

IU Internationale Hochschule

GI –SECMGT TAGUNG 2024-05-17

KI IM FOKUS

**EINBLICKE IN DIE MODELLE HINTER DEN AKTUELLEN
KI-ANWENDUNGEN IN DER CYBERSICHERHEIT**

Begriffsbestimmung KI

Maschinelles Lernen

Künstliche Neuronale Netze und Deep Learning

Generative KI

Ausblick

1

2

3

4

5

BEGRIFFSBESTIMMUNG KI

Aspekte
menschlicher
Intelligenz,
die durch KI
abgebildet
werden
sollen

Logisches Denken und Schlussfolgerungsfähigkeit

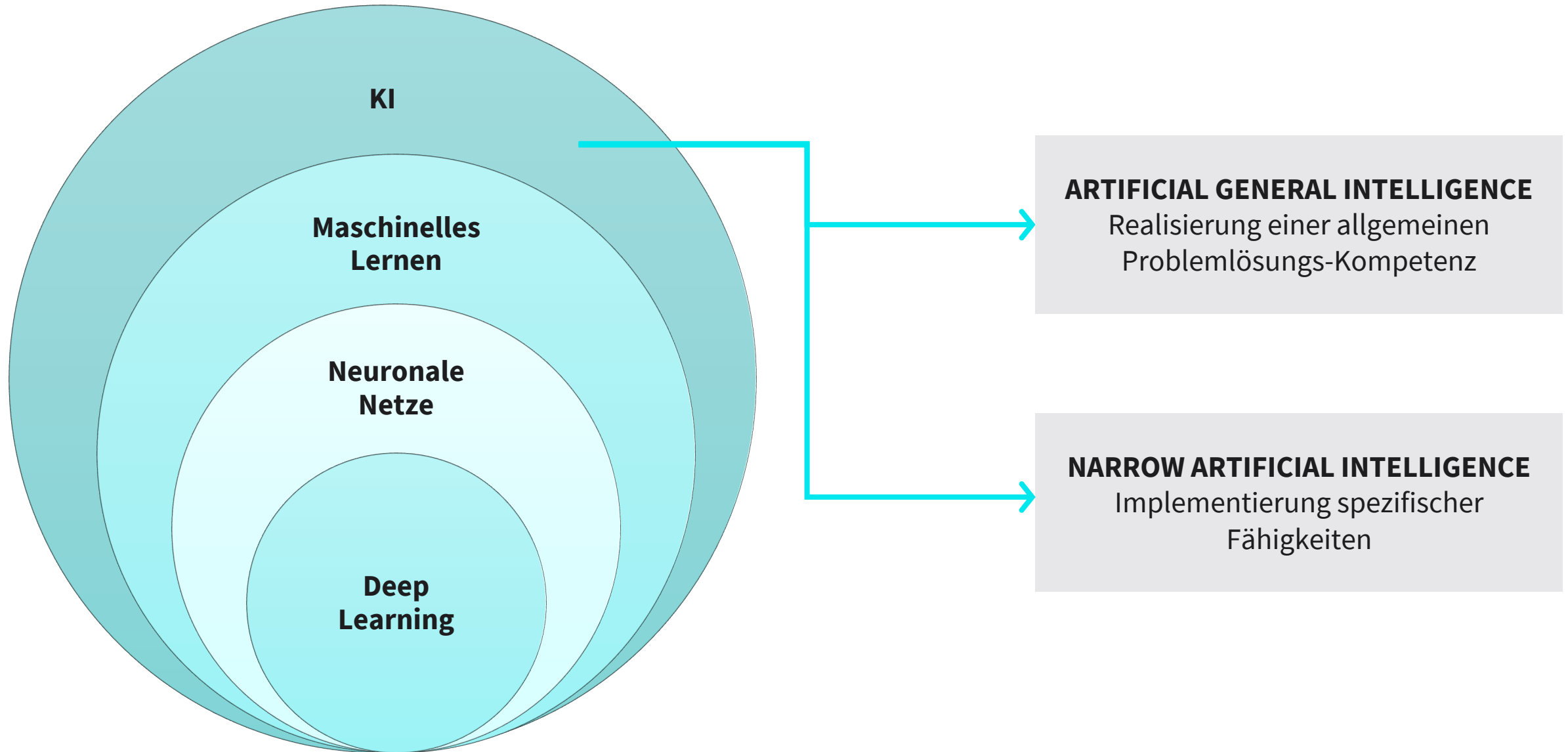
Wissensrepräsentation

Mustererkennung und -Interpretation

Sprachverarbeitung und -Verstehen

Visuelle Wahrnehmung

Adaptierung an neue Situationen und Kontexte

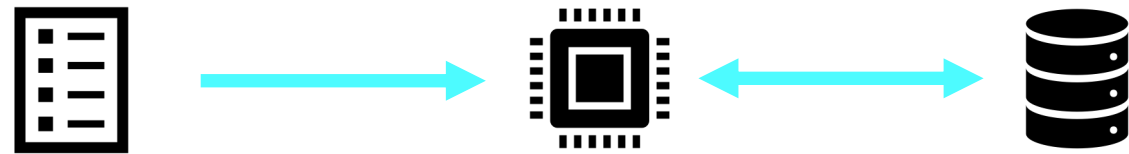


02

MASCHINELLES LERNEN

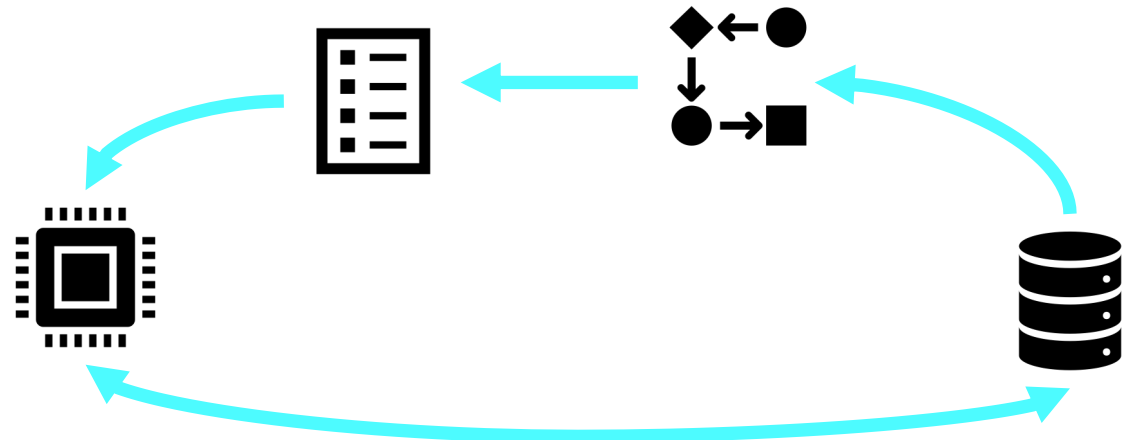
KLASSISCHE PROGRAMMIERUNG

Explizite Beschreibung der Verarbeitungsschritte (imperativ), oder des gewünschten Resultats (deklarativ)



MASCHINELLES LERNEN

System-Verhalten wird aus den Daten gelernt



„A computer program is said to **learn** from experience ***E*** with respect to some class of tasks ***T*** and performance measure ***P***, if its performance at tasks in ***T***, as measured by ***P***, improves with experience ***E***.“

Modell

$$f(\mathbf{x}; \boldsymbol{\theta})$$

erzeugt Ausgabe basierend auf
Eingaben (Merkmale) und Parametern

Algorithmus

A

nutzt

Performance-Maß

$$P[f(\mathbf{x}; \boldsymbol{\theta})]$$

zur Bestimmung von

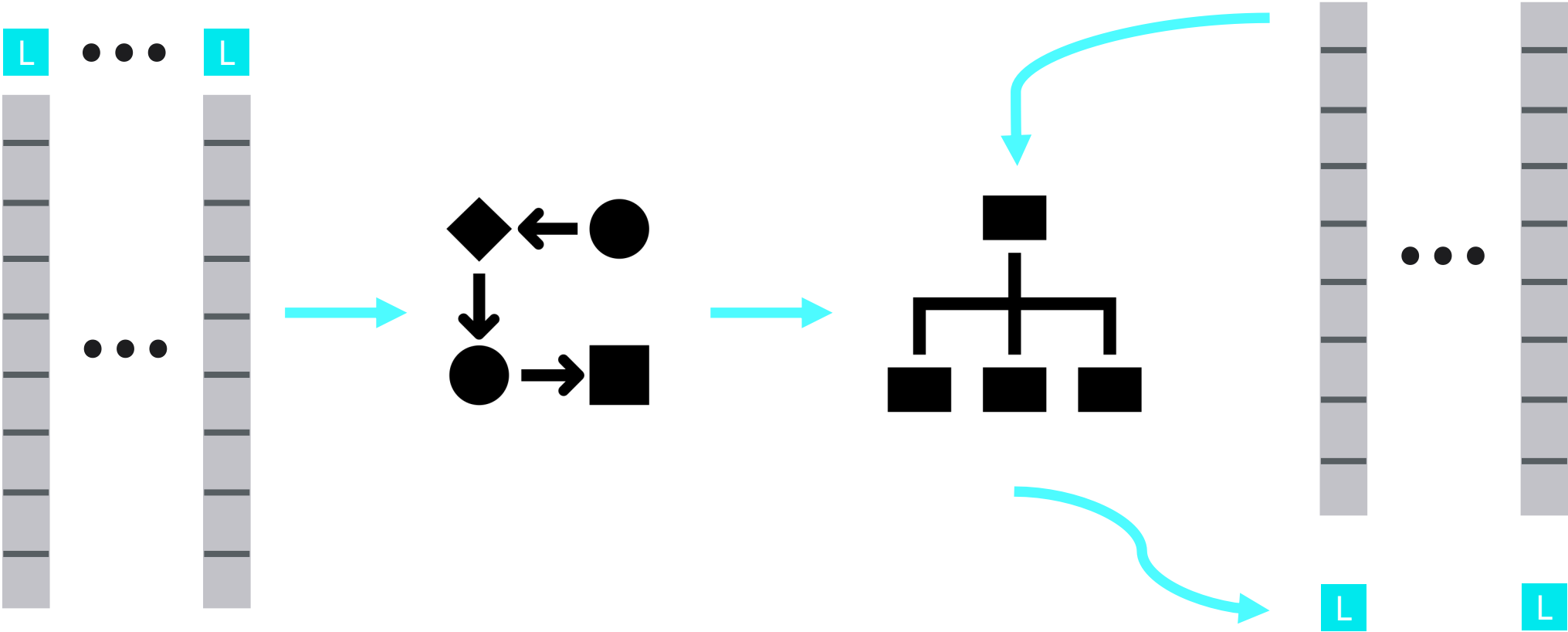
$\boldsymbol{\theta}$

$$E = \{\mathbf{x}_i \mid i = 1..n\}$$

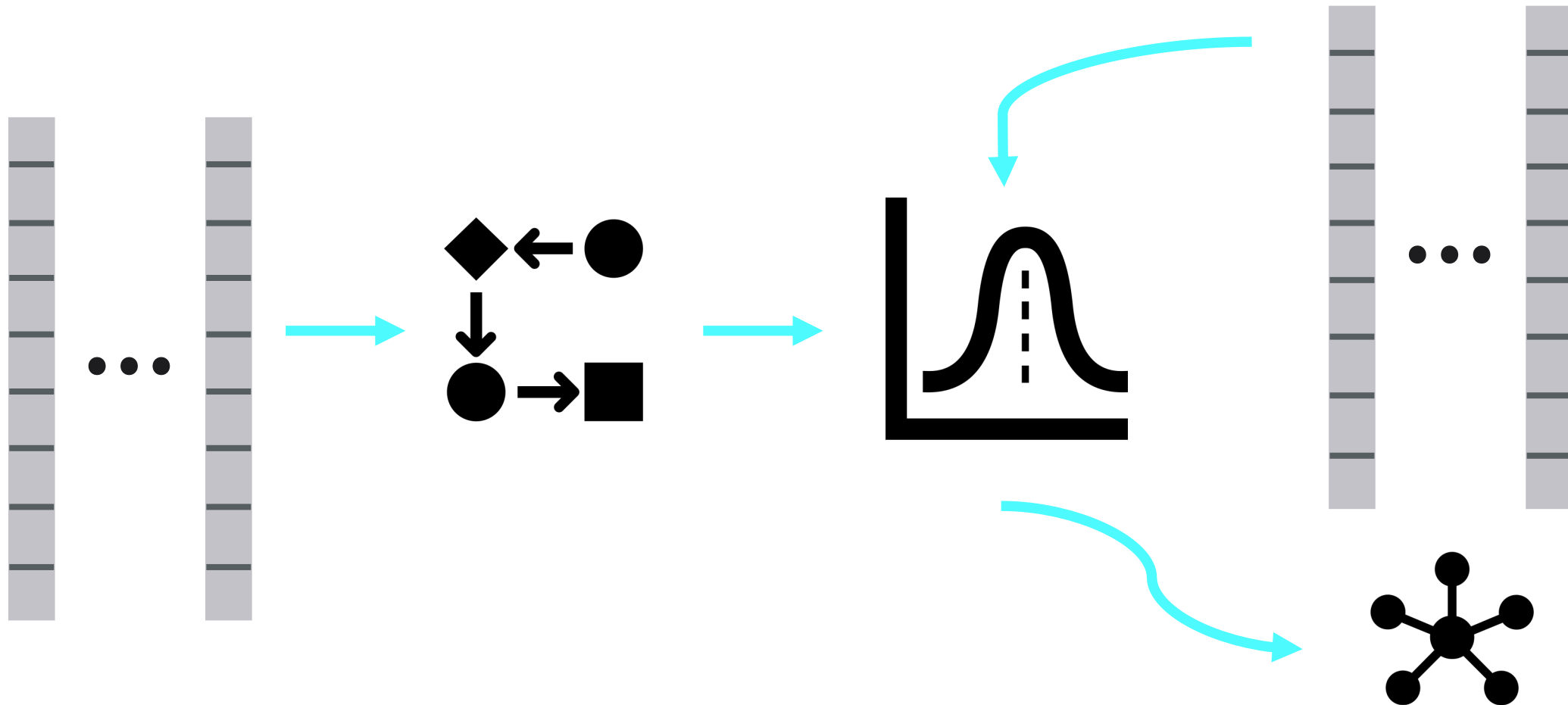
Trainingsdaten

Training

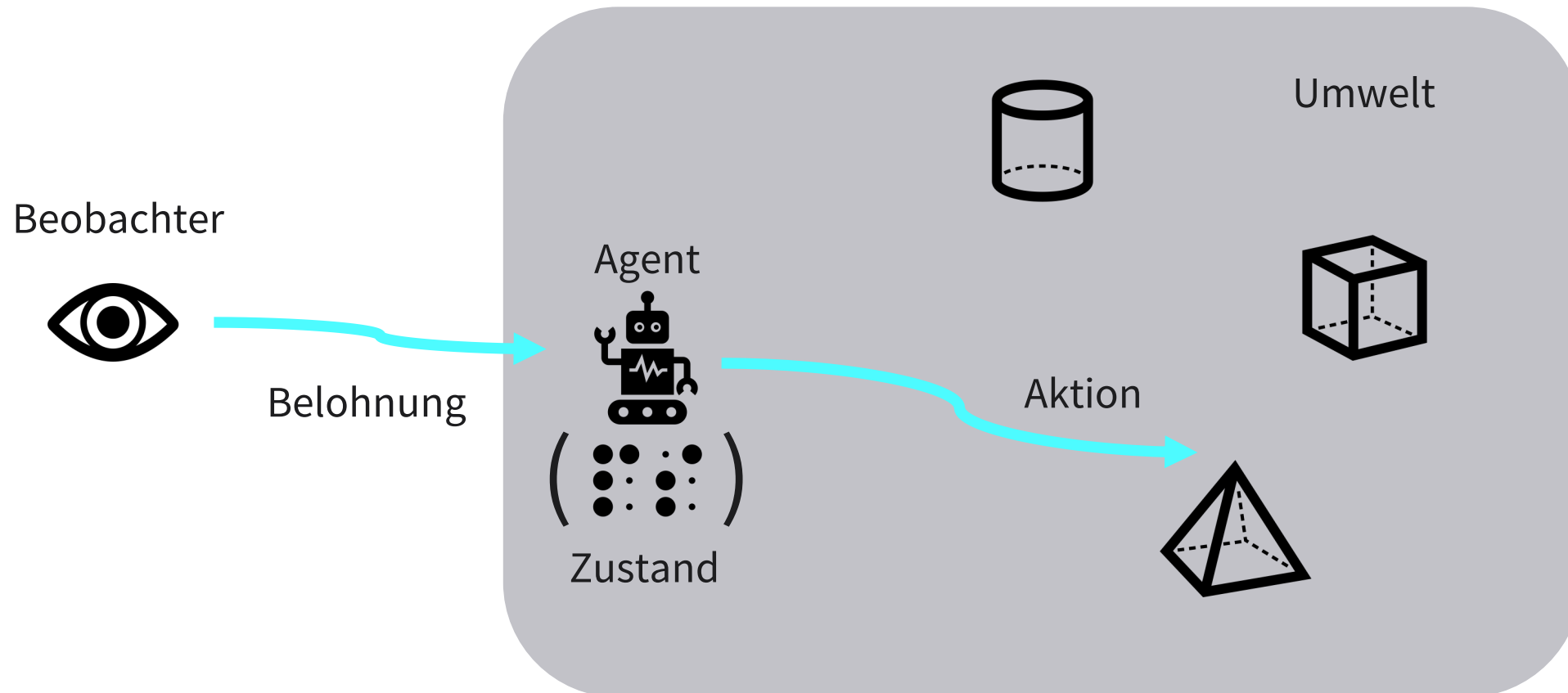
Anwendung



UNÜBERWACHTES LERNEN (UNSUPERVISED LEARNING)



BESTÄRKENDES LERNEN (REINFORCEMENT LEARNING)



Medizin

Diagnostik, Wirkstoff-Forschung, Optimierung medizinischer Leistungen ...

Bildung

Literatursuche, adaptive Lerninhalte, virtueller Tutor ...

Marketing & Sales

Ad Targeting, Individualisierung von Angeboten, Empfehlungen ...

Industrie

Robotik, Cyber-Physikalische Systeme, dynamische Produktionssteuerung, vorausschauende Wartung ...

Logistik, Transport & Verkehr

Autonomes Fahren, intelligente Verkehrsfluss-Steuerung, Supply-Chain-Optimierung

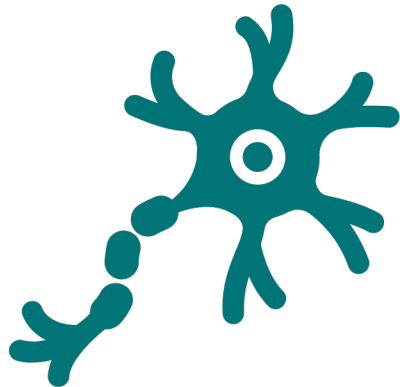
Cybersecurity

Erkennung von Phishing Mails, Malware, Netzwerk-Anomalien ...

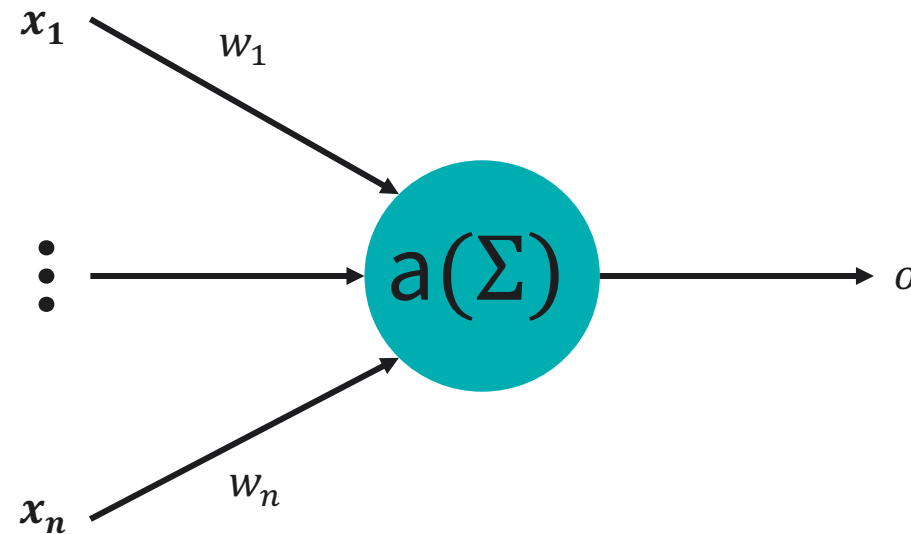
03

NEURONALE NETZE UND DEEP LEARNING

Nervenzelle



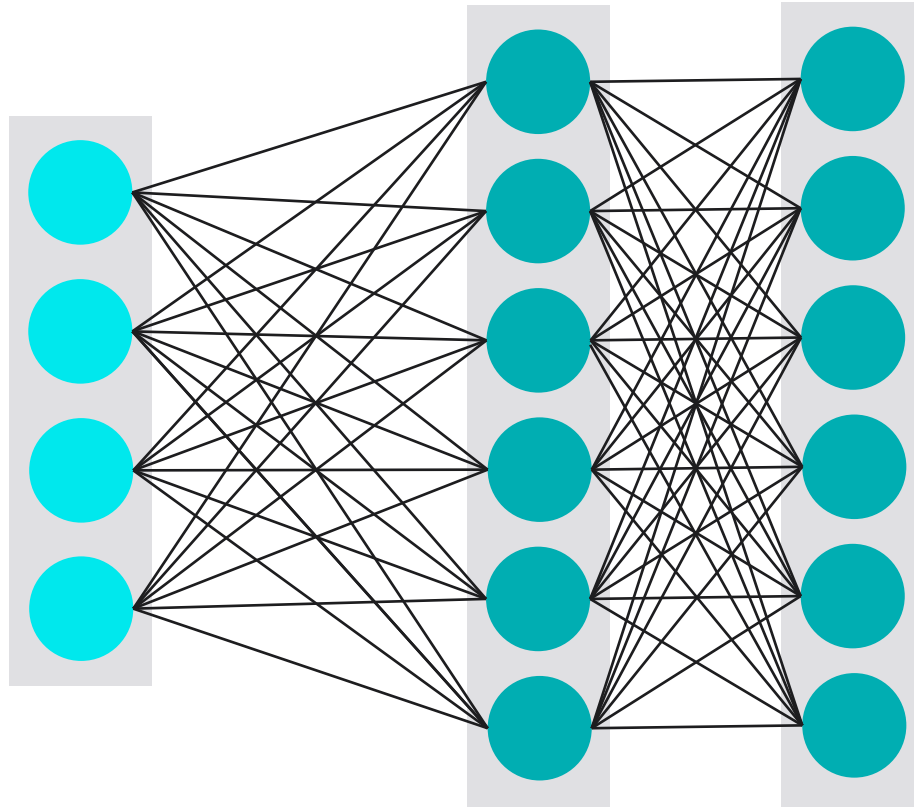
Verarbeitungseinheit eines KNN



$$z = w_1x_1 + w_2x_2 + \dots + w_nx_n + b = \mathbf{w}^T \mathbf{x} + b$$

$$o = a(z) = a(\mathbf{w}^T \mathbf{x} + b)$$

NEURONALE NETZE UND DEEP LEARNING



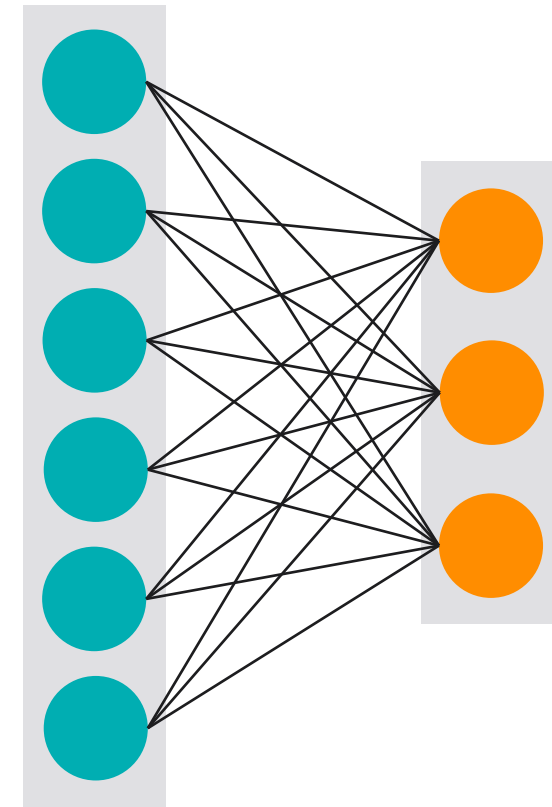
Eingabeschicht
Input Layer

Verdeckte Schichten
Hidden Layers

...

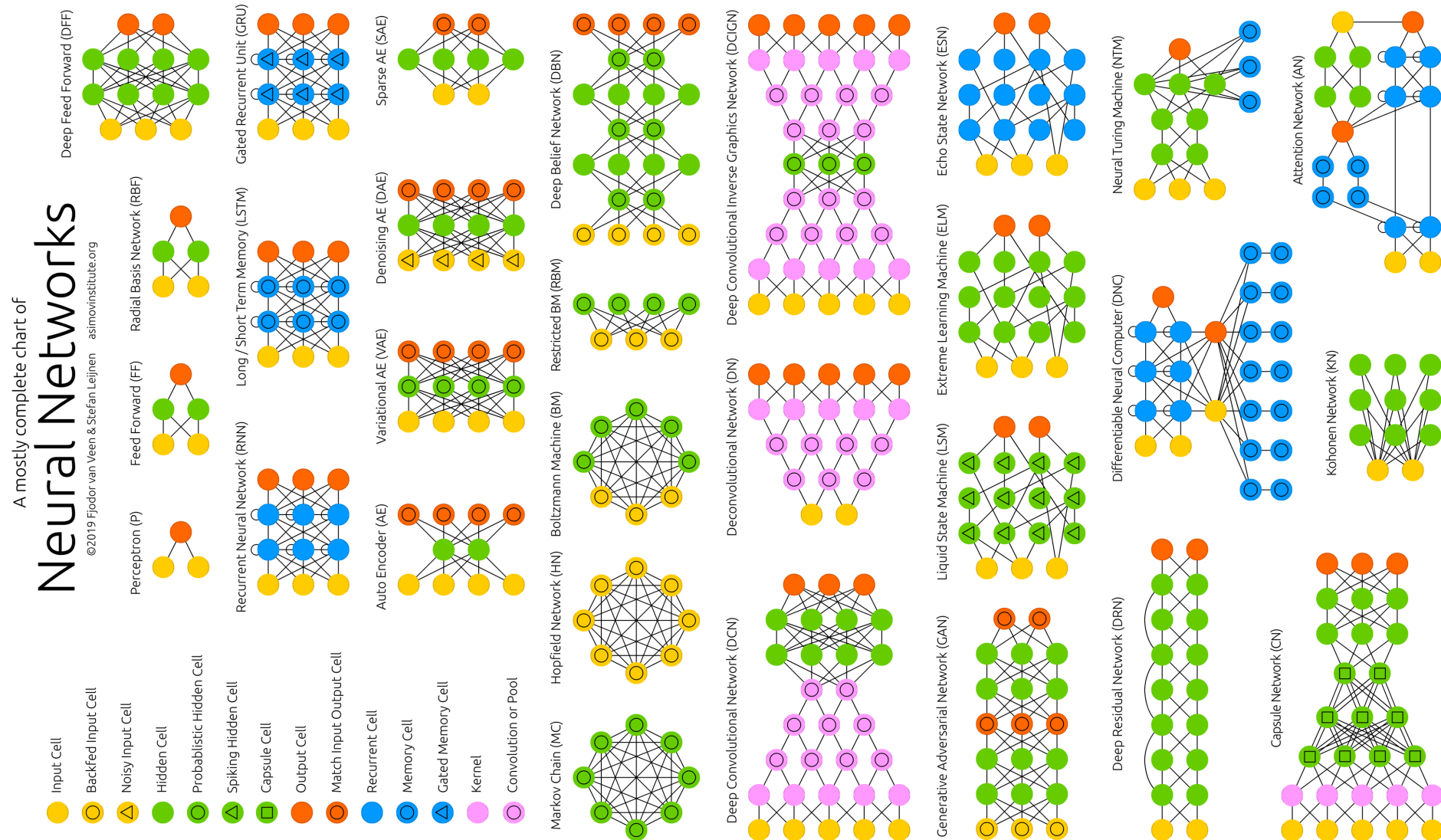
...

...



Ausgabeschicht
Output Layer

DER NEURONALE NETZE ZOO



04

GENERATIVE KI

Modell	Entwickler	Parameteranzahl
GPT-4	OpenAI	> 1 Bio. (unsicher)
BERT-Large	Google	340 Mio.
T5 (Text-to-Text Transfer Transformer)	Google	11 Mrd.
LLaMA 3	Meta	8, 70 und 400 (unveröffentl.) Mrd.
Claude 3	Anthropic	unbekannt
Mixtral 8x7B, 8x22B	Mistral AI	45 bzw. 141 Mrd.
Megatron-LM	NVIDIA	8.3 Mrd.

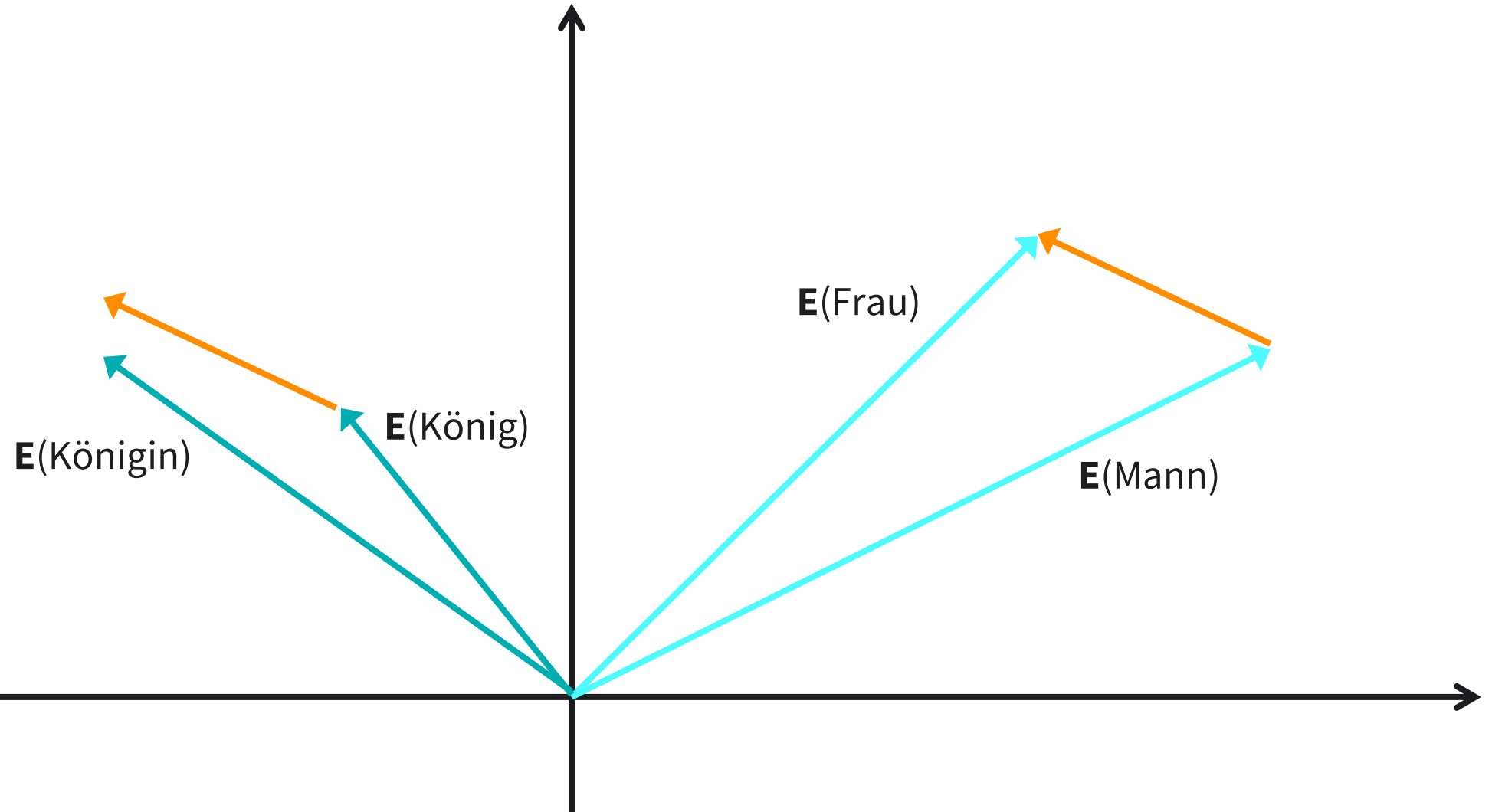
Kern- Einbettung (Embeddings)

Ideen

hinters Transformers / Attention
Mechanismus

LLMs

RLHF – Reinforcement Learning from
Human Feedback



LARGE LANGUAGE MODELS - ATTENTION MECHANISMUS / TRANSFORMERS

"Er saß auf der Bank und beobachtete die Vögel am Fluss,

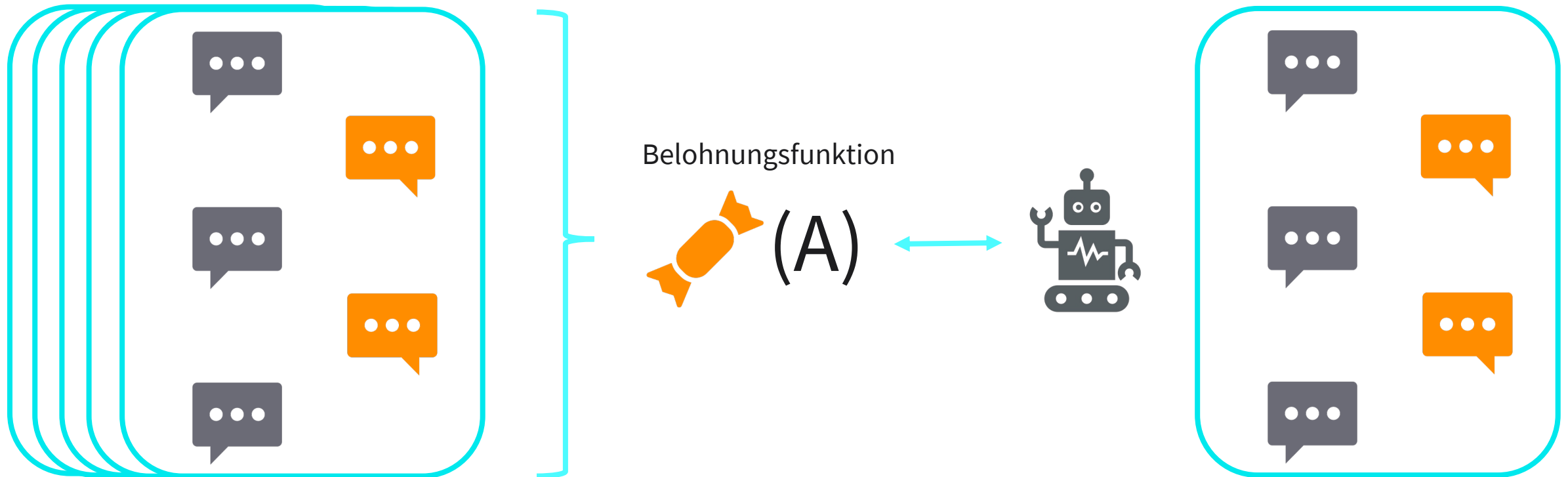


nicht weit von der Bank entfernt, wo er sein Konto hat."



“Mr. und Mrs. Dursley im Ligusterweg Nummer 4 waren stolz darauf, ganz und gar normal zu sein, sehr stolz sogar...”¹

“ChatGPT, erkläre mir den Begriff AI!”



Use Cases

Media-Content-Erstellung

Kunst und Design

Code Generierung

Automatisierte Erkennung von Schwachstellen

Phishing

Threat Intelligence

05

AUSBLICK

1

Effizienz

2

Multi-Modale AI

3

Virtuelle Agenten

4

Regulierung

5

Robotik

DANKE

IU Internationale Hochschule - Fernstudium
Mülheimer-Str. 38
53604 Bad Honnef

Prof. Dr. Thomas Zöller
 0174 4986251
 thomas.zoeller@iu.org