

			Legende: 1 - niedrig, 5 - hoch
Thema	Rel.	Inhalt (Auszüge)	Hyperlink
Hacking mit ChatGPT	4	<p>Was ist eigentlich Hacking? Die -Definition klingt denkbar trocken: Wer eine Informationstechnologie anders als von den Erfinder:innen gedacht nutzt und so eigene Interessen erreicht oder bestimmte Hindernisse umgeht, betreibt Hacking.</p> <p>Tatsächlich könnte man es auch als -kreative Zweckentfremdung bezeichnen – und gerade entstehen zahlreiche neue Technologien, die den Spielraum genau dafür bieten. Ich spreche dabei von künstlicher Intelligenz, im Besonderen generativen KI-Systemen. Dazu gehören beispielsweise große Sprachmodelle und deren User-Interfaces wie ChatGPT, Bild-generatoren wie -Midjourney oder Tools zur Generierung von Ton und Video wie Runway. [...]</p>	https://t3n.de/news/hacking-mit-chatgpt-eine-liste-potentieller-moeglichkeiten-und-gefahren-1571871/
IBM ersetzt Jobs durch Künstliche Intelligenz	5	https://www.tagesschau.de/wirtschaft/digitales/ibm-ki-arbeitsplaetze-100.html	
Chiphersteller profitieren vom KI-Boom	5	https://www.tagesschau.de/wirtschaft/unternehmen/nvidia-aktie-rekordhoch-kuenstliche-intelligenz-100.html	
Arbeitsminister Heil will KI "auf die Straße bringen"	4	https://www.tagesschau.de/wirtschaft/digitales/spd-heil-ki-arbeitswelt-100.html	
KI-Boom macht Nvidia zur Gelddruckmaschine	4	https://www.tagesschau.de/wirtschaft/unternehmen/nvidia-chiphersteller-ki-boom-kuenstliche-intelligenz-100.html	
Nvidia profitiert vom KI-Boom	4	https://www.tagesschau.de/wirtschaft/unternehmen/nvidia-ki-chips-quartalszahlen-kuenstliche-imntelligenz-boom-gewinn-100.html	
Abkommen zum Schutz vor KI-Missbrauch geschlossen	5	https://www.tagesschau.de/wirtschaft/ki-abkommen-102.html	
Strengere Regeln für Künstliche Intelligenz	4	https://www.tagesschau.de/ausland/europa/ki-eu-parlament-100.html	
How your data is used to improve model performance	4	https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance	
Wie lang die Leine für ChatGPT und Co. wird I	5	<p>Artificial Intelligence Verhandlungen über AI Act Wie lang die Leine für ChatGPT und Co. wird</p> <p>Stand: 06.12.2023 06:30 Uhr</p> <p>Künstliche Intelligenz kann Aufsätze schreiben oder helfen, Krankheiten zu diagnostizieren, aber kann auch zu Desinformation und Diskriminierung führen. Die EU will KI deswegen per Gesetz regulieren. - von Christian Kretschmer, SWR</p> <p>Der Hype fing vor rund einem Jahr an, mit diesem Satz: "Wir haben ein Modell mit dem Namen ChatGPT trainiert, das auf eine konversationelle Art und Weise interagiert." Mit diesem holprigen Understatement präsentierte das Unternehmen OpenAI seinen Chatbot auf der eigenen Website. Es folgten Jubelarien, Schreckensszenarien und vieles dazwischen. Die große Aufregung um ChatGPT hat sich gelegt, gleichzeitig gehören KI-Anwendungen mehr und mehr zum Alltag.</p> <p>Zu sehen ist das etwa bei "Robotspaceship", einer Mainzer Beratungsagentur, die für Kunden auch digitale Inhalte produziert. "Wir nutzen ChatGPT, um Konzepte für Podcasts zu entwickeln, oder auch Bildgeneratoren um in der Grafik Entwürfe zu erstellen", sagt Inhaber Oliver Kemmann. KI-Hilfsmittel könnten viele, darunter kreative Prozesse beschleunigen, meint der Innovationsberater.</p> <p>Doch nicht zuletzt wegen Fehlern und Verzerrungen in den Daten, mit denen die KI trainiert wurde, sagt Kemmann auch: "Wir brauchen eine Regulierung. Aber das muss richtig gemacht werden, wir dürfen nicht überregulieren."</p>	https://www.tagesschau.de/wissen/technologie/ki-regulierung-eu-100.html

Wie lang die Leine für ChatGPT und Co. wird II	5	<p>Regulierung auf EU-Ebene [.] Im Kern zielt der AI Act darauf ab, nicht die Technik, sondern die Anwendung von KI zu regulieren. Dafür gibt es verschiedene Risiko-Abstufungen. Verboten werden soll etwa das "Social Scoring" durch Künstliche Intelligenz, also die Bewertung von Bürgerinnen und Bürgern wegen deren sozialem Verhalten.</p> <p>Als "Hochrisiko-KI-Systeme" gelten solche, die etwa im Gesundheitswesen oder beim Job-Recruiting eingesetzt werden. Zum Beispiel, indem KI hilft, Krankheiten zu diagnostizieren oder Bewerber auszusortieren. Für Anwendungen, die wiederum nur ein begrenztes Risiko darstellen, soll es Transparenzpflichten geben, für jene mit minimalem Risiko keine weiteren Verpflichtungen.</p> <p>"KI darf Menschen nicht diskriminieren"</p> <p>Dieser risikobasierte Ansatz sei grundsätzlich sinnvoll, sagt Sandra Wachter, Professorin für Technologie und Regulierung an der Universität Oxford. Das gelte zumindest für KI-Systeme, die zur Entscheidungshilfe eingesetzt werden. Unter anderem in den Bereichen Migration, Strafrecht oder bei Versicherungen müsse etwa sichergestellt werden, dass KI Menschen nicht diskriminiere.</p> <p>In manchen Bereichen sei die "Unerklärbarkeit" von KI-Entscheidungen dagegen weniger dramatisch. "Wenn mir der Netflix-Algorithmus einen Film vorschlägt: Muss ich dann wirklich inhaltlich verstehen, warum er das getan hat", fragt Wachter. Generative KI wie ChatGPT dürfe dagegen keine "Black Box" sein. Und gerade hier gab es zuletzt Streit zwischen den EU-Institutionen.</p>	https://www.tagesschau.de/wissen/technologie/ki-regulierung-eu-100.html
Wie lang die Leine für ChatGPT und Co. wird III	5	<p>Hier geht es um die Frage, welche Regelungen für so genannte Basismodelle gelten sollen. Dabei handelt es sich um KI-Modelle, die mit sehr vielen Daten trainiert werden und für verschiedene Zwecke eingesetzt werden können: eine Art "Allzweck-KI" also. Prominentestes Beispiel ist das Modell "GPT 4", das etwa mit Unmengen an Texten aus dem Internet "gefüttert" wurde. Auf ihm basiert die aktuelle Version des Bots ChatGPT.</p> <p>EU-Parlament will Risikominimierung Das EU-Parlament hat im AI Act vorgesehen, eigene Regeln für die Basismodelle einzuführen und sie unter anderem dazu zu verpflichten, Risiken für Gesundheit, Grundrechte und Demokratie zu minimieren. Deutschland, Frankreich und Italien hatten im Laufe der EU-Verhandlungen - wohl nicht zuletzt auf Druck von heimischen KI-Unternehmen - aber darauf gedrängt, dass für die Basismodelle keine zusätzlichen Regeln gelten sollten. Stattdessen schlagen die drei Länder eine Selbstverpflichtung vor: Die KI-Entwickler müssten demnach in einer Art Beipackzettel unter anderem die Funktionsweise und Fähigkeiten ihres Modells darlegen.</p> <p>--> Notiz: Ist das euer ernst? Ihr wollt eine Packungsbeilage schreiben?</p>	https://www.tagesschau.de/wissen/technologie/ki-regulierung-eu-100.html
		<p>892 + Wir nehmen uns vor, weitere Regulierung vorzunehmen, insbesondere in Bezug auf die Basismodelle auf Grundlage einer Selbstverpflichtung der Hersteller. --> Wer wäre denn in der Lage, auf der Basis von Supercomputern KI-Basismodelle herzustellen?</p>	
Wie lang die Leine für ChatGPT und Co. wird IV	5	<p>Keine unnötigen Hürden</p> <p>Die deutsche Digitalwirtschaft spricht sich für eine solche Selbstverpflichtung aus. Eine "strikte und starre Regulierung" der Basismodelle sei dagegen aus zwei Gründen problematisch, sagt Ralf Wintergerst, Präsident des Branchenverbands Bitkom.</p>	https://www.tagesschau.de/wissen/technologie/ki-regulierung-eu-100.html
Wie lang die Leine für ChatGPT und Co. wird V	5	Zum einen machten es die vielfältigen Verwendungszwecke für die Anbieter dieser Art von KI unmöglich, das Risiko effektiv zu bewerten und zu vermindern. "Zweitens sind die technischen Entwicklungen gerade auf der Ebene der Modelle rasant, so dass feste Regeln im AI Act schnell überholt wären", sagt Wintergerst. Er ergänzt: "Eine verpflichtende Selbstregulierung bedeutet gerade nicht, dass es keine Regeln gibt." Die Anforderungen müssten aber praktisch umsetzbar und dynamisch anpassbar sein, keine "unnötigen Hürden durch zu starre Regeln".	https://www.tagesschau.de/wissen/technologie/ki-regulierung-eu-100.html
noch	6	<p>Ein fiktives Programm ist auf zwei Bildschirmen eines Computers zu sehen. Player: audio - Plötzlich im Datensatz. Wenn die KI mit Dir trainiert - 07.07.2023</p> <p>Künstliche Intelligenz KI-Trainingsdaten enthalten private Informationen. Doch oft sind private Daten darunter. mehr</p>	

Wie lang die Leine für ChatGPT und Co. wird VI	5	Doch einige Experten halten eine Selbstverpflichtung bei "Allzweck-KI" für nicht ausreichend. "Wenn eine Technologie so vielfältig und potentiell schädlich eingesetzt werden kann, dann fällt sie doch per Definition in eine Hochrisiko-Kategorie", sagt Technologieforscherin Sandra Wachter. Es brauche beides: Transparenz und Selbstverantwortung, aber auch klar vorgegebene Grenzen. "Das ist ein bisschen so, wie wenn man in den Supermarkt geht. Wenn ich eine Dose Suppe nehme, dann ist es wichtig, dass transparent darauf steht, welche Zutaten enthalten sind", sagt Wachter, "aber es muss auch Regeln geben, dass bestimmte Sachen eben nicht in der Suppe drin sein dürfen."	https://www.tagesschau.de/wissen/technologie/ki-regulierung-eu-100.html
KI-Trainingsdaten enthalten private Informationen - 07.07.23 I	5	Trainingsdaten sind der Rohstoff für KI-Systeme. Sie bestehen aus riesigen Mengen an Bildern und Texten aus dem Netz. Eine BR-Recherche zeigt nun: Darunter sind viele privaten Daten - ein Problem für den Datenschutz. [..] Bei der Analyse des weltweit wohl größten Trainingsdatensatzes für KI-Bildgenerierung haben BR-Datenjournalistinnen massenweise Daten gefunden, mit denen sich Personen identifizieren lassen: Gesichter und Namen, Geokoordinaten oder E-Mails, sogar Kontonummern. Der LAION5B-Datensatz, eine Abkürzung für "Large-scale Artificial Intelligence Open Network", übersetzt: "Groß angelegtes offenes Netzwerk für künstliche Intelligenz", besteht aus fünf Milliarden Links auf Bilder und ihren Beschreibungen im Internet. Er ist zugleich der einzige vergleichbare Trainingsdatensatz für KI-Modelle, der öffentlich zugänglich ist. --> siehe oben!	https://www.tagesschau.de/wissen/technologie/ki-trainingsdaten-privat-datenschutz-100.html
KI-Trainingsdaten enthalten private Informationen - 07.07.23 II	5	Problematische Daten bereits in Stichprobe KI-Trainingsdatensätze bestehen üblicherweise aus enormen Mengen an Texten und Bildern. Sie liefern den Rohstoff für KI-Systeme, die Texte und Bilder generieren, und derzeit von Millionen Menschen auf der Welt benutzt werden. Sogenannte Bildgeneratoren wie Stable Diffusion, Midjourney oder Dall-e von OpenAI funktionieren alle ähnlich: Menschen beschreiben mit kurzen Texteingaben, sogenannten Prompts, welches Motiv auf dem gewünschten Bild zu sehen sein soll. Die Programme erstellen dann mit Hilfe der Trainingsdaten ein neues Bild, oder so viele man möchte. Ende Juni 2023 reichte in den USA eine anonyme Gruppe Klage gegen das Unternehmen OpenAI ein, das unter anderem auch ChatGPT betreibt: Sie wirft der Firma unter anderem massenhafte Verletzungen der Privatsphäre vor. [..]	https://www.tagesschau.de/wissen/technologie/ki-trainingsdaten-privat-datenschutz-100.html
KI-Trainingsdaten enthalten private Informationen - 07.07.23 III	5	Ein Ergebnis der BR-Analyse: Zu 310.000 Bildverweisen im deutschsprachigen LAION-Teil konnte das Team von BR Data den exakten Aufnahmeort auslesen. Diese Exif-Daten, in denen die Ortsinformationen gespeichert sind, werden auch als "Restinformationen" bezeichnet. Sofern es keine begründeten Argumente gibt, sollen solche Daten nach Meinung des Bundesamts für Sicherheit und Informationstechnik (BSI) vernichtet werden, wenn Dateien weitergegeben werden. Datenschützer Kleinfeld: "Hochproblematisch"	https://www.tagesschau.de/wissen/technologie/ki-trainingsdaten-privat-datenschutz-100.html
KI-Trainingsdaten enthalten private Informationen - 07.07.23 IV	5	Für Eike Kleinfeld, tätig beim Hamburger Datenschutzbeauftragten, ist die massenhafte Verbreitung von Ortsinformationen aus Exif-Metadaten ein Problem, sofern es sich um sensible Informationen handelt, die einen Rückschluss auf natürliche Personen erlauben: "Die absolute Zahl ist natürlich hoch problematisch, wenn man sich vergegenwärtigt, dass da Millionen Bilder mit solchen Informationen liegen." LAION-Mitgründer Christoph Schuhmann war sich bisher des Problems nicht bewusst: "Auf das Problem werden wir jetzt das erste Mal hingewiesen", so Schuhmann gegenüber dem BR. --> Den restlichen Inhalt bitte der Quelle entnehmen.	https://www.tagesschau.de/wissen/technologie/ki-trainingsdaten-privat-datenschutz-100.html
Wie lang die Leine für ChatGPT und Co. wird VI	5	Gefahr massenhafter Desinformation Eine besondere Gefahr sieht Wachter etwa darin, dass generative KI-Modelle eingesetzt werden, um massenhaft Desinformation erzeugen. Oder auch genutzt werden, um leichter Straftaten zu begehen. "Es braucht Settings, dass man nicht so schnell herausfinden kann, wie man eine Bombe bastelt oder jemanden spurlos ermordet" , sagt Wachter. Bislang will etwa OpenAI, der Entwickler von ChatGPT, selbstständig entsprechende Antworten unterbinden. [..] Scheitern der Gesetzgebung auch denkbar <- siehe unten? Es bleibt bis zuletzt schwer absehbar, welche konkreten Regeln die EU den Entwicklern und Anwendern von Künstlicher Intelligenz auferlegt. Zuletzt wurde auch diskutiert, ob es ein abgestuftes Verfahren bei den Basismodellen geben sollte: also bestimmte Regeln nur für die größten beziehungsweise wirkmächtigsten unter ihnen. Auch ein Scheitern der Gesetzgebung sei denkbar, hieß es immer wieder.	https://www.tagesschau.de/wissen/technologie/ki-regulierung-eu-100.html

Müssen Künstler und Autoren für KI entschädigt werden I	5	<p>"Die Kosten von Intelligenz, von intelligenter Arbeit werden gegen Null tendieren. Ich hoffe, dass es so kommen wird", sagte Altman in einem Podcast.</p> <p>Der Siegeszug der Künstlichen Intelligenz könnte viele Arbeitsplätze überflüssig machen. Hinzu kommt: Derzeit bedienen sich KI-Bildgeneratoren bei Material, das sie aus allen Ecken des Internets in ihren Datenbanken speichern. Dabei nehmen sie keine Rücksicht auf Bilder, die urheberrechtlich geschützt sind.</p> <p>"Pferdekutscher fanden es auch schlecht, dass Autos automatisiert fahren konnten und man keinen Kutscher mehr brauchte. Ähnlich, wenn man jetzt Illustrator ist."</p> <p>Dass bei der KI überraschend gute Ergebnisse herauskommen, liegt daran, dass die Sprachprogramme mit Milliarden von Parametern gefüttert wurden, insbesondere auch mit den Inhalten derer, die dann von der KI ersetzt werden könnten. Unternehmen verleihen sich also das Wissen und Können der Welt ein und kopieren Stille, ohne die Kreativen dafür zu honorieren oder sie zu erwähnen.</p>	https://www.tagesschau.de/wirtschaft/digitales/kuenstliche-intelligenz-grafiker-autoren-urheberrechte-100.html
Müssen Künstler und Autoren für KI entschädigt werden II	5	<p>"Wenn dort eine neue Technologie kommt, sehe ich besonders im Silicon Valley Hunderte meiner Freunde, die sagen: Wow, wie kann ich das jetzt benutzen? Und vielleicht kann ich da ein Start-up aufmachen, was diese neue Technologie nutzt, um etwas noch produktiver zu machen, noch effizienter. In Deutschland ist die Einstellung erst erstmal: Was könnte damit schief gehen? Jobverlust? Wie müssen wir das erstmal regulieren, bevor es überhaupt richtig funktioniert?"</p> <p>Der ehemalige Journalist Michael Keusgen hat das Unternehmen Ella gegründet. Das Kölner Start-Up fütterte seine Sprachmodelle mit massenhaft Textdaten: mit Aufsätzen, Fachbüchern, aber auch mit Fiktionalem - Texte als Rohstoff. Allerdings hat Keusgen dafür die Rechte gekauft. So will er die Medienbranche revolutionieren, vor allem in Print- und Online-Redaktionen.</p> <p>Keusgens Sprachmodelle arbeiten wie alle großen KI-Programme: sie berechnen auf Basis statistischer Wahrscheinlichkeit, welches Wort oder welcher Satz als nächstes kommen könnte - und dabei kommt nicht immer Sinnvolles heraus. Die Erwartung kann also nicht sein, dass die KI immer die Wahrheit sagt, denn sie kann Fiktion nicht von der Realität unterscheiden. Die Antworten können, auch wenn sie keine Faktengrundlage haben, überzeugend wirken.</p>	https://www.tagesschau.de/wirtschaft/digitales/kuenstliche-intelligenz-grafiker-autoren-urheberrechte-100.html
<p>EU-Gesetz für Künstliche Intelligenz Mit 892 Seiten zur europäischen KI-Revolution? 02.02.24 I</p> <p>Notiz: wird die KI revolutioniert oder wird die Revolution durch die KI ausgelöst?</p>	5	<p>Kann Europa damit den Rückstand zu den US-Tech-Riesen aufholen?</p> <p>[..]</p> <p>EU-Kommissionschefin Ursula von der Leyen erklärte: "Wir hielten es von Anfang an für notwendig, auf europäischer Ebene klare Leitplanken zu setzen, um die Entwicklung und den Einsatz Künstlicher Intelligenz zu leiten. Und das ist jetzt der Gedanke hinter dem europäischen Gesetz zur Künstlichen Intelligenz."</p> <p>[..]</p> <p>"Der gefundene Kompromiss zum AI-Act legt nun das Fundament für die Entwicklung vertrauenswürdiger KI. Wir werden den maximalen Spielraum nutzen und Überregulierung vermeiden, damit unser Standort wettbewerbsfähig sein kann und die Wertschöpfung bei uns stattfindet."</p> <p>(Volker Wissing)</p> <p>KI-Basismodelle sollen Pflichten bekommen</p> <p>[..]</p>	https://www.tagesschau.de/ausland/europa/ki-gesetz-eu-100.html

<p>EU-Gesetz für Künstliche Intelligenz Mit 892 Seiten zur europäischen KI-Revolution? 02.02.24 II</p>	<p>5</p>	<p>Diese Basismodelle sollen in Europa je nach Risikoklasse bestimmte Pflichten bekommen, zum Beispiel beim Weitergeben von Informationen, bei der Risikoanalyse und beim Dokumentieren der Daten, mit denen die KI trainiert wird. --> Risikoanalyse durch KI?</p> <p>Damit dieser Ansatz nicht die Innovationskraft in Europa dämpft, sagte Wissings Parteikollegin Svenja Hahn, die den KI-Act im EU-Parlament über Jahre mitverhandelt hat, sei jetzt entscheidend: "...dass offene Fragen geklärt werden, zum Beispiel Wie funktioniert denn die Einstufung von Basismodellen in das Risikosystem in der Praxis - nach welchen Kriterien soll das erfolgen."</p> <p>Das war vor 3 Monaten, nach 2 Jahren Verhandlung in einem 892 Seiten starken Dokument unter den 28 Mitgliedsstaaten. Die Einstufung der Modelle nach Risikostufen ist weiterhin nicht festgelegt.</p> <p>Auch bei KI in der Strafverfolgung müsse die Kommission jetzt für Klarheit sorgen, damit durch unterschiedliche nationale Auslegungen eben keine Gesetzeslücken entstünden.</p>	<p>https://www.tagesschau.de/ausland/europa/ki-gesetz-eu-100.html</p>
<p>Mit 892 Seiten zur europäischen KI-Revolution? 02.02.24</p>	<p>5</p>	<p>Mit den USA und China mithalten Franziska Teubert, Geschäftsführerin des deutschen Start-up-Verbands, atmet auf, wenn der EU die endgültigen Verabschiedung des KI-Act gelingt. Denn mehr als auf jede Zeile komme es nun auf Tempo an:</p> <p>Gesetzestexte werden auch völlig überbewertet.</p> <p>"Die Regulierung ist nicht perfekt, aber man kann damit arbeiten. Regulierung schafft auch Verlässlichkeit für Unternehmen und Investoren. Eine fehlende EU-weite Regulierung hätte uns nur Flickenteppiche geliefert. 27 Einzellösungen in 27 Mitgliedstaaten."</p> <p>Jetzt, so ihr Appell, soll es endlich in die Umsetzung gehen: "Um mit den USA und China mithalten zu können, brauchen wir europäische KI-Champions, und wir müssen Sie langfristig weniger in einzelnen Ländern denken und stärker europäisch handeln."</p> <p>Yummy, der gute alte internationale Wettbewerb zwischen künstlichen Superintelligenzen kann bald losgehen.</p>	<p>https://artificialintelligenceact.eu/de/annex/3/</p>
<p>Mit 892 Seiten zur europäischen KI-Revolution? 02.02.24</p>	<p>5</p>	<p>KI-Modelle trainieren und testen</p> <p>Eine Linie, die auch Kommissionschefin von der Leyen vorgibt: KI-Startups und Mittelständler sollen nun Zugang zu Supercomputern der EU bekommen, also zu den nötigen Kapazitäten, um ihre KI-Modell zu trainieren, zu entwickeln und testen zu können:</p> <p>--> Startups und Mittelständler sollen KI-Basismodelle erstellen können?</p> <p>"Dies ähnelt dem, was Microsoft für Chat-GPT tut, indem es sie auf seine eigenen Supercomputern lässt. Wir werden auch gemeinsame europäische Datenräume in den Dienst von Start-ups stellen und riesige Datenmengen in allen EU-Sprachen zur Verfügung stellen, damit die KI auch für Nicht-Englisch-Sprecher funktioniert."</p> <p>All das sind nächste konkrete Schritte zur Weiterentwicklung einer europäisch geprägten KI. Und die Ambition, Dinge zu greifen, die man sich in Teilen noch gar nicht so recht vorstellen kann.</p>	<p>https://artificialintelligenceact.eu/de/annex/3/</p>
<p>Gemeinsam in Richtung Verteidigung I Stand: 26.04.2024 18:28 Uhr</p>	<p>5</p>	<p>Boris Pistorius und Sébastien Lecornu geben sich die Hand. Deutsch-französischer Kampfpanzer Gemeinsam in Richtung Verteidigung</p> <p>Nach jahrelangen Verhandlungen haben sich Deutschland und Frankreich auf den Bau eines gemeinsamen Kampfpanzersystems verständigt. Ein wichtiger Schritt für die beiden Länder und dieses Mal soll einiges anders ablaufen. Von Julia Borutta, ARD Paris</p> <p>Geradezu gelöst traten Verteidigungsminister Boris Pistorius und sein französischer Kollege Sébastien Lecornu vor die Presse. In flüssigem Französisch dankte Pistorius "dem lieben" Sébastien, bei diesem schwierigen Panzerprojekt immer wieder den direkten Draht zu ihm gesucht und auf diese Weise Lösungen gefunden zu haben. Frankreich und Deutschland hätten große Ambitionen, so Pistorius und das Kampfpanzersystem Main Ground Combat System (MGCS) stehe genau dafür.</p>	<p>https://www.tagesschau.de/ausland/europa/kampfpanzer-deutschland-frankreich-100.html</p>

Gemeinsam in Richtung Verteidigung II Stand: 26.04.2024 18:28 Uhr		<p>"Es geht um etwas völlig Neues", erklärte der Minister. Das MGCS ermögliche miteinander vernetzte Gefechtsfahrzeuge, die teilweise auch unbemannt miteinander kooperieren können. Außerdem autonomes taktisches Navigieren, eine robuste Cloud-Umgebung und resiliente, digitale Automatisierung. Künstliche Intelligenz werde ebenfalls dazu beitragen, "dass wir mit MGCS einen deutlichen qualitativen Fähigkeitsvorsprung für die Landes- und Bündnisverteidigung erreichen." [..]</p> <p>Künstliche Intelligenz werde ebenfalls dazu beitragen, "dass wir mit MGCS einen deutlichen qualitativen Fähigkeitsvorsprung für die Landes- und Bündnisverteidigung erreichen."</p>	https://www.tagesschau.de/ausland/europa/kampfpanzer-deutschland-frankreich-100.html
Gemeinsam in Richtung Verteidigung III Stand: 26.04.2024 18:28 Uhr		<p>Staat als Auftraggeber Sein Partner, der französische Verteidigungsminister Sébastien Lecornu, sagte es so: "Es geht nicht so sehr um den Panzer der Zukunft, sondern um die Zukunft des Panzers." Der Kern dieser Absichtserklärung sei, "dass wir 2040 einen gemeinsamen Panzer haben. Denn wir haben im Großen und Ganzen die gleichen Gegner und müssen gemeinsam trainieren." --> Deutschland und Frankreich haben gemeinsame Gegner? --> Wer könnte damit gemeint sein?</p> <p>Pistorius und Lecornu betonten, dass der Staat - anders als bei anderen Projekten - beim MGCS ganz klar als Auftraggeber auftrete und sich die Industrie entsprechend anzupassen habe. Das sei eine Lehre, die man aus den schwierigen Verhandlungen um das Luftkampfsystem FCAS gezogen habe.</p>	https://www.tagesschau.de/ausland/europa/kampfpanzer-deutschland-frankreich-100.html
Gemeinsam in Richtung Verteidigung IV Stand: 26.04.2024 18:28 Uhr		Der Schwung, den beide Minister heute zur Schau stellten, rührte vielleicht auch aus der Erleichterung, dieses schwierige Projekt endlich auf die Schiene gesetzt zu haben. Jahrelang konnte man sich nicht einigen.	https://www.tagesschau.de/ausland/europa/kampfpanzer-deutschland-frankreich-100.html
Gemeinsam in Richtung Verteidigung V Stand: 26.04.2024 18:28 Uhr		<p>[..] Nun also will man an einem Strang ziehen. Gleich zweimal bezog sich Pistorius auf die gestrige Europa-Rede Emmanuel Macrons an der Sorbonne-Universität und unterstützte seine Vision einer starken, wehrfähigen EU: "Wir brauchen ein europäisches Verständnis von Rüstungsindustrie." [..] Ende des Jahres soll der endgültige Vertrag fertig sein. 2025 werden die Parlamente über das Projekt abstimmen, damit der Panzer, so das Ziel, 2040 einsatzbereit ist.</p>	https://www.tagesschau.de/ausland/europa/kampfpanzer-deutschland-frankreich-100.html
AI-Act Entwurf 17.04.24 BERICHTIGUNG des in erster Lesung am 13. März 2024 festgelegten Standpunkts des Europäischen Parlaments im Hinblick auf den Erlass der Verordnung (EU) 2024/ [..] (Auszüge)	5	Diese Verordnung sollte die in einer Richtlinie {--> welche} des Europäischen Parlaments und des Rates zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit enthaltenen Bestimmungen nicht berühren. Darüber hinaus zielt diese Verordnung darauf ab, die Wirksamkeit dieser bestehenden Rechte und Rechtsbehelfe zu stärken, indem bestimmte Anforderungen und Pflichten, auch in Bezug auf die Transparenz, die technische Dokumentation und das Führen von Aufzeichnungen von KI-Systemen, festgelegt werden.	https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf
AI-Act Entwurf 17.04.24 BERICHTIGUNG des in erster Lesung am 13. März 2024 festgelegten Standpunkts des Europäischen Parlaments im Hinblick auf den Erlass der Verordnung (EU) 2024/ [..] (Auszüge)	5	Ferner sollten die in dieser Verordnung festgelegten Pflichten der verschiedenen Akteure, die an der KI-Wertschöpfungskette beteiligt sind, unbeschadet der nationalen Rechtsvorschriften unter Einhaltung des Unionsrechts angewandt werden, wodurch die Verwendung bestimmter KI-Systeme begrenzt wird, wenn diese Rechtsvorschriften nicht in den Anwendungsbereich dieser Verordnung fallen oder mit ihnen andere legitime Ziele des öffentlichen Interesses verfolgt werden als in dieser Verordnung.	https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf

<p>AI-Act Entwurf 17.04.24</p> <p>BERICHTIGUNG des in erster Lesung am 13. März 2024 festgelegten Standpunkts des Europäischen Parlaments im Hinblick auf den Erlass der Verordnung (EU) 2024/ [...]</p> <p>(Auszüge)</p>	5	<p>So sollten {--> überaus möglich, das hier müssen stehen muss} etwa die nationalen arbeitsrechtlichen Vorschriften und die Rechtsvorschriften zum Schutz Minderjähriger, nämlich Personen unter 18 Jahren, unter Berücksichtigung der Allgemeinen Bemerkung Nr. 25 (2021) des UNCRC über die Rechte der Kinder im digitalen Umfeld von dieser Verordnung unberührt bleiben, sofern sie nicht spezifisch KI-Systeme betreffen und mit ihnen andere legitime Ziele des öffentlichen Interesses verfolgt werden.</p> <p>--> In dem AI-Act steht nach meinem Ermessen ein bisschen zu oft das Wort "sollte".</p>	<p>https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf</p>
<p>AI-Act Entwurf 17.04.24</p> <p>BERICHTIGUNG des in erster Lesung am 13. März 2024 festgelegten Standpunkts des Europäischen Parlaments im Hinblick auf den Erlass der Verordnung (EU) 2024/ [...]</p> <p>(Auszüge)</p>	5	<p>in Erwägung nachstehender Gründe:</p> <p>(1) Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern, indem ein einheitlicher Rechtsrahmen insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme) in der Union im Einklang mit den Werten der Union festgelegt wird, um die Einführung von menschenzentrierter und vertrauenswürdiger künstlicher Intelligenz (KI) zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und der in der Charta der Grundrechte der Europäischen Union („Charta“) verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, sicherzustellen, den Schutz vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und gleichzeitig die Innovation zu unterstützen.</p>	<p>https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf</p>
<p>AI-Act Entwurf 17.04.24</p> <p>BERICHTIGUNG des in erster Lesung am 13. März 2024 festgelegten Standpunkts des Europäischen Parlaments im Hinblick auf den Erlass der Verordnung (EU) 2024/ [...]</p> <p>(Auszüge)</p>	5	<p>Diese Verordnung gewährleistet den grenzüberschreitenden freien Verkehr KI-gestützter Waren und Dienstleistungen, wodurch verhindert wird, dass die Mitgliedstaaten die Entwicklung, Vermarktung und Verwendung von KI-Systemen beschränken, sofern dies nicht ausdrücklich durch diese Verordnung erlaubt wird.</p> <p>Diese Verordnung sollte im Einklang mit den in der Charta verankerten Werten der Union angewandt werden, den Schutz von natürlichen Personen, Unternehmen, Demokratie und Rechtsstaatlichkeit sowie der Umwelt erleichtern und gleichzeitig Innovation und Beschäftigung fördern und der Union eine Führungsrolle bei der Einführung vertrauenswürdiger KI verschaffen.</p>	<p>https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf</p>
<p>AI-Act Entwurf 17.04.24</p> <p>BERICHTIGUNG des in erster Lesung am 13. März 2024 festgelegten Standpunkts des Europäischen Parlaments im Hinblick auf den Erlass der Verordnung (EU) 2024/ [...]</p> <p>(Auszüge)</p>	5	<p>Absatz 24</p> <p>Wenn und soweit KI-Systeme mit oder ohne Änderungen für Zwecke in den Bereichen Militär, Verteidigung oder nationale Sicherheit in Verkehr gebracht, in Betrieb genommen oder verwendet werden, sollten sie vom Anwendungsbereich dieser Verordnung ausgenommen werden, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt, etwa ob es sich um eine öffentliche oder private Einrichtung {--> eine private Einrichtung im Bereich Militär, Verteidigung oder nationale Sicherheit} handelt</p> <p>Die Frage ist doch dann, welches Regelwerk dann das Militär reguliert?</p>	<p>https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_DE.pdf</p>

Endgültiger Entwurf (2024)	5	<p>Die 27 EU-Mitgliedsstaaten haben die AI-Akte einstimmig gebilligt und damit die im Dezember erzielte politische Einigung bekräftigt. Auch der Ausschuss für Binnenmarkt und bürgerliche Freiheiten des Europäischen Parlaments stimmte mit 71:8 Stimmen (7 Enthaltungen) für das Ergebnis der Verhandlungen mit den Mitgliedstaaten über die AI-Akte. [..]</p> <p>Alternativ können Sie den vollständigen Text des endgültigen Entwurfs in einem PDF-Dokument einsehen. Bei den unten verlinkten Dokumenten handelt es sich um die neueste Version des AI-Gesetzes: Korrigendum" des Europäischen Parlaments vom 16. April 2024, mit dem Fehler in Sprache und Nummerierung in früheren Entwürfen korrigiert wurden.</p> <p>--> Der Hyperlink zur deutschen Version verweist jedoch auf den Entwurf vom 17.04.24 (Stand 07.05.24, 22:58)</p>	https://artificialintelligenceact.eu/de/das-gesetz/
Zusammenfassung des AI-Gesetzes auf hoher Ebene I	5	<p>Vier-Punkte-Zusammenfassung</p> <p>Das KI-Gesetz stuft KI nach ihrem Risiko ein:</p> <p>Unannehmable Risiken sind verboten (z. B. soziale Bewertungssysteme und manipulative KI). Der größte Teil des Textes befasst sich mit KI-Systemen mit hohem Risiko, die reguliert sind.</p> <p>Ein kleinerer Teil befasst sich mit KI-Systemen mit begrenztem Risiko, für die geringere Transparenzpflichten gelten: Entwickler und Betreiber müssen sicherstellen, dass die Endnutzer wissen, dass sie mit KI interagieren (Chatbots und Deepfakes). --> KI-Chatbots und Deepfakes werden als Systeme mit begrenztem Risiko eingestuft?</p>	https://artificialintelligenceact.eu/de/high-level-summary/
Zusammenfassung des AI-Gesetzes auf hoher Ebene II	5	<p>Das geringste Risiko ist unreguliert (einschließlich der meisten KI-Anwendungen, die derzeit auf dem EU-Binnenmarkt erhältlich sind, wie z. B. KI-gestützte Videospiele und Spam-Filter - zumindest im Jahr 2021; dies ändert sich mit der generativen KI).</p> <p>Die meisten Verpflichtungen treffen die Anbieter (Entwickler) von risikoreichen KI-Systemen.</p> <p>Diejenigen, die beabsichtigen, hochriskante KI-Systeme in der EU in Verkehr zu bringen oder in Betrieb zu nehmen, unabhängig davon, ob sie in der EU oder in einem Drittland ansässig sind. Und auch Anbieter aus Drittländern, bei denen der Output des Hochrisiko-KI-Systems in der EU verwendet wird.</p>	https://artificialintelligenceact.eu/de/high-level-summary/
Zusammenfassung des AI-Gesetzes auf hoher Ebene III	5	<p>Die Nutzer (Anwender) von KI-Systemen mit hohem Risiko haben einige Verpflichtungen, wenn auch weniger als die Anbieter (Entwickler).</p> <p>Dies gilt für Nutzer in der EU und für Nutzer in Drittländern, wenn der Output des KI-Systems in der EU verwendet wird.</p>	https://artificialintelligenceact.eu/de/high-level-summary/
Anhang III: Hochriskante AI-Systeme 02.05.24	5	<p>[..]</p> <p>(d) KI-Systeme, die für die Risikobewertung und Preisgestaltung in Bezug auf natürliche Personen im Falle von Lebens- und Krankenversicherungen verwendet werden sollen;</p> <p>(c) KI-Systeme, die dazu bestimmt sind, Notrufe natürlicher Personen auszuwerten und zu klassifizieren oder zur Disposition oder zur Festlegung von Prioritäten bei der Disposition von Notdiensten, einschließlich Polizei, Feuerwehr und medizinischer Hilfe, sowie von Triage-Systemen für Notfallpatienten verwendet werden.</p> <p>6. Strafverfolgung, soweit ihre Verwendung nach dem einschlägigen Unionsrecht oder dem nationalen Recht zulässig ist:</p> <p>(a) KI-Systeme, die dazu bestimmt sind, von oder im Namen von Strafverfolgungsbehörden oder von Organen, Einrichtungen, Ämtern oder Agenturen der Union zur Unterstützung von Strafverfolgungsbehörden oder in deren Namen verwendet zu werden, um das Risiko zu bewerten, dass eine natürliche Person Opfer einer Straftat wird;</p>	https://artificialintelligenceact.eu/de/annex/3/

Anhang III: Hochriskante AI-Systeme 02.05.24	5	<p>(b) KI-Systeme, die dazu bestimmt sind, von oder im Namen von Strafverfolgungsbehörden oder von Organen, Einrichtungen, Ämtern oder Agenturen der Union zur Unterstützung von Strafverfolgungsbehörden als Lügendetektoren oder ähnliche Instrumente verwendet zu werden;</p> <p>(c) KI-Systeme, die dazu bestimmt sind, von oder im Namen von Strafverfolgungsbehörden oder von Organen, Einrichtungen, Ämtern oder Agenturen der Union zur Unterstützung von Strafverfolgungsbehörden verwendet zu werden, um die Verlässlichkeit von Beweismitteln im Rahmen der Ermittlung oder Verfolgung von Straftaten zu bewerten; --> KI-Lügendetektoren, Beweismittel-bewertung (-überprüfung?)</p>	https://artificialintelligenceact.eu/de/annex/3/
Anhang III: Hochriskante AI-Systeme 02.05.24	5	<p>(d) KI-Systeme, die dazu bestimmt sind, von Strafverfolgungsbehörden oder in deren Auftrag oder von Organen, Einrichtungen, Ämtern oder Agenturen der Union zur Unterstützung von Strafverfolgungsbehörden verwendet zu werden, um das Risiko einer natürlichen Person, straffällig zu werden oder erneut straffällig zu werden, nicht ausschließlich auf der Grundlage der Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 zu bewerten, oder um Persönlichkeitsmerkmale und Eigenschaften oder frühere kriminelle Verhaltensweisen natürlicher Personen oder Gruppen zu bewerten; --> KI-Systeme könnten die Aufgabe von {den Job gibt es eigentlich nur bei Geheimdiensten?} bzw. Staatsanwälten oder Richtern übernehmen?</p> <p>(e) KI-Systeme, die von oder im Namen von Strafverfolgungsbehörden oder von Organen, Einrichtungen, Ämtern oder Agenturen der Union zur Unterstützung von Strafverfolgungsbehörden für die Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 im Rahmen der Aufdeckung, Untersuchung oder Verfolgung von Straftaten verwendet werden sollen.</p>	https://artificialintelligenceact.eu/de/annex/3/
Anhang III: Hochriskante AI-Systeme 02.05.24	5	<p>7. Migrations-, Asyl- und Grenzkontrollmanagement, soweit deren Einsatz nach dem einschlägigen Unionsrecht oder nationalen Recht zulässig ist:</p> <p>(a) KI-Systeme, die dazu bestimmt sind, von oder im Namen von zuständigen Behörden oder von Organen, Einrichtungen, Ämtern oder Agenturen der Union als Lügendetektoren oder ähnliche Instrumente verwendet zu werden; --> Lügendetektoren im Kontext der Migration?</p>	https://artificialintelligenceact.eu/de/annex/3/
Anhang III: Hochriskante AI-Systeme 02.05.24	5	<p>(b) KI-Systeme, die dazu bestimmt sind, von oder im Namen von zuständigen Behörden oder von Organen, Einrichtungen, Ämtern oder Agenturen der Union verwendet zu werden, um ein Risiko, einschließlich eines Sicherheitsrisikos, eines Risikos der irregulären Migration oder eines Gesundheitsrisikos, zu bewerten, das von einer natürlichen Person ausgeht, die in das Hoheitsgebiet eines Mitgliedstaats einzureisen beabsichtigt oder eingereist ist; --> Terrorismusbekämpfung</p>	https://artificialintelligenceact.eu/de/annex/3/
Anhang III: Hochriskante AI-Systeme 02.05.24	5	<p>(c) KI-Systeme, die dazu bestimmt sind, von oder im Namen von zuständigen Behörden oder von Organen, Einrichtungen, Ämtern oder Agenturen der Union verwendet zu werden, um die zuständigen Behörden bei der Prüfung von Anträgen auf Asyl, Visa oder Aufenthaltstitel und bei damit zusammenhängenden Beschwerden in Bezug auf die Berechtigung der natürlichen Personen, die einen Status beantragen, zu unterstützen, einschließlich der damit zusammenhängenden Bewertung der Zuverlässigkeit von Beweismitteln;</p>	https://artificialintelligenceact.eu/de/annex/3/
Anhang III: Hochriskante AI-Systeme 02.05.24	5	<p>(d) KI-Systeme, die dazu bestimmt sind, von oder im Namen von zuständigen Behörden oder von Organen, Einrichtungen, Ämtern oder Agenturen der Union im Rahmen des Migrations-, Asyl- oder Grenzkontrollmanagements zum Aufspüren, Erkennen oder Identifizieren natürlicher Personen verwendet zu werden, mit Ausnahme der Überprüfung von Reisedokumenten. --> Verfolgung von nicht straffälligen Personen?</p>	https://artificialintelligenceact.eu/de/annex/3/
Anhang III: Hochriskante AI-Systeme 02.05.24	5	<p>8. (a) KI-Systeme, die dazu bestimmt sind, von einer Justizbehörde oder in deren Auftrag eingesetzt zu werden, um eine Justizbehörde bei der Erforschung und Auslegung von Tatsachen und Gesetzen und bei der Anwendung des Rechts auf einen konkreten Sachverhalt zu unterstützen, oder die in ähnlicher Weise bei der alternativen Streitbeilegung eingesetzt werden sollen; --> Rechtliche Grauzonen / Präzedenzfälle</p>	https://artificialintelligenceact.eu/de/annex/3/
Anhang III: Hochriskante AI-Systeme 02.05.24	5	<p>(b) KI-Systeme, die zur Beeinflussung des Ergebnisses einer Wahl oder eines Referendums oder des Abstimmungsverhaltens natürlicher Personen bei der Ausübung ihres Stimmrechts bei Wahlen oder Referenden eingesetzt werden sollen. Dies schließt keine KI-Systeme ein, deren Ergebnisse natürlichen Personen nicht direkt zugänglich sind, wie etwa Werkzeuge, die zur Organisation, Optimierung oder Strukturierung politischer Kampagnen unter administrativen oder logistischen Gesichtspunkten eingesetzt werden. --> Wahlmanipulation</p>	https://artificialintelligenceact.eu/de/annex/3/
Artikel 15: Genauigkeit, Robustheit und Cybersicherheit	5	<p>1. KI-Systeme mit hohem Risiko sind so zu konzipieren und zu entwickeln, dass sie ein angemessenes Niveau an Genauigkeit, Robustheit und Cybersicherheit erreichen und während ihres gesamten Lebenszyklus in dieser Hinsicht konsistent funktionieren. -> in wie fern angemessen? --> s.u. angemessen im Verhältnis zum ermittelten Risiko, unten bezieht sich aber nur auf die Einwirkung von Dritten, nicht auf das Risiko, dass durch das System selbst entsteht.</p>	https://artificialintelligenceact.eu/de/article/15/

	5	2. Um die technischen Aspekte der Messung des in Absatz 1 genannten angemessenen Genauigkeits- und Robustheitsniveaus und anderer relevanter Leistungsindikatoren zu behandeln, fördert die Kommission in Zusammenarbeit mit den einschlägigen Interessengruppen und Organisationen wie Metrologie- und Benchmarking-Behörden gegebenenfalls die Entwicklung von Benchmarks und Messmethoden.	https://artificialintelligenceact.eu/de/article/15/
	5	3. Die Genauigkeitsgrade und die relevanten Genauigkeitsmetriken von KI-Systemen mit hohem Risiko sind in der beiliegenden Gebrauchsanweisung anzugeben. --> fair enough	https://artificialintelligenceact.eu/de/article/15/
	5	4. KI-Systeme mit hohem Risiko müssen so widerstandsfähig wie möglich gegenüber Fehlern, Störungen oder Unstimmigkeiten sein, die innerhalb des Systems oder der Umgebung, in der das System betrieben wird, auftreten können, insbesondere aufgrund ihrer Interaktion mit natürlichen Personen oder anderen Systemen. Zu diesem Zweck sind technische und organisatorische Maßnahmen zu treffen. --> müssen	https://artificialintelligenceact.eu/de/article/15/
	5	Die Robustheit von KI-Systemen mit hohem Risiko kann durch technische Redundanzlösungen erreicht werden, die Backup- oder Fail-Safe-Pläne umfassen können.	https://artificialintelligenceact.eu/de/article/15/
	5	KI-Systeme mit hohem Risiko, die nach dem Inverkehrbringen oder der Inbetriebnahme weiter lernen, sind so zu entwickeln, dass das Risiko, dass möglicherweise verzerrte Ergebnisse den Input für künftige Operationen beeinflussen (Rückkopplungsschleifen), beseitigt oder so weit wie möglich verringert wird, und dass sichergestellt wird, dass solche Rückkopplungsschleifen durch geeignete Abhilfemaßnahmen angemessen berücksichtigt werden. --> Den Job möchte ich nicht haben.	https://artificialintelligenceact.eu/de/article/15/
	5	5. KI-Systeme mit hohem Risiko müssen gegen Versuche unbefugter Dritter, ihre Nutzung, ihre Ergebnisse oder ihre Leistung durch Ausnutzung von Systemschwachstellen zu verändern, widerstandsfähig sein. Die technischen Lösungen, die die Cybersicherheit von KI-Systemen mit hohem Risiko gewährleisten sollen, müssen den jeweiligen Umständen und Risiken angemessen sein. --> müssen	https://artificialintelligenceact.eu/de/article/15/
	5	Die technischen Lösungen zur Behebung von KI-spezifischen Schwachstellen umfassen gegebenenfalls Maßnahmen zur Verhinderung, Erkennung, Reaktion, Behebung und Kontrolle von Angriffen, die darauf abzielen, den Trainingsdatensatz (Data Poisoning) oder bereits trainierte Komponenten, die beim Training verwendet werden (Model Poisoning), zu manipulieren, Eingaben, die das KI-Modell zu einem Fehler veranlassen sollen (gegnerische Beispiele oder Modellumgehung), sowie Angriffe auf die Vertraulichkeit oder Modellfehler. --> gegebenenfalls??	https://artificialintelligenceact.eu/de/article/15/

tbc..