

Dickow, Marcel; Voelsen, Daniel

## Research Report

# Das globale Ringen um die Zukunft der künstlichen Intelligenz: Internationaler Regulierungsbedarf und Chancen für die deutsche Außenpolitik

SWP-Aktuell, No. 24/2018

### Provided in Cooperation with:

Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

*Suggested Citation:* Dickow, Marcel; Voelsen, Daniel (2018) : Das globale Ringen um die Zukunft der künstlichen Intelligenz: Internationaler Regulierungsbedarf und Chancen für die deutsche Außenpolitik, SWP-Aktuell, No. 24/2018, Stiftung Wissenschaft und Politik (SWP), Berlin

This Version is available at:

<https://hdl.handle.net/10419/255530>

### Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

### Terms of use:

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*

# SWP-Aktuell

NR. 24 APRIL 2018

## Das globale Ringen um die Zukunft der künstlichen Intelligenz

Internationaler Regulierungsbedarf und Chancen für die deutsche Außenpolitik

*Marcel Dickow / Daniel Jacob*

Mit den aktuellen Entwicklungen im Feld der künstlichen Intelligenz ist eine neue Stufe im Prozess der Digitalisierung erreicht. Künstliche Intelligenz erlaubt es, die Vielzahl der heute gesammelten Daten auf gänzlich neue Weise auszuwerten. Unternehmen und Staaten wenden erhebliche Ressourcen auf, um sich diese Analyse-Möglichkeiten zunutze zu machen. Doch gilt auch: Künstliche Intelligenz ist von der Qualität der zugrundeliegenden Daten abhängig, sie ist für viele Aufgaben gänzlich ungeeignet und sie entzieht sich bisher weitgehend menschlicher Kontrolle. Deutschland sollte daher seinen Einfluss in internationalen Foren geltend machen, um den Einsatz künstlicher Intelligenz in politisch sensiblen Bereichen zu regulieren. Zudem sollte die Bundesregierung sorgfältig prüfen, auf welcher Datengrundlage, zu welchen Zwecken und unter welchen Bedingungen künstliche Intelligenz einen Beitrag zur außenpolitischen Strategiebildung leisten kann.

Künstliche Intelligenz (KI) erobert immer mehr Bereiche unseres Lebens. Unternehmen nutzen KI, um Profile ihrer Kundinnen und Kunden zu erstellen und Bewerbungen auszuwerten. In der Medizin erhofft man sich Fortschritte in Forschung wie Therapie. Und auch Staaten setzen verstärkt auf KI: Im Sinne des »predictive policing« will man Polizei und Nachrichtendienste in die Lage versetzen, Anzeichen für Verbrechen auszumachen, noch bevor diese begangen werden. Autonome, auf KI beruhende Waffensysteme sollen neue Formen der Kriegsführung ermöglichen. Schon in naher Zukunft ist außerdem damit zu rechnen, dass Staaten KI-Systeme für ihre außenpolitische

Strategiebildung nutzen werden, zum Beispiel durch die Echtzeit-Auswertung von Wirtschaftsdaten anderer Staaten.

Die Informationsverarbeitung durch KI sollen es in Zukunft ermöglichen, in der Vielfalt der Daten die Spreu vom Weizen zu trennen. Vorerst werden die eigentlichen Entscheidungen wohl beim Menschen verbleiben. Noch. Denn in puncto Geschwindigkeit und Analyse-Kapazität gerät der Mensch gegenüber der Maschine zunehmend ins Hintertreffen. Der »perfekten« Maschine die Entscheidung zu überlassen ist zum Beispiel bei zeitkritischen Anwendungen eine verlockende Vorstellung. Wie die Erfahrungen mit dem autonomen Fah-



ren zeigen, wird der Mensch am Ende aber, – wie noch bei jeder neuen Technologie – regulierend eingreifen müssen, um ungewollte Risiken zu vermeiden und Verantwortlichkeiten abzustechen.

Eine besondere Herausforderung ist dabei, dass KI als Technologie für die Politik nicht nur Gegenstand von Regulierungsbemühungen ist. In dem Maße, in dem öffentliche Institutionen KI-Systeme einsetzen, wird KI vielmehr den politischen Prozess selbst beeinflussen. Die gesetzgebenden Institutionen, Aufsichtsbehörden und internationalen Gremien stehen daher vor der Herausforderung, einen Teil ihrer eigenen Analyse- und Entscheidungsfundamentinstrumente regulieren zu müssen.

## Künstliche Intelligenz

Der Begriff KI (im Englischen »Artificial Intelligence«, AI) hat sich zu einem Sammelbegriff für eine Reihe von rechnergestützten Methoden entwickelt. Viele der heutigen KI-Anwendungen beruhen auf datengetriebenen Verfahren maschinellen Lernens. Diese Verfahren setzen große Mengen an vorstrukturierten Daten voraus, mit denen Algorithmen angeleitet werden müssen. Maschinen lernen so zu klassifizieren, also zum Beispiel auf Fotos Hunde von Katzen zu unterscheiden. Menge, Qualität und Repräsentativität der Trainings-

daten sind dabei entscheidende Faktoren für die spätere Aussagekraft der Ergebnisse.

## Starke und schwache KI

Datengetriebene KI-Systeme können in bestimmten Fällen bessere Klassifizierungsergebnisse liefern als der Mensch. Doch sie bleiben Speziallösungen für einzelne Probleme, die bisher keine Verallgemeinerungen erlauben. Schon das Erkennen von Wölfen überfordert ein System, das mit Fotos von Hunden und Katzen trainiert wurde. Aufgrund dieser inhärenten Beschränkungen werden die heute üblichen KI-Systeme auch als *schwache* KI bezeichnet. In Informatik wie Philosophie finden sich zwar immer wieder Stimmen, denen zufolge in Zukunft Maschinen auch mit höher entwickelten menschlichen Eigenschaften ausgestattet werden könnten, etwa mit der Fähigkeit, konzeptionell zu denken. Für diese sogenannte *starke* KI fehlen bislang aber jegliche Realisierungskonzepte.

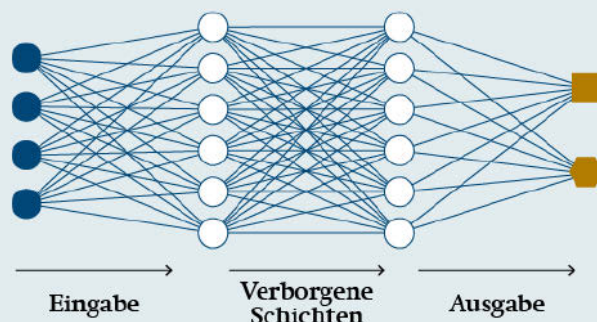
## Wie Maschinen lernen

Ein heute vorherrschendes Verfahren maschinellen Lernens ist das sogenannte tiefe Lernen mit neuronalen Netzen (*deep neural networks*). Diese Netze arbeiten mit mehreren Schichten von Verzweigungspunkten. Die einzelnen Schichten erfassen jeweils nur einfache Konzepte, deren Kombination jedoch komplexe Analysen erlaubt. Bei der Bilderkennung etwa wird eine Reihe von Merkmalen erfasst, die für sich genommen wenig aussagekräftig sind, im Zusammenspiel aber zum Beispiel eine Unterscheidung zwischen Hunden und Katzen ermöglichen.

Tiefe neuronale Netze besitzen eine Vielzahl solcher verborgener Schichten (*hidden layers*), in denen sich beim Training Wahrscheinlichkeitswerte herausbilden (siehe Abbildung 1). Zwar stehen Eingabe und Ausgabe immer noch in einem definierten mathematischen Verhältnis zueinander. Doch beruht dieses Verhältnis nicht wie bei Menschen üblich auf logischen Schlussfolgerungen, sondern auf statistischer Berechnung.

Abbildung 1

### Schematische Darstellung der Struktur eines neuronalen Netzwerks



Solche verschachtelten Klassifizierungsmethoden können für den Menschen intuitiv einfache, mit klassischen Methoden aber nur schwer zu programmierende Regeln aus einem beobachteten Verhalten ableiten. Dies hat jedoch einen Preis: Ohne (zeit-)aufwändige mathematische Verfahren lassen sich die Analyse-Ergebnisse solcher tiefen neuronalen Netze nicht validieren.

Das sogenannte verstärkende Lernen (*reinforcement learning*) macht sich die Struktur tiefer neuronaler Netze zunutze. Algorithmen werden hierbei so programmiert, dass sie Strategien zur Lösung von Problemen entwickeln, indem sie Erfolg (angezeigt durch Belohnung) maximieren. Dem System wird ein abstraktes Ziel vorgegeben, das es durch einen Prozess des Selbstlernens erreicht, also durch »trial and error«. Eine wichtige Rolle spielt verstärkendes Lernen inzwischen für komplexe Steuerungsaufgaben, zum Beispiel bei der Steuerung robotischer Systeme. Die inhärente Unsicherheit, wie das KI-System die Aufgabe löst, schränkt die Anwendungsbereiche darüber hinaus allerdings erheblich ein.

## Forschung zu KI

Seit Anfang der 2010er Jahre wurden im Bereich KI erhebliche Fortschritte erzielt. Ermöglicht wurden diese durch die zunehmende Verfügbarkeit von strukturierten Daten im Internet sowie die Steigerung der Rechenleistung und Speicherkapazität moderner Computer. Die Vernetzung von immer mehr Geräten im Sinne des »Internet of Things« (IoT) wird die Verfügbarkeit von nutzbaren Daten weiter steigern.

Die Entwicklung von KI wird maßgeblich von großen Internetunternehmen vorangetrieben. Sie investieren erhebliche Summen und befinden sich zunehmend in einem Wettbewerb um geeignetes Personal. Auch deshalb veröffentlichen einige der führenden Unternehmen in den USA Teile ihrer Forschungsergebnisse und stellen der Wissenschaftsgemeinschaft einzelne Softwarekomponenten als »open source« zur Verfügung.

Inzwischen sind viele Länder auf den Zug aufgesprungen und haben staatliche Förder- und Entwicklungsprogramme aufgelegt. Insbesondere China hat erhebliche Investitionen angekündigt und verbindet damit erklärtermaßen den Anspruch, den technologischen Vorsprung der USA aufzuholen. Obwohl im Vergleich deutlich abgeschlagen hat Russland seine Ambitionen in diesem Feld ebenfalls klar artikuliert. Auch die Ankündigung eines deutsch-französischen KI-Zentrums lässt sich als Reaktion auf diesen technologischen Wettstreit werten. Bislang ist das Ausmaß staatlichen Engagements in diesem Bereich allerdings schwer einzuschätzen: Selbst in demokratischen Staaten mangelt es an belastbaren Zahlen, die Aufschluss über das tatsächliche Investitionsvolumen geben könnten. In Staaten wie China und den USA kommt erschwerend hinzu, dass deren Zusammenarbeit mit Unternehmen gerade bei der militärischen Nutzung von KI dem Einblick der Öffentlichkeit größtenteils entzogen ist.

## Internationaler Regulierungsbedarf

Die spezifische Stärke von KI-Systemen ist zugleich der Grund dafür, warum sie einer Regulierung bedürfen: Über die verschiedenen Anwendungsfälle hinweg zeichnet sich KI dadurch aus, Daten ungleich schneller als Menschen und mit einem zunehmenden Grad an Eigenständigkeit auswerten zu können. Diese Fähigkeit birgt das Versprechen, besser informierte Entscheidungen treffen zu können. Im Ergebnis allerdings wird die Verantwortung für folgenreiche Entscheidungen an Computersysteme übertragen, deren Vorgehensweise für Menschen bisher kaum nachvollziehbar ist. Durchaus treffend wird KI daher bisweilen auch als »black box« bezeichnet.

Nun muss dies nicht in jedem Fall problematisch sein. Regulierungsbedarf entsteht indes überall dort, wo KI-Systeme in politisch sensiblen Bereichen genutzt werden. Orientierung für die Ebene der

internationalen Regulierung bieten hierbei die verschiedenen Normenordnungen des Völkerrechts. Will Deutschland die Wirksamkeit dieser Normenordnungen bewahren, gilt es, sie den besonderen Herausforderungen von KI-Systemen anzupassen.

## **KI und staatlicher Zwang**

Im Kontext der staatlichen Nutzung von KI-Systemen bilden menschenrechtliche Normen einen ersten wichtigen Ausgangspunkt. Sie lenken den Blick auf jene Anwendungen, bei denen der Einsatz von KI-Systemen mit staatlichem Zwang verbunden ist. Schon heute setzen Staaten wie die USA oder Großbritannien KI-Systeme in der Polizeiarbeit ein: Im Rahmen des »predictive policing« werden Prognosen dazu erstellt, an welchen Orten, zu welchen Zeitpunkten und von welchen Personen kriminelle Handlungen zu erwarten sind. Auch zur Unterstützung der Rechtsprechung werden KI-Systeme in den USA bereits eingesetzt, etwa bei der Bestimmung des Strafmaßes. Die Zuspitzung dieser Entwicklungen lässt sich in China beobachten: Dort führt die Regierung derzeit ein »Social Credit System« ein, mit dessen Hilfe das Verhalten der Bürgerinnen und Bürger in nahezu allen Lebensbereichen erfasst und automatisiert in ein sanktionsbewehrtes Rating übersetzt werden soll.

Noch weitgehend ungeklärt ist, ob und gegebenenfalls wie sich der staatliche Einsatz von KI-Systemen mit menschenrechtlichen Vorgaben vereinbaren lässt. Diese Frage stellt sich insbesondere für das Recht auf Gleichbehandlung und einen ordentlichen Gerichtsprozess (Art. 14 des International Covenant on Civil and Political Rights [ICCPR]) oder auch das Recht auf Privatsphäre (Art. 17 ICCPR). Erste Anhaltspunkte bietet eine EU-Direktive zum Schutz personenbezogener Daten im Rahmen der »Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung« (EU 2016/680).

Der militärische Einsatz von KI-Systemen fällt vorrangig in die Domäne des humanitären Völkerrechts. Eine Vielzahl von Staa-

ten investiert bereits massiv in die Entwicklung (teil-)autonomer Waffensysteme. Schon die nur partielle Übertragung von Entscheidungen über die Anwendung von Gewalt an KI-Systeme würde dabei in grundlegender Weise die Schutzmechanismen des humanitären Völkerrechts in Frage stellen. Als Reaktion auf diese Entwicklungen wurde im Rahmen der »Convention on Certain Conventional Weapons« (CCW) ein Expertengremium gebildet (*group of governmental experts*), das Vorschläge dazu erarbeiten soll, wie autonome Waffensysteme reguliert werden könnten.

## **KI und die Macht der Unternehmen**

Regulierungsbedarf besteht zudem mit Blick auf die Nutzung von KI-Systemen durch private Unternehmen. Wiederum bieten die menschenrechtlichen Normen des Völkerrechts Orientierung: Die Staaten sind auch dafür verantwortlich, die relevanten Rechtsgüter vor Verletzungen durch Dritte zu schützen. Weil die meisten Unternehmen in diesem Feld transnational agieren, müssen dazu einzelstaatliche Maßnahmen durch geeignete Formen internationaler Regulierung ergänzt werden.

Private Unternehmen wie Amazon, Google oder Baidu nutzen KI-Systeme dafür, umfangreiche Profile von ihren (potenziellen) Kundinnen und Kunden zu erstellen. Diese Profile dienen vielfach der vergleichsweise harmlosen Personalisierung von Werbung oder der Bereitstellung digitaler Dienstleistungen, wie zum Beispiel der Anzeige personalisierter Nachrichten. Personenbezogene Profile können aber auch Grundlage für folgenreiche Entscheidungen sein: So setzen etwa Banken zunehmend KI-Systeme ein, um die Kreditwürdigkeit ihrer Kundinnen und Kunden zu beurteilen. Auch bewerten Unternehmen wie LinkedIn mit Hilfe solcher Systeme die Profile von Arbeitssuchenden. Schließlich sind KI-Systeme ein wesentliches Element für die derzeitige Entwicklung autonomer Verkehrssysteme durch Firmen wie Tesla, Google oder Baidu.

Obschon diese Form der Nutzung von KI-Systemen durch Unternehmen nicht mit staatlicher Zwangsgewalt verbunden ist, hat sie erhebliche Auswirkungen auf das Leben von immer mehr Menschen. Es liegt in der Verantwortung der Staaten, diese Nutzung so zu regulieren, dass sie im Einklang mit menschenrechtlichen Vorgaben wie dem Diskriminierungsverbot (Art. 26 ICCPR) oder dem Recht auf Schutz der Privatsphäre steht (Art. 17 ICCPR). Bemerkenswert ist, dass einige der wichtigsten Unternehmen von sich aus eine gesellschaftliche Debatte über die Regulierung von KI-Systemen einfordern. Exemplarisch ist die Beteiligung führender Vertreter von Firmen wie Deepmind, Apple und IBM an der Erarbeitung der »Asilomar AI Principles«. Die 2017 im kalifornischen Asilomar konzipierten Prinzipien formulieren gesellschaftliche Anforderungen an die zukünftige Entwicklung von KI-Systemen. Sie weisen auch auf die Notwendigkeit hin, einen entsprechenden rechtlichen Rahmen für die Nutzung von KI zu schaffen.

## Regulierungsziele

Um dem skizzierten Regulierungsbedarf gerecht zu werden, bedarf es konkreter Lösungen, die den technischen wie politischen Besonderheiten des jeweiligen Anwendungsfalls Rechnung tragen. Bei aller Vielfalt lassen sich jedoch einige übergreifende Regulierungsziele ausmachen.

### »Garbage in, Garbage out«

Den gemeinsamen Ausgangspunkt bildet dabei das Ziel, bei der Nutzung von KI-Systemen zur maschinellen Unterstützung von Entscheidungen »falsche« Ergebnisse zu vermeiden, die Aussagekraft der Ergebnisse kritisch zu beleuchten und die negativen Auswirkungen von Fehlanalysen zu begrenzen. Wie beschrieben basiert die Leistungsfähigkeit heutiger KI-Systeme auf der induktiven Auswertung von Daten. Quantität und Qualität der verfügbaren Daten bedingen daher ganz unmittelbar ihre Leistungs-

fähigkeit. Es überrascht insofern nicht, dass sich in letzter Zeit Berichte über die Gefahr der Diskriminierung durch KI gehäuft haben. Das zentrale Problem war zumeist, dass KI-Systeme bestehende Diskriminierungen in den Datensätzen reproduzieren. Wenn sich beispielsweise in historischen Daten spiegelt, dass Männer häufiger Führungspositionen eingenommen haben als Frauen, kann dies ein KI-System zu der falschen Schlussfolgerung verleiten, dass Männer für solche Positionen grundsätzlich besser geeignet seien.

Die Datenauswahl spielt beim Einsatz von KI-Systemen mithin eine zentrale Rolle. Die Systeme selbst allerdings können keine Auskunft über die Güte der zugrundeliegenden Daten geben. Im Gegenteil, selbst bei unzureichender Datengrundlage werden sie immer ein Ergebnis erzeugen, auch wenn dieses nicht aussagekräftig ist. Erschwerend kommt hinzu, dass subtilere Formen datenbasierter Diskriminierung nur schwer zu erkennen sind. So mag es noch vergleichsweise einfach sein, einem KI-System, das Bewerberinnen und Bewerber evaluiert, den Zugriff auf die Information zu deren Geschlecht zu verwehren. Nicht ausgeschlossen ist damit aber, dass in die Analyse andere Faktoren eingehen, die mit dem Geschlecht korrelieren. Je weniger offensichtlich diese Korrelation ist, umso schwieriger wird es, sie alleine an den Ergebnissen abzulesen.

Es ist daher eine zentrale Verantwortung der Entwickler und Anwender von KI-Systemen, sorgfältig zu prüfen, ob die verfügbaren Daten für den jeweiligen Analysezweck geeignet sind. Weil diese Sorgfalt aber nicht immer vorausgesetzt werden kann, ist in politisch sensiblen Bereichen in drei Hinsichten ein regulierendes Eingreifen erforderlich:

## Transparenz

Als elementare Voraussetzung für die kritische Auseinandersetzung mit dem Wirken von KI-Systemen muss zunächst ein hinreichendes Maß an Transparenz geschaffen werden. Dafür ist es unerlässlich, dass öf-

fentliche wie private Institutionen Auskunft darüber geben, an welchen Stellen und zu welchem Zweck sie KI-Systeme einsetzen. Auf dieser Grundlage müssen Betroffene individuell nachvollziehen können, in welcher Weise und auf Basis welcher Daten KI-Systeme sich auf zentrale Bereiche ihrer Lebensführung auswirken. Aber auch politische Entscheidungsträgerinnen und Entscheidungsträger müssen in verständlicher Weise darüber informiert sein, wie öffentliche Stellen und private Akteure KI-Systeme nutzen.

Dieses Transparenz-Erfordernis genauer zu bestimmen ist eine technische wie rechtliche Herausforderung. *Technisch* ist es keineswegs trivial, aber doch möglich, eine entsprechende Auskunft auf verständliche Weise verfügbar zu machen. KI-Systeme sollten etwa so gestaltet werden, dass sie Auskunft über die jeweils entscheidenden Analyse-Faktoren geben, dass sie offenlegen, wie repräsentativ die Trainingsdaten für die reale Datenanwendung sind, und dass sie ausweisen, mit welcher Fehlerquote ihre Analyse behaftet ist. *Rechtlich* ist dabei zu klären, wie eine aussagekräftige Auskunft mit dem Datenschutz und dem Recht der Unternehmen auf Schutz ihres geistigen Eigentums zu vereinbaren ist. Nicht zuletzt besteht die Gefahr, dass die Betroffenen selbst oder interessierte Dritte solche Auskünfte nutzen, um die Datenbasis von KI-Systemen gezielt zu manipulieren.

Erste Ansätze zur Lösung dieser komplexen Problematik bietet die ab Mai verbindlich geltende Europäische Datenschutz-Grundverordnung (DSGVO). Diese regelt explizit die Auskunfts- und Widerspruchsrechte von Betroffenen im Falle automatisierter Datenauswertungen (Art. 22 DSGVO). Interessant sind in diesem Zusammenhang auch die Bemühungen der Stadtverwaltung von New York City, die kommunale Nutzung von KI-Systemen transparenter zu gestalten. Ende 2017 beschloss der Stadtrat, eine Expertengruppe einzurichten, die den Einsatz von »automated decision systems« in der öffentlichen Verwaltung New Yorks untersuchen soll. Die Gruppe soll in den nächsten Monaten ihre Arbeit aufnehmen.

## Menschliche Kontrolle

Der Reiz von KI besteht darin, bisher von Menschen ausgeübte Tätigkeiten an Maschinen zu delegieren. In politisch sensiblen Bereichen jedoch gilt es zu prüfen, in welchen Hinsichten das Wirken von KI-Systemen besonderer menschlicher Kontrolle zu unterwerfen ist.

Die Klassifizierungsmethoden moderner KI-Systeme werden häufig genutzt, um bislang verborgene statistische Zusammenhänge sichtbar zu machen. Derartige Datenkorrelation setzt aber Kausalität weder voraus noch kann sie diese nachweisen. Daher ist es unverzichtbar, auf KI basierende Entscheidungen einer menschlichen Plausibilitätskontrolle zu unterziehen. Sie setzt die bereits beschriebene Transparenz der genutzten Daten und Algorithmen voraus. Für eine solche Plausibilitätskontrolle muss zudem ausreichend Zeit bleiben, um das Vorgehen von KI-Systemen rekonstruieren zu können. Tatsächlich ist es in vielen Fällen auch rechtlich sinnvoll, eine solche umfassende Plausibilitätskontrolle zu verlangen. Wo Entscheidungen mit weitreichenden Folgen für die Betroffenen gefällt werden, kann sich menschliche Kontrolle nicht darauf beschränken, ein »Ja-Nein«-Dialogfeld auf dem Bildschirm zu bedienen. Erforderlich ist vielmehr, dass sich die Benutzer solcher Systeme aktiv mit deren System- und Anwendungsparametern auseinandersetzen.

Ein fiktives Beispiel verdeutlicht die Herausforderung: Eine Firma bietet eine KI-basierte Software an, die im Rahmen eines Auslandseinsatzes der Bundeswehr Satellitenbilder analysiert und Vorschläge zur Einsatzplanung liefert. Dazu muss in einem ersten Schritt die für das Training des Systems genutzte Datengrundlage auf Repräsentativität und Anwendbarkeit geprüft werden. Diese Prüfung sollte nicht der Firma überlassen werden, die die Software anbietet. In einem politisch derart sensiblen Bereich sollte dies stattdessen eine unabhängige Instanz übernehmen.

In einem zweiten Schritt müssen die lokalen Kommandeure im Einzelfall das



Ergebnis des Expertensystems bestätigen oder gegebenenfalls korrigieren, nachdem sie es einem dokumentierten Prüfvorgang unterzogen haben. Dazu ist es erforderlich, dass sie die nötige fachliche Kompetenz besitzen. Wie diese Kompetenz erarbeitet und erhalten bleiben kann, wenn sich Lageeinschätzungen in Zukunft immer stärker auf Expertensysteme stützen, bleibt eine noch zu beantwortende Frage.

### **Klare Verantwortlichkeiten**

Das Beispiel der Anwendung von KI bei der Planung militärischer Einsätze verweist auch auf die Notwendigkeit, bei der Nutzung wie bei der Zulassung KI-basierter Systeme klare Verantwortlichkeiten festzulegen. Das humanitäre Völkerrecht verlangt zum Beispiel, dass Mitglieder von Streitkräften vor Gewaltanwendungen eine juristische und moralische Abwägung vornehmen. Hierbei ist unter anderem zu klären, ob das gewählte militärische Mittel angemessen und sein Einsatz notwendig ist. Nach dem vorherrschenden Verständnis des Völkerrechts müssen Menschen solche Abwägungen treffen und dürfen sie nicht Maschinen überlassen. Nicht überzeugend ist daher der Vorschlag, KI-Systemen einen begrenzten Status als Rechtssubjekt zuzuerkennen und sie auf diesem Wege haftbar zu machen.

Ziel sollte es stattdessen sein, die Verantwortung von Menschen für die Nutzung von KI-Systemen klar zu benennen. Mit Blick auf die verschiedenen militärischen wie zivilen Anwendungsfälle gilt es dabei auch zu klären, welche Verantwortung den Herstellern von KI-Systemen zukommt.

### **Künstliche Intelligenz in der außenpolitischen Planung**

Es ist davon auszugehen, dass KI-Systeme schon in naher Zukunft auch die außenpolitische Planung und Entscheidungsfindung verändern werden. Die enorm erweiterten Möglichkeiten der Datenverarbeitung durch KI erlauben es, Prognosen zu

den Folgen spezifischer außenpolitischer Entscheidungen zu erstellen und deren Auswirkungen in Echtzeit zu erfassen. In gewisser Weise lässt sich dies als Erweiterung der klassischen nachrichtendienstlichen Analyse verstehen. Die automatisierte Auswertung durch KI-Systeme ermöglicht es nun allerdings, größere Datenmengen zu verarbeiten und Daten unterschiedlicher Art und Herkunft zu verknüpfen. So ist zum Beispiel zu erwarten, dass solche Systeme in Zukunft für die Krisenfrüherkennung genutzt werden, aber auch bei Pandemien oder der Analyse der globalen Migrationsströme. Das Auswärtige Amt (AA) richtet zu ebendiesem Zweck in der Abteilung für Krisenprävention, Stabilisierung, Konfliktnachsorge und Humanitäre Hilfe (Abt. S) gerade ein datenbasiertes Analyzesystem ein. Das System soll laut Auskunft des AA zunächst öffentlich zugängliche Daten zu sozialen, wirtschaftlichen und politischen Entwicklungen auswerten. Über die Analyse hinaus werden Staaten auch versuchen, KI zur Stärkung ihrer offensiven wie defensiven Cybersecurity-Kapazitäten zu nutzen.

Diese Anwendungen von KI-Systemen verfügen über das Potenzial, die Informationsgrundlage für außenpolitische Entscheidungen zu verbessern. Doch auch hier gilt, dass die Unterstützung durch KI-Systeme nur so gut sein kann, wie es die zugrundeliegenden Daten erlauben. Außerdem ist stets zu hinterfragen, für welche Analysen sich KI-Systeme eignen und für welche nicht. Auch die beste KI kann politische Urteilskraft nicht ersetzen. Schließlich muss der Einsatz solcher Systeme zumindest für die Entscheidungsträgerinnen und -träger in Parlament und Regierung transparent sein und stets angemessener menschlicher Kontrolle unterliegen. Erschwert wird dies allerdings dadurch, dass die außenpolitische Entscheidungsfindung traditionell in fast allen Staaten dem Einblick der Öffentlichkeit entzogen ist.



## Aufgaben für die deutsche Außenpolitik

Entwicklung und Anwendung von KI stehen weltweit noch am Anfang. Dies ist politisch eine Chance, bietet sich hier doch die Gelegenheit, die zukünftige technologische und politische Entwicklung aktiv zu gestalten. Die genannten Regulierungsziele liefern dafür einen normativen Orientierungspunkt. Mit Blick auf die jeweiligen Besonderheiten konkreter Anwendungsfälle müssen sie aber noch weiter ausgestaltet und spezifiziert werden.

Die Klärung der hiermit verbundenen ethischen, rechtlichen und politischen Fragen ist eine Kernaufgabe des Bundestags als Zentrum der demokratischen Öffentlichkeit. Es bedarf einer umfassenden Debatte darüber, wie und unter welchen Bedingungen KI in welchen gesellschaftlichen Bereichen genutzt werden soll. Und es muss eine Auseinandersetzung darüber geführt werden, welche Formen nationaler und vor allem internationaler Regulierung geeignet sind, entsprechende politische Vorgaben effektiv umzusetzen. Hierzu ist es unerlässlich, in der deutschen Debatte die entsprechenden Überlegungen und Prozesse im Rahmen der EU und der Vereinten Nationen zu berücksichtigen. Kürzlich ist etwa bekannt geworden, dass die EU-Kommission nicht nur die Forschungsförderung ausbauen will, sondern auch an Leitlinien zum Umgang mit den rechtlichen und ethischen Herausforderungen von KI arbeitet. Die International Telecommunications Union (ITU) widmet sich ebenfalls verstärkt diesem Thema. Und bei den Vereinten Nationen laufen im Rahmen der »Convention on Certain Conventional Weapons« (CCW) weiterhin die Verhandlungen über den Umgang mit autonomen Waffensystemen.

Es besteht also erheblicher Klärungsbedarf. Insofern erscheint es sinnvoll, den Rahmen der Debatte zu erweitern. Die im aktuellen Koalitionsvertrag vorgesehene »Daten-Ethik-Kommission« etwa könnte

eine Möglichkeit bieten, die notwendige parlamentarische Auseinandersetzung durch Beiträge aus Wissenschaft, Wirtschaft und Zivilgesellschaft zu ergänzen.

Neben diesen grundsätzlichen Klärungen ist es aber auch nötig, schon heute bei Fragen des Umgangs mit KI außenpolitisch handlungsfähig zu sein. International wird durchaus zur Kenntnis genommen, dass Deutschland mit dem Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) im Bereich der Grundlagenforschung sehr gut aufgestellt ist.

Wie in anderen Bereichen der Digitalisierung wird ein geeintes außenpolitisches Auftreten aber auch hier dadurch erschwert, dass die Zuständigkeit für KI-Belange über eine Reihe von Ressorts gestreut ist. Die Forschungsförderung obliegt dem Bundesministerium für Bildung und Forschung, während das Bundesministerium der Justiz für die rechtlichen Fragen der Anwendung von KI zuständig ist, das Arbeitsministerium wiederum kümmert sich um die Auswirkungen auf den Arbeitsmarkt. Mit Fragen der operativen Nutzung von KI beschäftigen sich vor allem das Bundesministerium des Innern, das AA und die Nachrichtendienste. Die Zuständigkeit für die einschlägigen Debatten in den verschiedenen internationalen Foren wiederum ist aufgeteilt zwischen AA, Bundesministerium für Wirtschaft und Energie und dem Kanzleramt.

Diese große institutionelle Streuung ist der thematischen Breite in gewisser Hinsicht durchaus angemessen, denn KI berührt in der Tat die verschiedensten Politikfelder. Will Deutschland seinen außenpolitischen Einfluss auf die künftige Entwicklung geltend machen, bedarf es jedoch gleichwohl einer stärkeren Koordinierung. Die Schaffung der Stelle einer Staatsministerin für Digitalisierung im Kanzleramt etwa ist eine vielversprechende Maßnahme, die Ansatzpunkt für einen im Kanzleramt angesiedelten Ressortkreis zum Thema KI sein könnte.

© Stiftung Wissenschaft und Politik, 2018  
**Alle Rechte vorbehalten**

Das Aktuell gibt die Auffassung der Autoren wieder.

In der Online-Version dieser Publikation sind Verweise auf SWP-Schriften und wichtige Quellen anklickbar.

SWP-Aktuelle werden intern einem Begutachtungsverfahren, einem Faktencheck und einem Lektorat unterzogen. Weitere Informationen zur Qualitätssicherung der SWP finden Sie auf der SWP-Website unter <https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/>

**SWP**  
Stiftung Wissenschaft und Politik  
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4  
10719 Berlin  
Telefon +49 30 880 07-0  
Fax +49 30 880 07-100  
[www.swp-berlin.org](http://www.swp-berlin.org)  
[swp@swp-berlin.org](mailto:swp@swp-berlin.org)

ISSN 1611-6364

*Dr. Marcel Dickow ist Leiter der Forschungsgruppe Sicherheitspolitik.*

*Dr. Daniel Jacob ist Wissenschaftler in der Forschungsgruppe Globale Fragen.*