„Es geht um den Kern von Sicherheit“

Die frühere Staatssekretärin Katrin Suder über Künstliche Intelligenz

Unendliche Datenmengen, immer stärkere Rechnerleistungen, immer weiter verbesserte Algorithmen: Diese Entwicklungen und ein möglicher Durchbruch beim Quanten-Computing bereiten den Boden für Künstliche Intelligenz als Schlüsseltechnologie, erklärt die ehemalige Verteidigungs-Staatssekretärin Katrin Suder im IP-Gespräch. Eine Debatte darüber ist überfällig.

IP: *Frau Suder, was ist Künstliche Intelligenz und warum spielt das Thema auf einmal in der Sicherheitspolitik so eine große Rolle?*
Katrin Suder: Schwierige Frage, denn schon für menschliche Intelligenz gibt es keine klare, weithin akzeptierte Definition. Aber ich würde es so sagen – Künstliche Intelligenz ist der Versuch, Funktionen menschlicher Intelligenz wie lesen, Muster erkennen, Fragen beantworten usw. mit Maschinen nachzubilden. Das ist ein ganz alter Menschheitstraum, denken Sie an die Geschichte vom Golem aus der jüdischen Mythologie. Ein bisschen technischer formuliert bezeichnet man mit KI Computerprogramme, die auf Rechnern laufen. Diese Computerprogramme sind so genannte (Deep) Learning Algorithm-Programme, die in gewisser Weise den Aufbau des Gehirns in Form von neuronalen Netzen nachbilden. Diese neuronalen Netze werden mit vielen Daten gefüttert, lernen und adaptieren sich dabei selbst …

IP: … *um den Menschen zu ersetzen?*
Suder: In bestimmten Funktionen und Aufgaben? Ja. Aber umfassend? Nein. Die Form von KI, die wir derzeit haben, nennt man „schwache KI“, ein Werkzeug, das alle möglichen, allerdings sehr spezifischen Aufgaben erledigen kann, zum Beispiel die Vorhersage, wann ein bestimmtes Bauteil ausfällt („predictive maintenance“ genannt) oder die Sprachsteuerung Ihres Handys. Sie können einer Maschine das Go-Spielen beibringen, aber sie kann dann noch lange kein Schach. Wenn Sie einer Maschine eine komplexe Frage stellen, kommt womöglich nur „42“ als Antwort heraus wie im Roman „Per Anhalter durch die Galaxis“ von Douglas Adams, wenn „nach dem Leben, dem Universum und dem ganzen Rest“ gefragt wird.

Sollte allerdings tatsächlich irgendwann die Entwicklung echter, so genannter „starker KI“ gelingen, also einer, die der Intelligenz des Menschen eben-

bürtig oder sogar überlegen wäre, würde das eine völlig neue Realität schaffen und sich auf alle Bereiche des Lebens auswirken.

IP: *Trotzdem ist die Sorge mit Blick auf die Sicherheitspolitik schon jetzt sehr groß – warum?*
Suder: Weil gerade verschiedene Entwicklungen zusammenkommen. Wenn wir über KI reden, reden wir im Wesentlichen über vier Komponenten – wie eben beschrieben die Algorithmen oder Programme, dazu „computing power“, also Rechnerleistung, dann braucht man Daten und man braucht Menschen, also Programmierer, Anwendungsentwickler. Blickt man auf jüngste Entwicklungen in den Algorithmen von Künstlicher Intelligenz, kann man erst einmal nichts Revolutionäres feststellen. Ich habe Ende der 1990er Jahre über neuronale Netze promoviert; im Vergleich zu damals hat man jetzt verbesserte mathematische Modelle und auch mehr Ebenen solcher Netze, aber diese methodischen Innovationen alleine bedeuten keinen Quantensprung.

IP: *Was wäre ein Quantensprung?*
Suder: Neben der oben beschriebenen Entwicklung von „starker KI“ wäre eine andere Nichtlinearität der Sprung zum Quanten-Computing. Und dieser scheint mir übrigens deutlich wahrscheinlicher, denn letztlich sind „nur“ noch Ingenieursfragen zu lösen. Um die Relevanz dieser Nichtlinearität im Bereich Rechnerleistung zu verdeutlichen. Quantencomputer würden in der Kryptologie von heute auf morgen alles verändern. Verschlüsselungen, die derzeit auch in Millionen Jahren nicht zu knacken sind, knackt ein Quantencomputer in einer Millisekunde. Alles vollzieht sich in einer Geschwindigkeit, die beispiellos ist …

DR. KATRIN SUDER war von August 2014 bis April 2018 Staatssekretärin im Bundesministerium der Verteidigung. Dort leitete sie u.a. die Abteilungen Ausrüstung und Cyber/Informationstechnik. Zuvor war sie Direktorin und Leiterin des Berliner Büros der Unternehmensberatung McKinsey, für die sie seit 2000 tätig war.

IP: *… und das wirkt sich auf Sicherheitspolitik aus?*
Suder: Aber ja – signifikant! Stellen Sie sich ein Szenario vor, in dem plötzlich die existierende Verschlüsselung nicht mehr sicher ist. Das ist übrigens einer der Gründe, warum Deutschland und insbesondere auch die Bundeswehr so stark in das Thema investieren. Richtigerweise. Aber zurück zur KI – was in jüngster Zeit passiert, ist, dass es unfassbar viel mehr Daten gibt, weil inzwischen überall Sensoren sind. Alles ist vernetzt, überall sind Chips, im Handy, im Auto, in all den Kameras, bald vielleicht standardmäßig in unserer Kleidung. Gleichzeitig gibt es zu geringen Kosten Rechnerleistung, um diese Datenmengen zu bewältigen. KI lebt von Daten, damit sie lernen kann. Denn das macht eine KI – Unmengen an Daten verarbeiten und abgleichen, immer besser werden, um ein spezifisches Problem zu lösen. Je mehr Daten, je schneller

die Computer, desto besser die KI; und dazu die Menschen, die diese Methode, diese Chance nutzen. Gerade entstehen praktisch täglich neue Anwendungen – auch im militärischen Bereich mit entsprechenden sicherheitspolitischen Implikationen. KI ist zentraler Bestandteil des „digitalen Gefechtsfelds" oder, ein bisschen drastischer formuliert, KI kann eine „Waffe" sein.

IP: *Dann sind wir schnell bei den so genannten „Killerrobotern".*
Suder: Da muss man unterscheiden. Was sind eigentlich Killerroboter? Letztlich geht es um Automatisierung und um autonome Entscheidungen von Waffensystemen. Automatisierung einzelner Funktionen von Waffensystemen gibt es natürlich heute schon und in großer Anzahl, von der automatischen Temperaturregulierung über Notfallprozeduren bis hin zur Flugstabilisierung. Der Eurofighter kann nicht stabil fliegen ohne einen Computer; tatsächlich sind in ihm über 80 verbaut. Das findet vermutlich kaum jemand problematisch. Worum es in der Diskussion eigentlich geht, ist der automatisierte und insbesondere der autonome Einsatz von kinetischer Wirkung gegen Menschen. Es ist wichtig, hier klar in der Definition zu sein. Die Flugabwehrsysteme auf Schiffen, die Rolling Airframe Missile (RAM)-Systeme schießen auch automatisiert und adjustieren ihre Ziele autonom. Diese Ziele sind allerdings keine Menschen, sondern mit hoher Geschwindigkeit und Präzision anfliegende Raketen, und RAMs sind der menschlichen Reaktionsfähigkeit deutlich überlegen. Auch das wird, zumindest mehrheitlich, nicht als problematisch angesehen. Aber die entscheidende Frage ist in der Tat – wird beim Einsatz kinetischer Gewalt gegen Menschen autonom entschieden bzw. wie geht man mit derartigen Entwicklungen um? Die Bundesregierung hat dazu ganz klar „nein" gesagt. Es braucht immer „the man in the loop" – ein Mensch ist in solche Entscheidungen eingebunden. Was andere Länder machen werden, ist – leider – nicht unter unserer Kontrolle. Aber Deutschland hat es ausgeschlossen und setzt sich, zu Recht, sehr dafür ein, hier mehr internationale Regulierung zu erwirken, so schwer das ist – auch weil es aufgrund der rasanten technologischen Entwicklung immer neue Fragen zu lösen gilt, immer mehr Grauzonen entstehen.

IP: *Was KI als Waffe bzw. das digitale Gefechtsfeld angeht – welche Entwicklungen sehen Sie?*
Suder: Auch dort gibt es immer mehr Sensoren, insbesondere Kameras, aber auch Satellitenbilder, Informationen aus dem Internet, Mobilfunkdaten und so weiter. Es werden immer mehr Daten und Informationen gewonnen und ausgewertet. Und dadurch, durch die Digitalisierung der Erhebung, Verarbeitung und Präsentation all dieser Daten, kann man Wirkungsüberlegenheit erlangen. Wer bessere Informationen hat, wem es gelingt, all diese Informationen zusammenzufügen, der gewinnt. Weil man mehr sieht; weil man genauer sieht, wo der Angreifer ist, was er tut, wie er ausgerüstet ist, usw. Umgekehrt wird man durch die stärkere Vernetzung und Digitalisierung – ob wir jetzt vom Eurofighter oder vom Schützenpanzer Puma sprechen, der ein stark digitalisiertes Fahrzeug ist, oder von der Abhängigkeit von Lageinformationen – auch immer verwundbarer. Digitalisierung heißt ja letztlich, dass alles mit-

einander (digital) verbunden ist. Und die Kehrseite ist Cyber – alles wird gehackt. Deshalb spielt Cybersicherheit, also der Schutz vor Angriffen auf Computer und Programme, so eine große, wenn nicht die zentrale Rolle. Damit sind wir beim Thema Cyberraum und der Frage, welche Rolle KI darin einnimmt. KI lässt sich zum Beispiel als Tool einsetzen, um Cyberangriffe zu fahren oder sich dagegen zu verteidigen. KI kann Cyberangriffsmuster erkennen, und wer es schafft, die beste KI zu entwickeln, hat wiederum einen Verteidigungs- oder gar Angriffsvorteil. Deshalb spielt KI sicherheitspolitisch eine so bedeutende Rolle – wie bei jeder Technologie geht es um Vorherrschaft. Wir befinden uns mitten in einem globalen Wettstreit, vor allem zwischen den USA und China. Vor etwa einem Jahr hat China seine KI-Strategie veröffentlicht – ein ausgesprochen ambitionierter Plan, in dem ganz klar das Ziel formuliert wird, bis 2025 Weltspitze werden zu wollen.

IP: *Dass Googles AlphaGo den weltbesten Spieler Ke Jie im Mai 2017 in Go besiegt hat, soll ja so etwas wie ein Sputnik-Schock für die Chinesen gewesen sein.*
Suder: Ja, ich glaube, genauso ist es. In China gibt es Unmengen von Daten, die Menschen scheinen dort williger zu sein, ihre Daten preiszugeben. Es herrscht ein anderes Verhältnis zur Privatsphäre mit anderen Datenschutzregeln. Gleichzeitig gibt es hochgradig vernetzte Sensorik und Prozessoren überall – Handys, Computer, Kameras usw. Und rund 1,5 Milliarden Chinesen, viele sehr technikaffin; „early adopters“, die jede Neuerung mitmachen. Gerade gegenüber China sollte der Westen seine Haltung überdenken. Bislang bestand in weiten Teilen die Hypothese, dass die Chinesen nur kopieren, aber nichts selbst entwickeln können. Dieses Bild gilt es dringend zu revidieren. Außerdem geht es bei KI jetzt insbesondere um Umsetzung; darum, Anwendungen auf die Schiene zu bringen. Das werden die Chinesen im großen Stil machen. Und wenn sich die Chinesen etwas vornehmen … man schaue nur auf die Belt and Road Initiative.

IP: *Haben wir es denn bei KI noch mit nationalstaatlichen Entwicklungen zu tun oder sind es große multinationale Konzerne wie Google und Apple? Anders gefragt: Wer steuert die Entwicklung eigentlich?*
Suder: Das ist genau der Kern vieler Debatten und insbesondere der Frage nach dem deutschen bzw. europäischen Weg, auch im Unterschied zu den USA, wo die Entwicklungen überwiegend unternehmerisch getrieben sind, und China, wo der Staat stark dominant ist. Den Umgang mit Daten – von Regulierung über die Bereitstellung von Daten, zum Beispiel des öffentlichen Sektors, bis hin zur Datenkunde an Schulen oder Fortbildungsinstitutionen – gilt es jetzt auszugestalten, mit Offenheit und ausgewogenem Blick auf Chancen und Risiken.

IP: *Gibt es neben den USA und China noch andere wichtige KI-Staaten? Russlands Präsident Wladimir Putin sagte neulich: „Wer KI beherrscht, beherrscht die Welt.“*
Suder: Ich fürchte, das ist wahr. Letztlich kann ich Russland allerdings nicht ausreichend einschätzen. Definitiv haben wir hier einen staatlichen Spieler, der im Cyber- und Informationsraum intensiv unterwegs ist.

IP: *Müsste man KI praktisch mit der Erfindung der Atombombe vergleichen?*
Suder: KI hat definitiv das Potenzial, die gesamte Dynamik im Cyberraum zu verändern. Es handelt sich um eine Fähigkeit, die Wirkungsüberlegenheit herstellen kann. Damit geht es um den Kern von Sicherheit. Zumal es, zumindest bislang, nicht gelungen ist, globale Regulierungen oder Kontrollregime zu etablieren. Es gibt darüber hinaus noch weitere Effekte, die sich sicherheitspolitisch auswirken könnten und zumindest mitgedacht werden sollten. KI verändert die Wirtschaft, in vielen Teilen disruptiv und kurzfristig. Was passiert, wenn ein Land aufgrund von KI auf einmal wirtschaftliche Überlegenheit, ja Monopolstellung genießt? Welche Auswirkungen haben globale Veränderungen in Wertschöpfungsketten?

IP: *Dass technologische Innovationen alles verändern, haben wir ja historisch schon öfter gesehen. Was ist diesmal anders?*
Suder: Richtig, jede industrielle Revolution hat auch sicherheitspolitische Aspekte. Im Unterschied zu früher läuft diesmal alles viel schneller ab. Als neue Produktionsmethoden wie das Fließband erfunden wurden, hat sich das natürlich auch auf den militärischen Sektor ausgewirkt; nun konnte man schneller mehr Waffen produzieren. Oder als Flugzeuge erfunden wurden, wurde der Luftraum zu einer militärischen Dimension. Bei der technologischen Entwicklung von KI hat das im Gegensatz dazu viel unmittelbarere, schnellere und globalere Auswirkungen – so als stünde Ihnen, nachdem Sie gerade Pfeil und Bogen zur Seite gelegt haben, ein hochmoderner Kampfjet zur Verfügung, der auch noch kaum etwas kostet und ebenso einfach wie unbemerkt einzusetzen ist. Deshalb bereitet mir das Thema auch solche Sorgen. Insbesondere weil auch eine Terrorgruppe sich solcher Technologien bemächtigen könnte. Das Missbrauchspotenzial ist enorm. Und KI „missbräuchlich" einzusetzen, kostet im Zweifelsfalle nichts. Es fällt auch nicht auf, wenn jemand KI entwickelt oder stiehlt. Man sieht nichts, man hört nichts, man riecht nichts, man kann es nicht auf einem Satellitenbild erkennen.

IP: *Meinen Sie damit einen Angriff auf Infrastruktur, der diese physisch zerstört? Oder eher so genannte „Psy-Ops", psychologische Operationen zur Beeinflussung der öffentlichen Meinung?*
Suder: Alles. Man muss die ganze Palette anschauen – das ist zwar oft nicht einfach und wird gerne missverstanden, aber der Auftrag an Beteiligte im Sicherheitsbereich ist es nun einmal, sich mit allen möglichen Szenarien zu befassen. Mich beschäftigen am meisten die physikalischen, die realen Auswirkungen, wenn Netze bzw. Verschlüsselungen und Sicherheitssysteme geknackt würden. Dann könnte ein Gegner Züge entgleisen lassen oder medizinische Geräte kontrollieren oder, wie geschehen in der Ukraine, „einfach nur" das Licht ausschalten. Die Szenarien sind da endlos, aber potenziell verheerend.

IP: *Nimmt die Politik das Problem ernst genug?*
Suder: Ja. Schauen Sie sich zum Beispiel an, was in der vergangenen Legisla-

tur in der Bundeswehr passiert ist – die Einordnung von Cyber als relevante, eigenständige militärische Dimension, der Aufbau des Cyberkommandos, innovative Experimente wie der Cyber Innovation Hub und Investitionen in das universitäre Forschungsumfeld CODE in München.

IP: *Reicht das?*
Suder: Das ist schwierig abzuschätzen. Aber letztlich ist das genauso wie mit der Entwicklung eines neuen europäischen Kampfflugzeugs – was die Chinesen und die Amerikaner machen, hat ganz andere Dimensionen. Sollte man es deshalb nicht tun? Doch, man sollte.

IP: *KI ist ja auch schon im Kleinen relevant, zum Beispiel bei der Datenverarbeitung zur Erstellung eines Lagebilds …*
Suder: Ja, völlig richtig. An sich ist KI nichts Schlimmes und erstmal auch nicht gefährlich. Im Gegenteil, es bieten sich unglaubliche Vorteile und Chancen. Zum Beispiel lässt sich die Zivilbevölkerung besser schützen, ein Gebot der Genfer Konvention. Auch kann die Bundeswehr ihre eigenen Leute besser schützen. Mit KI lassen sich Prozesse verbessern – Verwaltungsprozesse, Beschaffungsprozesse und auch militärische Prozesse. Zum Beispiel bei der Krisenfrüherkennung. Heute liest ein Referent Einträge in sozialen Medien wie Facebook, liest jede Menge Papiere und Veröffentlichungen, bestimmt auch die *IP*. Wie viele Dokumente kann er an einem Tag bewältigen? Vielleicht 100. Eine Maschine kann Tausende, ja Millionen Dokumente „lesen“. Bewerten und insbesondere Handlungsempfehlungen ableiten sowie Entscheidungen treffen, all das muss am Ende ein Mensch tun.

IP: *Müssen wir im Westen unsere Einstellungen zum Datenschutz überdenken?*
Suder: Ich glaube, wir müssen darüber diskutieren, wie wir mit Daten umgehen, aber eben auch mit Algorithmen. Die spannende Frage ist – wie stellen wir eigentlich sicher, dass wir wissen, was die Algorithmen tun? Wer kontrolliert die Algorithmen? Das bedarf einer breiten Diskussion, und natürlich ist dies auch eine sicherheitspolitische Frage. Nehmen wir das Beispiel Krisenfrüherkennung – je nach Algorithmus bestimmen diese oder jene Faktoren das Ergebnis. Und wenn das dann lautet „Mit 35-prozentiger Wahrscheinlichkeit wird in acht Monaten im Land XY eine Krise ausbrechen.“ Was machen wir mit so einer Information? Das heißt, dass wir die Leute ganz anders ausbilden müssen; die meisten können mit Statistiken erst einmal nichts anfangen.

In jedem Fall brauchen wir mehr gesellschaftliche Debatten. Im Moment gibt es leider oft undifferenzierte Sichtweisen, teilweise Unkenntnis oder pauschale Ablehnung. Dabei gibt es kein Unternehmen, das sich nicht damit beschäftigt. An der Digitalisierung führt kein Weg vorbei. Kurz, wir müssen über Daten reden, wir müssen über Algorithmen reden, aber eben auch über die Zukunft der Arbeit und über Bildung. Und wie wir miteinander leben wollen – in einer Welt voller KI.

Die Fragen stellten Henning Hoff, Uta Kuhlmann und Joachim Staron.