10.6094/behemoth.2020.13.1.1035

BEHEMOTH A Journal on Civilisation
2020 Volume 13 Issue No. 1

Die Prognose sicherheitsrelevanter Ereignisse mittels Künstlicher Intelligenz

Zukunftsvorstellungen, Erwartungen und Effekte auf Praktiken der Versicherheitlichung

The Prediction of Security Threats using Artificial Intelligence

Imaginations, Expectations and Effects on Practices of Securitization

Jens Hälterlein

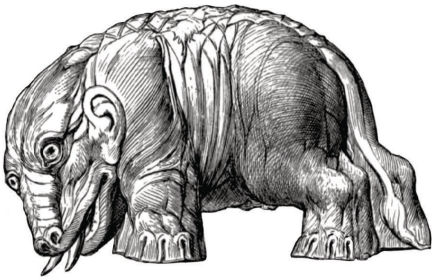
Abstract

The paper analyses the imaginations, expectations and techno-scientific promises that play a crucial role in understanding the importance of artificial intelligence in contemporary security culture. It addresses a number of questions: Which imaginations of the future and which scenarios mobilize the development and use of AI-based security technologies? Which approaches to AI are seen as "technological fix" for security problems? Which expectations and promises derive from these technologies? Finally, the paper analyses the effects that these technologies have on practices of securitization.

Keywords, dt.: Künstliche Intelligenz, Sicherheitstechnologien, katastrophische Zukünfte, Prognose, Versicherheitlichung

Keywords, engl.: Artificial Intelligence, Security Technologies, Catastrophic Futures, Prediction, Securitization

Jens Hälterlein is a research fellow at the Centre for Security and Society at University Freiburg. He has worked in several technology and security related projects. His current research fields are: Science and Technology Studies, Surveillance Studies and Critical Security Studies. He is particularly interested in Predictive Policing, Smart CCTV and the Governance of Artificial Intelligence. **E-Mail: jens.haelterlein@css.uni-freiburg.de**



Künstliche Intelligenz (KI) hat seit jeher unterschiedliche Zukunftsvorstellungen hervorgerufen. Hoffnungsvolle Visionen eines gesellschaftlichen Fortschritts durch KI (Minsky 1990; Moravec 1990) stehen Worst-Case-Szenarien von KI als Hybris des menschlichen Geistes gegenüber (Weizenbaum 1977). Diese Zukunftsvorstellungen sind von der KI-Forschung nicht zu trennen und haben deren Entwicklung maßgeblich beeinflusst (Bory 2019). So führten technologisch-wissenschaftliche Innovationen auf dem Gebiet der KI zu hohen Erwartungen hinsichtlich des transformativen Potenzials von KI-Anwendungen in unterschiedlichen Praxiskontexten. Diese Erwartungen brachten wiederum Investitionen in öffentliche und private Forschung mit sich (Ahrweiler 1995). Nachdem sich diese Erwartungen als überzogen herausstellten, durchschritt KI bereits mehrfach ein „Tal der Enttäuschung" (Fenn 1995, 8), die sogenannten „KI-Winter" (Ceruzzi 2011, 106), die mit Aufmerksamkeitsverlust, Enttäuschungen und dem Rücklauf von Investitionen einhergingen. Gegenwärtig befindet sich KI wieder in einer Phase des Aufschwungs. Durch Fortschritte im Maschinellen Lernen**[1]**, das mittlerweile in zahlreichen Praxiskontexten erprobt ist oder bereits zum Einsatz kommt (Fraunhofer 2018, 24ff.), hat KI nicht nur in Bezug auf Mobilität, Produktion, Pflege und Medizin Zukunftsvorstellungen mobilisiert. Der Einsatz von KI könne ebenso zu einschneidenden Veränderungen in der Art und Weise führen, wie Zivile Sicherheit**[2]** gewährleistet werden soll (Fiott/Lindstrom 2018). Ein transformatives Potenzial wird dieser Technologie zum einen für polizeiliche Aufgaben – Videoüberwachung, die Erstellung von Täterprofilen, die Bestimmung der Rückfallwahrscheinlichkeit von verurteilten Straftäter*innen und die Prognose von Straftaten – zugeschrieben. Zum anderen könne KI auch bei der Sicherung von kritischen Infrastrukturen, der Abwehr von Cyber-Angriffen, der Kontrolle von Migrationsbewegungen und der Eindämmung von Epidemien zur Anwendung kommen. Nachdem diese Zukunftsvorstellungen zunächst von Forscher*innen und Entwickler*innen sowie in den Medien artikuliert wurden, haben in den letzten Jahren zahlreiche Regierungen nationale Strategiepapiere veröffentlicht, in denen sie ihre Visionen der zukünftigen Entwicklung, Anwendung und Regulierung von KI-Technologien präsentieren und dabei Zivile Sicherheit als eines von mehreren vielversprechenden Einsatzfeldern behandeln.**[3]**

In den Science and Technology Studies und der Techniksoziologie stellt die Analyse der Effekte von technologiebezogenen Zukunftsvorstellungen und Erwartungen ein wichtiges Forschungsfeld dar. So wurde unter anderem untersucht, wie Versprechen des zukünftigen Erfolgs von Technologien private oder staatliche Investitionen in Forschung und Entwicklung mobilisieren (Konrad/Alvial-Palavicino 2017), wie Leitbilder und Szenarien Forscher*innen als epistemische Orientierung dienen, indem sie technische Entwicklungsoptionen vorselektieren (Dierkes et al. 1992; Schulz-Schaeffer 2013) und wie sozio-technische Zukunftsvisionen die Entwicklung umstrittener Technologien gegenüber der Öffentlichkeit rechtfertigen, indem sie ein positives Bild deren zukünftigen Einsatzes entwerfen (Jasanoff/Kim 2015). Allerdings wurde auch gezeigt, wie diese Visionen wiederum selbst zum Anlass gesellschaftlicher Kontroversen werden (Brown et al. 2016). KI-basierte Sicherheitstechnologien standen in diesem Forschungsfeld bislang allerdings nicht im Fokus.

[1] Maschinelles Lernen kann definiert werden als „Generierung von ‚Wissen' aus ‚Erfahrung', indem Lernalgorithmen aus Beispielen ein komplexes Modell entwickeln. Das Modell, und damit die automatisch erworbene Wissensrepräsentation, kann anschließend auf neue, potenziell unbekannte Daten derselben Art angewendet werden." (Fraunhofer 2018, 8)

[2] „Zivile Sicherheit" operiert nicht mehr entlang der kategorialen Unterscheidung zwischen innerer und äußerer Sicherheit, sondern geht von einem Bedrohungskontinuum aus (Kaufmann 2011). Namensgebend ist „Zivile Sicherheit" auch für ein Forschungsprogramm des Bundesministeriums für Bildung und Forschung (BMBF), in dem seit 2007 die Entwicklung von innovativen Sicherheitslösungen gefördert wird.

[3] Im November 2018 veröffentlichte auch die Bundesregierung ihre *Nationale Strategie für Künstliche Intelligenz* (NSKI 2018) unter dem Titel „Artificial Intelligence made in Germany" (vgl. https://www.bmbf.de/files/Nationale_KI-Strategie.pdf. Vgl. auch: https://www.ki-strategie-deutschland.de/home.html).

Der vorliegende Beitrag untersucht die Zukunftsvorstellungen, Erwartungen und „technoscientific promises“ (Felt/Wynne 2007, 24ff.), die für das Verständnis der gegenwärtigen Bedeutung dieser Technologien eine zentrale Rolle spielen. Hierzu wird eine Reihe von Fragen adressiert: Durch welche Zukunftsvorstellung und Szenarien werden die Entwicklung und der Einsatz von KI-basierten Sicherheitstechnologien mobilisiert? Welche Ansätze der KI-Forschung werden als ‚technological fix‘ für die Lösung von Sicherheitsproblemen behandelt? Welche Erwartungen und Versprechen verbinden sich mit diesen Technologien? Abschließend wird untersucht, welche Effekte diese Technologien in Praktiken der Versicherheitlichung entfalten. Damit schließt der Beitrag an eine Reihe von Studien aus dem Kontext der Critical Security Studies an, die gezeigt haben, dass Technologien als materielle Infrastruktur für die Produktion von Wissen, Bewertungen und Strategien fungieren, indem sie Identifikationen, Kategorisierungen, Risikokalkulationen und Verhaltensprognosen produzieren (Amicelle et al. 2015).

1. Katastrophische Zukünfte

Die von Craig Calhoun als „emergency imaginary“ (2004, 392) bezeichnete Imagination katastrophischer Zukünfte bildet den gemeinsamen Bezugspunkt einer Reihe von Studien zur gegenwärtigen Sicherheitskultur. Zentrales Kennzeichen dieses Zukunftsbezugs und damit der gegenwärtigen Sicherheitskultur ist nicht das Katstrophische selbst, sondern ein fundamentaler Wandel in der Wahrnehmung von Unsicherheit (Furedi 2009). Als paradigmatisch für diesen Wandel gilt für viele Autor*innen der Abschlussbericht der National Commission on Terrorist Attacks upon the United States (2004), welche nach den Terroranschlägen vom 11.09.2001 eingesetzt wurde. Eine der zentralen Aussagen des Berichts betrifft das Versagen der US-Sicherheitsbehörden, die Anschläge durch Bedrohungsszenarien vorherzusehen und dadurch gegebenenfalls zu verhindern, was von der Kommission in erster Linie als Mangel an Vorstellungskraft gedeutet wird, das Unerwartete zu erwarten und entsprechend zu handeln (ebd., 344ff.; vgl. auch Salter 2008). An die Stelle wahrscheinlicher Zukünfte, deren Konstruktion aus der Kenntnis der Vergangenheit erfolgt, sollen fortan mögliche Zukünfte treten, die auf der Imagination von Worst-Case-Szenarien basieren (Aradau 2010, 2). Die Aufforderung der Kommission, die Ausübung von Imagination zur Routine werden zu lassen (ebd.), hat bei vielen Sicherheitsbehörden dazu geführt, die Aufmerksamkeit auf „unknown unknowns“ (Rumsfeld 2002) und Bedrohungen, „die verschiedenartiger, weniger sichtbar und weniger vorhersehbar sind“ (Rat der Europäischen Union 2009, 30), zu richten.

In Anbetracht von high impact-low probability-Ereignissen beziehungsweise possibilistischen Risiken (Amoore 2016, 140) hat sich ein Handeln unter Unsicherheit verbreitet, das diese Ereignisse antizipiert und ihnen begegnet, indem es ihr Eintreten vorsorglich verhindert beziehungsweise vorbeugt (Krasmann 2011, 55) oder indem es den Umgang mit diesen einübt, um einen Zustand der „preparedness“ zu erreichen (Aradau 2010). Kennzeichnend für den „war on terror“ sind folglich das präemptive Ergreifen von Maßnahmen gegen potenzielle Terroristen, das unabhängig von empirischen Evidenzen für zukünftige Anschläge erfolgen kann (Aradau/van Munster 2011), sowie Katastrophenschutzübungen oder Planspiele, in denen Worst-

Case-Szenarien terroristischer Angriff mit Chemiewaffen (Adey/Anderson 2012) oder Pockenerregern (Uncertain Commons 2013, 62f.) simuliert werden. Des Weiteren ist die Imagination katastrophischer Zukünfte zu einem Kennzeichnen der Post-9/11-Medienlandschaft geworden. In dieser von Richard Grusin als „premediation" (2004) bezeichneten Praxis besteht die Rolle der Medien nicht in der Darstellung dessen, was bereits geschehen ist, sondern darin, was (schlimmstenfalls) geschehen könnte. Dadurch werde das Publikum, so Grusin, affektiv auf den Ernstfall vorbereitet, so dass sich die Sicherheitsakteure nach dem Eintreten des Ernstfalls an einem bereits bekannten Affekthaushalt der zivilen Bevölkerung orientieren können (ebd., 27).

2. Expertensysteme

Ein weiterer zentraler Aspekt der gegenwärtigen Sicherheitskultur ist das Bedürfnis nach neuen Technologien mittels derer katastrophische beziehungsweise sicherheitsrelevante Ereignisse antizipiert und Entscheidungsprozesse bei deren Präemption oder der Vorbereitung auf deren Eintreten unterstützt werden können (Ceyhan 2008; Amoore/de Goede 2005; Weber/Kämpf 2020). In der Folge von 9/11 kam es zu einer massiven Expansion von geheimdienstlichen Überwachungssystemen, die zur massenhaften Erfassung und Auswertung von Kommunikationsdaten, Finanztransaktionen und Bewegungsprofilen einzelner Risikogruppen oder auch ganzer Bevölkerungen eingesetzt werden (Mattelart 2010). Seit einigen Jahren setzen auch Polizeibehörden bei der Gefahrenprävention und Strafverfolgung neben der Nutzung polizeilicher Daten aus Vorgangsbearbeitungs-, Fahndungs- und Auskunftssystemen verstärkt auf sogenannte Open-Source-Intelligence (OSINT), also öffentlich zugänglichen Informationen, zum Beispiel aus sozialen Medien. Zudem wurde die bereits bestehende polizeiliche Videoüberwachung von gefährdeten beziehungsweise gefährlichen Räumen und Situationen (Flughäfen, Bahnhöfe, Grenzkontrollen, Demonstrationen, Sportveranstaltungen etc.) ausgebaut und durch Drohnen, Body Cams und Systeme zur automatischen Nummernschilderkennung ergänzt. Kennzeichnend für diese Entwicklung ist zum einen, dass die Erhebung beziehungsweise Produktion von heterogenen Datenmengen bislang unbekannten Ausmaßes (‚big data') mit der Notwendigkeit einhergeht, neue Methoden für deren automatisierte Auswertung zu entwickeln.**[4]** War das ‚connecting the dots' noch eine Herausforderung für den menschlichen Analysten (der dabei durchaus auf technische Hilfsmittel zurückgriff), ist das ‚finding the needle in the haystack' in erster Linie eine technische Herausforderung. Zum anderen besteht eine grundlegende Differenz zwischen Delikten wie Wohnungseinbrüchen und Autodiebstählen, die sich durchaus mit Hilfe von regelbasierten Expertensystemen prognostizieren lassen, und weniger alltäglichen Handlungen und Ereignissen wie terroristischen Anschlägen, Cyberangriffen auf kritische Infrastrukturen oder dem Auftreten von Epidemien. Denn während regelbasierte Expertensysteme Wahrscheinlichkeiten für Ereignisse auf der Basis mathematischer Modelle berechnen (Reichertz 1994), lassen sich katastrophische Ereignisse mit diesen Systemen nicht vorhersagen (Opitz/Tellmann 2011, 28). Grund dafür ist das Fehlen von Theorien, die Ereignisse regelbasiert ableiten, das heißt deduktiv von der allgemeinen Re-

[4] Der Begriff ‚big data' wird heute zumeist mit Bezug auf die drei Vs – Volume, Variety, Velocity – verwendet, ohne ein genaues Kriterium für Größe, Heterogenität und Geschwindigkeit anzugeben (Mayer-Schönberger/Cukier 2013). In frühen Formulierungen bezog sich ‚big data' hingegen auf dem Umstand, dass die Erhebung, Speicherung und Auswertung dieser Datenmengen nicht mehr mit vorhandenen Softwarelösungen geleistet werden kann (Lazer 2017, 21).

gel auf den Einzelfall schließen. Diese Theorien dienen Expertensystemen als notwendige Grundlage für Modellierungen, probabilistische Risikokalküle und Prognosen. Terroristische Handlungen und andere katastrophische Ereignisse erscheinen aus der Perspektive etablierter Theorien aber arbiträr beziehungsweise irrational (Furedi 2009, 204).**[5]** Regelbasierte Expertensysteme werden daher mit Blick auf Worst-Case-Szenarien als unzureichend kritisiert, da schlichtweg die Wissensbasis fehle, um verlässliche Prognosen zu erstellen (ebd., 205). Deshalb entstand ein verstärktes sicherheitspolitisches Interesse an der Frage, wie neue Techniken aus dem Kontext der KI für Sicherheitszwecke eingesetzt werden können, wodurch sich der Fokus auf Maschinelles Lernen (ML) verschoben hat (Lyon 2014, 1).

3. Maschinelles Lernen

Systeme, die auf ML basieren, sind in der Lage, selbstständig Muster und Zusammenhänge in großen, unstrukturierten Datenmengen zu erkennen und sodann Prognosen für zukünftige Ereignisse zu erstellen. ML formuliert das techno-wissenschaftliche Versprechen der Prognostizierbarkeit von zukünftigen Ereignissen, indem es den Zugriff auf ein Wissen ermögliche, das zwar in den Daten enthalten, für den menschlichen Betrachter aber nicht wahrnehmbar sei (Aradau/Blanke 2016, 378f.).**[6]** Auch wenn große Mengen von Daten schon immer für Statistiken, Modellierungen und Prognosen verwendet wurden (Hacking 2010), erhalten Daten nun eine andere Bedeutung, insofern sie als Ermöglichungsbedingung für ein alternatives Verfahren der Wissensproduktion angesehen werden (Kitchin 2014, 2). Wissensproduktion muss nicht mehr notwendigerweise bedeuten, empirisch fundierte Vermutungen anzustellen, Hypothesen und Modelle zu konstruieren und diese mit datenbasierten Experimenten und Beispielen zu testen. Beim ML analysiert ein Algorithmus zunächst ein Set an Trainingsdaten, die entweder bereits klassifiziert (‚gelabelt') wurden oder durch den Algorithmus klassifiziert werden. Das Ergebnis dieser Trainingsphase ist die Konstruktion eines prognostischen Modells, mittels dessen sich wiederum Aussagen über ein Set an Testdaten treffen lassen. In einem iterativen Test- und Lernverfahren wird das Modell so lang angepasst, bis die gewünschte Prognosegüte erreicht ist und das System auf alle verfügbaren Daten angewendet werden kann (Zweig et al. 2018). Durch ML produzierte Prognosen sind das Produkt eines abduktiven Schlussfolgerns,**[7]** das Bedrohungen für Referenzobjekte und entsprechende Ziele für präemptives Handeln nicht aus bestehenden Kriterien oder Regeln ableitet, sondern diese in einem generativen Prozess erschafft (Amoore/Raley 2016, 4). Ein regelbasiertes Programmieren von Prognosemodellen für Expertensysteme, welches die vorherige Kenntnis dieser Regeln immer schon voraussetzt, wird dadurch potenziell obsolet. Zudem können sich selbstlernende Systeme besser an eine sich schnell verändernde Umwelt beziehungsweise Datenlage anpassen. Sie lernen kontinuierlich weiter und verbessern damit ihre Performance, anstatt Unbekanntes als Ausnahme von der Regel ausblenden zu müssen.

Auch wenn regelbasierte Expertensysteme weiterhin eine wichtige Rolle für Sicherheitspraktiken spielen, hat das Zusammenspiel aus Verfügbarkeit immer größerer Datenmengen, größerer Datenspeicher und schnellerer Prozessoren nicht nur die Entwicklung ML-basierter Verfahren beschleunigt,

[5] Die produktive Rolle von menschlicher Expertise verschiebt sich in Richtung qualitativer und/oder experimenteller Verfahren der Wissens- und Theorieproduktion (vgl. exemplarisch: Fischer/Pelzer 2016).

[6] Tatsächlich bedarf es für einen solchen Prozess einer komplexen Infrastruktur aus menschlicher Arbeit sowie immateriellen und materiellen Ressourcen (vgl. https://anatomyof.ai/).

[7] Die Abduktion „sucht angesichts überraschender Fakten nach einer sinnstiftenden Regel, [...] welche das Überraschende an den Fakten beseitigt" (Reichertz 2003, 43). „Endpunkt dieser Suche ist eine [...] Hypothese. Ist diese gefunden, beginnt der Überprüfungsprozess" (ebd.).

sondern auch bei sicherheitspolitischen Akteuren zu der Erwartung geführt, eine durch Worst-Case-Szenarien und possibilistische Risiken charakterisierte Zukunft intelligibel und somit regierbar zu machen (ebd.). Das Interesse an ML-basierten Sicherheitstechnologien fußt also letztendlich auf zwei Voraussetzungen: Einerseits speist sich ihre Anziehungskraft auf sicherheitspolitische Akteure aus der Antizipation katastrophischer Zukünfte, dem emergency imaginary, und der daraus resultierenden, dringenden Handlungsanforderung, trotz aller Unsicherheiten das Eintreten des Worst-Case zu verhindern. Andererseits basiert der erhoffte handlungsentlastende Effekt solcher Technologien auf dem epistemischen Versprechen der neueren KI-Forschung, selbstlernende Algorithmen zu erschaffen, die zukünftige Ereignisse verlässlicher als ein Mensch prognostizieren und dadurch dessen Entscheidungsprozesse anleiten können.

4. Effekte ML-basierter Sicherheitstechnologien

Für den sicherheitspolitischen Umgang mit neuen Bedrohungslagen sind ML-basierte Sicherheitstechnologien ein ‚Game Changer', da sie der Begrenztheit des Wissens von Sicherheitsexperten neue Formen der Wissensgenerierung entgegensetzen und durch die Prognose zukünftiger Ereignisse handlungsentlastend auf Entscheidungen unter Unsicherheit wirken können. Der Einsatz dieser Technologien hat aber auch unabhängig von ihrem Nutzen für die Sicherheitsakteure eine Reihe von Effekten auf Prozesse der Versicherheitlichung:

- Die Möglichkeit, basierend auf der Analyse großer, heterogener Datenmengen Prognosen zu erstellen, forciert die Erhebung von neuen Daten und den erweiterten Zugriff auf vorhandene Daten (Lyon 2014, 6). Dadurch verwischen die Grenzen zwischen staatlicher Überwachung, Überwachungskapitalismus und Selbstüberwachung zusehends. Denn die Datenmengen, die für das Training von selbstlernenden Algorithmen notwendig sind, stehen staatlichen Akteuren (legal) häufig nicht zur Verfügung. Daher sind es in der Regel privatwirtschaftliche Akteure, die auf der Basis nutzergenerierter Daten neue, leistungsfähigere ML-Systeme entwickeln und diese dann wiederum an staatliche Akteure verkaufen.**[8]** Fragen des Datenschutzes und der digitalen Privatsphäre werden damit implizit auch zu Fragen der Zivilen Sicherheit.
- ML-basierte Prozesse können zu Identifikationen, Klassifikationen und Beurteilungen von Risiken führen, durch die ‚racial profiling' und andere Formen diskriminierender Sicherheitspraktiken reproduziert oder sogar verstärkt werden. Eine Studie der NGO ProPublica (Angwin et al. 2016) zeigt, dass die Software COMPAS, welche in einigen Bundesstaaten der USA genutzt wird, um die Rückfallwahrscheinlichkeit von Straftäter*innen zu bestimmen, Schwarze Menschen systematisch schlechter bewertet als Weiße Menschen. Ähnliche Effekte lassen sich in Folge der Anwendung einer ML-basierten Software bei der Analyse von Fluggastdaten in Australien beobachten, die zu einer Intensivierung der im Kontext der Kontrolle von Migrationsbewegungen typischen Formen von vorurteilsbelasteten Kategorisierung und Identitätszuschreibung führt (Ajana 2015). Introna und Wood (2004) weisen in einer Studie über biometrische Gesichtserkennungssysteme auf einen starken Ethnie- und

[8] Öffentlich skandalisiert wurde ein solches Vorgehen zuletzt mit Blick auf das Unternehmen *Clearview AI*.

Geschlechter-Bias eines der von ihnen untersuchten Systeme hin, das Männer besser als Frauen, und dunkle besser als helle Hautfarben detektierte.

- Die Anwendung selbstlernender Algorithmen kann dazu führen, dass Prognosen und somit auch die daran gekoppelten Entscheidungsprozesse opak erscheinen. Zwar können Prognosen hinsichtlich ihrer Plausibilität beurteilt und Entscheidungen immer einem menschlichen Akteur als Letztinstanz (‚human in the loop') überlassen werden. Jedoch zeichnen sich insbesondere die derzeit leistungsfähigsten ML-Systeme, die sogenannte Künstliche Neuronale Netze verwenden, durch ein hohes Maß an Intransparenz hinsichtlich des Zustandekommens ihrer Prognosen aus. Als Black Box erschweren diese Systeme die Kontrolle durch externe Instanzen und die Nachvollziehbarkeit der Generierung von Output aus Input (Chan/Bennett Moses 2015). Dadurch könnte der Einsatz dieser Systeme wiederum Konsequenzen für die Anwendbarkeit von bestehenden Anti-Diskriminierungsgesetzen haben (Leese 2014).

Angesichts dieser Effekte, die der Einsatz ML-basierter Sicherheitstechnologien auf Praktiken der Versicherheitlichung hat, bleibt die Legitimation dieser Praktiken prekär und wird zum Anlass gesellschaftlicher Kontroversen. Die politische Zukunftsvision, Zivile Sicherheit durch den Einsatz von KI zu gewährleisten, wird sich ebenso an der Vermeidung katastrophischer Ereignisse wie am Umgang mit diesen Kontroversen messen lassen müssen.

Literatur

Adey, P.; Anderson, B. (2012) Anticipating emergencies. Technologies of preparedness and the matter of security. In: *Security Dialogue* 43(2): 99-117.

Ahrweiler, P. (1995) KI West und KI Ost. Die Institutionalisierung eines Hochtechnologiefachs in Deutschland. In: Rammert W. (ed.) *Soziologie und Künstliche Intelligenz – Produkte und Probleme einer Hochtechnologie*. Frankfurt a.M.: Campus.

Ajana, B. (2015) Augmented borders. Big Data and the ethics of immigration control. In: *Journal of Information, Communication & Ethics in Society* 13(1): 58-78.

Amicelle, A.; Aradau, C.; Jeandesboz, J. (2015) Questioning security devices. Performativity, resistance, politics. In: *Security Dialogue* 46(4): 293-306.

Amoore, L. (2016) Vigilant Visualities. The Watchful Politics of the War on Terror. In: *Security Dialogue* 38(2): 215-232.

Amoore, L.; de Goede, M. (2005) Governance, risk and dataveillance in the war on terror. In: *Crime Law and Social Change* 43(2-3): 149-173.

Amoore, L.; Raley, R. (2016) Securing with algorithms. Knowledge, decision, sovereignty. In: *Security Dialogue* 48(1): 1-8.

Angwin, J.; Larson, J.; Mattu, S.; Kirchner, L. *(2016) Machine Bias*. There's software used across the country to predict future criminals. And it's biased against blacks. *In: ProPublica*. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (06/04/2020)

Aradau, C. (2010) Security That Matters. Critical Infrastructure and Objects of Protection. In: *Security Dialogue* 41(5): 491-514.

Aradau, C.; van Munster, R. (2011) *Politics of catastrophe. Genealogies of the unknown*. Abingdon, Oxon: Routledge.
Aradau, C.; Blanke, T. (2015) The (Big) Data-security assemblage. Knowledge and critique. In: *Big Data & Society* 2(2): 205395171560906.
Aradau, C.; Blanke, T. (2016) Politics of prediction. In: *European Journal of Social Theory* 20(3): 373-391.
Bory, P. (2019) Deep new. The shifting narratives of artificial intelligence from Deep Blue to AlphaGo. In: *Convergence* 25(4): 627-642.
Brown, N.; Rappert, B.; Webster, A. (2016) *Contested futures: A sociology of prospective techno-science*. London: Routledge.
Calhoun, C. (2004) A World of Emergencies. Fear, Intervention, and the Limits of Cosmopolitan Order. In: *Canadian Review of Sociology/Revue canadienne de sociologie* 41(4): 373-395.
Ceruzzi, P. (2011) Manned Space Flight and Artificial Intelligence. „Natural" Trajectories of Technology. In: Ferro, D.; Swedin, E. (eds.) *Science Fiction and Computing: Essays on Interlinked Domains*. McFarland: Jefferson.
Ceyhan, A. (2008) Technologization of Security. Management of Uncertainty and Risk in the Age of Biometrics. In: *Surveillance and Society* 5(2): 102-123.
Chan, J.; Bennett Moses, L. (2015) Is Big Data challenging criminology? In: *Theoretical Criminology* 20(1): 21-39.
Dierkes, M.; Hoffmann, U.; Marz, L. (1992): *Leitbild und Technik – Zur Entstehung und Steuerung technischer Innovationen*. Berlin: Edition Stigma.
Felt, U.; Wynne, B. (2007) *Taking European knowledge society seriously*. European Union, Expert Group Report. Brussels: European Commission.
Fenn, J. (1995) *The Microsoft system software hype cycle strikes again*. Stamford: Gartner Group.
Fischer, M.; Pelzer, R. (2016) *Die Logik des Anschlags. Zur Zielwahl dschihadistischer Terroristen in Europa*. Frankfurt: Campus.
Fiott, D.; Lindstrom, G. (2018) *Artificial intelligence. What implications for EU security and defence?* Paris: EUISS. (Brief, 10/11/2018)
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (2018) *Maschinelles Lernen. Eine Analyse zu Kompetenzen, Forschung und Anwendungen*. München.
Furedi, F. (2009) Precautionary Culture and the Rise of Possibilistic Risk Assessment. In: *Erasmus Law Review* 2 (2). 197-220.
Grusin, R. (2004) Premediation. In: *Criticism 46*(1): 17-39.
Hacking, I. (2010) *The taming of chance*. Cambridge: Cambridge University Press.
Introna, L.; Wood, D. (2004) Picturing algorithmic surveillance: the politics of facial recognition systems. In: *Surveillance and Society* 2(2-3): 177-198.
Jasanoff, S.; Kim, S.-H. (2015) (eds.) *Dreamscapes of modernity. Sociotechnical imaginaries and the fabrication of power*. Chicago u.a.: The University of Chicago Press.
Kaufmann, S. (2011) Zivile Sicherheit. Vom Aufstieg eines Topos. In: Hempel, L.; Krasmann, S.; Bröckling, U. (eds.) *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*. Wiesbaden: Springer VS (Leviathan Sonderheft, 25).
Kitchin, R. (2014) Big Data, new epistemologies and paradigm shifts. In: *Big Data & Society* 1(1): 205395171452848.
Konrad, K.; Alvial-Palavicino, C. (2017) Evolving Patterns of Governance of, and by, Expectations: The Graphene Hype Wave. In: Bowman, D.; Stokes, E.; Rip, A.

(eds.) *Embedding New Technologies into Society: A Regulatory, Ethical & Societal Perspective*. Singapore: Pan Stanford Publishers.

Krasmann, S. (2011) Der Präventionsstaat im Einvernehmen. Wie Sichtbarkeitsregime stillschweigend Akzeptanz produzieren. In: Hempel, L.; Krasmann, S.; Bröckling, U. (eds.) *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*. Wiesbaden: Springer VS (Leviathan Sonderheft, 25).

Lazer, D.; Radford, J. (2017) Data ex Machina. Introduction to Big Data. In: *Annual Review of Sociology* 43(1): 19–39.

Leese, M. (2014) The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-discriminatory Safeguards in the European Union. In: *Security Dialogue* 45(5): 494-511.

Lyon, David (2014) Surveillance, Snowden, and Big Data. Capacities, consequences, critique. In: *Big Data & Society* 1(2): 205395171454186.

Mattelart, Armand (2010) *The Globalization of Surveillance: the Origin of the Securitarian Order*. Cambridge: Polity Press.

Minsky. M. (1990) *Metropolis*, Stuttgart: Klett-Cotta.

Moravec, H. (1990) *Mind Children. Der Wettlauf zwischen menschlicher und künstlicher Intelligenz*. Hamburg: Hoffmann und Campe.

National Commission on Terrorist Attacks upon the United States (2004) *The 9/11 Commission Report*. http://govinfo.library.unt.edu/911/report/911Report.pdf (06/04/2020)

Opitz, S.; Tellmann, U. (2011) Katastrophische Szenarien: Gegenwärtige Zukunft in Recht und Ökonomie. In: Hempel, L.; Krasmann, S.; Bröckling, U. (eds.) *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*. Wiesbaden: Springer VS (Leviathan Sonderheft, 25).

Rat der Europäischen Union (2009) *Europäische Sicherheitsstrategie. Ein sicheres Europa in einer besseren Welt*. https://www.consilium.europa.eu/media/30806/qc7809568dec.pdf (06/04/2020)

Reichertz, J. (1994) Polizeiliche Expertensysteme: Illusion oder Verheißung? In: Hitzler, R.; Honer, A.; Maeder, C. (eds.) *Expertenwissen. Die institutionalisierte Kompetenz zur Konstruktion von Wirklichkeit*. Opladen: Westdeutscher Verlag.

Reichertz, J. (2003) *Die Abduktion in der qualitativen Sozialforschung*. Opladen: Leske & Budrich.

Rumsfeld, Donald (2002) *Department of Defense News Briefing*. https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636 (60/04/2020)

Salter, M. (2008) Securitization and desecuritization. A dramaturgical analysis of the Canadian Air Transport Security Authority. In: *Journal of International Relations and Development* 11(4): 321-349.

Schulz-Schaeffer, I. (2013) Scenarios as Patterns of Orientation in Technology Development and Technology Assessment. Outline of a Research Program. In: *Science, Technology & Innovation Studies* 9(1): 23-44.

Uncertain Commons (2013) *Speculate this!* Durham, London: Duke University Press.

Weber, J.; Kämpf, K. (2020) Technosecurity Cultures: Introduction. In: *Science as Culture* 29(1): 1-10.

Weizenbaum, J. (1977) *Die Macht der Computer und die Ohnmacht der Vernunft*. Frankfurt am Main: Suhrkamp.

Zweig, K.; Wenzelburger, G.; Krafft, T. (2018) On Chances and Risks of Security Related Algorithmic Decision Making Systems. In: Hälterlein, J.; Ostermeier, L. (eds.) *Predictive Security Technologies. Special Issue of European Journal for Security Research* 3(2): 181-203.