



Terminologie

Kompetenznetzwerk CNAI

Autor	Geschäftsstelle CNAI
Version	1.0
Datum	15.12.2021

INHALTSVERZEICHNIS

1. ZIEL DIESES DOKUMENTS UND GELTUNGSBEREICH	3
2. TERMINOLOGIE IN BEZUG AUF DATEN(QUELLEN)	4
3. TERMINOLOGIE IN BEZUG AUF «LERNEN AUS DATEN(QUELLEN)»	6
4. ZUSÄTZLICHE TERMINOLOGIE.....	10



1. Ziel dieses Dokuments und Geltungsbereich

Mit der Etablierung von einem Kompetenznetzwerk für künstliche Intelligenz («*Competence Network for Artificial Intelligence*» – CNAI) soll der Einsatz von künstlicher Intelligenz und anderer neuer Technologien innerhalb der Bundesverwaltung (und darüber hinaus) nachhaltig gefördert werden.

Eines der Ziele des Kompetenznetzwerks CNAI ist die Einführung einer einheitlichen Terminologie zum Erreichen eines gemeinsamen Verständnisses für die im Zusammenhang mit künstlicher Intelligenz und neuen Technologien relevanten Begriffe auf Ebene der Bundesverwaltung.

Eine gemeinsame Sprache erleichtert den aktiven Erfahrungs- und Wissensaustausch innerhalb des Kompetenznetzwerks CNAI und darüber hinaus. Zudem vereinfacht sie die Kommunikation bezüglich Ideen, Vorhaben und Dienstleistungen in diesem Bereich.

Das entsprechende Terminologie-Management seitens der Geschäftsstelle CNAI stellt somit einen zentralen Grundstein für die Funktionen des CNAI im Allgemeinen und seiner Geschäftsstelle im Speziellen dar.

Dieses Terminologie-Management basiert auf den im BFS und dessen Kompetenzzentrum für Datenwissenschaft («*Data Science Competence Center*» – DSCC) bereits vorhandenen Dokumenten und auf den Dokumenten, welche im Rahmen der Bundesratsentschlüsse zum Aufbau des Netzwerks CNAI, inklusive Geschäftsstelle, erarbeitet wurden.

Ergänzungen bereits erklärter Begriffe sollen nur dann erfolgen, wenn sie für die Abgrenzung weiterer neuer Technologien erforderlich sind. Das Glossar wird in Zusammenarbeit mit den Netzwerkknotenpunkten diesbezüglich und zielführend weiterentwickelt und soll die zukünftige Begriffswelt des CNAI veranschaulichen.

Besitzerin des Dokuments ist die Geschäftsstelle CNAI.

Das vorliegende Dokument wird periodisch überarbeitet und die aktuelle Version (Versionsnummer und Datum als Referenz) hat Gültigkeit.

Schreibkonvention

Solange ein Begriff nicht explizit definiert wurde, wird der Begriff in Anführungszeichen gesetzt, z. B. «Datenwissenschaft».



2. Terminologie in Bezug auf Daten(quellen)

Im Allgemeinen können **drei Arten von Datenquellen** unterschieden werden:

- verwaltungsinterne (z. B. «statistische Daten»¹, administrative Daten, amtliche Daten, Geodaten des Bundes, «Open Government Data» – OGD²) und
- verwaltungsexterne Datenquellen (z. B. offene Daten) sowie
- cyberphysische Systeme (wie Daten von vernetzten Sensoren im Rahmen des «Internets der Dinge» – IoT), welche sowohl eine verwaltungsinterne als auch eine verwaltungsexterne Datenquelle sein können.

Die integrierte Verwendung der verwaltungsinternen und -externen Datenquellen zusammen auch mit Daten aus cyberphysischen Systemen eröffnet der Daten(r)evolution für politische Entscheidungsträger ein enormes Potential. Gerade mit Blick auf eine Nutzung dieses Datenpotentials unter der Verwendung «datenscientifischer Methoden» kann ein grosses Anwendungspotenzial für die «Datenwissenschaft» erschlossen werden. So können bspw. Datenquellen zusammengeführt werden, um bisher nicht abgedeckte Nutzerbedürfnisse zu erfüllen oder um grundsätzlich abgedeckte Nutzerbedürfnisse besser zu erfüllen. Daraus ergeben sich neue Möglichkeiten, um möglichst zeitnah zu verschiedenen Problemstellungen relevante Informationen zu generieren und den politischen Entscheidungsträgern zur Verfügung zu stellen.

Zudem können im Allgemeinen **drei Arten von Datentypen** unterschieden werden:

- strukturierte Daten, die formatiert und in ein wohldefiniertes Datenmodell umgewandelt wurden. Die Rohdaten werden in vordefinierte Felder abgebildet, die dann einfach extrahiert und, z. B. über SQL, gelesen werden können. Relationale SQL-Datenbanken, bestehend aus Tabellen mit Zeilen und Spalten, und klassische Tabellen mit Zeilen und Spalten sind Beispiele für strukturierte Daten; und
- semi-strukturierte (oder halbstrukturierte oder teilweise strukturierte) Daten, welche einige konsistente und eindeutige Merkmale aufweisen, ohne sich auf eine starre Struktur zu beschränken, wie sie z. B. für relationale

¹ Statistische Daten sind alle Daten, welche zu statistischen Zwecken erhoben oder weitergegeben wurden, insbesondere gestützt auf das Bundesstatistikgesetz und unterliegen damit dem Statistikgeheimnis.

² Offene Daten meint Daten, die frei, ohne wesentliche rechtliche, finanzielle oder technische Einschränkungen, genutzt, verarbeitet, ausgewertet und weitergegeben werden dürfen. Rechtlich muss die kostenfreie Nutzung und Weiterverarbeitung der Daten gewährleistet sein; technische Offenheit betont, dass offene Daten maschinell bearbeitbar sein müssen. Bei der Publikation von Daten als offenen Daten müssen Datenschutz-, Informationsschutz- und Urheberrechtsbestimmungen sowie Geschäftsgeheimnisse gewahrt bleiben.



Datenbanken erforderlich ist. Ein Beispiel sind Bilder: wenn ein Bild beispielsweise von einem Smartphone aufgenommen wird, weist es einige strukturierte Attribute wie Geotag, Geräte-ID und Zeitstempel auf. Nach dem Speichern können Bildern auch Tags wie «Haustier» oder «Katze» zugewiesen werden, um eine Struktur bereitzustellen; und

- unstrukturierte Daten sind Daten, welche in absoluter Rohform vorliegen. Diese Daten sind aufgrund ihrer komplexen Anordnung und Formatierung schwer zu verarbeiten. Die unstrukturierte Datenhaltung kann Daten aus vielen Formen annehmen, darunter Social-Media-Posts, Chats, Luft- und Satellitenbilder³, IoT-Sensordaten, E-Mails und Präsentationen.

³ Luft- und Satellitenbilder können sowohl in strukturierter Form (Sichtweise einer Messmatrix) wie in unstrukturierter Form (unkalibrierte Bilder) vorliegen.



3. Terminologie in Bezug auf «Lernen aus Daten(quellen)»

Begriff	Definition
Datenwissenschaft	<p>Datenwissenschaft («<i>Data Science</i>») ist die interdisziplinäre Wissenschaft des Lernens aus Daten (des Datenverstehens), mit dem Ziel, Erkenntnisse aus Daten zu gewinnen, auf deren Basis datenbasierte Entscheidungsgrundlagen erstellt werden können.</p> <p>Die Datenwissenschaft umfasst, wie die Statistik, den gesamten Prozess der Problemformulierung, der Erfassung, Auswahl, Vorbereitung und Analyse von Daten sowie der Evaluation, Interpretation, Kommunikation und Bereitstellung der gewonnenen Erkenntnisse.</p> <p>Im Gegensatz zu traditioneller (und erweiterter) Statistik ist die Vorgehensweise der Datenwissenschaft aber das induktive Vorgehen, das von Daten ausgeht, d. h. «<i>data first</i>».</p> <p>Im Zentrum der Datenwissenschaft stehen ein Problemlösungsprozess sowie ein Prozess der kontinuierlichen Verbesserung, der darauf abzielt, komplexe, unstrukturierte und datenreiche Probleme durch die Anwendung innovativer datenwissenschaftlicher Methoden (z. B. Methoden aus dem «maschinellen Lernen» und dem Bereich der «künstlichen Intelligenz»), Techniken und Praktiken zu lösen.</p> <p>Datenwissenschaft wird auch als «das Kind von Statistik und Informatik» bezeichnet. Diese Kind-Metapher schlussfolgert angemessen, dass die Datenwissenschaft (idealerweise das Beste) von beiden Elternteilen erbt, aber schließlich zu einer eigenen Entität heranwächst. Ihr Fokus trennt sie von ihren Eltern.</p>

Begriff	Definition
Künstliche Intelligenz (KI)	<p>Künstliche Intelligenz (KI – «<i>Artificial Intelligence</i> – AI»), heute manchmal als «maschinelle Intelligenz» («<i>Machine Intelligence</i>») bezeichnet, wird definiert als «einen Computer so bauen oder programmieren, um Dinge zu tun, die normalerweise menschliche oder biologische Fähigkeiten («Intelligenz») erfordern», z. B. visuelle Wahrnehmung (Bilderkennung), Spracherkennung, Sprachübersetzung, visuelle Übersetzung und Spiele spielen (mit konkreten Regeln).</p> <p>Bei KI geht es um «intelligente» Maschinen («<i>smart machines</i>»), die Aufgaben ausführen können, die normalerweise von Menschen ausgeführt werden («lernende Maschinen»; «<i>learning machines</i>»), d. h. Maschinen «intelligent» machen.</p>
KI-System	<p>Ein KI-System («<i>AI System</i>») ist ein maschinenbasiertes System, welches für vom Menschen klar definierte Problemstellungen, Vorhersagen, Empfehlungen oder Entscheidungen machen kann, welche reale oder virtuelle Umgebungen beeinflussen. KI-Systeme können mit unterschiedlichem Ausmass an Autonomie ausgestattet werden.</p>
KI-Entscheidungen	<p>KI-Entscheidungen sind Schlussfolgerungen von KI-Systemen mit realweltlichen Auswirkungen.</p> <p>Diese sind auf der Ebene des Designs des Systems, der strategischen Ebene (Entscheid über Einsatz des Systems) und der taktischen Ebene (Ausgestaltung der Interaktion mit der Person, die das System nutzt) von menschlichen Entscheidungen abhängig.</p>
KI-Technologie	<p>KI-Technologie bezeichnet einzelne, in Computer implementierbare Funktionen für die Erreichung von KI (z. B. «maschinelles Lernen»).</p> <p>Ein KI-System bezeichnet somit eine strukturierte, kontextgebundene Kombination von KI-Technologien zwecks Erreichens von KI.</p>
«Natural Language Processing» (NLP)	<p>«Natural Language Processing» (NLP) ist ein Teilgebiet der KI, welches sich mit der Analyse, dem Verständnis und der Generierung von geschriebenen und gesprochenen Wörtern und Sätzen (natürlicher Sprache) beschäftigt. Die meisten NLP Techniken und Methoden basieren auf «maschinellern Lernen» und extrahieren so die Bedeutung und Zusammenhänge aus menschlicher Sprache. Anwendungsgebiete sind z. B. Texterkennung («<i>Text Recognition</i>»), Spracherkennung («<i>Speech Recognition</i>»), Bots, «Chatbots» und digitale Assistenten.</p>

Begriff	Definition
Maschinelles Lernen (ML)	<p>Maschinelles Lernen (ML – «Machine Learning») ist ein weiteres Teilgebiet der KI, welches «den Computern die Lernfähigkeit verleiht».</p> <p>ML untersucht die Konstruktion von Algorithmen, die durch den Einsatz von Computern Daten analysieren und dabei automatisch lernen, sich anpassen und verbessern (anhand von konkreten vom Menschen vorgegebenen Regeln). Das resultierende statistische Modell ermöglicht bspw. Vorhersagen und Klassifizierungen von (noch nicht gesichteten) Daten, welche entscheidungsunterstützend eingesetzt werden können.</p> <p>In der KI ist ML das wichtigste Teilgebiet, das sich mit dem Problem des induktiven Denkens auseinandersetzt. Die Vorgehensweise von ML ist somit das induktive Vorgehen, das von Daten ausgeht, d. h. «<i>data first</i>».</p>

ML kann grob in drei verschiedene Teilbereiche unterteilt werden: überwachtes, unüberwachtes und verstärktes Lernen. Diese Trennung ist nützlich, um die grundlegenden ML Bausteine zu verstehen. Die aktuelle Forschung untersucht allerdings, wie man/frau die verschiedenen ML Arten miteinander kombinieren kann.

Begriff	Definition
Überwachtes Lernen	<p>Beim überwachten Lernen («supervised learning») wird der ML-Algorithmus mit Daten trainiert, und ein menschlicher Beobachter bzw. Benchmark-Daten überwachen den Lernerfolg.</p> <p>Konkret werden ML-Algorithmen mithilfe eines Trainingsdatensatzes, welches eine Vielzahl an «<i>Features</i>» («<i>inputs</i>») und eine «Zielvariable» («<i>output</i>», z. B. «richtig» oder «falsch») beinhaltet, in einem iterativen Prozess trainiert. Dabei lernt der Algorithmus automatisch (komplexe) Muster zwischen den «<i>Features</i>» und der Zielvariable ohne explizite (menschliche) Anweisungen. Mithilfe der gelernten Muster können für (noch nicht gesichtete) Daten Vorhersagen oder Klassifizierungen vorgenommen werden.</p> <p>Bspw. ist tiefes Lernen («Deep Learning») eine Teilsparte des überwachten Lernens und verwendet eine spezialisierte Form von ML-Algorithmen aus der Gruppe der «künstlichen neuronalen Netze».</p>

Begriff	Definition
Unüberwachtes Lernen	<p>Das unüberwachte oder unbeaufsichtigte Lernen («unsupervised learning») zielt darauf ab, Zusammenhänge und Abhängigkeiten in Daten ausfindig zu machen und diese gegebenenfalls zu Merkmalen weiter zu verarbeiten.</p> <p>Beim unüberwachten Lernen bestehen die Trainingsdaten aus Eingabedaten («<i>inputs</i>»), ohne dass ein Hinweis auf die erwartete Leistung des Systems vorliegt, d. h. eine Zielvariable (z. B. «richtig» oder «falsch») liegt nicht vor.</p> <p>Im Gegensatz zum überwachten Lernen wird der ML-Algorithmus somit nur mit «<i>Features</i>» trainiert. Auf Basis der «<i>Features</i>» entdeckt der Algorithmus selbstständig Muster in den Daten. Dies ermöglicht es von nicht sichtbaren Strukturen in den Daten zu lernen (bspw. mittels «<i>Clustering</i>»).</p> <p>Unüberwachtes Lernen ähnelt dem menschlichen Lernen; durch Beobachtungen, Erfahrungen und Analogien.</p>
Verstärktes Lernen	<p>Das verstärkte Lernen («reinforcement learning») steht für eine Reihe von ML-Methoden, bei denen ein «Agent» selbstständig eine «Strategie» erlernt, um erhaltene Belohnungen zu maximieren. Dabei wird dem «Agenten» nicht vorgezeigt, welche Aktion in welcher Situation die beste ist, sondern er erhält zu bestimmten Zeitpunkten eine Belohnung, die auch negativ sein kann. Anhand dieser Belohnungen approximiert er eine «Nutzenfunktion», die beschreibt, welchen Wert ein bestimmter Zustand oder Aktion hat.</p> <p>Verstärktes Lernen findet bspw. seine Hauptanwendung in Planungsproblemen wie der Navigation (z. B. der «Agent» muss ein Ziel erreichen, und die Belohnung kann mit Zeit oder Entfernung verknüpft werden) und Videospiele (z. B. der «Agent» muss spielen, und seine Belohnung ist mit dem Endergebnis des Spiels verknüpft).</p>

4. Zusätzliche Terminologie

Begriff	Definition
Blockchain	Eine «Blockchain» erlaubt es einem Kollektiv von Akteuren, auch ohne vertrauenswürdige zentrale Instanz einen vertrauenswürdigen gemeinsamen «Ledger» zu führen. Blockchain-technologie wird auch als « <i>Distributed Ledger</i> »-Technologie (DLT) bezeichnet.
Chatbots	<i>Chatbots</i> sind Dialogsysteme mit natürlichsprachlichen Fähigkeiten (Text oder Audio). Sie werden, oft in Kombination mit statischen oder animierten Avataren, auf Websites oder in Instant-Messaging-Systemen verwendet, wo sie Interessenten und Kunden zu relevanten Produkten oder Dienstleistungen führen respektive sich um Anliegen der Interessenten und Kunden kümmern oder Fragen beantworten.
Cloud Computing / Cloud Services	<i>Cloud Computing</i> ist die Bereitstellung von Computingressourcen (z.B. Server, Speicher, Datenbanken, Netzwerkkomponenten, Software, Analyse- und intelligente Funktionen) über das Internet. Dabei wird in der Regel nur für die Clouddienste (« <i>Services</i> ») gezahlt (« <i>pay as you go</i> »), die tatsächlich genutzt werden. In der Regel werden hoch standardisierte Leistungen als <i>Cloud-Services</i> angeboten. Im Gegenzug sind diese Leistungen extrem schnell verfügbar (oft innerhalb von Minuten).
Internet der Dinge (IoT)	Das Internet der Dinge (« Internet of Things » – IoT) ist ein Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Gegenstände miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen.

