Sandra Pravica

Variablen des Unberechenbaren. Eine Epistemologie der Unwägbarkeiten quantitativer Voraussageverfahren in Sicherheit und Militär

Abstract

Berechnung und Unberechenbarkeit stehen in den Bereichen Sicherheit, Militär und *intelligence* in einem besonderen Spannungsverhältnis. Einerseits gehören hier quantitative, insbesondere digitale Vorausberechnungen von Sachverhalten und Situationen zum technologischen Standard, andererseits ist das Wissen in diesen strategischen Domänen seit jeher von Ungewissheit und Unwägbarkeiten bestimmt. Im Beitrag wird anhand von Beispielen der datenbasierten *security policy* im Rahmen des *war on terror* dieses spezifische Zusammenspiel von Berechnung und Unberechenbarkeit untersucht. Dann wird aufgezeigt, wie quantitative Verfahren mit anderen Mitteln und Fertigkeiten wie Visualisierung oder Imagination ineinandergreifen müssen, um effektiv einsetzbar zu sein. Abschließend wird der Begriff der Unberechenbarkeit diskutiert.

Calculations and the incalculable are in a particular state of tension in the security, military, and intelligence fields. On the one hand, quantitative, and especially digital, prognostications of actions and scenarios are part of standard operating procedures. On the other hand, knowledge in this sphere is confronted with uncertainties and imponderables. In the article, the interplay between predictions and unpredictability in these strategic endeavors is examined on the basis of examples from data-based security policy in the ›war on terror‹. A discussion follows on how quantitative methods need to be combined with other processes, such as visualization and imagination, in order to be implemented truly effectively. Finally, the term incalculability/unpredictability is discussed.

1. Vorausberechnungen angesichts von Unkalkulierbarem

In militärischen Planungen und Strategien sowie generell bei Maßnahmen im Bereich von *Security*[1] sind Wissens- und Entscheidungsprozesse in einem hohen Maße von Unwägbarem und Ungewissem bestimmt. Solche ›negativen‹ Momente haben für militärstrategisches und militärplanerisches Denken genauso wie für Geheimdienstwissen seit jeher besondere Relevanz, sie stellen spezifische, mehr oder weniger unkalkulierbare epistemische Anteile dieser strategischen Wissendomänen dar.[2]

1 Bis auf Weiteres verwende ich hier die Ausdrücke »Sicherheit« und »*Security*« im Sinne von *security policy*, und damit im »klassischen« Feld von Sicherheit, das heißt: nationale und internationale Sicherheit.

2 Vgl. Carl von Clausewitz: *Vom Kriege*. *Hinterlassenes Werk*, Berlin 1980; Eva Horn: *Der geheime Krieg. Verrat, Spionage und moderne Fiktion*, Frankfurt am Main 2007.

Theoretisch verhandelt werden sie mittels Begriffen wie Friktion, Ungewissheit, Nichtwissen oder *unknowns*.[3] Zugleich sind politische Strategie und Sicherheit aber Bereiche, in denen – etwa seit der Mitte des zwanzigsten Jahrhunderts auch digitale – Vorausberechnungen von Sachverhalten oder Situationen zum technologischen Standard gehören. Außerdem spielen seit mehreren Jahrzehnten prognostische Verfahren, die sich auf die Auswertung großer Datenmengen stützen, eine wichtige Rolle.[4] Vorausberechnung und das, was ich im Folgenden als »Unberechenbarkeit« konzeptuell näher bestimmen möchte, liegen also in Sicherheit und Militär sehr dicht beieinander und stehen in einem besonderen Spannungsverhältnis.[5]

Zudem kommen die Verfahren in hochriskanten Anwendungskontexten zum Einsatz, in denen konkretes Handlungs- und Entscheidungswissen unter Zeitdruck gefordert ist. In den strategischen Bereichen *Security*, *Intelligence* und Militär sind Einschätzungen und »Vorausberechnungen« zukünftigen Geschehens beispielsweise relevant, um das Verhalten eines Feindes abzusehen, dessen Potentiale einzuschätzen, Krisenherde aufzuspüren, Terroranschlägen zuvorzukommen oder auch »klassisch« auf operativer Ebene bei der Flugabwehr. Mit Mario Bunges Differenzierungen zum Begriff der angewandten Forschung ließe sich hier von ›technologischem Wissen‹ sprechen und genauer, von einem Bereich »operativer technologischer Theorien«.[6] Diese beschäftigen sich laut Bunge mit »dem Verhalten von Menschen und Mensch-Maschine-Komplexen in näherungsweise realen Situationen«.[7]

Die vorliegende Studie geht der Frage nach, wie Berechnung und Unberechenbarkeit bei quantitativen, digitalen Vorhersageverfahren, die für die Bereiche Sicherheit und Militär entwickelt und dort eingesetzt werden, formal und konzeptuell zusammenspielen. Da die Unwägbarkeiten dieser Verfahren sich vor allem bei deren Einsatz bemerkbar machen, werden hier Anwendungsfälle fokussiert. Davon ausgehend stelle ich begriffliche Überlegungen zum Konzept der Unberechenbarkeit an. Die

3 Vgl. Clausewitz: *Vom Kriege*, a.a.O., S. 115–123; vgl. Christopher Daase und Oliver Kessler: »Knowns and Unknowns in the ›War on Terror‹. Uncertainty and the Political Construction of Danger«, in: *Security Dialogue* 38 (2007), Heft 4, S. 411–434; vgl. Herman Kahn und Irwin Mann: *Techniques of Systems Analysis*, Santa Monica, CA 1957, S. V, 36 und 94.

4 Vgl. Office of Science and Technology Policy Executive Office of the President (Hg.): *Obama Administration Unveils ›Big Data‹ Initiative. Announces $200 Million in New R&D Investments*, Washington, D.C. 2012.

5 Im vorliegenden Beitrag stehen Beispiele von Anwendungen im Bereich Sicherheit im Vordergrund. Eine klare Grenze zu den im Militärischen zum Einsatz kommenden Ansätzen und Verfahren lässt sich, insbesondere im Zuge jüngerer Anti-Terrormaßnahmen, nicht mehr eindeutig ziehen. Es kommen jedoch auch Datenverfahren zur Sprache, die spezifisch militärischen Anwendungen dienen.

6 Jüngere Forschungen zum Anwendungskontext naturwissenschaftlichen Wissens widersprechen der begrifflichen wie realen Trennung von reiner und angewandter Forschung: Vgl. etwa den Band: Martin Carrier und Alfred Nordmann (Hg.): *Science in the Context of Application*, Dordrecht 2011.

7 Mario Bunge: »Technik als angewandte Naturwissenschaft«, in: Thomas Zoglauer (Hg.): *Technikphilosophie. Texte*, Freiburg, München 2002, S. 149–166, hier S. 150–153.

momentane weitgehende Quantifizierung und digitale Verfügbarwerdung vieler Wissens- und Lebensbereiche sowie die Grenzen dieser Strategien möchte ich zwar ausgehend von der Geschichte und Epistemologie der Berechenbarmachung des »Denkens« und der »Welt« erwägen.[8] Dabei wird »Unberechenbarkeit« aber nicht – der klassischen Leitdifferenz »Uncertainty – Risk« folgend – als Gegenstück zu »Berechenbarkeit« im Allgemeinen thematisiert, sondern in erster Linie von spezifischen Anwendungskontexten der Datenverfahren her epistemologisch konturiert. Zunächst gehe ich auf digitale Prognoseverfahren, die im Rahmen aktueller Sicherheitsmaßnahmen eingesetzt werden, sowie auf Probleme, die sich bei ihrer Applikation zeigen, ein. Sodann geht es mir um die Frage, welche Erkenntnismittel im strategischen Denken herangezogen werden, wenn Berechnungen an ihre Grenzen kommen. Abschließend diskutiere ich Aspekte von Unberechenbarkeit als epistemologisches Konzept.

2. *Datenbasierte* security policy *und die Unberechenbarkeit terroristischer Aktivitäten*

Anstrengungen zur Erforschung und Implementierung von Mitteln, die eine Intervention *vor* einer bevorstehenden Katastrophe ermöglichen würden, indem sie diese in irgendeiner Weise vorwegnähmen – sei es rechnerisch, imaginativ oder fiktiv –, intensivierten sich nach den New Yorker Anschlägen vom 11. September 2001 und rückten in den Fokus der medialen Auseinandersetzung. Staatliche Akteure, besonders die USA, und überstaatliche Akteure wie die Europäische Union initiierten in den Jahren nach »9/11« im Rahmen der Terrorbekämpfung Projekte und Programme, die auch einen Schwerpunkt auf Datentechnologien setzten.[9] Dabei handelt es sich um Mittel, mit denen sowohl potenzielle »terroristische Individuen« als auch »terroristische Aktivitäten« zu Präventionszwecken ausgemacht werden sollen. Die Implementierung solcher Maßnahmen erfolgt im Zusammenhang mit dem sich spätestens seit dem zwanzigsten Jahrhundert selbst zu rechtfertigen scheinenden Titelwort der »Sicherheit«.[10] Sie affizieren die Gegenwart auf spezifische Weise vermittelt über Zukünftiges und lassen jene zeitliche Logik erkennen, die Richard Grusin

8 Vgl. hierzu: Sybille Krämer: *Berechenbare Vernunft. Kalkül und Rationalismus im 17. Jahrhundert*, Berlin, New York 1991; sowie: Klaus Mainzer: *Die Berechnung der Welt*, München 2014.

9 Vgl. Samuel Nunn: »Tell Us What's Going to Happen. Information Feeds to the War on Terror«, in: Arthur Kroker und Marilouise Kroker (Hg.): *Critical Digital Studies. A Reader*, Toronto 2013, S. 293–311, hier: S. 307; sowie: Jeffrey W. Seifert: *Data Mining and Homeland Security. An Overview*, Washington, D.C. 2008; *Indect. For the Security of Citizens,* Projektwebsite: http://www.indect-project.eu/ (aufgerufen: 24.1.2016).

10 Vgl. Andrea Schrimm-Heins: *Gewissheit und Sicherheit. Geschichte und Bedeutungswandel der Begriffe certitudo und securitas*, Bayreuth 1990, S. 123f.

als *premediation* beschrieben hat.[11] Im Rahmen dieser Logik gilt es, stets den *worst case* anzunehmen, diesen gleichsam vorwegzunehmen, um dann dem Kommenden ohne Gefahr eines nachfolgenden Traumas begegnen zu können. Lässt man sich auf eine solche temporale Konfiguration ein, so muss die »Zukunft immer schon vorvermittelt und -bedacht« worden sein, »bevor sie sich in Gegenwart oder Vergangenheit verwandelt«.[12] Ulrich Bröckling ordnet die in diesem Zuge etablierten Sicherheitsmaßnahmen einem neuen »Präventionsregime« zu, das er *precautionary principle* nennt.[13] Ziel dessen ist neben dem zuvorkommenden Vermeiden eines Übels der Zustand einer *preparedness*, eines Gewappnetseins für das Schreckliche und zugleich der Aufschub desselbigen.[14] In der Folge wird eine – irgendwie immer anstehende – Bedrohung zum Grund einer Veränderung in der Gegenwart, wie eben der Implementierung von Sicherheitsprogrammen.[15] Ein solches permanentes Vorbereitetsein wird jüngst als aktuelles Paradigma von Sicherheitspolitiken unter dem Begriff der Resilienz diskutiert, den Stefan Kaufmann als einen neuen Modus »Unsicherheit zu regieren« herausstellt.[16]

Schon mehrere Jahrzehnte vor »9/11« und den anschließenden Reaktionen und Maßnahmen, und das heißt auch bevor die für prädiktive digitale Verfahren notwendige Sammlung und Verwertung von Datenmengen im – derzeit – bis zu 22-stelligen Zettabyte-Bereich[17] unter dem Schlagwort »Big Data« zum industriellen Massenphänomen wurde, sind entsprechende Datentechnologien bereits unter anderen Namen im staatlich-militärischen Umfeld entwickelt worden und noch im Einsatz[18] – wenn auch lange weitgehend auf das Militär, das polizeiliche Umfeld, aber auch auf wissenschaftliche Anwendungen und Raumfahrt beschränkt.[19] So greifen im *Securi-*

11 Vgl. Richard Grusin: *Premediation. Affect and Mediality After 9/11*, Basingstoke 2010.
12 Vgl. ebd., S. 4 und 12.
13 Ulrich Bröckling: »Dispositive der Vorbeugung. Gefahrenabwehr, Resilienz, Precaution«, in: Christopher Daase, Philipp Offermann und Valentin Rauer (Hg.): *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*, Frankfurt am Main 2012, S. 93–108, hier S. 103.
14 Vgl. ebd., S. 102.
15 Vgl. Brian Massumi: »Fear (The Spectrum Said)«, in: *Positions* 13 (2005), Heft 1, S. 31–48, hier S. 35.
16 Vgl. Stefan Kaufmann: »Resilienz als Sicherheitsprogramm. Zum Janusgesicht eines Leitkonzepts«, in: Martin Endreß und Andrea Maurer (Hg.): *Resilienz im Sozialen*, Wiesbaden 2015, S. S. 295–312, hier S. 296.
17 Vgl. Heinrich Geiselberger und Tobias Moorstedt (Hg.): *Big Data – Das neue Versprechen der Allwissenheit*, Berlin 2013, S. 305.
18 Unter anderem beispielsweise als »Multi-Sensor-Datenfusion«, vgl. David L. Hall und James Llinas: »An Introduction to Multisensor Data Fusion«, in: *Proceedings of the IEEE* 85 (1997), Heft 1 S. 6–23, hier S. 6; vgl. auch: Yvonne Hofstetter: *Sie wissen alles*, *Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen*, München 2014, S. 18.
19 Vgl. ebd., S. 88 und 90; vgl. zur Formulierung des Schlagworts »Big Data« im Jahre 1997 bei der Forschung zu Visualisierungstechniken der NASA: Michael Cox und Michael Ellsworth: »Application-controlled demand paging for out-of-core visualization«, in: *Proceedings of the*

ty-Bereich vorausberechnende digitale Verfahren, die mit Datenmengen nicht mehr konkret vorstellbarer Größenordnung operieren, wie »*predictive analysis*«, »*predictive data mining*« oder »*predictive modelling*« ineinander, beziehungsweise werden in Kombination mit verschiedenen, voneinander gesonderten elektronischen »Sicherheitstechnologien« genutzt, etwa unter Einbeziehung von Fernsehüberwachungsanlagen, staatlichen und firmeneigenen Datenbanken, elektronischen Überwachungssystemen, datenbasierten Profilingtechniken, Szenarioanalysen, Strafverfolgungsdatenbanken oder biometrischen Daten.[20] Konzeptuell betrachtet bilden die Datenverfahren eine unverzichtbare Komponente für dieses Zusammenwirken, da sie der Logik des *precautionary principle* entsprechen und in dessen Perspektive das ideale ergänzende Instrumentarium darstellen. Sie versprechen, kommende Ereignisse anzuzeigen und die Möglichkeit bereitzustellen, vorbeugend einzugreifen. Damit würden sie eine »*perfect predictive action*« – im Sinne des *precrime*-Systems im Film *Minority Report* – ermöglichen.[21] Eine solche politische Intention unterlag als Modell den frühen Entwürfen der »Anti-Terrorismus«-Programme vieler Staaten, wie in einem von Yonah Alexander herausgegebenen Band dargelegt wird.[22] Auch wenn vonseiten der Politikwissenschaft und -beratung bereits in der ersten Dekade des neuen Jahrhunderts ernsthafte Bedenken bezüglich der Eignung prädiktiver Datenanalysen für die Aufdeckung gerade von terroristischen Vorhaben geäußert wurde, verfolgte man den Ansatz weiter und es kann davon ausgegangen werden, dass auch zukünftig in technische, datenbasierte Strategien der Terrorverfolgung investiert wird, welche in geheimdienstlichen Operationen und militärischen Maßnahmen zum Einsatz kommen.[23]

8th conference on Visualization '97, Los Alamitos, CA 1997, S. 235–244, hier S. 235. Gemessen am Einsatz der Verfahren in den genannten Bereichen, fing die US-amerikanische National Security Agency vergleichsweise spät – mit der Terrorbekämpfung der 2000er Jahre – an, auf die Überwachung der neuen Kommunikationswege durch umfassende Datenanalyse zurückzugreifen. Vgl. Micheal V. Hayden: *Playing to the Edge. American Intelligence in the Age of Terror*, New York 2016, S. 4ff.

20 Vgl. Nunn: »Tell Us What's Going to Happen«, in: Kroker (Hg.): *Critical Digital Studies*, a.a.O., S. 294. Für einen Überblick neuerer, im Rahmen von Homeland-Security-Anliegen eingesetzter IT-Technologien vgl. Giorgio Franceschetti und Marina Grossi (Hg.): *Homeland Security Technology Challenges. From Sensing and Encryptring to Mining and Modeling*, Palo Alto, 2009.

21 Vgl Steven Spielberg: Minority Report, Film 2002; vgl. »Minority Report«, in: *IMDb*, http://www.imdb.com/title/tt0181689/ (aufgerufen: 24.1.2016).

22 Vgl. Yonah Alexander (Hg.): *Combatting Terrorism. Strategies of Ten Countries*, Ann Arbor, MI 2002.

23 Vgl. Jeff Jonas und Jim Harper: »Effective Couterterrorism and the Limited Role of Predictive Data Mining«, in: *Policy Analysis* 584 2006; vgl. Edward Tverdek: »The Limits to Terrorist Profiling«, in: *Public Affairs Quaterly* 20 (2006), Heft 2, S. 175–203; vgl. Office of Science and Technology Policy Executive Office of the President (Hg.): *Obama Administration Unveils ›Big Data‹ Initiative*; vgl. Department of Homeland Security. Privacy Office: *2015 Data Mining Report to Congress*, Washington, 2016.

Die Hoffnung auf ›maschinelle‹ Ansätze und Lösungen bei drängend scheinenden Sicherheitsherausforderungen rührt nicht nur daher, dass diese eine höhere Verlässlichkeit im Vergleich zu menschlichen Ausdauer- und Aufmerksamkeitskapazitäten versprechen.[24] Es ist vor allem die neue Quantität des Datenaufkommens, die schiere Menge an anfallenden Daten, die mit herkömmlichen Mitteln der Datenanalyse nicht zu bewältigen ist.[25] Wie im kommerziellen Bereich wächst die Menge der für Sicherheitsbehörden und Verteidigungsministerien sowie für Geheimdienste verfügbaren Daten auf nicht absehbare Zeit weiter an. Neben den Informationsflüssen, die von polizeilichen Technologiesystemen produziert werden, nimmt die Bandbreite und Menge geheimdienstlich und militärisch relevanter Daten zu: Mobilfunkdaten, E-Mails und Textdokumente, Satellitenbilder oder auf koordinierten Diensten basierende Daten wie die speziell den US-Streitkräften zur Verfügung stehenden, sogenannten »ISR-Daten« (*Intelligence*, *Surveillance and Reconnaissance*).[26] Jonathan S. Feinstein und Edward H. Kaplan sprechen vom neuen Problem der »overcollection« bei US-amerikanischen Geheimdiensteinrichtungen im Zuge der Terrorbekämpfung.[27] Im Verteidigungsbereich ist der steigende Gebrauch von *Unmanned Aerial Vehicles*, den sogenannten Drohnen, ein neuer ausschlaggebender Faktor der Produktion von Bildern und Videos, der jährlich Datenmengen im Petabyte-Bereich hervorbringt.[28] Durch die neuen Größenordnungen von Datensammlungen entsteht einerseits eine opake »Informationslawine«, die Gefahr läuft, zu akkumulierter nutzloser Information zu werden.[29] Andererseits vermutet man in den Informationsmengen aber ein enormes Wissenspotential. Davon, *dass* die Datenmassen relevantes Wissen von strategischer Bedeutung bergen, wird dabei mehr oder weniger fraglos ausgegangen.[30] So stellt die Generierung eines strategisch bedeutsamen und zuverlässigen Wissens aus den Datenmassen die eigentliche, für die beteiligten Disziplinen dann auch epistemologische Herausforderung dar, zumal sich Sicherheitsinstitu-

24 Vgl. Anonym: »DARPA seeks deep-learning AI to cope with flood of information«, in: *Homeland Security News Wire*, 16.4.2009, http://www.homelandsecuritynewswire.com/darpa-seeks-deep-learning-ai-cope-flood-information (aufgerufen 24.1.2016.).

25 Vgl. ebd.

26 Vgl. Ted Girard: »Big Data and Virtualization. A Formidable Defense«, in: *Defense Systems. Knowledge Technologies and Net-Enabled Warfare*, 5.5.2015, https://defensesystems.com/articles/2015/03/05/comment-defense-big-data-and-virualization.aspx (aufgerufen 24.1.2016); Seifert: *Data Mining and Homeland Security*, a.a.O., S. 0f; Nunn: »Tell Us What's Going to Happen «, in: Kroker (Hg.): *Critical Digital Studies*, a.a.O., S. 293.

27 Vgl. Jonathan S. Feinstein und Edward H. Kaplan: »Counterterror intelligence operations and terror attacks«, in: *Public Choice* 149 (2011), S. 281–295, hier S. 282.

28 Vgl. Anonym: »DARPA seeks deep-learning AI to cope with flood of information«, in: *Homeland Security News Wire*, a.a.O.

29 Vgl. Alexandre A. Motta, Alexandre S. Alves und Nelson F. F. Ebecken: »Data mining in military systems«, in: *WIT Transactions on Modelling and Simulation* 45 (2007), S. 171–180, hier S. 171. Eig. Übers.

30 Vgl. ebd., S. 170ff; sowie: Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery,* Potomac, MD 2005, S. 1; vgl. Motta: »Data mining in military systems«, in: *WIT Transactions on Modelling and Simulation* 45, a.a.O., S. 173.

tionen mehr und mehr in ihrem Handeln auf die Auswertung von elektronisch gespeicherten Daten verlassen.[31]

Ein aktuell gebräuchliches Instrument, Wissen aus großen Datenmengen zu gewinnen, welches auch prädiktive Aussagen zulässt, ist das »Datamining« und insbesondere Verfahren der »knowledge discovery«, genannt »Knowledge Discovery in Databases« (KDD).[32] Das inzwischen interdisziplinär verfasste Forschungsfeld des Datamining ging aus dem Bereich des ›maschinellen Lernens‹ – eine Domäne der künstlichen Intelligenz – hervor.[33] Der prädiktive, gewissermaßen *synthetische* Zug, der aus der Daten*analyse* resultiert, basiert auf der Figuration zuvor unbekannter Muster durch Zusammenhänge innerhalb der Daten.[34] Drei Kernmethoden für diese Art der »knowledge discovery« sind Algorithmengruppen, die als *classification*, *association* und *clustering* bezeichnet werden.[35] Der synthetische Aspekt des Datamining, aus dem die Hoffnung herrührt, Neues oder bisher Verborgenes »aufzudecken«, ist für strategische Erwägungen in Sicherheit und Militär besonders vielversprechend, da hier das Wissen und der Zugang zu Information vielfach beschränkt sind und der Faktor »Nichtwissen« eine vordergründige Rolle spielt, wenn es beispielsweise um feindliche Strategien, Potenziale und Aktivitäten geht.[36] Man ver-

31 Vgl. Office of Science and Technology Policy Executive Office of the President (Hg.): *Obama Administration Unveils ›Big Data‹ Initiative*, a.a.O., S. 1; Girard: »Big Data and Virtualization. A Formidable Defense«, in: *Defense Systems*, a.a.O.; vgl. Department of Homeland Security: *2015 Data Mining Report to Congress*, a.a.O.

32 Vgl. Giorgio Franceschetti und Marina Grossi: »Preface«, in: Giorgio Franceschetti und Marina Grossi (Hg.): *Homeland Security Technology Challenges. From Sensing and Encryptring to Mining and Modeling*, Palo Alto, 2009, S. XV–XIX, hier: S. XVIf; vgl. Hetal Thakkar und Carlo Zaniolo: »Mining Databases and Data Streams«, in: Franceschetti (Hg.): *Homeland Security Technology Challenges*, a.a.O., S. 103–142; hier 106ff; vgl. Seifert: *Data Mining and Homeland Security*, a.a.O., S. 2 und 26.

33 Vgl. Thakkar: »Mining Databases and Data Streams«, in: Franceschetti (Hg.): *Homeland Security Technology Challenges*, a.a.O., S. 104. In seinem Buch zu »neugierigen Strukturvorschlägen im maschinellen Lernen« diskutiert Sebastian Harrach, inwiefern die Rede vom »Lernen« in diesem Zusammenhang Sinn macht und schlägt stattdessen vor, von »Autoadaptionsprozessen« respektive von »Musterbildung autoadaptiver Systeme« zu sprechen. Vgl. Sebastian Harrach: *Neugierige Strukturvorschläge im maschinellen Lernen. Eine technikphilosophische Verortung*, Bielefeld 2014, S. 21–24.

34 Bereits in den späten 1960er Jahren war Mustererkennung – jedoch nicht die Erkennung noch *unbekannter* Muster – ein wichtiger Teilaspekt der Forschung zur künstlichen Intelligenz, da er die Voraussetzung für automatisches Sprachübersetzen und Problemlösen darstellte. Die entscheidenden Fortschritte hinsichtlich des maschinellen Lernens bei der Übersetzung erfolgten jedoch erst in den 2000er Jahren mit der maschinellen Übersetzung auf der Grundlage statistischer Methoden, die mit Datenmengen in einem größeren Maßstab arbeiten. Vgl. Hubert L. Dreyfus: *Was Computer nicht können. Die Grenzen künstlicher Intelligenz*, Frankfurt am Main 1989, S. 46f; vgl. Philipp Koehn: *Statistical Machine Translation*, Cambridge 2012; vgl. »Machine Translation«, in: *Research at Google*, http://research.google.com/pubs/MachineTranslation.html (abgerufen: 6.7.2016).

35 Vgl. Thakkar: »Mining Databases and Data Streams«, in: Franceschetti (Hg.): *Homeland Security Technology Challenges*, a.a.O., S. 106ff.

36 Vgl. Motta: »Data mining in military systems«, in: *WIT Transactions on Modelling and Simulation* 45, a.a.O., S. 171.

traut darauf, mit der Analyse großer Datenmengen »Unsichtbares sichtbar zu machen«, wie aus einem Präsentationspapier des sogenannten *Multistate Anti-Terrorism Information Exchange* (MATRIX) von 2003 hervorgeht, einem inzwischen eingestellten Pilotprojekt für das US-amerikanische Department of Homeland Security zur Terrorismusbekämpfung.[37] MATRIX kombinierte zum ersten Mal im großen Maßstab Detailinformationen zu US-Amerikanerinnen und -Amerikanern, die zu kommerziellen Zwecken gesammelt worden waren, mit polizeilich und regierungsbehördlich aufgezeichneten Daten.[38] So setzt auch eine Vielzahl der jüngeren Initiativen für die US-amerikanische innere Sicherheit auf Datamining als Schlüsselbestandteil.[39] Das geheimdienstliche Sammeln und Auswerten von Daten durch die National Security Agency und das MATRIX-Projekt stellen nur zwei von zahlreichen, in diesem Zusammenhang ins Leben gerufenen Initiativen dar.[40] Neuere Ansätze des Datamining, wie *web mining* und *data stream mining,* ermöglichen quasi Echtzeitanalysen von Webinhalten ohne eine Aufzeichnung und Speicherung der Daten, wie es die genannten etablierteren Methoden des KDD voraussetzen.[41] Prognosen mit politischem Gehalt auf der Grundlage der Sammlung und Auswertung großer Datenmengen werden nicht nur von staatlichen Akteuren und politischen Institutionen vorangetrieben, sondern beispielsweise auch von Start-up-Unternehmen, die im Überschneidungsbereich von Handel, Dienstleistung und Politik agieren.[42]

Eine Strategie zur Prävention eines Terroranschlags ist es beispielsweise, bekannte oder noch unbekannte »Terroristen« zu identifizieren und zu lokalisieren und an-

37 Seisint Inc. (Hg.): Seisint's FACTS For The MATRIX Project, Boca Raton 2003, S. 3, Herv. i. Orig.; vgl. zu MATRIX auch: Florian Rötzer: »Matrix ist in Florida«, in: Heise Online, 6.8.2003, http://www.heise.de/tp/artikel/15/15388/1.html (abgerufen: 24.1.2016); sowie: Robert O'Harrow, Jr.: *No place to hide*, New York 2006.

38 Aus diesem Grund waren die Versuche zur Durchsetzung des Programms von Anfang an mit zuvor so nicht gekannten Problemen und Auseinandersetzungen zum Datenschutz verbunden, die den umfassenden Einsatz letztendlich auch verhinderten. MATRIX kann jedoch als konzeptuell richtungsweisend für das Profiling auf Datengrundlage im Zuge der Terrorismusbekämpfung gesehen werden. Vgl. O'Harrow: *No place to hide*, a.a.O, S. 122ff.

39 Vgl Department of Homeland Security: *2015 Data Mining Report to Congress*, a.a.O.

40 Vgl. Seifert: *Data Mining and Homeland Security*, a.a.O. Als geheimdienstlich eingesetze Programme, die mit Datamining arbeiten und von denen die Öffentlichkeit – jeweils verzögert – durch »geleakte« Information erfuhr, sind außerdem »Stellarwind« und »Prism« zu nennen. Vgl. Hayden: *Playing to the Edge*, a.a.O., S. 64–91; vgl. Glenn Greenwald und Even MacAskill: »NSA Prism program taps in to user data of Apple, Google and others«, in: *The Guardian*, 7.6.2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (aufgerufen: 9.7.2016).

41 Vgl. Thakkar: »Mining Databases and Data Streams«, in: Franceschetti (Hg.): *Homeland Security Technology Challenges*, a.a.O., S. 122ff.

42 Vgl. etwa die Firmenwebsite von *Recorded Future*: www.recordedfuture.com (aufgerufen: 24.1.2016) und: Tom Cheshire: »The News Forecast. Can you Predict the Future by Mining Millions of Web Pages for Data?«, in: Wired.Co.UK, 10.11.1011, http://www.wired.co.uk/magazine/archive/2011/12/features/the-news-forecast (aufgerufen: 24.1.2016); sowie zu den von Kalev Leetaru entwickelten Programmen vgl. Florian Peil: »Schwache Signale«, in: *Zenith*, Juli/August 2013, S. 68–71.

schließend eine Kombination von Überwachungs- und Kontrollmaßnahmen auf sie auszurichten, so dass einer »terroristischen Aktitivität« verhindernd zuvorgekommen werden kann.[43] Nicht nur stellt Datamining ein Mittel dar, »terroristische Aktivitäten« individueller, bereits verdächtiger Personen festzustellen, etwa durch Aufzeichnungen von Reisen, Geldtransfers und Kommunikation; es wird auch dazu eingesetzt, um bisher noch nicht verdächtigte Personen durch die Erfassung auffälliger Verhaltensmuster als potenzielle Täter zu identifizieren.[44] So wurde im Rahmen präventiver Maßnahmen mit Hilfe von Datamining versucht, Muster »typischer terroristischer Aktivitäten« zu gewinnen und entsprechende Profile zu erstellen.[45] Das erwähnte MATRIX-Projekt, welches Datenanalysen auf der Grundlage eines weitreichenden kooperativen Informations*sharing* der Datenquellen von Staaten und politischen Institutionen ermöglichen sollte, beinhaltete anfangs eine Komponente, die die entwickelnde Firma Seisint »High Terrorist Factor« nannte.[46] Mittels der Analyse von Informationen wie Alter, Geschlecht, Handlungen rund um Führerschein, Pilotenausbildungen, Nähe zu »schmutzigen« Adressen oder Telefonnummern, Kredithistorie, Anomalien bei der Sozialversicherungsnummer und Angaben zu Ethnizität generierte die Firma eine Liste von 120 000 Namen mit hohem »Terrorismusfaktor«.[47] Anhand der Liste wurden zwar Verhaftungen vorgenommen, der Faktor wurde aber aufgrund ungeklärter Datenschutzprobleme aus dem Projekt eliminiert, außerdem konnte das zugrundeliegende Geheimdienstwissen nicht ohne weiteres weitreichend bei der Strafverfolgung eingesetzt werden.[48] Solche Begrenzungen oder der Entzug von Information durch Geheimhaltung und Klassifizierung stellen epistemologische Besonderheiten der Bereiche *Intelligence* und Sicherheit dar – möchte man, wie Peter Galison und Eva Horn dies tun, davon ausgehen, dass in diesen Feldern »Wissen« hergestellt und verhandelt wird.[49] Sie begrenzen jedenfalls auch die Effektivität und Reichweite von Vorausberechnungen in den hier untersuchten Anwendungsfeldern. Auf ein ähnliches Vorgehen mittels sogenannter *signature strikes* im Rahmen US-amerikanischer militärischer »Antiterror«-Einsätze weist Gregoire Cha-

43 Vgl. Nunn: »Tell Us What's Going to Happen «, in: Kroker (Hg.): *Critical Digital Studies*, a.a.O., S. 294.
44 Vgl. Seifert: *Data Mining and Homeland Security. An Overview*, a.a.O., S 0.
45 Vgl. Nunn: »Tell Us What's Going to Happen «, in: Kroker (Hg.): *Critical Digital Studies*, a.a.O., S. 294.
46 Vgl. Seifert: *Data Mining and Homeland Security. An Overview*, a.a.O., S. 14f.
47 Vgl. ebd; vgl. O'Harrow: *No place to hide*, a.a.O, S. 102.
48 Vgl. ebd. Dass die US-amerikanischen Initiativen zur Terrorismusbekämpfung schon kurz nach dem 11. September 2001 verstärkt mit Auseinandersetzungen zum Datenschutz einhergingen, die sich zwischen Kongress, Regierungspolitikern und Geheimdienst-Agenturen abspielten, geht auch hervor aus: Hayden: *Playing to the Edge*, a.a.O.
49 Galison arbeitet heraus, dass die geheimdienstliche Klassifizierung von Wissen und dessen Entzug gegenüber der Öffentlichkeit auch hinderlich für wissenschaftlichen Fortschritt sein kann. Vgl. Peter Galison: »Removing Knowledge«, in: *Critical Inquiry* 31 (2004), S. 229–243; vgl. auch: Eva Horn und Sara Ogger: »Knowing the Enemy. The Epistemology of Secret Intelligence«, in: *Grey Room* 11 (2003), S. 58–85.

mayou hin.[50] Solche Angriffe richten sich gegen Personen, »deren Identität noch unbekannt ist, aber deren Verhalten die Zugehörigkeit zu einer ›terroristischen Organisation‹ vermuten lässt«.[51] Laut Chamayou erfolgt die Zielauswahl mittels des Verfahrens der sogenannten »Lebensmusteranalyse (*pattern of life analysis*)«.[52]

Ich greife einige Momente des Dataminingprozesses heraus, die im Hinblick auf Unberechenbarkeit interessant sind. *Patterns*, potentiell bedeutende Verbindungen innerhalb der Daten, die zuvor unbekannt waren oder nicht direkt beobachtbar sind, bilden einen wesentlichen Bestandteil des ersten Stadiums dieses Prozesses, der Bildung eines Modells, mithilfe dessen die Wirklichkeit ausschnitthaft und vereinfacht dargestellt, also »modelliert« wird.[53] Bereits die Wahl des Modelltyps, beispielsweise Bayesisches Netz, Regelmodell oder neuronales Netz, bestimmt über Hypothesenmöglichkeiten und Lösungsraum, also auch darüber, wie die »Erkenntnis« bezüglich der Wirklichkeit, die mithilfe des Datamining gewonnen wird, letztlich beschaffen ist.[54] Das ›prädiktive Modell‹ und seine Variablen werden nach der Maßgabe eines zuvor formulierten zu lösenden Problems entwickelt. Das Modell repräsentiert den Wirklichkeitsauschnitt – teils ähnlich wie eine Straßenkarte (engl. *map*) einen Fahrweg.[55] »Variablen« sind in diesem Zusammenhang sogenannte Attribute, also Merkmale, von »Objekten«. Bei diesen kann es sich um Prozesse, Sachverhalte oder auch Personengruppen handeln. Es werden funktionale Zusammenhänge zwischen sogenannten unabhängigen Variablen oder »Prädiktoren« – bekannten Werten, die in das Modell eingehen – und den sogenannten abhängigen oder Zielvariablen, die eben die Werte darstellen, die das Modell als neue Einsicht hervorbringt, formuliert.[56] Entsprechend der »Welt«, die mit ihnen zur Darstellung und Bearbeitung kommt, sind die Wechselwirkungen, die ein Modell abbildet, hochkomplex, bei lernenden Algorithmen kann es sich um mehrere Millionen Dimensionen handeln.

50 Vgl. Gregoire Chamayou: *Ferngesteuerte Gewalt. Eine Theorie der Drohne*, Wien 2014, S. 57–59.
51 Ebd. 57f.
52 Vgl. ebd. 58.
53 Hofstetter: *Sie wissen alles*, a.a.O., S. 109 und 122; Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 1.
54 Vgl. Welches Modell gewählt wird, ist wiederum abhängig von der Art der Variablen, mit denen gearbeitet werden soll. Vgl. Richard Lackes: »Stichwort: Datamining«, in: Gabler Springer Verlag (Hg.): *Gablers Wirtschaftslexikon*, http://wirtschaftslexikon.gabler.de/Archiv/57691/35/Archiv/57691/35/Archiv/57691/data-mining-v 8.html (abgerufen: 7.7.2016); vgl. Eddie Soong: »How to choose a statistical model«, in: *Data Science Central*, 23.6.2015, http://www.datasciencecentral.com/profiles/blogs/how-to-choose-a-statistical-model (abgerufen: 7.7.2016).
55 Diese Analogie verwenden Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 1. Ich möchte an dieser Stelle mit ihr lediglich auf einen Unterschied und das Repräsentationsverhältnis von Modell und Wirklichkeit verweisen. Bereits wenn zeitliche Verläufe in das Modell eingetragen oder lernende Algorithmen eingesetzt werden, ist die Analogie nicht mehr angemessen.
56 Vgl. Hofstetter: *Sie wissen alles*, a.a.O., S. 109.

In einem nächsten Schritt ist das Modell zu testen, seine Gültigkeit jenseits des Trainings-Datensets, mit dem es erstellt wurde, muss »verifiziert« werden.[57] Erst indem das Modell auf die Masse an Daten, über die etwas in Erfahrung gebracht werden soll, appliziert wird, ergibt sich eine Beschreibung eines bestimmten Wirklichkeitszustandes, an der wiederum Algorithmen ansetzen können, um die gewünschten »informierten Entscheidungen« zu errechnen.[58] Da die zugrundegelegten Daten letztlich vergangenem Geschehen entstammen, handelt es sich bei den so gewonnenen Zukunftsprognosen strenggenommen um Erklärungen für die Vergangenheit, wie Hofstetter anmerkt.[59] So lässt sich davon sprechen, dass diese Prognosepraktiken eine »konservative Futurisierung« vornehmen.[60] Für die Zuverlässigkeit und Genauigkeit der mit prädiktiven Modellen gewonnen Aussagen ist es entscheidend, dass sie mit großen Mengen von Daten durchgerechnet werden. Einige Forscher haben schon in der frühen Anwendungsphase kritisch herausgestellt, dass Datamining gerade aufgrund dieser Voraussetzung kein geeignetes Mittel darstellt, um potentielle terroristische Aktivitäten im Vorfeld eines Anschlags aufzudecken.[61] Um das »Verhalten« einer Sachlage, eines Zusammenhangs oder auch einer Person mittels *predictive* Datamining »vorauszusagen«, bedarf es einer erheblichen Anzahl an Beispielfällen des fraglichen Verhaltens; nur mit diesen kann ein verlässliches Voraussagemodell erstellt werden. Vorhersagen zu Konsumverhalten und Kreditkartenbetrug beruhen auf Millionen von vergangenen Fällen des einschlägigen Verhaltens.[62] Terrorismus tritt jedoch nicht mit hinreichender Regelmäßigkeit auf und auch nicht in ausreichend wiedererkennbarer Form, um mit einem gültigen prädiktiven Modell repräsentiert zu werden, wie Jeff Jonas und Jim Harper herausstellen. Anschläge würden sich, so ihr Argument, in Planung und Ausführung zu sehr voneinander unterscheiden, als dass es tatsächlich sinnvolle »Verhaltensmuster« gäbe, die die Vorbereitung von Terrorismus anzeigten.[63] Das Problem umgekehrt über die Entdeckung von Anomalien, das Abweichen von der Norm zu lösen, würde im Falle einer intendierten Aufdeckung terroristischer Aktivitäten ebenso fehlgehen. Denn dies setzte voraus, dass Muster »typischen«, beispielsweise »amerikanischen« Verhaltens erstellt würden, etwa zu Internetnutzung, Telefongesprächen, Arztbesuchen, Einkäufen, Reisen, Lesen *et cetera*.[64] Es müsste allen Abweichungen von normalen Mus-

57 Vgl. Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 1; vgl. Thakkar: »Mining Databases and Data Streams«, in: Franceschetti (Hg.): *Homeland Security Technology Challenges*, a.a.O., S. 106.
58 Hofstetter: *Sie wissen alles*, a.a.O., S. 119 und 122f.
59 Vgl. ebd.
60 Vgl. Stefan Willer: »Prognose«, in: Gert Ueding (Hg.): *Historisches Wörterbuch der Rhetorik*, Bd. 10, Tübingen 2012, S. 958–966.
61 Vgl. Seifert: *Data Mining and Homeland Security*, a.a.O., S. 3.
62 Vgl. ebd.
63 Jonas: »Effective Couterterrorism and the Limited Role of Predictive Data Mining«, in: *Policy Analysis* 584, a.a.O., S. 7f.
64 Vgl. ebd., S. 8.

tern nachgegangen werden, was aufgrund der üblichen Bandbreite verschiedener Verhaltensweisen nicht erfolgversprechend ist. Jonas und Harper wenden ein, dass es für Personen mit terroristischen Absichten naheliegend ist, möglichst unauffällig zu agieren und sich »so normal wie möglich« zu verhalten, sich also den bestehenden Normalitätsmustern gerade anzupassen.[65] Vergleichsweise erfolgreich angewendet wird der Datamining-Ansatz der Normabweichung jedoch mit der Methode der *Anomalie Detection* bei der Bekämpfung von Cyberkriminalität. Aufgrund der größeren zugrundeliegenden Fallmenge ist der Ansatz in diesem Bereich erfolgversprechender, obwohl auch hier der permanente Wandel in der Art der Cyberattacken eine der größten methodischen Schwierigkeiten darstellt.[66] Erfolge werden auf diesem Feld momentan beispielsweise mit der Aufdeckung von Anomalien in Echtzeit durch die Analyse von Log-Dateien erzielt.[67] Die Grenzen des mit Datamining zu gewinnenden Wissens, so scheint es, liegen jeweils schlichtweg dort, wo die benötigte Information noch nicht – also auch nicht ›latent‹ – in die zugrundegelegten Datenbanken eingegangen ist. Allerdings können relevante Informationen, auch wenn sie vorhanden sind, unnauffindbar bleiben, wenn – sofern solche vorausgesetzt werden müssen – Analysekategorien angewendet werden, die ungeeignet sind. Auch Verfahren des maschinellen Lernens führen in diesen beiden Fällen nicht weiter.

Konkrete Konsequenzen zeitigen die dargelegten Schwierigkeiten bei der Aufdeckung terroristischer Aktivitäten durch Mustererkennung darin, dass Sicherheitssysteme eine hohe Anzahl zu unrecht Verdächtigter, sogenannter *false positives*, anzeigen.[68] Das Beispiel des US-Senators Ted Kennedy, der fünfmal ›versehentlich‹ an Flugreisen gehindert wurde, da sein Name fälschlicherweise auf einer Terrorverdächtigenliste auftauchte, zeugt von den realen Auswirkungen der methodischen Probleme und lässt ähnliche Vorkommnisse innerhalb der weniger prominenten fliegenden Bevölkerung nur vermuten.[69] Im kommerziellen Bereich relativiert das Problem der falsch positiven Ergebnisse nicht die Vorteile des *predictive* Datamining, denn ein paar überflüssig geschaltete Online-Werbebanner tangieren nur geringfügig das Budget, in das sie ohnehin bereits einkalkuliert wurden. Im Sicherheitsbereich kann es dagegen zu schwerwiegenden Einbußen und juristischen wie politischen Schwierigkeiten führen.

65 Vgl. ebd.

66 Vgl. Paul Dokas u.a.: »Data Mining for Network Intrusion Detection«, in: *Proc. NSF Workshop on Next Generation Data Mining*, Baltimore, MD 2002, S. 21–30, hier S. 21.

67 Vgl. etwa: Hongyuan Cui, Jiajun Yang, Ying Liu, Zheng Zheng und Kaichao Wu: »Data mining-based DNS Log Analysis«, in: *Ann. Data. Sci.* 1 (2014), Heft 3–4, S. 311–323.

68 Vgl. Jonas: »Effective Couterterrorism and the Limited Role of Predictive Data Mining«, in: *Policy Analysis* 584, a.a.O., S. 8.

69 Vgl. Anonym: »Der Senator auf der Terroristen-Liste«, in: *Süddeutsche Zeitung*, 17.5.2010, http://www.sueddeutsche.de/politik/flughafenkontrolle-der-senator-auf-der-terroristen-liste-1.644168 (aufgerufen 24.1.2016).

Datamining und maschinelles Lernen werden auch für die Verbesserung militärischer Technologie mit dem Zwecke operationaler und taktischer Anwendungen eingesetzt.[70] Die Forschung und Entwicklung im Bereich der Flugabwehr (engl. *antiaircraft defense*) bildet ein wichtiges Anwendungsfeld etwa zur Verbesserung der Technologie sogenannter *electronic countermeasures* (ECM). Es handelt sich dabei um ein offensiv oder defensiv einsetzbares elektronisches Mittel, das feindliche Erkennungssysteme wie Radar, Infrarot oder Laser ablenken oder austricksen soll.[71] Mit Datamining strebt man Einsicht in Bedrohungsparameter an, zu denen normalerweise nur begrenzt Information zur Verfügung steht.[72] Auch auf dem Gebiet der automatischen Zielerkennung und der Freund-Feind-Erkennung (engl. *identification friend or foe*) stellt maschinelles Lernen einen wichtigen Ansatz der Forschung und Entwicklung dar.[73] Die visuelle Detektion von Menschen im Unterschied zu anderen Lebewesen und Objekten ist hier die zentrale Schwierigkeit.[74] Die Probleme, die bei der automatischen Zielerkennung und der Freund-Feind-Erkennung immer wieder auftauchen, einerseits und der verstärkte Einsatz von nicht nur Überwachungs-, sondern auch Kampfdrohen andererseits lassen erahnen, dass es sich bei diesem Forschungsfeld um eine der größten Herausforderungen für prädiktive Datenverfahren speziell im militärischen Bereich handelt.[75]

Bislang habe ich die Ausdrücke »Terror« oder »terroristische Aktivität« nur unkommentiert verwendet. Deren Präsenz im Zusammenhang aktueller Sicherheitsthemen muss jedoch hintergründig im Zusammenhang mit den historisch spezifischen Auffassungen und Konzeptionen des ›Feindes‹ begriffen werden, an denen die Mittel der Militär- und Sicherheitsstrategien ansetzen. Nach dem Ende des Ost-West-Konflikts steht der klassische zwischenstaatliche Krieg nicht mehr als drohende Auseinandersetzungsform im Vordergrund. Von daher sprechen Mary Kaldor und Herfried Münkler von »neuen« respektive »asymmetrischen« Kriegen.[76] Diese ver-

70 Aufgrund von Überschneidungen in den zugrundeliegenden Datenbanken im militärischen und im Sicherheitsbereich, muss eine Trennung in strategisch und operativ für die hier untersuchten Verfahren allerdings nicht grundsätzlich gemacht werden.

71 Vgl. Motta: »Data mining in military systems«, in: *WIT Transactions on Modelling and Simulation* 45, a.a.O., S. 171.

72 Vgl. ebd., S. 171f.

73 Vgl. Anonym: »DARPA seeks deep-learning AI to cope with flood of information«, in: *Homeland Security News Wire*, 16.4.2009, a.a.O.

74 Vgl. Alessandro Bissacco und Stefano Soatto: »Visual Detection and Classification of Humans, Their Pose, and Their Motion«, in: Franceschetti (Hg.): *Homeland Security Technology Challenges*, a.a.O., S. 47–72.

75 Vgl. Marina Fang: »Nearly 90 Percent Of People Killed In Recent Drone Strikes Were Not The Target«, in: *The Huffington Post*, 15.10.2015, http://www.huffingtonpost.com/entry/civilian-deaths-drone-strikes_us_561fafe2e4b028dd7ea6c4ff (aufgerufen: 9.7.2016).

76 Vgl. Herfried Münkler: »Die neuen Kriege«, in: *Der Staat im Bürger* 54 (2004), Heft 4, S. 179–184; Mary Kaldor: »In Defence of New Wars«, in: *Stability* 2 (2013), Heft 2, S. 1–16; vgl. auch die kritische Diskussion der Begriffs »asymmetrischer Krieg«: Raul Zelik: »Asymmetrischer Krieg«, in: *Wörterbuch des Krieges/Dictionary of War*, Berlin 2008, S. 36–48.

änderten Konfliktlagen sind durch die Beteiligung nicht-staatlicher Akteure gekennzeichnet sowie dadurch, dass die Grenzen zwischen kriegerisch-politischer Gewalt und Verbrechen verschwimmen; außerdem sind vermehrt Zivilisten von gewaltsamen Auseinandersetzungen betroffen.[77] Als neue Feind- und zugleich »Abwehrmodelle« sind in der theoretischen Reflexion dementsprechend »Netzwerke« und »Schwärme« erwogen worden.[78] Für die US-amerikanische National Security Agency wurde durch diesen Wandel des ›feindlichen Gegenüber‹ eine umfassende Erneuerung der bewärten Überwachungstechnologien nötig.[79] Die Assoziation einer unkalkulierbaren Gefahr entspricht also den momentan verfügbaren Konzeptionen des Feindes als einem ungleichen, dezentralen und gestaltlosen Gegenüber. Aktuelle Feindkonzeptionen begünstigen damit die Vorstellung des gänzlich Unberechenbaren. Letzteres spielt entsprechend auch in die Rechtfertigungs- und Implementierungsstrategien datenbasierter Sicherheitsmaßnahmen hinein. So besehen eröffnet Unberechenbarkeit als epistemologisches Konzept auch eine kritische Perpektive auf den politischen Umgang mit digitalen Prognoseverfahren.

3. Von der Kalkulation zur Visualisierung, Imagination und Fiktion

Der vorherige Abschnitt thematisierte Grenzen der digitalen Vorausberechnung beim Einsatz zur ›Aufdeckung‹ dessen, was als »terroristische Aktivität« verstanden wird. Damit zeichnete sich eine Form der Unberechenbarkeit ab, die spezifisch für die epistemologische Beschaffenheit von strategischen Bereichen wie Sicherheit und *Intelligence* genannt werden kann. Im Folgenden geht es hingegen um nicht-kalkulierende Umgangsweisen mit Unwägbarkeiten. Mit einem Blick auf etwaige Wechsel von Medien und Erkenntnisweisen im Zuge des Umgangs mit rechnerischen prognostischen Mitteln soll Unberechenbarkeit als epistemologisches Konzept quasi von ihren Rändern her weiter konturiert werden.

Zunächst führt solcherlei wieder zum »synthetischen« Zug des Datamining zurück, der sogenannten Mustererkennung (engl. *pattern recognition*). Es geht also um Verfahren, bei denen die Muster, auch »Regeln« genannt, von den Daten selber nahegelegt und somit ›entdeckt‹, und nicht wie bei der klassischen Rasterfahndung – noch bei deren Anwendungen nach den 2000er Jahren war die Voraussetzung eines Täterprofils erfolgsentscheidend – und anderen Verfahren der Datenanalyse, die lediglich »bestätigend« verfahren, hypothetisch von einem Nutzer oder Forscher an

77 Vgl. Kaldor: »In Defence of New Wars«, a.a.O.
78 Vgl. John Arquilla und David Ronfeldt: »Networks, Netwars and the fight for the future«, in: *FirstMonday* 6 (2001), Heft 10; vgl. Eva Horn: »Die Ungestalt des Feindes«, in: *MLN* 123 (2008), Heft 3, S. 656–675.
79 Vgl. Hayden: *Playing to the Edge*, a.a.O., S. 4f. und 32.

die Daten herangetragen werden.[80] Im Kreditwesen könnte dies etwa – um ein simples Beispiel aufzugreifen – einen Analysten, der die Risiken für Kreditausfall bestimmen möchte, dazu bringen, mittels Datamining nicht nur festzustellen, dass Personen mit vielen Schulden und niedrigem Einkommen ein hoher Risikofaktor zukommt, sondern auch, dass das Alter ein relevanter Risikofaktor ist – von sich aus wäre er selbst hierauf nicht gekommen.[81] Mit solchen »autonomen« Entdeckungen arbeitet auch die für Geheimdienstzwecke entwickelte Software.[82] Methoden zur selbständigen Mustererkennung sind zum Beispiel die erwähnten Verfahren »Assoziation« und »*clustering*«. Beides sind Formen des sogenannten *non-supervised computational learning*, bei dem keine vorher bekannte Kategorie die Algorithmen anleitet.[83] »Lernen« bedeutet hier das eigenständige, »neugierige« Finden von Ableitungen.[84] Zwar werden die durch Muster gefundenen Zusammenhänge durch Algorithmen ›errechnet‹. Die Muster resultieren jedoch selbst aus Assoziationsregeln, geben also eher »Beschreibungen« der Beziehungen innerhalb einer Datenbank ab.[85] Denn die angezeigten Relationen sind selbst nicht als analytische Formeln verfügbar. Dieses prozessinterne, vom Berechnen wegführende Moment stellt einen Übergang zu einem anderen Erkenntnismittel als dem der Kalkulation dar, denn die eigentlichen Einsichten werden hier zumeist vermittels Visualisierung und grafischer Aufbereitung gewonnen, welche oft erst den »Aha-Effekt« herbeiführen, der neue Einsichten bringt.[86] Vorteil der grafischen Darstellung ist es zwar, dass Muster und Relationen sowie außergewöhnliche oder fehlende Werte visuell aufbereitet besser wahrnehmbar sind als mit Listen von Zahlen und Text. Gleichwohl stellt es aber wiederum eine Schwierigkeit dar, die zahlreichen Dimensionen und Variablen eines Modells auf einem zweidimensionalen Computer-Monitor zu repräsentieren. Visua-

80 Vgl. Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 3; vgl. zur Rasterfahndung: David Gugerli: »Die Suche nach dem Muster: Horst Herold«, in: David Gugerli: *Suchmaschinen. Die Welt als Datenbank*, Frankfurt am Main 2009, S. 52–69; vgl. Thakkar: »Mining Databases and Data Streams«, in: Franceschetti (Hg.): *Homeland Security*, a.a.O., S. 104.

81 Vgl. Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 3.

82 Vgl. Hofstetter: *Sie wissen alles*, a.a.O., S. 13.

83 Vgl. Motta: »Data mining in military systems«, in: *WIT Transactions on Modelling and Simulation* 45, a.a.O., S. 177; Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 10.

84 Vgl. Harrach: *Neugierige Strukturvorschläge im maschinellen Lernen*, a.a.O.

85 Vgl. Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 8.

86 Siehe Beispiele von Visualisierungen beim Datamining bei: Daniel A. Keim: »Datenvisualisierung und Data Mining«, in: *Datenbank-Spektrum* 2 (2002), S. 30–39; vgl. Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 6.

lisierung und vieldimensionale Daten stehen sich hier bisweilen gleichsam unvereinbar gegenüber.[87]

Das Visuelle, von dem im Zusammenhang mit Datamining die Rede ist, kann mit Sybille Krämers Überlegungen zum »erkennenden ›Sehen‹« epistemologisch als »operative Bildlichkeit« konkretisiert werden.[88] Da mit den prädiktiven Modellen zuverlässig Ausschnitte der Wirklichkeit abgebildet werden sollen und die *patterns* Zusammenhänge des jeweiligen Wirklichkeitsausschnitts anzeigen, sind sie ›referenziell‹. Sie nehmen auf ein ›Außerhalb‹ des Bildes Bezug und sind nicht dazu gedacht, für sich selbst zu stehen – ebendies unterscheidet operative Bilder von Bildern, die aufgrund eines ästhetischen Gehalts für sich selbst stehen können. Dass Bilder »operativ« sind, besagt Krämer zufolge außerdem, dass es sich bei ihnen nicht lediglich um Abbildungen von etwas handelt, sondern dass das Dargestellte mit dem Visualisierungsprozess »gehandhabt«, »beobachtet«, »exploriert« und zum Teil auch hervorgebracht wird, im Sinne einer epistemischen Konstitutionsleistung – was wie gezeigt auf die Visualisierungen beim Datamining zutrifft.[89] Die digitalen Anwendungen zur *Datavisualization* schaffen »Evidenz« indem sie Einsichten zustandebringen, die nicht schon in ihre Konstruktion eingeflossen sind.[90] Das Stichwort der Evidenz führt zurück zu Problemen beim Einsatz des Datamining im *Security*-Kontext. Denn die mit den Verfahren entdeckten Muster sind nicht selbsterklärend. So ist der Übergang vom Rechnerischen zum Visuellen als eine Änderung des epistemischen Mittels und damit der Erkenntnisweise zu verstehen, auch wenn die grafische Aufarbeitung computergestützt erfolgt. Denn, ähnlich wie das ›Sehen‹ des Vorliegens bestimmter wissenschaftlicher Tatsachen unter einem Mikroskop als »gerichtetes Wahrnehmen« erlernt werden muss, liegen die mit den Datenvisualisierungen gewonnenen Einsichten nicht als zahlenmäßig feststellbares Ergebnis vor, sondern ihr Erkennen bedarf der visuellen Einübung.[91] Im Umgang mit den Datenanwendungen erfahrene Personen werden benötigt, um die gefundenen Zusammenhänge zu interpretieren. Und die neuen Werkzeuge zur Datenvisualisierung, deren Entwicklung momentan stark vorangetrieben wird, erfordern Experten, deren Augen da-

87 Vgl. Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 6; vgl. Usama Fayyad und Georges G. Grinstein: »Introduction«, in: Usama Fayyad (Hg.):
Information Visualization in Data Mining and Knowledge Discovery, San Francisco 2002, S. 1–18, hier: S. 5; vgl.: Thakkar: »Mining Databases and Data Streams«, in: Franceschetti (Hg.): *Homeland Security Technology Challenges*, a.a.O., S. 120.

88 Sybille Krämer: »Operative Bildlichkeit. Von der ›Grammatologie‹ zu einer ›Diagrammatologie‹? Reflexionen über erkennendes ›Sehen‹«, in: Martina Hessler und Dieter Mersch (Hg.): *Logik des Bildlichen. Zur Kritik der ikonischen Vernunft*, Bielefeld 2009, S. 94–121.

89 Ebd., S. 103ff.

90 Vgl. ebd., S. 108. Ich habe an dieser Stelle Krämers Vokabular zu Diagrammen aufgegriffen.

91 Vgl. Ludwik Fleck: *Entstehung und Entwicklung einer wissenschaftlichen Tatsache. Einführung in die Lehre vom Denkstil und Denkkollektiv*, Frankfurt am Main 1980, S. 34 und 163; vgl. Ludwik Fleck: *Erfahrung und Tatsache*, Frankfurt am Main 1983.

rin geschult sind, die Bedeutungen der angezeigten Muster zu ›sehen‹ und zu verstehen.[92]

Expertise und Erfahrung über die konkrete Anwendung von Dataminingmethoden hinaus stellen also wichtige Voraussetzungen dar, um die mit Datamining produzierten Informationen überhaupt erst in handlungsrelevantes, strategisches Wissen transformieren zu können. Des Weiteren werden angesichts des Versagens oder der Nichtanwendbarkeit des Quantitativen von Wortführern der Wissensbereiche Strategie und *Security* jedoch auch Mittel wie Imagination oder Fiktion zum Vorgriff auf Zukünftiges erwogen. Der kalkulative Ansatz alleine, so zeigen Beispiele aus der Geschichte des strategischen Denkens, reicht für die Bereitstellung von konkretem Handlungs- und Entscheidungswissen nicht hin. – Es sei nicht Aufgabe eines Geheimdienstmitarbeiters genau vorherzusagen, was passieren wird, befindet Isaac Ben-Israel 1989, sondern ein solcher hätte darauf hinzuweisen, was passieren *könnte*.[93] Angesichts der Frage, wie sich der Möglichkeitsraum kommender Gefahren ausloten lässt, verweist er auf die Vorstellungskraft des *intelligent officers*. Ein solcher müsse seiner freien Imagination hypothetische Einschätzungen respektive Theorien abgewinnen und diese dann an vorhandenen Fakten prüfen.[94] Prädiktive Einschätzungen aus in der Vergangenheit oder Gegenwart gesammelten Daten zu erstellen hält er dagegen für grundsätzlich falsch und hinderlich.[95] Ob ein Krieg ausbricht oder nicht, sei nicht logisch ableitbar. Ben-Israel ist nicht der einzige Geheimdienst- und Strategieexperte, der auf freie Imagination als das Mittel der Wahl verweist, wenn es darum geht, schwer abschätzbare zukünftige Vorkommnisse zu präfigurieren.

Besonders elaboriert und interessant ist in diesem Zusammenhang das Zusammenspiel der rechnerischen und nichtrechnerischen Mittel, die der US-Amerikaner Herman Kahn in der Zeit des Kalten Krieges, unter anderem als Mitarbeiter der RAND-Corporation angesichts des »Undenkbaren«, wie er es nennt, für die Einschätzung der Zukunft vorschlägt.[96] Undenkbar ist für ihn nicht in erster Linie ein Feind oder dessen Verhalten. Das feindliche Andere – hier der sowjetisch geführte Ostblock – ist in Kahns strategischem Ansatz noch als berechenbares Gegenüber mit nachvollziehbaren Zielen und Handlungen konzipiert, dessen Überlegungen sich antizipieren lassen.[97] Undenkbar oder unvordenkbar ist für ihn vielmehr die ›absolute Katastrophe‹, ein Atomkrieg der beiden »Supermächte«. Kahns Anstrengungen gin-

92 Vgl. Two Crows Corporation (Hg.): *Introduction to Data Mining and Knowledge Discovery*, a.a.O., S. 6.
93 Isaac Ben-Israel: »Philosophy and Methodology of Intelligence – The Logic of Estimate Process«, in: *Intelligence and National Security* 4 1989, Heft 4, S. 690–718, hier S. 701.
94 Vgl. ebd., S. 667 und 713.
95 Ebd., S. 671.
96 »Thinking About the Unthinkable« ist ein Buchtitel Kahns: Herman Kahn: *Thinking About the Unthinkable*, New York 1962.
97 Vgl. Horn: *Der geheime Krieg*, a.a.O., S. 478.

gen dahin, dieses Undenkbare zu imaginieren, zu beschreiben, vorauszuberechnen, zu durchdenken und somit »handhabbar« zu machen. Obwohl Kahns Ansätze der *Systems Analysis* und *Operations Research* gewissermaßen paradigmagegebend waren, was die Berechnung möglichen zukünftigen Geschehens im strategischen Denken und der Politikberatung angeht, gehen in seinen Arbeiten die rechnerischen Methoden auch immer mit nicht-berechnenden Hand in Hand.[98] Besonders deutlich wird die Flankierung seines Ansatzes mit nicht-quantitativen Mitteln im Kapitel »Some strange aids to thought« des Buches *Thinking About the Unthinkable*.[99] Abstrakte Modelle, Szenarien, Kriegs- und Friedensspiele und historische Beispiele sind die Instrumentarien, die Kahn zufolge zusammen mit den quantitativen *major tools*, *Operations Research* und *Systems Analysis*, dazu beitragen sollen, das strategische Denken zu orientieren.[100] In der Reihe der dort dargelegten Denkhilfsmittel sind das »historische Beispiel« und »fiktionale Literatur« wohl am weitesten von einem quantitativen Ansatz entfernt.[101]

Auch im Rahmen der jüngeren »Antiterrormaßnahmen« wird angesichts von unkalkulierbaren künftigen Bedrohungen auf Fiktion zurückgegriffen, wie Samuel Nunn darstellt.[102] Das US-amerikanische Homeland Security Council gab zuerst 2004 eine Liste mit möglichen Katastrophen-Szenarios, genannt »all-hazards planning scenarios«, heraus.[103] Diese besteht zu großen Teilen aus Szenarien möglicher terroristischer Angriffe, wie chemischen, biologischen, radioaktiven oder *Cyber*-Attacken.[104] Nunn weist darauf hin, dass sich für diese Imaginationen zukünftiger Angriffe, die als Verdächtigungsmuster auch in die datenbasierten Instrumente des *war on terror* eingingen, größtenteils Vorlagen aus US-amerikanischen Filmproduktionen angeben lassen, wie etwa die Vorstellung eines Angriffs auf den Superbowl im

98 Vgl. Kahn: *On Thermonuclear War*, a.a.O., S. 9f.
99 Vgl. Kahn: *Thinking About the Unthinkable*, a.a.O., S. 127–175.
100 Vgl. ebd., S. 127.
101 Vgl. ebd. 172–175.
102 Vgl. Nunn: »Tell Us What's Going to Happen «, in: Kroker (Hg.): *Critical Digital Studies*, a.a.O., S. 295–302.
103 Vgl. The Homeland Security Council (Hg.): *Planning Scenarios. Executive Summaries. Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities*, Washington, D.C. 2004, http://www.altheim.com/lit/planning_scenarios_exec_summary.html (aufgerufen: 24.1.2016); vgl. auch: Eric Lipton: »U.S. Report Lists Possibilities for Terrorist Attacks and Likely Toll«, in: *The New York Times*, 16.3.2005, http://www.nytimes.com/2005/03/16/politics/us-report-lists-possibilities-for-terrorist-attacks-and-likely-toll.html (aufgerufen 24.1.2016). Vgl. zur Aktualisierung der sogenannten National Planning Scenarios: Mary T. Tyszkiewicz, Edward R. McCleskey und Russell Miller: »Updating the National Planning Scenarios. Using Wicked Problems and Capability-Based Planning Concepts for Homeland Security«, in: *Journal of Homeland Security and Emergency Management* 9 (2012), Heft 1, Art. 32, S. 1–32.
104 Vgl. The Homeland Security Council (Hg.): *Planning Scenarios. Executive Summaries*, a.a.O. Das aktuelle Programm des DHS zur *preparedness* bei Cyberangriffen heißt »Cyber Storm«: https://www.dhs.gov/cyber-storm (abgerufen: 9.7.2016).

Film *Black Sunday*.[105] Am Institute for Creative Technologies der University of Southern California habe es Treffen offizieller Militärmitarbeiter mit Regisseuren, Produzenten und Drehbuchschreibern gegeben, um zuvor noch nicht erwogene Terrorismus-Szenarien zu entwickeln und Material für den Entwurf von Präventivstrategien zu erhalten.[106] Auch aktuell scheint also der datenbasierte, rechnerische Ansatz alleine nicht auszureichen, um handlungsrelevantes Wissen für strategische Zwecke bereitszustellen. Die quantitativen Verfahren müssen mit anderen, nicht computergestützten *skills*, Praktiken und Mitteln – dazu zählen auch Narration und Fiktion – ineinandergreifen, um überhaupt effektiv einsetzbar zu sein.

4. Uncertainty *und Unberechenbarkeit*

Dass in den Bereichen Sicherheit und Militär epistemische Prozesse wie Theoriebildung, Entscheidungsfindung oder Lageeinschätzungen in einem besonderen Maße von Unwägbarkeiten bestimmt sind, bildete den Einsatzpunkt des vorliegenden Beitrages. Meine These ist, dass der aktuelle Umgang mit Bedrohungen und Gefahren einen Begriff von Unberechenbarkeit nahelegt, der mit den vorangegangenen Überlegungen zu Problemen digitaler Berechnungen im Einsatz für Sicherheitsbelange und dem folgenden Abgleich mit dem Begriff der *uncertainty* als epistemologisches Konzept verstanden werden kann und als solches weiterführt.

Ungewissheit bildet im Sicherheitsbereich einen Gegenstand methodischen und technischen Wissens, welches den Zweck hat, faktische Einsichten für den Umgang mit ebendiesem Ungewissen bereitzustellen.[107] Eine maßgebliche begriffliche Auseinandersetzung mit Ungewissheit im Hinblick auf strategische und taktische Überlegungen im Krieg nahm Carl von Clausewitz im neunzehnten Jahrhundert vor. Die unzähligen Ungewissheiten unter denen im Krieg gehandelt werden muss, die wesentliche, unvorhergesehene Veränderungen im Kriegsgeschehen hervorbringen – Wetter, körperliche Belastungsgrenzen, schwierige Nachrichtenlagen, aber auch psychische und emotionale Faktoren –, nennt er »Friktionen«.[108] Während es bei Clausewitz – in Abhebung von der kriegstheoretischen Literatur vor ihm – zunächst einmal darum ging, Unwägbarkeiten im Kriegsgeschehen überhaupt theoretisch zu berücksichtigen, nehmen Autoren im zwanzigsten Jahrhundert begriffliche Ausdiffe-

105 Vgl. Nunn: »Tell Us What's Going to Happen «, in: Kroker (Hg.): *Critical Digital Studies*, a.a.O., S. 301f.
106 Vgl. ebd., S. 295.
107 Vgl. Daase: »Knowns and Unknowns in the ›War on Terror‹ «, in: *Security Dialogue* 38, a.a.O., S. 414.
108 Vgl. Clausewitz: *Vom Kriege*, a.a.O., S. 115–123; hier S. 116.

renzierungen von *uncertainties* vor.[109] Mit den Mitteln der Kriegsführung im Zweiten Weltkrieg kommt Ungewissheit vor allem als »technische Ungewissheit« in den Blick. Technologische Innovationen, die im Kriegsverlauf emergierten, wie die Implementierung von Radar, Entschlüsselungsfortschritte oder Verbesserungen der Ausstattung von Panzern, Flugzeugen und Schiffen, stellten Fortschritte für die Kriegsführung dar und beförderten teils einen ›erfolgreichen‹ Kriegsverlauf.[110] Neue Technologien wurden dabei häufig ungetestet eingesetzt, denn die Zeit, Erfahrung mit ihnen zu sammeln, stand oft nicht zur Verfügung.[111] Neben Vorteilen brachten die Technologien durch fehlende Verlässlichkeit und Unberechenbarkeit auch Probleme im Kriegsverlauf mit sich, so musste etwa der Kolbenmotor der Boeing B-29 Langstreckenbomber, während deren Einsatz schon begonnen hatte, mehrfach überarbeitet werden.[112] Philip Scrantons These ist, dass *technological uncertainty* auch in Friedenszeiten der ständige Begleiter technischer Innovation ist. Das heißt, Technologien kommen zur Anwendung, ohne dass sie ganz verstanden worden sind und ohne dass noch die spezifischen Probleme, die sie mit sich bringen, bekannt wären.[113] Da sich der mit dem vorliegenden Beitrag herausgearbeitete Begriff der Unberechenbarkeit in den Bereichen Sicherheit und Militär speziell auf jüngere Konzeptionen der Unsicherheit im Zuge der Terrorismusbekämpfung bezieht, muss Scranton hier nicht widersprochen werden.

In der Nachkriegssituation des Kalten Krieges, von der die Arbeiten Kahns zeugen, stellt sich die Lage ein Stück komplizierter dar, als es das Konzept der *technological uncertainty* zu fassen vermag. Die neue Komplexität der Situation rührt aber nicht zuletzt von jenem Nichtwissen her, welches die epistemisch zentrale Rolle des Feindes in den Überlegungen notwendigerweise mit sich bringt.[114] Kahn unterteilt die *uncertainties* in diesem Zusammenhang in drei Kategorien: erstens eine »statistische Ungewissheit«, die Ereignisse fasst, deren Wahrscheinlichkeit »objektiv«, also als Zahlenwert angebbar ist; zweitens eine sogenannte »reale Ungewissheit«, mit der Personen Ereignissen subjektiv eine Probabilität zuschreiben, für die aber keine generelle Einigung zu erzielen ist; und drittens »Ungewissheiten, die Handlungen und Reaktionen des Feindes geschuldet sind«.[115] Eine andere methodische Unterteilung

109 Vgl. Thomas Jäger und Rasmus Beckmann: »Carl von Clausewitz' Theorie des Krieges«, in: Thomas Jäger und Rasmus Beckmann (Hg.): *Handbuch Kriegstheorien*, Wiesbaden 2011, S. 214–226, hier S. 216.

110 Vgl. Philip Scranton: »The Challenge of Technological Uncertainty«, in: *Technology and Culture* 50 (2009), Heft 2, S. 513–518, hier S. 514.

111 Vgl. Kahn: *Techniques of Systems Analysis*, a.a.O., S. 4 und: Philip Scranton: »The Challenge of Technological Uncertainty«, in: *Technology and Culture* 50, a.a.O., S. 513–518, hier S. 514.

112 Vgl. Scranton: »The Challenge of Technological Uncertainty«, in: *Technology and Culture* 50, a.a.O., S. 514.

113 Vgl. ebd.

114 Vgl. Kahn: *Techniques of Systems Analysis*, a.a.O., S. 36.

115 Vgl. Kahn: *Techniques of Systems Analysis*, a.a.O., S. 36. Eig. Übers.

– mit Referenz zur Wissenschaftstheorie – nimmt der Geheimdienstexperte Ben-Israel vor. Er schlägt vor, *intelligence*-Probleme entlang einer Skala der Komplexität anzuordnen, an deren einem Ende »rein technische Probleme« platziert sind, lösbar mit direkter Messung, und an deren anderem Ende sich Probleme finden, die von Ungewissheit gekennzeichnet und nicht mit algorithmischen Methoden lösbar sind. Erstere werden mit Rückgriff auf das Vokabular Karl Poppers »Uhren« genannt, aufgrund ihres mechanischen, kalkulierbaren Charakters, und zweitere »Wolken«, um deren komplexe Beschaffenheit und ihr unvorhersagbares Verhalten anzuzeigen.[116] Die beiden genannten Positionen nehmen also jeweils eine Differenzierung von *uncertainty* vor, für die der Anteil an quantitativen Verfahren entscheidend ist. Unberechenbarkeit spielt dagegen in der Konzeption politischer Gefahren und Risiken hier noch keine Rolle.

Die neue Extremform nicht berechenbaren Wissens, die mit dem 21. Jahrhundert und den auf »9/11« folgenden Sicherheitsmaßnahmen in den theoretischen Debatten festgestellt wird, geht damit einher, dass Nichtwissen für politische Entscheidungsprozesse gleich wichtig geworden ist wie Wissen.[117] Im Zuge der asymmetrischen Kriegsführung müsse mit wesentlich mehr *unknowns* umgegangen und gerechnet werden, stellen Christopher Daase und Oliver Kessler heraus.[118] Sie referieren hiermit auf eine Äußerung des ehemaligen US-amerikanischen Verteidigungsministers Donald Rumsfeld im Vorfeld des dritten Golfkrieges bezüglich des Nichtwissens um den irakischen Besitz von Massenvernichtungswaffen im Rahmen der Rechtfertigung eines militärischen Einsatzes: »We […] know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know«.[119] Insbesondere die mit dem Zusatz »The absence of evidence is not evidence of absence«[120] ausgedrückte formale Negativität macht deutlich, dass in jüngerer Zeit mit der im Zitat als zweites genannten Variante eine Extremform von Nichtwissen ins Spiel gebracht wird, die beispielseise bei Kahns Umgang mit dem »Undenkbaren« noch keine Rol-

116 Vgl. Ben-Israel: »Philosophy and Methodology of Intelligence «, in: *Intelligence and National Security* 4, a.a.O., S. 681. Zwar bietet die von Ben-IsraAktuell vorgeschlagene Skala Platz für die Verortung von Zwischenphänomenen, dennoch liegt ihr eine Polarisierung zugrunde, die aktuell etwa mit der Position vergleichen lässt, dass Cognition und *Computation* inkompatibel sind. Vgl. z.B.: Roger Schank: »The fraudulent claims made by IBM about Watson and AI«, in: *Roger Schank* 2016, http://www.rogerschank.com/fraudulent-claims-made-by-IBM-about-Watson-and-AI (aufgerufen: 9.7.2016).

117 Vgl. Daase: »Knowns and Unknowns in the ›War on Terror‹ «, in: *Security Dialogue* 38, a.a.O., S. 412.

118 Vgl. ebd., S. 415.

119 U.S. Department of Defense: *DoD News Briefing – Secretary Rumsfeld and Gen. Myers*, News Transcript/Press Operations, 12.2.2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=2636 (aufgerufen 1.8.2016).

120 Vgl. Sharon Ghamari-Tabrizi: *The Worlds of Herman Kahn. The Intuitive Science of Thermonuclear War*, Cambridge, Mass. 2005, S. 1.

le spielt. Denn worin die Bedrohung in dessen Setting besteht, darüber gibt es Informationen respektive konkrete Fragen, es geht um den atomaren Erstschlag und dessen Konsequenzen. Für die Bestimmung von »Unberechenbarkeit« ist Daases und Kesslers Differenzierung in Methoden, die Dinge verhandeln, derer wir uns nicht hundertprozentig sicher sind – diese stellen *known unknowns* bereit – und der Tatsache, dass wir akzeptieren müssten, dass es Dinge gibt »von denen wir noch nicht mal träumen« und für die uns keine Methode des Vorausahnens zur Verfügung steht – womit die sogenannten *unknown unknowns* angezeigt wären –, relevant.[121] Die Wortwahl »nicht hundertprozentig sicher« und »nicht erträumbar«, zeigt den Unterschied an, auf den es mir ankommt. *Uncertainty* ist, wie das »nicht ganz« Sichere, zumeist nicht im negativen Sinn als ein gänzlich Unvorstellbares gedacht, wie es als Hintergrund aktueller Präventionspolitik figuriert und welches in etwa besagt: »Man weiß weder, wer oder was die Katastrophe auslösen, noch wann und in welcher Form sie uns ereilen wird«.[122] Die oben mit den digitalen Vorhersageverfahren thematisch gewordene formale Unberechenbarkeit entspricht diesem spezifischen Nichtwissen, das lediglich in negativer Form angebbar ist. Mit dem gebräuchlichen Begriff der *uncertainty* sind diese Differenzierungen nicht hinreichend zu fassen. Äußerungen Luciano Floridis zum gesellschaftlichen Wert von *uncertainties* mögen dies abschließend verdeutlichen. Diesen sieht er unter anderem darin, dass sie Fragen und Diskussionen angeregen. »Ungewissheit« in einer Sache bedeute, dass es zu ihr lediglich Fragen, jedoch keine Antworten gibt. Damit ist sie als Begriff eher den oben genannten *known unknowns* zuzuordnen. Er betont: »A liberal, tolerant, and fair society is one in which a healthy degree of uncertainty is both welcomed and fostered«.[123] Absolut negativ bestimmt, aufgrund ihres »Unwerts« sei jedoch Unwissenheit, »[i]t is not uncertainty but rather ignorance that is an absolute disvalue«.[124]

Auch wenn *uncertainty* teils probabilistisch bestimmt werden kann, lässt sie sich nicht in jedem Fall berechnen. Dennoch macht gerade die Ambiguität von Bedrohlichem einerseits und nicht rechnerisch Fassbarem andererseits, welche dem Begriff der Unberechenbarkeit im Unterschied zu *uncertainty* anhaftet, diesen ein Stück weit mehr geeignet als ›Ungewissheit‹, den aktuellen Einsatz digitaler Wahrscheinlichkeitsberechnungen im Kontext politischer Konflikte und Bedrohungen kritisch zu reflektieren. Mit dem Konzept der Unberechenbarkeit rücken als ›Rückseite‹ der weitgehenden Berechnungsbestrebungen und des Vertrauens in datenbasierte technologische Lösungen, die derzeit viele Wissens- und Lebensbereiche prägen, auch de-

121 Vgl. Daase: »Knowns and Unknowns in the ›War on Terror‹ «, in: *Security Dialogue* 38, a.a.O., S. 413.
122 Bröckling: »Dispositive der Vorbeugung «, in: Daase (Hg.): *Sicherheitskultur*, a.a.O., S. 100.
123 Vgl. Luciano Floridi: »Uncertainty: Technology's Secret Weapon in Encouraging Us to Explore«, in: *The Guardian*, 1.9.2014, http://www.theguardian.com/technology/2014/sep/01/uncertainty-clarity-philosophy (aufgerufen 10.7.2016).
124 Ebd.

ren besondere Begrenzungen und Auswirkungen hinsichtlich des Politisch-Strategischen in den Blick. Die Unberechenbarkeit, die mit den verfügbaren Feindkonzeptionen und momentanen Gefahrenlagen assoziiert ist, stützt auf der einen Seite die Rechtfertigung weitreichender ›datafizierender‹ Sicherheitsmaßnahmen und ist in diesem Sinn auch wiederum historisch spezifisches Produkt des aktuellen Umgangs mit Bedrohungen. Als solche fügt sie – wie die obigen Bemerkungen zur jüngeren Geschichte der Verbindung von politischer und technologischer *uncertainty* nahelegen – durch ihre inhaltliche Unbestimmtheit und Negativität dem Begriff der Ungewissheit einen neuen Aspekt hinzu.

Die Problematisierung des Verhältnisses von berechnenden und nicht-berechnenden Verfahren machte gleichzeitig deutlich, dass der Einsatz von digitalen Prädiktionen auf Big-Data-Grundlage im Sicherheits-Kontext – und hierin unterscheiden sie sich gerade nicht von früheren quantifizierenden Verfahren des politisch-strategischen Denkens – das Zusammenspiel mit Kompetenzen und *skills* wie gerichtetes Sehen, Imagination und Erfahrung und mit Mitteln wie Narration und Fiktion erfordern. Im Zuge der weitreichenden Bestrebungen und hohen Investitionen hinsichtlich der ubiquitären Integration digitaler Technologie darf dies nicht aus dem Blick geraten. Sich dieser Einsicht nicht zu stellen, heißt mit dafür zu sorgen, dass IT-Expertenwissen sich von anderen, etwa geisteswissenschaftlichen Wissensbereichen institutionell und disziplinär zunehmend weiter entfernt.