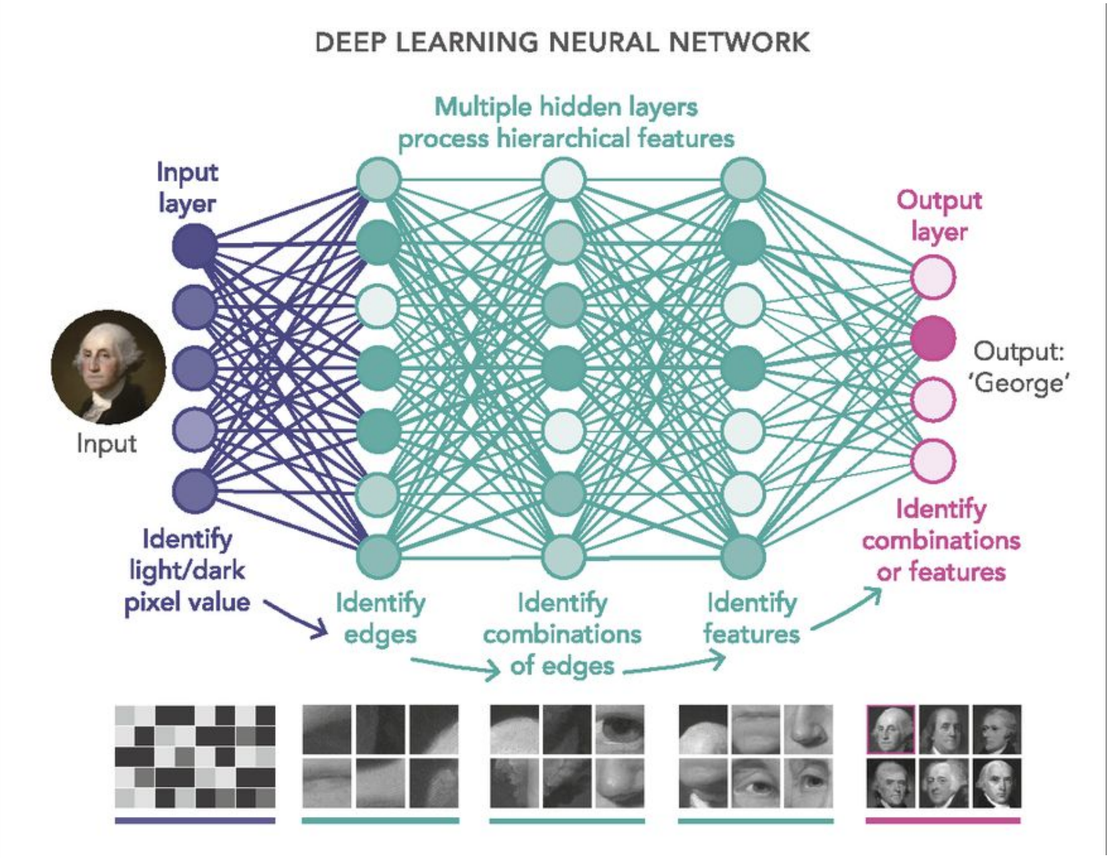


Schematische Darstellung einer einfachen neuronalen Vernetzung
Quelle: https://de.wikipedia.org/wiki/Neuronales_Netz

Bonus: Künstliche Intelligenz - Neuronale Netze und Deep Learning /II



Neuronales Netz für die Analyse von Krebszellen
Quelle: https://analyticalscience.wiley.com/do/10.1002/micro.2994



Neuronales Netz mit Deep-Learning
Quelle: https://www.pnas.org/content/116/4/1074