



# Verantwortbarkeit als Designprinzip wehrtechnischer Systeme

Prof. Dr. Wolfgang Koch

Überraschenderweise hat die gedankliche Präzisierung des Begriffs „Unsicherheit von Daten“ und der methodisch nachvollziehbare Umgang damit ihre Wurzeln in der Rechtsprechung. Diese möchte auf der Grundlage für sich genommen ungewisser Zeugnisse in einer Gesamtbetrachtung vernünftig und „recht“ urteilen.

Subjektive Wahrscheinlichkeiten und ihre Verknüpfung – heute *Bayesian Learning* genannt – kennen bereits rabbinische Juristen im Spanien des 12. und 13. Jahrhunderts.<sup>1</sup> Sie fragten, ob man unsichere Aussagen systematisch „fusionieren“ kann: Wie akkumuliert man Einzelwahrscheinlichkeiten, um aus dem Ergebnis ein sichereres Urteil zu gewinnen? Diese Frage, lange vor dem presbyterianischen Pfarrer Thomas Bayes (1702–1761) gestellt, dessen Bedeutung der Mathematiker Pierre-Simon Laplace (1749–1827) erkannte, bleibt zeitlos relevant.

Im Zeitalter der Digitalisierung erwächst aus diesen Wurzeln ein mächtiger Baum, der nicht nur, aber auch die Wehrtechnik revolutioniert. „Künstlich intelligente“ Maschinen, die ungewisse Daten fusionieren, um daraus Handlungsoptionen zu generieren, werden die Möglichkeiten menschlichen Wahrnehmens und Wirkens weit über „natürliches“ Maß steigern. Noch weit mehr als bisher werden insbesondere die Aufklärungs- und Waffensysteme künstlich intelligent sein, mit denen die Bundeswehr Deutschlands Souveränität und die seiner Bündnispartner verteidigt, ihre Bürgerinnen und Bürger und die territoriale Integrität der Staatsgebiete schützt sowie Staaten und Gesellschaften widerstandsfähig gegen äußere Bedrohungen hält. Aber auch für Sicherheitsbehörden öffnen sich neue Wege zur Gefahrenabwehr im Inneren.

Gerade nach dem 24. Februar 2022 muss auch die deutsche Gesellschaft die militärischen Möglichkeiten künstlich intelligenter Maschinen erfassen, aber auch die Beherrschbarkeit der mit ihnen verbundenen ethischen Risiken verstehen und in ihre politische Meinungsbildung einbeziehen. Dies ist nicht nur unverzichtbar, um höchst reale Gefahren wirksam abwehren zu können, sondern auch, um politischen Einfluss auf die weitere Technologieentwicklung zu behalten, der Demokratien von Technokratien unterscheidet.<sup>2</sup> Vor allem am „scharfen Ende der Digitalisierung“<sup>3</sup>, also in der Wehrtechnik, bei der es um „Leben oder Tod“ gehen kann, zeigen sich die generellen Probleme der Digitalisierung wie in einem Brennglas. Denn auch für autonome Fahrzeuge, in der Medizin und beim Arbeitsschutz, um Beispiele zu nennen, entstehen analoge Probleme.

### Gesteigerte Wahrnehmung, vergrößerte Wirkungskreise

Mit künstlich intelligenten Maschinen tut sich unsere Gesellschaft jedoch schwer. Wer nach China blickt, erschrickt: Bald sind alle Chinesinnen und Chinesen sensoruell „getrackt“, datentechnisch erfasst und durch *Social Credits* maschinell bewertet. Das soll zu mehr Sicherheit führen; doch was geschähe bei derartiger Überwachung mit unseren bürgerlichen Freiheiten, mit der Demokratie als Lebensform? Aber auch eine weitere Frage will beantwortet sein: Soll unsere Demokratie wehrhaft sein? Demokratische Gemeinwesen müssen sich auch äußerer Feinde erwehren können, etwa durch Abwehr hybrider Kriegführung und Desinformation. Zwar scheinen die Debatten um bewaffnete Drohnen im Rahmen der von Bundeskanzler Scholz ausgerufenen Zeitenwende und dem Beschluss, diese für die Bundeswehr zu beschaffen, beendet zu sein. Aber zeigten sie nicht, wie wenig der Protest gegen die Wiederbewaffnung der 1950er-Jahre trotz verfassungsrechtlicher Verankerung der Bundeswehr in der bundesdeutschen Gesellschaft überwunden war? Ist er es jetzt? Was wird geschehen, wenn sich die Schockstarre des 24. Februar 2022 wieder lösen wird?

Künstlich intelligente Maschinen gestalten nicht nur die äußere und innere Gefahrenabwehr tiefgreifend um, sondern auch unsere Gesellschaft als solche. Wie jede technische Innovation, die unser

Künstlich intelligente Maschinen gestalten nicht nur die äußere und innere Gefahrenabwehr tiefgreifend um, sondern auch unserer Gesellschaft als solche.

Wahrnehmungsfeld erweitert und unseren Wirkungskreis vergrößert, bergen sie eigene Gefahren und wecken in unserer Gesellschaft Ängste, die nicht nur unbegründet sind. Umso mehr bedarf es nüchterner Debatten über die Allgegenwart vernetzter Sensoren und die Welt der Algorithmen, die aus ungeheuren Datenströmen maschinen- und menschenverwertbare Information fusionieren, der Grundlage teil- und vollautomatischer Aktionen, gerade auch „am scharfen Ende“.

„Kognitive“ und „volitive“ Maschinen verfügen zwar selbst weder über Wahrnehmung noch einen Willen, steigern jedoch menschliche Fähigkeiten bewusster Wahrnehmung und absichtlicher Willensbildung. Wie bleibt der Mensch aber seiner neuen Macht geistig und seelisch gewachsen? Wie bleibt er derartigen Maschinen gegenüber letztverantwortlich überlegen, die ihm sonst unzugängliche Massendaten erschließen und seine Entscheidungen in automatisierte Aktion höchster Tragweite transformieren? Ohne die künstlich intelligente Assistenz dieser Maschinen könnten wir in der komplexen Technosphäre, die uns im Bereich der Verteidigung immer dichter umschließt, jedenfalls nicht mehr verantwortlich wirken. Wie kann ihr technisches Design die verantwortete Beherrschbarkeit erleichtern?

### Ziele künstlich intelligenter unterstützten rechten Handelns

Wer über ethisch akzeptables und rechtlich zulässiges Handeln im Kontext künstlich intelligenter Maschinen nachdenkt, über das man Rechenschaft ablegen kann, muss sich der Ziele rechten Handelns bewusst werden, das solcherart unterstützt wird. Für den Philosophen Robert Spaemann (1927–2018) bestehen „künstliche Dinge“ – insbesondere künstlich intelligente Maschinen – „aus einem Woraus und einem Was. Ihr ‚Wie‘ und ‚Wozu‘ liegt nicht in ihnen, sondern im Menschen. Ein Naturding ist hingegen dadurch charakterisiert, dass ‚Was‘ und ‚Wozu‘ in ihm selbst in eins fallen. Der Zweck ist die Form der Sache selbst, darum also auch das Wort *entelecheia*: ich trage das Ziel in mir“<sup>4</sup>.

Nur wenn man weiß, woher man kommt und das Ziel kennt, kann man rechte Wege wählen. Was leitete den bundesdeutschen Kanzler,

der Westdeutschland in die NATO führte? Seine Gründe erweisen sich gerade in unserer Gegenwart als zeitlos und sollen auch „das ‚Wie‘ und ‚Wozu‘“ künstlich intelligenter Waffensysteme der Bundeswehr prägen. Die NATO sei eine Gemeinschaft freier Nationen, entschlossen, „das gemeinsame Erbe der abendländischen Kultur, die persönliche Freiheit und die Herrschaft des Rechts zu verteidigen“, unterstrich Konrad Adenauer (1876–1967) an jenem 9. Mai 1955 des westdeutschen NATO-Beitritts, dem fünften Jahrestag der Schuman-Erklärung, der Geburt des vereinten Europa also, und dem zehnten Jahrestag der Wehrmacht kapituliert. Daher entsprächen ihre Ziele „angesichts der politischen Spannungen in der Welt vollständig den natürlichen Interessen des deutschen Volkes, das sich [...] wie kaum ein anderes Volk nach Sicherheit und Frieden sehnt“. Gemeinsame Verteidigung müsse jedoch eingebettet sein in „die Förderung der allgemeinen Wohlfahrt der Völker und zur Bewahrung ihres gemeinsamen Kulturerbes zu einer Zusammenarbeit in wirtschaftlichen und kulturellen Fragen“. Deutschland werde „alle seine Kräfte darauf verwenden, dass die menschliche Freiheit und die menschliche Würde erhalten bleiben“.<sup>5</sup>

### Verantwortbarkeit als systemtechnisches Designprinzip

Als Konzeptionär zog Wolf von Baudissin (1907–1993) für „Adenauers Armee“, die der bundesdeutsche Gründungskanzler schuf, im Sinne „menschlicher Freiheit und Würde“ nicht nur Lehren aus einem Verbrecherstaat, sondern auch aus einem „totalen Krieg“, der von der Hochtechnologie seiner Zeit geprägt war: „Das aufs höchste technisierte Gefecht verlangt, dass die Verantwortung an sehr vielen unteren Stellen gesehen und getragen wird“, formuliert er bereits 1954, also zwei Jahre vor der *Dartmouth Summer School*, die den Begriff „Künstliche Intelligenz“ prägte.<sup>6</sup> „Daher muss alles getan werden“, setzt er fort, „um den Menschen vor Situationen zu stellen, die seine Verantwortung herausfordern und ihn die Folgen von Tun und Unterlassen erleben lassen.“<sup>7</sup>

Verantwortbarkeit ist demnach ein fundamentaleres Konzept als etwa *Human in* oder *on the Loop*. Denn auch Automation, sogar Hochautomation von Waffensystemen kann verantwortbar sein,

wenn die Reaktionszeiten für Menschen zu kurz oder die Datenfülle zu groß werden. Künstlich intelligente Maschinen müssen gerade dann technische Beherrschbarkeit und ihren verantwortungsvollen Einsatz gewährleisten. Der Mensch ist immer eingebunden, nicht nur durch die Entscheidung, derartige Maschinen tatsächlich einzusetzen, sondern sie so zu erforschen, zu entwickeln, zuzulassen, zu beschaffen und die Einsatzvorbereitung so auszulegen, dass ihr militärischer Einsatz ethisch akzeptabel und rechtskonform bleibt.

Zugleich ist für den Einsatz und im Einsatz Wissen zu vermitteln, durch das die verantwortlich handelnden Menschen einerseits algorithmischer Entscheidungsunterstützung vertrauen können und andererseits die Grenzen kennen, die jede derartige Assistenz besitzt (Fehleinschätzungen, „blinde Flecken“, Artefakte, Stör- und Täuschbarkeit durch Gegner). Insbesondere müssen auf künstlich intelligenten Maschinen basierende Erkenntnisse für Menschen plausibel „erklärbar“ sein, auch wenn sie im Detail nicht mehr nachvollziehbar sind. Zugleich ist zu verhindern, dass menschliche Operateure kritiklos maschinelle Handlungsempfehlungen ohne eigenes Abwägen bestätigen.

### Künstlich intelligent unterstützte Aufklärung und Wirkung

Die *AI Strategy* des US-amerikanischen Verteidigungsministeriums definiert Artificial Intelligence (AI) als „die Fähigkeit von Maschinen, Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern“. Dies schließt längst etablierte Technologien ein, zum Beispiel Autopiloten für Flugzeuge, Raketensteuerung und Signalverarbeitungssysteme. „Die meisten Durchbrüche der letzten Jahre in diesem Bereich konzentrierten sich jedoch auf das maschinelle Lernen (ML), ein Teilgebiet der Künstlichen Intelligenz. Maschinelles Lernen ist eng mit der Statistik verwandt und ermöglicht es Maschinen, aus Daten zu lernen.“<sup>8</sup>

Im Sinne dieser pragmatischen Definition treiben KI-Algorithmen einen Informationskreislauf an, indem sie massenhaft anfallende Informationsbruchstücke aus verteilten Sensornetzen und umfassenden Datenbanken fusionieren, die von Menschen nicht

Künstlich intelligente Maschinen müssen gerade bei Hochautomation technische Beherrschbarkeit und ihren verantwortungsvollen Einsatz gewährleisten.



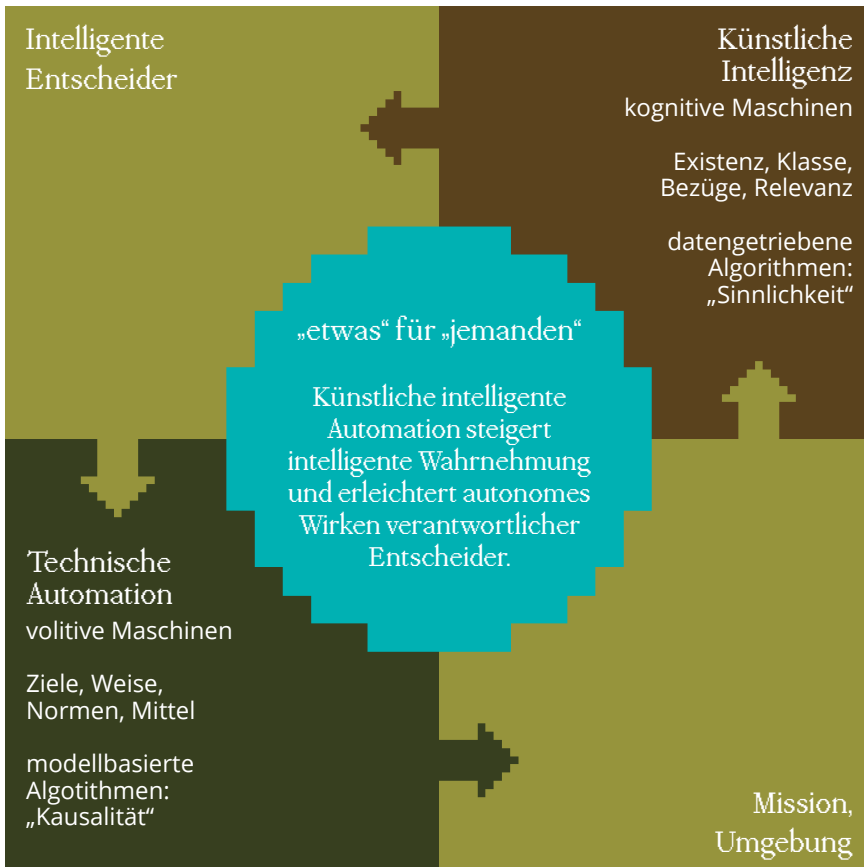


Abbildung 1: Kognitive und volitive Unterstützung für den intelligenten Verstand und den autonomen Willen verantwortungsvoll handelnder militärischer Entscheiderinnen und Entscheider. Quelle: Fraunhofer FKIE.

ohne maschinelle Assistenz nutzbar sind. Wie in Abbildung 1 dargestellt, unterstützen sie den bewusst wahrnehmenden Verstand militärischer Entscheiderinnen und Entscheider beim Verstehen komplexer, weiträumiger und sich dynamisch verändernder Lagen und bei der Durchsetzung seines Willens durch lageadäquate Maßnahmen, indem sie seine absichtlichen Entscheidungen in automatisch ausgeführte Befehlsketten übersetzen.

Die Vorstellungen von Vernunft und Willen und damit von Bewusstsein und Verantwortung bringen Personen in den Blick, die „jemand“ und nicht „etwas“ sind. Kognitive und volitive Assistenzsysteme hingegen sind und bleiben unabhängig von ihrem technischen Entwicklungsstand

immer eine „Sache“, verfügen nicht selbst über Kognition oder Volition. Die fundamentale Dichotomie „etwas *versus* jemand“ ist zu betonen, um sowohl übertriebenen Erwartungen als auch übertriebenen Ängsten zu begegnen, die sich in den gesellschaftlichen Debatten über künstlich intelligente Automatisierung in der Verteidigung zeigen.

Erstmals in Deutschland begleitet gedankliches Ringen um die technische Umsetzung ethischer und rechtlicher Prinzipien im Sinne der Verantwortbarkeit ein militärisches Großprojekt von Beginn an. Im künftigen europäischen Luftkampfsystem sind bemannte Jets neuester Generation Elemente eines komplexen und umfassend vernetzten *System of Systems*. Unbemannte *Remote Carrier* schützen als *Loyal Wingmen* die Pilotinnen und Piloten und begleiten sie in Kampfmissionen. Ziel der Arbeitsgemeinschaft Technikverantwortung für ein Future Combat Air System (FCAS) ist es, Ethik, Recht und politisches Wollen technisch zu operationalisieren.<sup>9</sup> Die nachfolgende Diskussion bezieht sich daher beispielhaft auf künftige Luftkampfsysteme.

### **Ethical AI-Demonstrator für ein künftiges Luftkampfsystem**

Um den Einsatz künstlich intelligenter Maschinen gerade in Stresssituationen realitätsnah zu erfahren, wird zurzeit ein *FCAS Ethical AI-Demonstrator* entwickelt. Dieses Ausbildungsinstrument lässt Soldatinnen und Soldaten den Einsatz von künstlich intelligenter Automation in einem militärischen Szenario mit allen damit verbundenen Aspekten der psychischen Belastung möglichst realitätsnah erleben.<sup>10</sup>

Ausgewählte Features ermöglichen die Interaktion mit einem realen, für den militärischen Einsatz entwickelten KI-Modell, um einen realistischen Blick auf die Möglichkeiten, Grenzen, ethischen Implikationen und technischen Anforderungen dieser Technologie in der Praxis zu gewähren. Mit Unterstützung der Luftwaffe entstanden die zugrundeliegenden Szenarien. Da dieses Vorgehen ein Novum ist, besitzt es naturgemäß experimentellen Charakter. Ohne ein Menschenbild jedoch, das verantwortlichen Technikgebrauch ermöglicht, ohne den Staatsbürger in Uniform, ist jede digitale Assistenz für moralisch akzeptable Entscheidungen fraglich.

Der *FCAS Ethical AI-Demonstrator* wird im Rahmen der weiteren Fähigkeitsentwicklung der Luftwaffe dazu beitragen, verantwortete Beherrschbarkeit durch ein entsprechend ausgelegtes Systemdesign zu garantieren. Beispielhaft genannt seien:

- ➔ Nutzerinnen und Nutzern muss der Umgang mit künstlich intelligenter Unterstützung in seinen Möglichkeiten und Grenzen vertraut sein, insbesondere dass diese sich vollständiger Nachvollziehbarkeit entzieht und für gegnerische Angriffe anfällig ist. Trainiert werden müssen die Einschätzung der Plausibilität (*Explainability*) und die Situationsabhängigkeit des ethischen Rahmens.
- ➔ Zulassung und Qualifizierung sind Schlüsselthemen für künftige Luftkampfsysteme, *System of Systems* aus bemannten und unbemannten Komponenten. Robuste KI-basierte Systeme werden sowohl datengetriebene als auch modellbasierte Algorithmen umfassen. Systemisch wären datengetriebene Algorithmen durch modellbasiertes *Reasoning* „einzuhegen“ – *AI in the Box*.
- ➔ Nachzuweisen sind vorhersagbare Systemeigenschaften, Insensibilität gegenüber unbekanntem Einflüssen, Adaptivität gegenüber variablem Einsatzkontext und *Graceful Degradation*. Test- und Charakterisierbarkeit, *Explainability* bei kritischen Komponenten und systemimmanente *Compliance to a Code of Conduct* sind zwingende Voraussetzungen für Zulassung und Qualifizierung.

Umfassende Analysen zur technischen Beherrschbarkeit und persönlicher Verantwortlichkeit dieser Art sind generell bei digitalisierungsdominierten Rüstungsprojekten unverzichtbar und sollten soweit wie möglich öffentlich sichtbar, transparent und überprüfbar durchgeführt werden. Andernfalls wären der gravierende Paradigmenwechsel und die materiellen Aufwendungen für große Rüstungsvorhaben politisch, gesellschaftlich und finanziell kaum durchsetzbar.

### Systemtechnische Umsetzung des Verantwortungsbegriffs

Abbildung 2 veranschaulicht Kernelemente eines am Verantwortungsbegriff ausgerichteten *Systems Engineering* als Dreiecksrelation. Sie geht von Personen oder Personengruppen aus

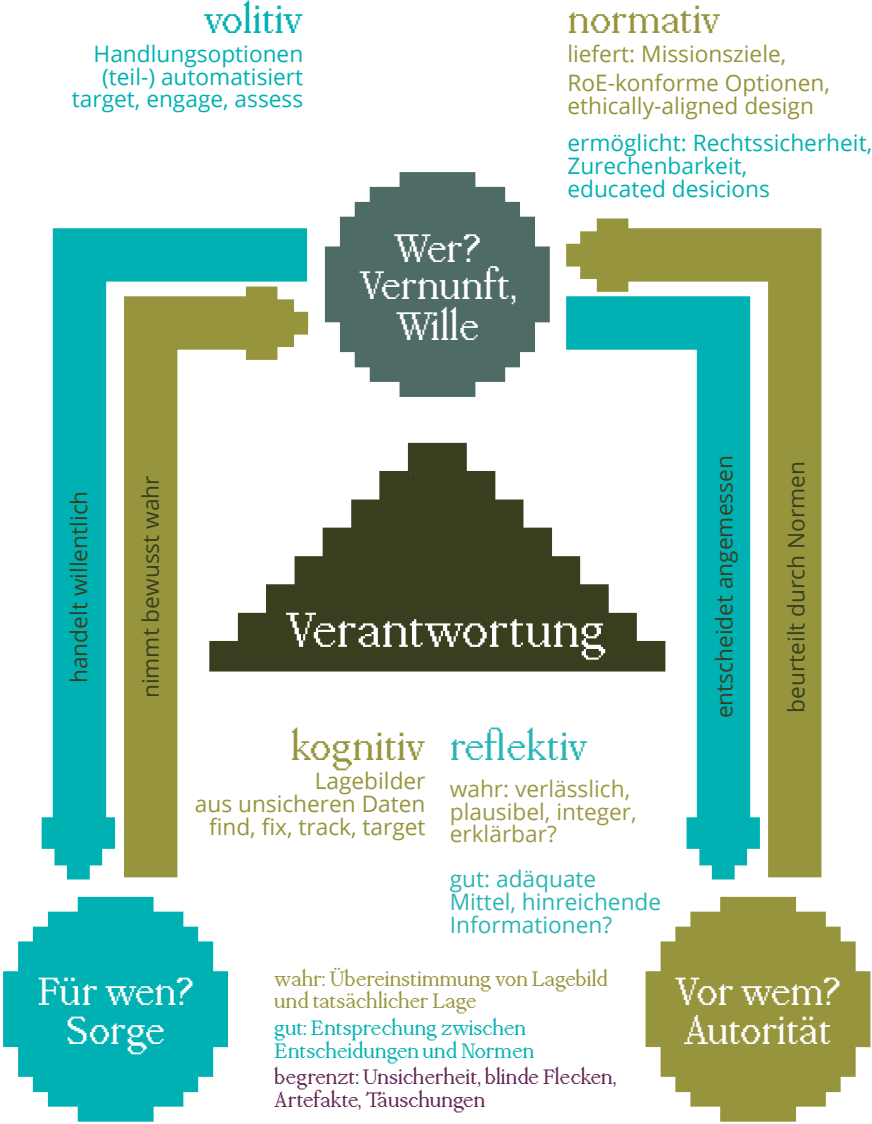


Abbildung 2: Künstlich intelligente automatische Assistenz, die verantwortungsvollen Einsatz militärischer Systeme unterstützt.  
Quelle: Fraunhofer FKIE.

und etabliert charakteristische Beziehungen zwischen ihnen. Verantwortungsvolle Systemauslegung ist demnach per Definition anthropozentrisch.

- ➔ Wer trägt Verantwortung? Die Entwicklung militärischer Fähigkeiten erfordert auf verschiedenen Ebenen verantwortliches Handeln, in der Forschung, Entwicklung, Zertifizierung und Qualifizierung militärischer Systeme, aber auch bei der Vorbereitung und Durchführung militärischer Operationen.
- ➔ Für wen wird Verantwortung getragen? Die Beziehung zwischen verantwortlichen Personen und denjenigen, für die sie verantwortlich sind, ist durch die Begriffe „Sorge“ und „Vertrauen“ gekennzeichnet und daher durch prospektives Agieren und Reagieren bestimmt.
- ➔ Wem gegenüber wird Verantwortung übernommen? Verantwortung impliziert die Vorstellung von einer personenhaften Autorität, die sich durch Urteilsfällung ausprägt. Die verantwortliche Person erkennt diese Autorität durch Rechtfertigung an. Diese Beziehung ist retrospektiver Natur.

Als grundlegende Begriffe erscheinen das „Wahre“, hier pragmatisch umrissen als Entsprechung zwischen einem Lagebild und der tatsächlichen Lage, und das „Gute“, definiert als Entsprechung zwischen getroffenen Entscheidungen und zugrundeliegenden Normen. Im *Fog of War* werden diese Entsprechungen aufgrund der Ungewissheiten in den Daten, den *Blind Spots* und Artefakten der KI sowie wegen gegnerischer Störung und Täuschung jedoch niemals vollkommen sein.

Freiwillig übernommene Verantwortung, die sich in „Sorge“ und „Vertrauen“ zeigt sowie in der Bereitschaft, sich vor einer Autorität zu rechtfertigen und im Gehorsam gegenüber Normen richtig zu entscheiden, erhält den Zusammenhalt militärischer Kräfte im Kampf. Sie kann und soll durch **normative** und **reflektive** Assistenzsysteme technisch unterstützt werden. Rein rechtliche Konstrukte wie die „Haftung“, die im zivilrechtlichen Kontext unverzichtbar sind, erweisen sich gerade in militärischen Einsätzen als unzureichend.

Gemäß diesen Überlegungen können Maschinen niemals verantwortungsvoll oder unverantwortlich, das heißt „gut“ oder „böse“ handeln, indem sie auf moralische Herausforderungen in der einen oder anderen Weise reagieren, sondern nur Menschen. Im übertragenen Sinne jedoch fördern „gute“ Systeme ihren moralisch akzeptablen und effizienten Einsatz zur Zielerreichung, während „böse“ Systeme ihren unverantwortlichen Einsatz zur Zielerreichung erleichtern.

### Kernelemente reflektiver und normativer Assistenzsysteme

Ein reflektives Assistenzsystem ermöglicht sowohl bei der Einsatzvorbereitung als auch im Einsatz, feindliche Objekte in verschiedenen Szenarien mit und ohne künstlich intelligenter Unterstützung als solche zu erkennen, zu identifizieren und zu verfolgen. Wichtig ist in diesem Zusammenhang die Nutzung mehrerer, sich komplementär ergänzender Sensoren. Künstlich intelligent gewonnene Vorschläge werden in ihrer Gewichtung grafisch hervorgehoben. Optionale Bestätigungsdialoge liefern detailliertere Informationen zu den von der KI erkannten oder vorausgewählten Objekten und bereichern sie mit Kontextwissen an. Die konkrete Auslegung der reflektiven Assistenz wird von der Art des Einsatzes und der konkreten Situation im Rahmen eines Einsatzes abhängig sein.

Bei der Gestaltung eines technischen Systems zur normativen Assistenz müssen zunächst die Möglichkeiten und Grenzen der Umsetzung rechtlicher Grundsätze in technische Designprinzipien bedacht werden.<sup>11</sup> Der Einfachheit halber sei der normative Rahmen im Folgenden durch die *Rules of Engagements* (RoEs) vorgegeben. RoEs sollten grundsätzliche Risiken künstlich intelligenter Automation widerspiegeln. Einige Elemente seien hervorgehoben:

- Bestimmte Rechtsprinzipien scheinen sich prinzipiell nicht in eine algorithmische Form übersetzen zu lassen, zum Beispiel das Proportionalitätsprinzip. Diese müssen als solche klar identifiziert werden.

- ➔ Wenn eine algorithmische Implementierung möglich ist (zum Beispiel die Unterscheidung zwischen Zivilistinnen und Zivilisten und Kombattantinnen und Kombattanten), sind bestimmte Schwellenwerte vorausgesetzt. Auf taktischer Ebene sollten regelbasierte RoEs meist implementierbar sein.
- ➔ Beispiele für Schwellenwerte, die in militärischen Dokumenten genannt werden, sind: möglich (< 30 Prozent), vermutlich (30–90 Prozent) und wahrscheinlich (> 90 Prozent).
- ➔ Sind Rechtsgrundsätze quantitativ erfassbar, sollte ihre rechtskonforme Implementierung durch technisches Systemdesign erreicht werden, gegebenenfalls ergänzt durch *Sandboxing* und *Auditing*.
- ➔ Für die Entwicklung umfassend rechtskonformer Systeme muss die systemische Kombinierbarkeit mehrerer Einzelösungen gegeben sein, die zum Beispiel bestimmte *Boxes* um künstlich intelligente Automation bilden.
- ➔ Prinzipiell nicht maschinell zu unterstützen ist die Entscheidung über zugrundeliegende „Werte“.

## Fazit

Der Digitalrat Bundesministerium der Verteidigung stellt fest: „Die Digitalisierung betrifft mehr als den Aspekt der technischen Innovation. Sie beeinflusst die gesamte Denk- und Handlungsweise der Bundeswehr auf allen Ebenen im Sinne eines ‚Digitalen Selbstverständnisses der Bundeswehr‘.“<sup>12</sup> In diesem Sinne wäre festzuhalten:

- ➔ Digitales Ethos und eine entsprechende Moral gehören zu den auf- und auszubauenden menschlichen Kompetenzen, um wehrtechnische Systeme verantwortungsvoll zu entwickeln und einzusetzen. Insbesondere befähigen sie Führungskräfte, „die Potenziale und Auswirkungen von

digitalen Technologien einschätzen zu können sowie in einer digitalisierten Umgebung zu steuern/führen“, wie der Digitalrat formuliert. Es wäre insbesondere zu überlegen, für den Auf- und Ausbau ethischer Kompetenz das bewährte Instrument der Inneren Führung im Sinne der digitalen Transformation der Streitkräfte weiterzuentwickeln.

- ➔ Neben dem operativen Mehrwert künstlich intelligenter Wehrtechnik, um Fähigkeitslücken der Bundeswehr zu schließen, ihr Fähigkeitsspektrum zu erweitern und dafür Konzepte, Verfahren oder organisatorische Maßnahmen zu entwickeln, sind ethische Kompetenzen im Umgang mit digitalen Technologien und ethische Akzeptanz vor dem Gewissen der einzelnen Soldatinnen und Soldaten, aber auch vor der Gesellschaft, wesentliche Kennzeichen geglückter Innovation.
- ➔ Analog zum Eid des Hippokrates der Ärzte, die ebenso wie Soldatinnen und Soldaten zur Verantwortung verpflichtet sind, wäre die bei der Gründung der Bundeswehr für unerlässlich gehaltene Vereidigung im Kontext der Digitalisierung mit frischem Blick zu sehen. Für von Baudissin gehörte es „zu den wesentlichen Aufgaben der Militärgeistlichen, auf die Heiligkeit des Eides, wie auch des Gelöbnisses zu weisen, dem Rekruten den Ernst der Übernahme seiner Dienstpflichten auf sein eigenes Gewissen, zugleich aber auch die von Gott gesetzten Grenzen jeder und auch dieser Verpflichtung aufzuzeigen“<sup>13</sup>.

In diesem Geiste verabschiedete sich Konrad Adenauer 1963 von der Bundeswehr „als dem sichtbarsten Ausdruck des Wiederaufbaus Deutschlands, als Wiederherstellung der Ordnung, als Beweis der Eingliederung in die Front freier Völker zum Schutze unseres Vaterlandes“<sup>14</sup>. Auch für künftige wehrtechnische Systeme soll seine Feststellung gelten: „Soldaten, wenn wir nicht unsere Streitmacht geschaffen hätten, hätten wir Freiheit und Frieden schon lange verloren. So haben Sie, Soldaten, durch die Arbeit, die Sie geleistet haben, in Wahrheit dem deutschen Volke den Frieden geschenkt und erhalten.“



Künstlich intelligente Maschinen werden auch die Verteidigung Europas prägen, da die militärische Technosphäre ohne die Welt der Algorithmen unbeherrschbar ist. Ganz im Sinne ihrer konzeptionellen Identität liegt die Bedeutung der Künstlichen Intelligenz für die Bundeswehr auch gemäß ministeriellen Texten „nicht in der Entscheidung Mensch oder KI, sondern in einer effektiven und skalierbaren Kombination von Mensch und KI, um eine bestmögliche Aufgabenerfüllung zu gewährleisten“<sup>15</sup>.

Bei der Nutzung künstlich intelligenter Maschinen verdichten sich technische, ethische und rechtliche Herausforderungen der KI, die sich generell stellen. Daher ergeben sich auch für die wehrtechnische Forschung neuartige Aufgaben.<sup>16</sup> Das technische Design derartiger Maschinen muss eine militärische Kernforderung erfüllen: „Kennzeichnende Merkmale militärischer Führung sind die persönliche Verantwortung militärischer Entscheider und die Durchsetzung ihres Willens in jeder Lage“, wie die „Konzeption der Bundeswehr“ 2018 bekräftigt.<sup>17</sup>

Verantworteter Waffeneinsatz und effektive „Wirkung im Ziel“ schließen sich nicht aus. Entscheidend ist die Frage: Welcher normative Rahmen trägt den sicherheitspolitischen und operativen Realitäten des 21. Jahrhunderts Rechnung und ermöglicht zugleich die Nutzung künstlich intelligenter Maschinen? Damit wirken diese im Sinne einer „Förderung der allgemeinen Wohlfahrt der Völker und zur Bewahrung ihres gemeinsamen Kulturerbes“, wie es Konrad Adenauer in seiner Rede am 9. Mai 1955 zur Aufnahme der Bundeswehr in die NATO formulierte.

- 1 N. Rabinovitch (1973). *Probability and Statistical Inference in Ancient and Medieval Jewish Literature*. University of Toronto Press.
- 2 N. Bossong/A. Rieks/W. Koch (2022). Künstliche Intelligenz für die Landesverteidigung. In: *Frankfurter Allgemeine Zeitung* vom 31.1.2022, Nr. 25, 18.
- 3 A. Rieks (2022). Digitalisierung ist die DNA der Luftwaffe. Interview mit Generalleutnant Dr. Ansgar Rieks, Stellvertreter des Inspektors der Luftwaffe. In: *Hardthöhenkurier* 1/2022, 30ff. [https://www.hardthoehenkurier.de/hhkemags/hhkfreemags/2022-01/index\\_40.html#page=31](https://www.hardthoehenkurier.de/hhkemags/hhkfreemags/2022-01/index_40.html#page=31) (letzter Zugriff: 10.10.2022).
- 4 R. Spaemann u. a. (2005). *Natürliche Ziele. Geschichte und Wiederentdeckung teleologischen Denkens*. Stuttgart: Klett-Cotta, 51f.
- 5 K. Adenauer (1955). *Aufnahme der Bundesrepublik Deutschland in die NATO*. Paris: Palais de Chaillot, 9.5.1955.
- 6 Schon in diesem Jahr wird versprochen, aber bis heute nicht eingelöst, „dass jeder Aspekt des Lernens oder jedes andere Merkmal der Intelligenz im Prinzip so genau beschrieben werden kann, dass eine Maschine sie simulieren kann“. In: John McCarthy/Marvin Minsky/Nathaniel Rochester/Claude Shannon (1956). *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. <http://raysolomonoff.com/dartmouth/boxa/dart564props.pdf> (letzter Zugriff: 10.10.2022).
- 7 W. v. Baudissin (1969). *Soldat für den Frieden. Entwürfe für eine zeitgemäße Bundeswehr*. München: Piper Verlag, 234.
- 8 G. Allen (2022). *Understanding AI Technology. A concise, practical, and readable overview of Artificial Intelligence and Machine Learning technology designed for non-technical managers, officers, and executives*. Joint Artificial Intelligence Center (JAIC), Department of Defense, USA: <https://apps.dtic.mil/sti/pdfs/AD1099286.pdf> (letzter Zugriff: 10.10.2022).
- 9 [www.fcas-forum.eu](http://www.fcas-forum.eu)
- 10 W. Koch (2022). *Elements of an Ethical AI Demonstrator for Responsibly Designing Defence Systems*. 2022 25th IEEE International Conference on Information Fusion (FUSION), pp. 1–8.
- 11 T. Singer (2022). KI im operationellen Kontext: Zur technischen Übertragbarkeit von Regeln des humanitären Völkerrechts auf Künstliche Intelligenz. In: W. Koch (Hrsg.) (2022). *Künstlich intelligente Maschinen? Fragen an Techniker und Juristen*. Sonderdruck der *Neuen Juristischen Wochenschrift*, München: C.H. Beck, 35f.
- 12 Erster Bericht zur Digitalen Transformation Erster Bericht zur Digitalen Transformation. In: Bundesministerium der Verteidigung 10/2019, 27. <https://www.bmvg.de/resource/blob/143248/7add8013a0617d0c6a8f4ff969dc0184/20191029-download-erster-digitalbericht-data.pdf> (letzter Zugriff: 10.10.2022).
- 13 von Baudissin, a. a. O., 181.
- 14 K. Adenauer (1963). *Ansprache in Wunstorf, Germany. Parade of the Bundeswehr*, 12.10.1963. <https://www.konrad-adenauer.de/quellen/reden/1963-10-12-ansprache-wunstorf> (letzter Zugriff: 10.10.2022).
- 15 Erster Bericht zur Digitalen Transformation, a. a. O., 27.
- 16 W. Koch (2020). *Zur Ethik der wehrtechnischen Digitalisierung – Informations- und ingenieurwissenschaftliche Aspekte*. In: M. Rogg u. a. (Hrsg.) (2020). *Ethische Herausforderungen digitalen Wandels in bewaffneten Konflikten*. Hamburg: GIDS, 17ff.
- 17 *Konzeption der Bundeswehr*. In: Bundesministerium der Verteidigung 2018,83. <https://www.bmvg.de/resource/blob/26544/9ceddf6df2f48ca87aa0e3ce2826348d/20180731-konzeption-der-bundeswehr-data.pdf> (letzter Zugriff: 10.10.2022).