Enquete-Kommission
Künstliche Intelligenz

Deutscher Bundestag

Deutscher Bundestag
Enquete-Kommission
Künstliche Intelligenz
Kommissionsdrucksache
19(27)93

19.12.2019

Projektgruppe „KI und Staat“

Zusammenfassung der vorläufigen Ergebnisse*
Stand: 18. Dezember 2019

Die Projektgruppe „KI und Staat“ hat sich mit staatlichem Einsatz von Künstlicher Intelligenz (KI) vor allem im Hinblick auf Verwaltung, Smart City und Open Data, Innere Sicherheit, Äußere Sicherheit und IT-Sicherheit befasst.

Aufgrund der breiten Anwendungsbereiche und der hohen Bedeutung einer ausführlichen Debatte und vielseitigen Betrachtung von KI durch den Staat hat sich die Projektgruppe in drei Arbeitsgruppen (AGen) gegliedert. Die AGen haben gemeinsam unterschiedliche Themenblöcke, die jeweils den staatlichen Einsatz von KI betreffen, bearbeitet:

- AG 1: KI in der öffentlichen Verwaltung, gemeinwohlorientierte Anwendungen, Teilhabe
- AG 2: Smart City und Open Data
- AG 3: Innere Sicherheit, Äußere Sicherheit/Verteidigung/Militär, IT-Sicherheit

Während der Bearbeitung und Debatte der drei Themenblöcke hat die Projektgruppe festgestellt, dass es für alle drei Bereiche stets wiederkehrende Empfehlungen gibt, wie der Staat KI-Systeme planen, einsetzen und evaluieren sollte. Diese Empfehlungen berücksichtigen, dass der Staat insbesondere bei der Nutzung von teilhaberelevanten KI-Systemen aufgrund seiner hoheitlichen Aufgaben einer besonderen Sorgfaltspflicht unterliegt, wenn die Entscheidung für den Einsatz von KI-Systemen getroffen wird und Anforderungen an Transparenz- und Nachvollziehbarkeit erfüllt sein müssen. Damit wird ein informierter Umgang ermöglicht, es können Anpassungen vor dem Hintergrund gesellschaftlicher Werte und Normen sowie eine Wahlfreiheit für Bürgerinnen und Bürger entstehen. Das gilt insbesondere dann, wenn ein KI-System in der entscheidungsvorbereitenden oder Entscheidungsphase angewendet wird.

Im Ergebnis enthält dieser Bericht einen umfassenden Katalog an themenübergreifenden Handlungsempfehlungen und darüber hinaus einzelne AG-spezifische Handlungsempfehlungen.

Zu den wichtigsten Handlungsempfehlungen für alle AGen gehören:

Systematische Identifizierung von Einsatzgebieten für KI

Behörden sollten den Einsatz von KI-Systemen für Verwaltungsvorgänge bzw. Prozesse systematisch prüfen. In den Ministerien des Bundes sollten ein Monitoring und ein strukturierter Erfahrungsaustausch unter den KI-einsetzenden Behörden stattfinden.

* Diese Zusammenfassung spiegelt die Position der Mehrheit der Projektgruppenmitglieder wider, Sondervoten werden erst im Rahmen des Abschlussberichtes eingebracht.

Kompetenzen aufbauen

Es sollte Ziel sein, möglichst vielen Verwaltungsmitarbeiterinnen und -mitarbeitern ein Verständnis für die Funktionsweisen, Vorteile und Herausforderungen von KI-Systemen und mögliche Risiken in Bezug auf unerwünschte Diskriminierung aufzuzeigen. Bereits die Verwaltungsausbildung und das Studium für angehende Verwaltungsmitarbeiterinnen und -mitarbeiter müssen ein breites Wissensprofil zu Digitalisierung und KI- Systemen vermitteln.

Transparenz schaffen und Risiken systematisch klassifizieren

Für staatlich genutzte KI-Systeme, die auf einem durch Methoden des maschinellen Lernens gelernten, statistischen Modell basieren, ist immer eine Risikoklassifikation durchzuführen. Basierend auf der Risikoklassifikation sind die entsprechenden Transparenz- und Nachvollziehbarkeitsforderungen zu bestimmen.

KI-gestützte Entscheidungen regelmäßig auf Diskriminierungsfreiheit überprüfen

Es muss sichergestellt werden, dass staatlich entwickelte und genutzte KI-Systeme in ihrer Nutzung (unter Umständen also in Zusammenwirkung mit menschlichen Entscheiderinnen und Entscheidern) nicht diskriminieren.

Partizipation fördern

Behörden sollten beim Einsatz von KI-Systemen durch die Verwaltung einen partizipativen, bürgernahen Ansatz verfolgen. Die Gesellschaft sollte jedenfalls dann immer einbezogen werden, wenn Einzelne in Grundrechten berührt werden könnten. Darüber hinaus ist es notwendig, die Bevölkerung breit und umfänglicher zu KI aufzuklären, damit die Menschen verstehen und erkennen können, welche Vor- und Nachteile spezifische Anwendungen haben.

<u>AG 1: KI in der Verwaltung und internationale Vorbilder</u>

Die AG 1 befasste sich im Schwerpunkt mit Fragen der Beschaffung und des Einsatzes von KI-Systemen und Algorithmischen Entscheidungssystemen (ADM-Systemen) im administrativen Bereich. Welche Vorbilder und Potenziale gibt es für die Verwendung von KI in der öffentlichen Verwaltung und bei der Erbringung öffentlicher Dienstleistungen? Wie können Widerspruchs-, Antrags- und Formularverfahren mithilfe von KI automatisiert werden? Welche gemeinwohlorientierten Anwendungen lassen sich auf Grundlage von KI durch den Staat oder mittels staatlicher Förderung (Social Innovation Fonds, smarte Antragsstellung und Bearbeitung) entwickeln? Des Weiteren untersuchte die AG, wie eine bessere Partizipation und Teilhabe von Bürgerinnen und Bürgern durch und mit KI gelingen können und wie sie sich im Einsatzprozess von KI einbringen können. Dabei wurde auch in den Blick genommen, welche Anwendungen und Projekte es hierzulande bereits gibt, welche internationalen Anwendungen und Konzepte bei der Digitalisierung der Verwaltung als Vorbild dienen können und wie Deutschland gezielt von diesen Vorbildern lernen kann.

Die AG konzentrierte sich bei ihrer Untersuchung vor allem auf die Potenziale, die der Einsatz von KI für Verwaltung und Gesellschaft bietet, leitete daraus Empfehlungen für den Umgang mit der Technologie ab und definierte Leitlinien für den Einsatz von KI-Systemen in der Verwaltung.

Einigkeit bestand in der Projektgruppe darüber, dass KI-Anwendungen in der öffentlichen Verwaltung stets am Menschen orientiert sein und auf Basis der Verwaltungsprinzipien erfolgen müssen. Für Bürgerinnen und Bürger muss transparent und nachvollziehbar sein, bei welchen Verwaltungsvorgängen KI-Systeme eingesetzt werden, insbesondere dann, wenn KI-Systeme in der entscheidungsvorbereitenden oder Entscheidungsphase angewendet werden. Lernende künstliche Systeme dürfen jedoch keine Ermessens- oder Beurteilungsspielräume füllen. Die Unabhängigkeit von Drittanbieter-Plattformen ist anzustreben.

Es wurde festgestellt, dass Digitalisierung und Automatisierung in der öffentlichen Verwaltung Vorteile für Bürgerinnen und Bürger, Zivilgesellschaft, Organisationen und Unternehmen ebenso wie für die Verwaltungsmitarbeiterinnen und -mitarbeiter ermöglichen. So können Assistenzsysteme dabei eine deutliche Steigerung von Qualität und Effizienz von Verwaltungsvorgängen bewirken und die Daseinsvorsorge stärken. Sie können Anfrageprozesse und Bearbeitungsvorgänge transparenter und schneller machen, Verwaltungsentscheidungen unterstützen und eine höhere Bürgerzufriedenheit ermöglichen. Durch die Entlastung der Mitarbeiterinnen und Mitarbeiter von monotonen Aufgaben und hin zu mehr individueller und persönlicher Beratung kann sich ihr Aufgabenbereich verschieben. Ein weiterer gesellschaftlicher Vorteil des Einsatzes von KI in der Verwaltung kann bei einer Kostenersparnis liegen.

Es werden Qualitätskriterien benötigt, nach denen eine kontinuierliche Evaluation von KI-Systemen möglich ist und nach denen über den staatlichen Einsatz von KI-Systemen entschieden wird. Es bestand Dissens darüber, ob KI-Systeme der höchsten Risikoklasse eingesetzt werden dürfen.

Auch für die Verwaltung gilt, dass es bei den Anforderungen an die Transparenz und Nachvollziehbarkeit von KI-Systemen ebenso wie bei der Vermeidung von Diskriminierung in erheblichem Maße auf die Qualität und die Integrität der eingesetzten Daten und ihrer Struktur ankommt. Möglichst vollständige und durchgehende Open-Data-Bestände sind dafür eine Voraussetzung. Durch eine einheitliche Open-Data-Plattform werden sowohl personelle Ressourcen effizienter eingesetzt als auch leistungsfähigere KI-basierte Algorithmen und Analysen ermöglicht.

Der Staat kann darüber hinaus als innovativer Treiber für die Entwicklung gemeinwohlorientierter KI-Systeme agieren. Die Einrichtung eines Social Innovation Fonds hat auch für den Bereich Verwaltung das Potenzial, die Entwicklung gemeinwohlorientierter Lösungen zu ermöglichen.

Die Projektgruppe ist der Ansicht, dass die Zivilgesellschaft von mehr Transparenz des Verwaltungshandelns, vereinfachter Partizipation und auch von einer höheren Teilhabe durch einen barrierefreieren und schnelleren Zugang zu Informationen, Angeboten und Leistungen der öffentlichen Verwaltung profitieren kann und empfiehlt weitere Pilotprojekte von KI in der Verwaltung.

Die Projektgruppe empfiehlt im Besonderen, dass KI-Systeme in der Verwaltung für teilhaberelevante KI-Anwendungen genutzt werden. Im Mittelpunkt sollen dabei insbesondere sprachlich barrierefreie Angebote stehen, die Verringerung von Zugangshürden, die Beschleunigung von Verwaltungsprozessen sowie die Entlastung von Verwaltungsmitarbeiterinnen und -mitarbeitern.

Weiterhin empfiehlt die Projektgruppe einen Rechtsanspruch auf Widerspruch gegen KI-Empfehlungen in Verwaltungsprozessen, sodass Bürgerinnen und Bürger im Zweifel Anspruch auf menschliche Bearbeitung geltend machen können.

Eine weitere Betrachtung der gesetzlichen Grundlagen ergab, dass ein Screening zu möglichen Anpassungen von Rechtsnormen oder Prüfungen sinnvoll ist.

AG 2: Smart City und Open Data

Der vorliegende Teilbericht beschäftigt sich mit zwei eng zusammenhängenden Themenfeldern, die zunächst unabhängig voneinander betrachtet werden. Zum einen werden (kontextspezifisch) Ausführungen zum Thema Open Data gemacht. Zum anderen wird das Thema Smart Cities eingeführt. In diesem Teilabschnitt geht es um einen konzeptionellen Ansatz (Open Data) sowie einen konkreten, äußerst komplexen Anwendungsfall (Smart City), die beide im Kern insofern verbunden sind, als dass Smart Cities als eine sehr zentrale Quelle für Open Data gesehen werden müssen und andererseits wiederum davon nachhaltig profitieren.

Unter dem Open Data-Ansatz wird verstanden, dass grundsätzlich nicht personenbezogene Daten öffentlich, frei verfügbar und ohne jegliche Nutzungseinschränkung bereitgestellt werden. Im spezifischen Kontext smarter Metropolregionen, Städte und ländlicher Gebiete geht es dabei primär um Government-Daten (z. B. Verwaltungsdaten), also Daten aus den Kontexten der staatlichen Hoheit sowie durch den Staat gemessene, freie Daten (z. B. Wetter).

Bei „Smart City“ handelt es sich ebenso wie bei KI um eine Art Oberbegriff. Vor allem sind damit Lebensräume der Menschen gemeint (Stadt, Gemeinde, ländliches Leben), die im Kontext der Digitalisierung umfänglich anders oder neu gestaltet werden. Entgegen dieser weit umfassenden Beschreibung sind Smart Cities im engeren Sinne Städte oder Metropolregionen (z. B. Berlin oder Hamburg), die als konzentriert urbane Lebensräume das Handlungsfeld für Digitalisierung darstellen.

Die Verbindung von Open Data, Smart Cities und KI liegt darin, dass gerade der städtische Raum als Aggregationsraum für Daten (Internet of Things, eGovernment, Mobility, Smart Living etc.) dienen kann, diese insbesondere im Rahmen des Trainings von KI-Systemen eingesetzt werden können und somit neue Anwendungen entstehen bzw. Anwendungsfelder der KI im urbanen Lebensraum erschlossen werden. Hieraus können sowohl eine höhere Sicherheit, bessere Resilienz, ökologisch nachhaltigere Lebensräume sowie ökonomisch neuartige Konzepte entstehen, inklusive junger Unternehmen und Start-ups.[1] Wesentlicher erscheint noch, dass diese Anwendungen dazu beitragen, dass die Lebensqualität und die Partizipationsmöglichkeiten für die Gemeinschaft signifikant gesteigert werden können.

Wichtige Voraussetzungen für ein Abschöpfen dieser Potenziale sind:

- **Die Schaffung eines operativ umsetzbaren Rechtsrahmens für KI-Anwendungen in der Stadt als legitimes Entscheidungsunterstützungssystem** (insbesondere Harmonisierung der Rechtsebenen). Dieser Rechtsrahmen muss dabei sowohl hinsichtlich der Nutzungsoptionen der Daten als auch der Einsatzfelder der KI Rechtssicherheit bieten, da sonst abgeleitete Systeme keine hinreichende Planungsbasis erhalten. Darüber hinaus muss der Rechtsrahmen auch klar regeln, welche Kompetenzen hier Bundesrecht, Landesrecht oder ggf. auch regionale Rechtsfelder[2] betreffen.

[1] Gerade aus ökonomischer Sicht scheinen dabei Verbindungen zur Mobilität, zur Umweltökonomie etc. sinnvoll. Etwas verkürzt formuliert greifen hier Circular Economy und Digitalisierung mit dem Schwerpunkt Open Data und KI ineinander.

[2] Ein einfaches Beispiel zeigt, dass z. B. Küstenstädte, bei denen Hafendaten gemessen und als Open Data zur Verfügung gestellt werden, zwar einerseits sogar internationales Recht betreffen können, andererseits aber im Normalfall entweder nur spezifisch einzelne Städte betroffen sind und daher ggf. kein genereller Rechtsrahmen auf Bundesebene von Nöten ist.

- **Die Sicherstellung der rechtmäßigen Bereitstellung von anonymisierten Daten,** die (lizenzfrei) in einem **maschinenlesbaren Format** (hohe Datenqualität) zur Verfügung gestellt werden. Außerdem ist das Open-Data-Gesetz auszuweiten. Hierbei ist zu überlegen, ob neben der Bereitstellung von Open Data auch geeignete Auswertungsinstrumente als Open Source mit bereitgestellt werden müssten bzw. sollten.
- Die **Qualitätsüberprüfung der Daten** hinsichtlich Konsistenz, Integrität und möglicher Verzerrungen muss hohe Priorität genießen. Dabei bedarf es qualifizierter Vertrauenszentren bzw. Personen. Auf der operativen Ebene wäre zu überlegen, ob an die städtischen Rechenzentren, öffentliche Datenzentren verpflichtend angeschlossen werden sollte.
- **Sicherstellung der Kontinuität der Speicherung, Verfügbarkeit und regelmäßigen Erhebung** der Daten auf Basis einer funktionsfähigen robusten digitalen Infrastruktur sowie Weiterentwicklung der notwendigen Distributionsportale und Datenbanken.
- Förderung und finanzielle Unterstützung von **Pilotvorhaben für neuartige KI-basierte Anwendungen im Smart City-Kontext**, die die Besonderheiten deutscher Städte und Regionen hinsichtlich deren Rahmenparameter, wie Größe, Fläche, Lage, Wirtschaftskraft etc., berücksichtigen.[3]

Als generelle Zielstellung der Open Data- sowie Smart City-Strategie im Zusammenhang mit dem leitenden Thema KI muss dabei gelten, dass der Einsatz von Open Data dazu beiträgt, dass die Lebensqualität durch den Einsatz von KI-Systemen, die mit Hilfe dieser Daten trainiert wurden, mittel- und langfristig in den umbauten Lebensräumen, vor allem den Städten, nachhaltig ansteigt.

Smart Cities sind insofern zumeist noch keine Einzelsysteme, die hier im Mittelpunkt gegenwärtiger oder zukünftiger KI-Systeme stehen, sondern vielmehr ist es das breite Anwendungsspektrum verschiedenster Systeme.[4]

Der Nutzwert für die Menschen in den Smart Cities ist, je nach strategischer Ausrichtung der jeweiligen Kommunen, vor allem dann gegeben, wenn sich die Lebensqualität unter Wahrung der Freiheitsrechte erhöht. Dabei wird unter Erhöhung der Lebensqualität nicht allein die individuelle Lebensqualität verstanden (bessere Mobilität, angenehmeres Leben im Alter etc.), sondern auch die kollektive Lebensqualität (saubere Umwelt, bessere Luft, weniger Verschmutzung). KI-Systeme können dabei im Rahmen von Smart City-Konzepten vor allem dazu beitragen, insgesamt die Steuerung des sozio-technischen komplexen Systems eines urbanen Lebensraums zu verbessern.

Schwierig ist die Bewertung wirtschaftlicher Rahmendaten, wie z. B. geschätzte Energieeinsparungen in der Smart City durch intelligente Verteilungssysteme, oder auch, ob z. B. Umwelteffekte durch die Systeme oder ein geändertes Nutzungsverhalten ein(ge)treten (sind). Im ersten

[3] Die bisherigen Konzepte und Forschungen in dem Zusammenhang beziehen sich sehr häufig auf den asiatischen Raum, der vollkommen andere Rahmenbedingungen hat und bietet. Selbst Fallbeispiele aus Europa, hier insbesondere das vielzitierte Beispiel Estland, können nur schlecht und selten umfänglich mit den Herausforderungen eines souveränen Staates, wie Deutschland mit seinem europäischen Gesamtgefüge, verglichen werden.

[4] Genau vor dem Hintergrund erscheint die Förderung eines breiten Open Data-Ansatzes inklusive der Schaffung entsprechender Infrastruktur ein wesentlicher Schlüssel zur Erschließung der Potenziale einer Smart City als Ermöglichungsstrategie.

Fall gilt, dass natürlich zu erwarten ist, dass intelligente Verteilungssysteme entsprechend effizientere Energienutzung ermöglichen. Allerdings sind vielfach die in Studien publizierten Daten reine Schätzwerte (eher grobe Näherungswerte).[5]

AG 3: Innere Sicherheit, Äußere Sicherheit, IT-Sicherheit

Die AG 3 befasste sich mit der Bedeutung von KI im Sicherheitsbereich. Dabei wurden die drei Themenbereiche Innere Sicherheit, Äußere Sicherheit und IT-Sicherheit getrennt voneinander untersucht, um den spezifischen Implikationen, die KI für die verschiedenen Materien aufweist, angemessen Rechnung zu tragen. Vorangestellt werden kann, dass sich insbesondere in den Bereichen der Inneren und Äußeren Sicherheit große Konfliktlinien innerhalb der Projektgruppe abzeichneten.[6]

Themenbereich Innere Sicherheit

Die Projektgruppe ist sich einig, dass KI-Systeme auch im Bereich der Inneren Sicherheit Chancen und Risiken für Bürgerinnen und Bürger bieten. Die Chancen sollten für Staat und Gesellschaft unter Rechtskonformität nutzbar gemacht werden. Bei allen Maßnahmen und so auch beim Einsatz von KI-Systemen im Bereich der Inneren Sicherheit muss eine Abwägung zwischen dem Recht auf Sicherheit und der möglichen Einschränkung von Bürger- und Grundrechten vorgenommen werden. Wie in der Verwaltung muss auch hier in besonderer Weise bei den hoheitlichen Aufgaben des Staates darauf geachtet werden, dass in und durch die Maßnahmen keine Diskriminierung entsteht. Die Systeme der Inneren Sicherheit müssen dementsprechend auch besonderen Anforderungen an Nachvollziehbarkeit und Transparenz entsprechen.

Bearbeitet und diskutiert wurden in der Projektgruppe verschiedene Projekte und der aktuelle Stand beim Einsatz von KI-Systemen im Bereich der Inneren Sicherheit, einschließlich der damit verbundenen Risiken und Potenziale. Darunter finden sich Pilotprojekte in Deutschland, wie das Projekt zur Gesichtserkennung am Berliner Bahnhof Südkreuz, EU-Projekte wie „Roborder“ oder der Einsatz von Predictive Policing in Deutschland.

Zu den wichtigsten Handlungsempfehlungen der Projektgruppe im Bereich der Inneren Sicherheit gehört eine breite gesellschaftliche Debatte zum Einsatz von KI-Systemen im Bereich der Inneren Sicherheit. Eine Ausweitung von Investitionen in KI-Technologien, die einen Mehrwert und Fortschritt für den Sicherheitsbereich bedeuten, wird ebenfalls empfohlen. Dabei sollte jedoch jedes KI-System auch im Bereich der Inneren Sicherheit möglichst nach einem Risikoklassenmodell einer Risikoklasse zugeordnet werden und folglich den Anforderungen entsprechen.

[5] Vor dem Hintergrund wird eine Befassung mit der amtlichen Wirtschafts- und Sozialstatistik empfohlen. Die bisherigen Konzepte erscheinen aufgrund der Interdependenz der Einzelbereiche, die gemessen und erhoben werden, nicht schlüssig. Bei der Weiterentwicklung des Open Data Gesetzes sollen Öffnungsklauseln entwickelt werden, die z. B. neue Erhebungs-, Erfassungs- und Auswertungsmethoden erlauben sowie die Publikation von Daten auch in Form verarbeitbarer Rohdaten ermöglichen.

[6] Zu einzelnen Aspekten der Inneren Sicherheit und zum Bereich der Äußeren Sicherheit wurde von der Fraktion DIE LINKE. bereits ein Sondervotum angekündigt.

Themenbereich Äußere Sicherheit

Auch im Bereich der Äußeren Sicherheit und Verteidigung sieht die Projektgruppe eine Vielzahl von KI-Anwendungen, deren Einsatz positive Effekte bringen kann und die allgemein nicht umstritten sind. Bei dem kritischen Bereich der Tödlichen Autonomen Waffensysteme (“Lethal Autonomous Weapon Systems (LAWS)“) erzielte die Projektgruppe den Konsens, dass diese Waffen international geächtet werden sollen. Uneinigkeit bestand allerdings in der Frage, ob die Verhandlungen mit dem Ziel eines Verbots geführt werden sollten. Bislang fehlt eine international allgemein anerkannte Definition von „autonomen Waffensystemen“, was die Befassung mit dem Thema erschwerte.

Die Mehrheit der Projektgruppe einigte sich darauf, dass bei Regulierungsfragen die LAWS im Zentrum stehen müssen und dass die Bundesregierung sich auch in Zukunft auf internationaler Ebene rüstungskontrollpolitisch für eine internationale Ächtung von tödlichen autonomen Waffensystem einsetzen sollte. Dabei soll ein Weg verfolgt werden, mit dem eine möglichst große Gruppe von Staaten eingebunden werden kann, um einer Ächtung eine starke Wirkung zu verschaffen. Eine ausschließlich nationale Regulierung ist auch mit Blick auf zukünftige, gegenwärtig noch nicht absehbare sicherheitspolitische Bedrohungen für die Mehrheit der Projektgruppe nicht zielführend.

Damit eine wirksame Ächtung gelingen kann, müssen nach Meinung der Projektgruppe alle Anstrengungen unternommen werden, um zu einer international anerkannten Definition und völkerrechtlichen Einordnung von tödlichen autonomen Waffensystemen zu kommen. Die Convention on Conventional Weapons (CCW) bleibt dafür auch in Zukunft das richtige Forum.

Die Mehrheit der Projektgruppe sprach sich auch dafür aus, dass bei der sicherheitsrelevanten KI-Forschung eine starke Kooperation im Rahmen der EU vorangetrieben werden soll, um die europäische Position zu stärken und die Technologieführerschaft bei schnellen Innovationen nicht anderen Staaten, beispielsweise den USA oder China, zu überlassen. Die Chancen, die für KI im Bereich Sicherheit und Verteidigung entstehen, sollen immer im Einklang mit völkerrechtlichen und ethischen Maßstäben – umfassend betrachtet und wo sinnvoll – genutzt werden.

Themenbereich IT-Sicherheit

Die Integrität und Sicherheit digitaler Strukturen, Technologien und Produkte ist zunehmend Grundlage allen öffentlichen und gesellschaftlichen Lebens. Die IT-Sicherheit wird daher in immer mehr Bereichen auch zur staatlichen Aufgabe und Verantwortung, für deren Wahrnehmung auch auf Lösungen aus dem Bereich lernender KI-Systeme zurückgegriffen werden kann.

Die Projektgruppe kommt überein, dass auch bei lernenden künstlichen Systemen die Herausforderung besteht, Sicherheitsimplikationen der Technologie möglichst frühzeitig zu identifizieren und Maßnahmen zur Erhöhung der Sicherheit des maschinellen Lernens zu erhöhen. Ein Spezifikum bei lernenden künstlichen Systemen ist dadurch gegeben, dass zur Erkennung von unautorisierten Manipulationen Abweichungen von der manipulationsfreien Funktionsweise des Systems festgestellt werden müssen. Das setzt ein hohes Maß an Transparenz und Nachvollziehbarkeit des Systems voraus – ein Kernproblem bei vielen Ansätzen der lernenden künstlichen Systeme. Angesichts der Verbreitung lernender künstlicher Systeme ist es nach Ansicht der Projektgruppe umso wichtiger, sich frühzeitig mit der Sicherheit derartiger Systeme bzgl. möglicher Angriffe von außen zu befassen und Strategien zur Erhöhung des Schutzniveaus dieser Systeme zu entwickeln.

Um sich Fragen nach politischen Handlungsempfehlungen zur Erhöhung der IT-Sicherheit von lernenden künstlichen Systemen annähern zu können, sind Mapping und Kategorisierung der Angriffsoberflächen erste Schritte, die die Projektgruppe empfiehlt. Ziel ist es hierbei, eine umfassende Analyse in der Art durchzuführen, dass das Resultat auf möglichst viele lernende künstliche Systeme zutrifft. Angesichts der Vielfalt der Ansätze innerhalb des lernenden künstlichen Systems wird man wahrscheinlich weitere Ausdifferenzierungen nach unterschiedlichen Modell-Klassen und technischen Ansätzen benötigen. Eine solche erste Übersicht ermöglicht es, die konkreten Angriffsvektoren für lernende künstliche Systeme zu abstrahieren und darauf aufbauend Empfehlungen für IT-Sicherheit und Resilienz zu entwickeln.

Die Projektgruppe ist überzeugt, dass der größte Teil der Anwendungsmöglichkeiten beim Einsatz von KI-Systemen durch den Staat zum Wohle des Menschen gestaltet werden kann, wenn die empfohlenen Voraussetzungen erfüllt sind. Gleichzeitig ist man sich einig, dass weiterhin intensive Forschung und auch eine breite Debatte zum Einsatz von KI notwendig sind, um diesen verantwortungsvoll und effizient zu begleiten.

Hinweis: Die Projektgruppe „KI und Staat“ hat in einer ersten Projektgruppenphase von Februar 2019 bis September 2019 getagt und einen Teilbericht erstellt, der in die Gesamtberichterstattung einfließen wird. Übergreifende Themen wie Daten, Recht, Nachhaltigkeit etc. werden durch die Enquete-Kommission selbst weiter vertieft und dabei auch die Ergebnisse anderer Gremien, wie die der Datenethikkommission, ausgewertet. Darüber hinaus werden die Themen KI und Arbeit, Bildung Forschung, KI und Mobilität sowie KI und Medien aktuell in separaten Projektgruppen bearbeitet.

Mitglieder der Projektgruppe „KI und Staat“ sind:

für die Fraktion der CDU/CSU:

- der Abgeordnete Christoph Bernstiel,
- Prof. Dr. Alexander Filipović als sachverständiges Mitglied,
- Prof. Dr. Jörg Müller-Lietzkow als sachverständiges Mitglied,
- der Abgeordnete Stefan Sauer,
- Dr. Sebastian Wieczorek als sachverständiges Mitglied,

für die Fraktion der SPD:

- die Abgeordnete Saskia Esken,
- Jan Kuhlen als sachverständiges Mitglied,
- Lena-Sophie Müller als sachverständiges Mitglied,
- die Abgeordnete Siemtje Möller als stellvertretendes Mitglied,

für die Fraktion der AfD:

- der Abgeordnete Peter Felser,
- der Abgeordnete Dr. Marc Jongen,

für die Fraktion der FDP:

- der Abgeordnete Carl-Julius Cronenberg,
- der Abgeordnete Manuel Höferlin als stellvertretendes Mitglied,

für die Fraktion DIE LINKE.:

- die Abgeordnete Anke Domscheit-Berg als Vorsitzende der Projektgruppe,
- Prof. Dr. Katharina Zweig als sachverständiges und stellvertretendes Mitglied,

und für die Fraktion BÜNDNIS 90/DIE GRÜNEN:

- die Abgeordnete Tabea Rößner,
- Dr. Stefan Heumann als sachverständiges und stellvertretendes Mitglied.

Nähere Informationen über https://www.bundestag.de/ausschuesse/weitere_gremien/enquete_ki