

Zeitschrift für Diskursforschung  
2. Beiheft 2018

**Zeitschrift für  
Diskursforschung**  
Journal for  
Discourse Studies

**Diskursive Konstruktion und  
schöpferische Zerstörung**

2. Beiheft

Saša Bosančić | Stefan Böschen |  
Cornelius Schubert (Hrsg.)

**BELTZ JUVENTA**

# Inhalt

<i>Saša Bosančić, Stefan Böschen, Cornelius Schubert</i> Editorial: Innovationsdiskurse und Diskursinnovationen	3
<i>Robert Jungmann und Cristina Besio</i> Semantiken des sozialen Wandels Zur diskursiven Gestaltung von Innovation	11
<i>Stefan Böschen, Andreas Lösch, Linda Nierling</i> Degrowth: diskursive Normalisierung als innovatorische Radikalisierung?	43
<i>Clemens Blümel</i> Legitimes Sprechen über Innovation? Die Nutzung von Innovationsverständnissen im wissenschafts- politischen Feld	71
<i>Joscha Wullweber</i> Nanotechnologie als Allgemeinwohl Zur politisch-ökonomischen Konstruktion von Innovation	103
<i>Simon Egbert, Bettina Paul</i> Moderne Verfahren der Lügendetektion als sicherheits- politische Innovationen Technikgenese zwischen diskursiven Versprechungen und materialen Rückwirkungen	129
<i>Inka Bormann, Tobias Schröder, Jasmin Luthardt</i> Zur diskursiven Herstellung von Innovation Überlegungen zur Kombination von Kognitions- und Diskursforschung	160

<i>Lilli Braunsch, Jannis Hergesell, Clelia Minnetian</i>	
Stumme Ökonomisierung	
Machteffekte in Innovationsdiskursen	183
Die Autorinnen und Autoren	216

Simon Egbert, Bettina Paul

## Moderne Verfahren der Lügendetektion als sicherheitspolitische Innovationen

Technikgenese zwischen diskursiven  
Versprechungen und materialen Rückwirkungen

**Zusammenfassung:** Geneseprozesse von Sicherheitstechnologien sind von Grund auf diskursiv gerahmt, da das als innovatorische Triebkraft wirkende Sicherheitsrisiko selbst diskursiv konstituiert ist. Dieses reziproke Verhältnis zwischen Sicherheitstechnologien und der Diskursivität von Sicherheitsprogrammen bildet die Hintergrundfolie des Beitrags. Konkretisiert am Beispiel der modernen Lügendetektionsverfahren, wie sie seit den Anschlägen vom 11. September 2001 in Sicherheitsprogrammen eingebunden werden, analysiert der Beitrag die Zirkularität zwischen diskursiven Sicherheitsinnovationen und materialen Technologien. Dabei verweist er auf die analytische Relevanz der Techniksoziologie und der Innovationstheorie für die Diskursforschung.

**Schlagwörter:** Soziotechnische Interaktion, Lügendetektion, Sicherheitspolitik, Dispositivanalyse, Technikgenese

**Summary:** Innovation processes of security technologies are fundamentally discursively framed as their main driving forces are anticipated security risks which are discursively constituted themselves. This reciprocal relation between security technologies and the discursivity of security programmes constitutes the background of the article. Drawing on the example of contemporary deception detection procedures and especially those technologies that were put forth as a reaction to 9/11, we analyse the circularity between discursively constituted security programmes and material technologies. It is our aim to show the analytical value of science and technology studies for discourse theory.

**Keywords:** Sociotechnical interaction, lie detection, security politics, dispositif analysis, social construction of technology

## 1. Die Soziotechnizität der Sicherheitsgesellschaft – eine Einleitung

In Zeiten zunehmender Vorfeldorientierung der Sicherheitspolitik steigt der Bedarf an Prognoseinstrumenten und damit die Nachfrage nach technologisch-wissenschaftlichen Apparaturen, die eine rational untermauerte „Defuturisierung“, also bereits in der Gegenwart die Bereitstellung von Zukunftswissen versprechen (Luhmann 1990, S. 130; vgl. a. Esposito 2007, S. 60, 84). Bei dem Versuch, den allgegenwärtigen Wunsch nach (nationaler) Sicherheit einzulösen, setzen beispielsweise die US-Behörden darauf, aufwendige Forschungen für die Entwicklung neuer Verfahren der Lügendetektion, mit dem Ziel der Prognostik von abweichendem Verhalten, zu finanzieren. Diesem Prozess ist eine komplexe soziotechnische Interaktionsdynamik inhärent, in deren Kontext die Genese und Anwendung moderner lügendetektorischer Verfahren zu lesen ist. Ihr Konstruktions- und Erforschungsprozess ist dabei von Grund auf diskursiv gerahmt, da die als Innovationskraft wirkende Identifikation einer (nationalen) Sicherheitsgefahr ihrerseits diskursiv konstituiert ist, diese sich im Rahmen des Geneseprozesses in die Technologien einschreibt und in deren Anwendung reproduziert und aktualisiert wird. Demgegenüber schränken die materialen Eigenschaften der jeweiligen Sicherheitstechnologien ihre Fähigkeiten ein, symbolisch und/oder faktisch einen Zugewinn an Sicherheit zu generieren. Was legitimerweise als sinnvolle Sicherheitstechnologie positioniert werden kann, hängt somit eng von der materialen Komposition der jeweiligen Technologie ab.

Dieses reziproke Verhältnis von Diskursivität und Materialität weist auf eine zentrale Facette des soziotechnischen Zusammenspiels hin, das für die Sicherheitsgesellschaft der Gegenwart kennzeichnend ist (Zedner 2009, S. 72 ff.; Singelstein/Stolle 2012, S. 32 ff.). Zugleich bildet es mit Bezug auf die modernen Verfahren der Lügendetektion ein treffendes empirisches Beispiel für die analytische Notwendigkeit einer wechselseitigen Integration von techniksoziologischer Innovationsforschung und Diskurs- bzw. Dispositivanalyse. Denn: im Verlauf der Genese lügendetektorischer Verfahren verknüpfen sich Sicherheitsdiskurs und technische Möglichkeiten zur (antizipierten) Vorhersage menschlichen Verhaltens, womit die Trennung zwischen sozialer Sphäre auf der einen und technischer Sphäre auf der anderen Seite nicht nur obsolet, sondern analytisch kontraproduktiv wird. Dabei geht es um ein vorweggenommenes, in diesem Sinne fiktives, jedenfalls kein tatsächlich gegenwärtig vorliegendes Verhalten, sondern um ein erwartetes

gewalttätiges Verhalten in der Zukunft, für das suggeriert wird, man könne es bereits in der Gegenwart über psychophysiologische Signale detektieren.

Im Folgenden möchten wir am Beispiel von modernen Verfahren der Lügendetektion veranschaulichen, dass ihr Entwicklungs- und Produktionsprozess vom Sicherheitsdiskurs und dem dort zirkulierenden Wissen bedingt ist und umgekehrt deren innovatorischer Prozess wiederum auf diesen Diskurs zurückwirkt. Im Zuge unserer Argumentation gehen wir zunächst auf unser technikoziologisches Innovationsverständnis und dessen Einbettung in die Diskurs- bzw. Dispositivtheorie ein. Einer Skizze der technischen Grundlagen von Praktiken der Lügendetektion sowie zweier, entsprechend fundierter Sicherheitsmaßnahmen folgt die Analyse der soziotechnischen Diskurspraktiken in Bezug auf eine der avanciertesten innovatorischen Hoffnungen der amerikanischen Sicherheitsbehörden im Anti-Terror-Kampf, dem „Future Attribute Screening System“ (FAST). Dazu stellen wir zum einen die Wirkung des Diskurses auf die Technologie, zum anderen die Effekte der Technologie auf den Diskurs vor. Den Abschluss bildet schließlich eine Zuspitzung unserer Argumentation auf die Notwendigkeit einer ‚Technikoziologisierung‘ der Diskursanalytik.

## 2. Praktiken der Lügendetektion aus Perspektive von Science & Technology Studies und Diskursanalyse

Ausgangspunkt unserer Überlegungen ist die Überzeugung, dass technische Artefakte und Systeme stets und unumgänglich soziotechnische Produkte sind. Dies impliziert, dass ihr Entstehungsprozess nicht teleologisch, sondern als (nicht-lineare) Genese zu begreifen ist, die von diskursiven Rahmenbedingungen und sozialen Dynamiken, mithin durch Disruptionen und Diffusionen gekennzeichnet ist. Damit folgen wir der Kernidee der Science and Technology Studies, die von einer grundsätzlichen soziotechnischen Konstitution bzw. Hybridität gesellschaftlicher Interaktionskontexte und technischer Artefakte ausgehen (vgl. Bijker/Pinch 2012 mit weiteren Verweisen). Dies ist mit der methodologischen Annahme verbunden, dass die sozialwissenschaftliche Analyse gleichermaßen die an gesellschaftlichen Praktiken beteiligten menschlichen und nicht-menschlichen Aktanten<sup>1</sup>

---

1 Der Aktantenbegriff stammt aus der Semiologie nach Greimas und zielt auf all jene Figuren, die in einer Geschichte bzw. Szene als handlungsmächtige Entitäten auftreten und verweist in seiner technikoziologischen Wendung Latourscher Prägung gerade darauf, dass Menschen und Nicht-Menschen gleichermaßen wesentlich an Hand-

(Latour 1998, S. 35 ff.) zu berücksichtigen hat. Auf Innovations- bzw. technische Geneseprozesse bezogen – die wir hier im engeren, techniksoziologischen Sinne und gemäß der klassischen Arbeiten von Bijker (1995, 2012; Pinch/Bijker 1984) verstehen – zeigt sich die soziotechnische Hybridität im Aushandlungsprozess zwischen all jenen sozialen AkteurInnen- bzw. Aktantengruppen, die einen Einfluss auf die Gestaltung, Funktionen und Einsatzzwecke der Technologie haben bzw. die als Zielgruppen für den Einsatz der Technologie anvisiert werden (vgl. a. Rammert 2008, S. 311 f.).<sup>2</sup> Dies schließt u. a. ein, die Einsatzinteressen und NutzerInnenerwartungen zu berücksichtigen, ebenso wie zu reflektieren, welche eminente Rolle ästhetische Referenzen und Kosten-Nutzen-Kalkulationen im innovatorischen Prozess von technischen Systemen spielen (vgl. a. Rammert 2010). All dies wirkt schließlich ein auf die Ausformung der Technologie, schreibt sich ein in jenes Produkt, das am (vorläufigen) Ende des Innovationsprozesses steht, womit dieses spezifische »Skipts« aufweist (Akrich 1992, S. 208) bzw. materialisierte Sinnvorschläge repräsentiert (vgl. Lindemann 2014, S. 187).<sup>3</sup> Technologien, so unsere weitere These, gehen in diesem eingeschriebenen diskursiven Wissen allerdings nicht in Gänze auf, sie verfügen vielmehr in ihrer materialen Charakteristik über spezifische Qualitäten, die sie mit einer konstitutiven Eigenlogik ausstatten, die wesentlich auf den jeweiligen diskursiven Kontext zurückwirkt.<sup>4</sup> Diese Eigenlogik impliziert eine spezifische Wirkmacht von technischen Artefakten, die umfasst, dass diese einen Unterschied machen, indem sie als produktive Vermittler auftreten, da sie andere beteiligte Entitäten zu beeinflussen im Stande sind (Latour 2010,

---

lungsvollzügen beteiligt sein können (vgl. Latour 1998, S. 35; 2002, 372; 2012, 285). Siehe dazu auch Fußnote 8.

- 2 Dabei sind die klassischen Arbeiten aus dem Kontext des Social Construction of Technology-Ansatzes (SCOT) u. E. trefflich kompatibel mit den gegenwärtigen Bestrebungen, gesellschaftliche Innovationsprozesse fernab von ökonomischen und technischen Fokussierungen zu untersuchen und sozialtheoretisch zu fundieren (s. Rammert 2010; Hutter et al. 2016; Rammert et al. 2016).
- 3 Siehe dazu auch Rammert (2008, S. 292): „Techniken werden absichtsvoll entworfen und kunstfertig hergestellt, um angestrebte Leistungen wirkungsvoll, dauerhaft und verlässlich erwartbar zu erzielen.“
- 4 Anzumerken ist dabei, dass die Chronologisierung von Innovationsdiskurs als zeitlich vorgängige Voraussetzung der Technologie eine analytische Trennung und Reihenfolge beinhaltet, die heuristische Gründe hat und sich in der Praxis ungleich verwobener darstellt. Der an vorliegender Stelle genutzte Begriff der Zirkularität soll genau dies naheliegen. Wir sprechen indes von *Rückwirkungen*, da der Diskurs im vorliegenden Fall – dessen Wissenstopoi in die Technologie eingeschrieben werden – dem Artefakt vorausgeht.

S. 92) und mithin Diskurse präformieren und die dort vollzogenen Praktiken prägen.

Das dargelegte Innovationsverständnis wird an dieser Stelle in einen diskurstheoretischen Rahmen eingebettet, der die aktuelle Debatte um die Stellung von Materialität im Diskurs berührt.<sup>5</sup> Wir folgen Silke van Dyks (2013) Vorschlag, die Materialität des Diskursiven mit dem Begriff des *Dispositivs* in die diskurstheoretische Analyse zu integrieren. Als solches ist demnach das „Netz zu begreifen, das die heterogenen Elemente dieser Welt miteinander verknüpft“ (S. 47; ähnlich: Jäger 2006, S. 89 ff.). Van Dyk folgt damit dem breit rezipierten Zitat von Foucault, in dem er den Begriff des *Dispositivs* wie folgt bestimmt:

„Was ich unter diesem Titel festzumachen versuche ist erstens ein entschieden heterogenes Ensemble, das Diskurse, Institutionen, architektonische Einrichtungen, reglementierende Entscheidungen, Gesetze, administrative Maßnahmen, wissenschaftliche Aussagen, philosophische, moralische oder philanthropische Lehrsätze, kurz: Gesagtes ebenso wie Ungesagtes umfaßt [sic]. Soweit die Elemente des *Dispositivs*. Das *Dispositiv* selbst ist das Netz, das zwischen diesen Elementen geknüpft werden kann.“ (Foucault 1978, S. 119 f.)

Van Dyk liest diese Aussage konsequent verknüpfungsorientiert und artefaktsensibel, indem sie vor allem auf die Aufzählung der heterogenen Elemente im Zitat abstellt (van Dyk 2013, S. 51 f.; vgl. a. Denninger et al. 2014, S. 31 ff.). Eine solche artefakt- bzw. verknüpfungssensible Lesart des Foucaultschen *Dispositiv*verständnisses konvergiert mit den Interpretationsvorschlägen von Waldenfels (1991, S. 283), Wrana/Langer (2007, Abs. 6), Lemke (2014, S. 255 ff.) und anderen, denen zufolge Foucaults Denken durchaus nicht auf rein sprachliche Forschungsgegenstände reduzierbar sei. Hochgradig anschlussfähig ist diese *Dispositiv*konzeptualisierung für die vorliegende Analyse auf zweierlei Weise: Zum einen kann schon begrifflich und damit von vornherein die genuine Soziotechnizität der (diskursiven) Welt analytisch in Rechnung gestellt werden. Dies zieht ein methodologisches Umdenken in Richtung einer symmetrischen Analyseperspektive von Menschen und Nicht-Menschen nach sich. Zum anderen wird die spezifische, heterogene Verbindung der multimodalen Diskurselemente hervorgehoben. Denn: wichtig ist vor allem der Blick auf das soziotechnische En-

---

5 Für eine konzise Zusammenfassung der in der Debatte hervorgebrachten Argumente, einschließlich der wichtigsten Literaturverweise, siehe van Dyk et al. (2014, S. 347 ff.).



semble der Lügendetektion und dessen Konstitutionsbedingungen, also die wechselseitigen Verweisungen von Mensch und Material (vgl. dazu auch Manderscheid 2014, S. 8).

Verbunden mit dem oben skizzierten Dispositivkonzept ist ein weites Diskursverständnis, welches den Begriff des Diskurses nicht allein für empirisch zu identifizierende Einzeldiskurse reserviert. In diesem Sinne ist das Diskursive nicht als Untereinheit einer allumfassenden „symbolischen Sinnwelt“ und damit als „Grundebene“ zu begreifen, wie es z. B. Reiner Keller vorschlägt (Keller et al. 2015, S. 302 ff.), sondern als *Diskursuniversalismus* im Sinne Laclau/Mouffes (2012\1991, S. 141 ff.). Das Diskursive – konstituiert durch sich überlappende und bisweilen parallel auftretende Diskurse – ist demnach omnipräsent und sinnhafte Wahrnehmung daher nur auf Basis diskursiv gebrochener Perspektivität und entsprechend präformierten Wissens möglich (vgl. a. Wrana/Langer 2007, Abs. 13).<sup>6</sup> Demgemäß kann zwar durchaus von der Existenz einer vom Menschen unabhängigen Welt ausgegangen werden, diese ist aber stets nur diskursiv gefiltert erkennbar („Diskursimmanenz“, van Dyk 2013, S. 49; Denninger et al. 2014, S. 28 ff.; van Dyk et al. 2014, S. 351 f.). Dies impliziert aber wiederum nicht, dass hier nicht von einer potenziellen materialen Eigenmächtigkeit ausgegangen wird. Im Gegenteil: Vielmehr wird gerade betont, dass materiale Artefakte eigenständige Handlungsrelevanz besitzen können, die explizit auch in ihren materialen Qualitäten begründet liegen. In diesem Sinne hat die Materialität eines technischen Instruments direkte Auswirkungen auf dessen Gebrauch und auf die menschliche Perzeption seiner Kompetenzen und Funktionen.

In dem die Multidimensionalität des Diskursiven anerkannt und analytisch in Rechnung gestellt wird, impliziert ein solches Diskursverständnis nicht nur die analytische Integration von Materialität bzw. material verfasster Artefakte, sondern ebenso das Verwerfen einer Differenzierung zwischen diskursiven und nicht-diskursiven Praktiken: Alles, was der Mensch denkt und tut, ist diskursiv vermittelt bzw. wirkt konstituierend auf Diskurse zurück und ist demnach als diskursive Praktik aufzufassen (Laclau/Mouffe 2012\1991, S. 143). Dabei ist eine terminologische Differenzierung zwischen unterschiedlichen Arten diskursiver Praktiken zwar durchaus sinnvoll – um unterschiedliche Spielarten und Wirkmachtgrade diskursiver

---

6 Diese These steht wohlgerne nicht im Widerspruch zur begrifflichen Konzeptualisierung von Reiner Keller (Keller et al. 2015, S. 303). Die Debatte über die Fassung des Diskursbegriffs ist vielmehr heuristisch-terminologischer denn erkenntnistheoretischer Natur (zur Kritik von Keller an Laclau/Mouffe siehe Keller 2011, S. 164).

Konstruktionen zu analysieren – eine Gruppe davon indes als „nicht-diskursiv“ zu beschreiben, wäre – zumindest vor dem hier vertretenen Diskursuniversalismus – schlichtweg kontradiktorisch.<sup>7</sup>

Diskursivität schließt also nicht nur sprachliche Entitäten ein, sondern gleichermaßen Handlungen, Tätigkeiten und materiale Objekte (vgl. Denninger et al. 2014, S. 25 ff.). Als Dispositive sind in diesem Rahmen sodann jene Diskurzusammenhänge oder – je nach Forschungsfokus – diskursive Interaktionskontexte zu verstehen, in deren Rahmen technische Artefakte eine vermittelnde Rolle spielen, mithin als Mediatoren auftreten, indem sie bestimmte Tätigkeiten oder Aussagen ermöglichen, provozieren, unterdrücken oder hemmen (vgl. a. Bührmann/Schneider 2008, S. 103; Keller 2011, S. 42; van Dyk 2013, S. 54). Als eine der vordringlichsten Aufgaben einer entsprechend ausgerichteten Dispositivanalyse kann also die Rekonstruktion ebenjener soziotechnischen Zirkularität gelten, die aus dem Wechselverhältnis von technischer Materialität und gesellschaftlicher Diskursivität besteht. Technische Artefakte bzw. Systeme werden dabei als *Diskursaktanten*<sup>8</sup> verstanden, die ebenso wie menschliche AkteurInnen an diskursiven Praktiken beteiligt sind und direkte („harte“) wie indirekte („weiche“) Effekte zeitigen können: Als direkte (Rück-)Wirkungen sind jene Eingriffe von Artefakten in Diskurse und diskursive Praktiken zu verstehen, die unmittelbar über sie selbst transportiert werden und keiner menschlichen Zwischenschaltung bedürfen, so wie z. B. die materiale und effektvolle Wider-

---

7 So wird auch schon vorgeschlagen, jene Praktiken, die bislang als nicht-diskursive Praktiken bezeichnet wurden, als „*nicht-diskursrelevante Praktiken*“ zu benennen (Keller et al. 2015, S. 310; Hervorh. i. O.). Siehe zur Debatte zusammenfassend Keller et al. (2015, S. 295 ff.) und Wrana (2012, S. 126 ff.).

8 Der Ausdruck Diskursaktant bietet sich hier an, da er zwar eine methodologische Symmetrie von Menschen und Nicht-Menschen postuliert, dies aber gerade nicht auf Basis einer Trivialisierung des soziologischen Kernbegriffs der „AkteurIn“ tut, der ja traditionell mit dem intentionalen menschlichen Subjekt verbunden ist und Ausgangspunkt zahlreicher kritischer Latour-Rezeptionen war. Teile der Kritik basieren aber auf einem Missverständnis, da Latour mitnichten konstatiert, dass Menschen und Nicht-Menschen vollständig bzw. in Bezug auf ihre Intentionalität gleichartig seien (Latour 2010, S. 131; vgl. a. Kneer 2010, S. 319 f.). Es geht also beim Aktantenbegriff lediglich darum, sowohl Menschen wie Nicht-Menschen im Sinne ihrer Wirkungsmacht in soziotechnischen Interaktionskontexten in gleicher Weise Rechnung zu tragen. Damit folgen wir dem semiotischen oder auch erzähltheoretischen Herkunftskontext des Begriffs „Aktant“, in dessen Rahmen auf diese Weise Partizipanten einer Narration bezeichnet werden, wobei es unerheblich ist, ob diese menschlich oder nicht-menschlich sind (vgl. Latour 1998, S. 35, 2010, S. 95, 123; s. z. B. Greimas/Courtés 1982, S. 5 f.).

ständigkeit, die eine betonierte Boden- bzw. Bremsschwelle charakterisiert.<sup>9</sup> Als indirekte (Rück-)Wirkung ist demgegenüber ein über Menschen bzw. deren Wahrnehmung mediatisierter Diskurseffekt der Technologie zu verstehen, so z. B. die gemeinhin angenommene Objektivierungskompetenz technischer Artefakte, die letztere zu besonderen diskursiven Referenzen macht, da ihnen bestimmte Qualifikationen und Problemlösungsfähigkeiten zugeschrieben werden.

Für das vorliegende empirische Beispiel ergibt sich aus diesen theoretischen Grundannahmen, dass die modernen Verfahren der Lügendetektion im Rahmen eines Geneseprozesses entwickelt und erprobt werden, der von Grund auf soziotechnisch konstituiert und damit in Gänze diskursiv durchdrungen ist. Daraus folgt, dass eine dispositivanalytische Untersuchung gegenwärtiger lügendetektorischer Innovationsprozesse gleichermaßen die einschlägigen diskursiven Wissensbestände und Nutzungserwartungen sowie die materialen Eigenschaften der genutzten Apparaturen und deren Effekte auf ihre(n) jeweiligen Kontextdiskurs(e) zu untersuchen hat. Was wir im Folgenden also versuchen herauszustellen ist die Reziprozität von (US-Sicherheits-) Diskurs und Materialität im Verlauf dieser Genese und Verwendung der Technologie. So wirkt in der (vor allem) gegenwärtigen US-amerikanischen Lügendetektionsanwendung die diskursive Praxis der dortigen Sicherheitsbehörden, die technologisch mediatisierte Sicherheitsmaßnahmen als legitime und effektive Mittel in ihrem „Krieg gegen den Terror“ rationalisieren und damit die Technologie durch den von ihnen maßgeblich mitgestalteten Sicherheitsdiskurs rahmen. Umgekehrt beflügelt letzterer aber auch, insbesondere durch die Proklamation der Notwendigkeit und Nützlichkeit von technologischen Neuerungen zur Bekämpfung von (terroristischer) Sicherheitsgefahren, die spezifische Ausprägung der technischen Entwicklung der Lügendetektion, indem z. B. auf Basis des behördlichen terroristischen Risikonarrativs Gelder für die Finanzierung von avancierten Sicherheitstechnologien bereitgestellt werden.

---

9 Natürlich benötigen die Bodenschwellen menschliche Zwischenschaltung, um konzipiert und installiert zu werden. Sind sie allerdings einmal aufgestellt, haben sie völlig selbstständig einen (situativen) Effekt: unabhängig von der menschlichen Wahrnehmung werden sie das jeweilige Auto beschädigen, falls mit zu hoher Geschwindigkeit gefahren wird. Latour benutzt dieses Beispiel, um auf die Moralität von Materialität hinzuweisen (z. B. Latour 1998, S. 42 f.).

### 3. Grundlagen und moderne Praktiken der Lügendetektion

Die Aussagen einer Person auf ihren Wahrheitsgehalt überprüfen zu können, ist ein ebenso historisches wie gegenwärtiges gesellschaftliches Verlangen. Wissenschaftlich-technologische Verfahren, die diesem Wunsch nachzukommen streben, werden unter dem Begriff Lügendetektion (bzw. „deception detection“) subsumiert.<sup>10</sup> Sie folgen allesamt der psychophysiologischen Hypothese, dass kognitive Vorgänge körperliche Reaktion zeitigen (vor allem eine höhere Aktivität des Nervensystems) und ein ursächlicher Zusammenhang zwischen beiden Ebenen hergestellt werden kann (z. B. Gamer/Vossel 2009, S. 207). Instrumente der Lügendetektion messen dabei nicht täuschendes (Aussage-)Verhalten an sich, sondern zunächst unspezifische körperliche Reaktionen (wie z. B. den Puls, die Hautleitfähigkeit und Atemtätigkeit). Selbige werden im Rahmen einer bestimmten Fragestrategie als Indikatoren für Betrug und Täuschung definiert – z. B. in Form des Kontroll- bzw. Vergleichsfragentest, wie sie auch bei der „Future Attribute Screening Technology“ (s. u.) genutzt wird. Im Rahmen eines solchen Tests mit der Verhörtaktik gemäß des Kontrollfragentests wird mit einem Fragekorpus gearbeitet, der direkt nach der im Fokus stehenden Handlung fragt. Die physiologischen Reaktionen der untersuchten Person auf diese Tatfragen werden mit ihren körperlichen Resonanzen auf Kontroll- bzw. Vergleichsfragen in Beziehung gesetzt (Putzke et al. 2009, S. 613). Diese beziehen sich dabei auf sozial missbilligtes Verhalten und werden so allgemein gestellt, dass es unwahrscheinlich ist, sie wahrheitsgemäß verneinen zu können. Auch (in Bezug auf die inkriminierte Tat) unschuldige Personen sollen somit eine emotionale Belastung verspüren, die sodann als Vergleichswert fungiert. Der methodische Ansatz dieser Teststrategie folgt nun der Idee, dass unschuldige Personen auf die Kontrollfragen heftiger reagieren als auf die Tatfragen, schuldbeladene Personen dagegen bei den Tatfra-

---

10 Das wohl bekannteste einschlägige Gerät ist der in den 1920er Jahren entwickelte Polygraf. Bereits von Beginn an wurde die Validität dieses und vergleichbarer Verfahren kritisiert (vgl. Grubin/Madsen 2005). Trotz der Kritik wurde indes nicht auf die Nutzung polygrafischer Untersuchungen verzichtet. Sie werden beispielsweise in Japan im Rahmen polizeilicher Ermittlungen, in den USA u. a. in Einstellungsverfahren der Sicherheitsbehörden und in Isreal von dortigen Sicherheitsinstitutionen eingesetzt (Seiterle 2010, S. 69 ff.). Für Deutschland wird derzeit ihre „Renaissance“, vor allem bezogen auf Familienrechtsstreitigkeiten, konstatiert (Putzke 2013, S. 14). Siehe allgemein zur Lügendetektion auch Paul/Egbert (2014).

gen ein höheres Niveau somatischer Aktivität zeigen (Gamer/Vossel 2009, S. 208 f.).

Es waren insbesondere die Anschläge vom 11. September 2001, die eine nachhaltige Innovationsdynamik im Bereich der lügendetektorischen Verfahren initiiert haben (Littlefield 2009; Baesler 2015). So sind in den USA bereits mehrere Verfahren im Einsatz bzw. in Erprobung, denen allesamt gemein ist, dass sie an neuralgischen Punkten (insbesondere an Flughäfen) als anlassunabhängige Screeningtools eingesetzt werden (sollen). Sie arbeiten nach der Maxime, dass äußerlich ablesbare körperliche Parameter einen Aufschluss über betrügerisches Verhalten oder böse Absichten eines ansonsten unverdächtigen Menschen geben und einen robusten Anfangsverdacht für weitergehende Überprüfungen bereitstellen können. Intendiert sind die Verfahren demnach als „primary screening procedures“, die einen handfesten Verdacht generieren und Personen für detaillierte Folgeüberprüfungen selektieren sollen (DHS 2008b, S. 25).

Eines der ersten Programme dieser Art ist das seit 2006 bestehende „*Screening of Passengers by Observation Techniques*“-Programm (SPOT) der US-Transportation Security Administration (TSA) von der US-Heimatschutzbehörde (Department of Homeland Security, DHS). Grundidee ist, dass eigens geschulte „Behavior Detection Officers“ (BDO) im Terminalbereich Passagiere herausfiltern, deren Körpersprache oder Verhalten Anzeichen von Stress, Angst oder Täuschung erkennen lassen (TSA o. J.; DHS 2008c; Maccario 2013, S. 151). Die BDO arbeiten stets paarweise und sollen verdächtiges Verhalten bei Passagieren beobachten oder im Rahmen kurzer Gespräche ein solches provozieren (DHS 2013, S. 3). Erklärtes Ziel dieses im Jahr 2003 initiierten Programms ist es, Personen aufzugreifen, die ein Sicherheitsrisiko darstellen könnten (DHS 2008a). Unterstützt wird die TSA im Training ihrer Beamten dabei von dem Psychologen Paul Ekman, dem Urheber des „Facial Action Coding Systems“ (FACS), welches von Mikroexpressionen im Gesicht ausgeht, die unbewusst gezeigt würden, mithin unkontrollierbar seien und in einem direkten Zusammenhang mit Emotionen stünden (Ekman/Rosenberg 2005; Adey 2009). Das Programm gilt unter SicherheitsvertreterInnen als äußerst erfolgreich (Maccario 2013, S. 151 f.), da von 232.000 selektierten Personen für „secondary screenings“ immerhin 1710 verhaftet wurden, die sich allerdings fast ausschließlich auf ausstehende Haftbefehle, Schmuggel und andere, terrorismusunabhängige Delikte bezogen (Weinberger 2010, S. 414), weshalb die Kritik an diesem

Programm ebenso grundsätzlich wie nachhaltig ist (s. z. B. McCulloch/Wilson 2016, S. 86; Maguire 2016, S. 165).<sup>11</sup>

Als gezielte Weiterentwicklung des SPOT-Programms ist die „*Future Attribute Screening Technology*“ (FAST) zu verstehen, welche seit 2007 vom „Science and Technology Directorate“ des DHS entwickelt wird (DHS 2015). FAST basiert ebenfalls auf dem FACS-System, hat aber nicht – wie bei SPOT – zum Ziel, über ein Gespräch mit der anvisierten Person oder per menschlichem Beobachten Indikatoren für verdächtiges Verhalten aufzudecken. Anknüpfend an das Projekt „Hostile Intent“ des DHS (2008d) ist vielmehr das Ziel, Personen mit „malintent“<sup>12</sup> maschinell gestützt herauszufiltern (DHS 2008a, S. 2), weshalb die FAST immer wieder als Minority-Report-Technologie rezipiert wird (für viele: Schneider/Merkle 2007; Weinberger 2011) – ungeachtet der vielfachen Unterschiede zwischen dem literarischen bzw. filmischen Vorbild und den hier praktizierten Prognostik-Versuchen. Entwickelt wurde ein „Screening Mobile Module“ (FAST M<sup>2</sup>), eine Art überdimensionaler Container, der nicht nur an Flughäfen, sondern auch an anderen Orten von Großevents zum Einsatz kommen kann (DHS o. J.a). Erhoben werden sollen u. a. die Atmung, der Kreislauf, die Augen- sowie Körperbewegungen (Burns 2007, S. 7). Ein anschauliches Beispiel für jene Gedanken, die konkret anvisiert werden, wenn von „malintent“ die Rede ist, zeigt eine Illustration des DHS, in der eine junge Frau durch die Sicherheitsschleuse geht und der per Gedankenblase folgende kognitiven Inhalte zugeschrieben werden: „After I get through I cause a disturbance“, „After I’ll get through I’ll detonate a bomb“, „After I get through I’ll deliver a package“.<sup>13</sup> Ergänzt werden die in der Illustration präsentierten Fragen durch die gezeigten Überprüfungen in einem Promotion-Video des DHS (DHS o. J.a). Dort wird den kontrollierten Personen beispielsweise die Frage gestellt: „Are you attempting to smuggle an explosive device into the

---

11 Zu betonen ist dabei, dass das SPOT-Programm und seine Nachfolger keineswegs die einzigen technologisch-innovativen Sicherheitsbestrebungen des DHS und seines Science and Technology Directorate markieren. Beispielhaft zu ergänzen ist das „*Automated Virtual Agent for Truth Assessments in Real-Time*“ (AVATAR)-Programm, in deren Rahmen die rein maschinelle Interviewführung – statt z. B. der BDO – anvisiert wird (DHS o. J.c). Weitere Verfahren werden bei Paul/Egbert (2014) vorgestellt.

12 Konkret definiert als „(t)he mental state of individuals intending to cause harm to our citizens or our infrastructure“(DHS 2014).

13 Die DHS-Illustration war ursprünglich auf der Seite [www.sharkride.com/blog/2008/09/25/dhs-hostile-thoughts-detector/](http://www.sharkride.com/blog/2008/09/25/dhs-hostile-thoughts-detector/) zu sehen, die indes mittlerweile nicht mehr aufrufbar ist. Das Bild findet sich aber noch bei Wikipedia: [www.wikipedia.org/wiki/File:Dhs-fast.png](http://www.wikipedia.org/wiki/File:Dhs-fast.png) (Abruf 15.06.2016).

expo today?“ Oder auch: „Do you plan to detonate an explosive at the expo today?“

In den folgenden beiden Kapiteln wenden wir uns nun der soziotechnischen Innovationsdynamik zu, die insbesondere das FAST-Programm rahmt und die diskursiven Effekte auf die Technologie impliziert, ebenso wie die technologischen Rückwirkungen auf den Sicherheitsdiskurs.

#### 4. Sicherheitspolitische Präformation: die terroristische Bedrohung als Innovations-Triebkraft

*„Das Verlangen nach greifbarer Wahrheit, konkreten Resultaten [...] ist das Vermächtnis des Lügendetektors.“*  
(Baesler 2013, S. 97)

Wie bereits angedeutet, ist die FAST als genuine Weiterentwicklung des SPOT-Programms zu verstehen. Die Motivation, die bereits mit SPOT anvisierten Ziele – eine möglichst frühzeitige Identifizierung von ansonsten unverdächtigen Personen per psychophysiologischer Überwachung zu ermöglichen – zu rationalisieren, insbesondere Geschwindigkeit und Validität des Detektionsverfahrens zu optimieren, bezieht sich auf spezifische Anforderungen und Hoffnungen, die sich direkt aus dem Diskurs um die nationale Sicherheit der USA speisen. Die „Future Attribute Screening Technology“ ist in diesem Sinne eine materiale Manifestation von diskursiv geformten Rationalitäten<sup>14</sup> der US-Sicherheitsbehörden.

Das erklärte Ziel, das hinter den hier zitierten Innovationen der DHS steht, ist die Stärkung der nationalen Sicherheit der USA (s. z. B. DHS 2008a, S. 2). Gegründet wurde die Behörde als direkte Reaktion auf die Anschläge vom 11. September 2001 in der Intention, sicherheitspolitische Kompetenzen zu bündeln und zu sublimieren (s. US-Congress 2002). Das „Science and Technology Directorate“ des DHS und insbesondere deren „Homeland Security Advanced Research Projects Agency“ (HSARPA) hat

---

14 Rationalitäten werden hierbei verstanden als Denk- und Bearbeitungsweisen der Realität (vgl. Krasmann 2003, S. 71 ff.). Wir greifen hier auf das Konzept der Rationalitäten aus den Gouvernementalitätsstudien zurück, da dieses nicht nur die diskursiven Wissensbestände und grundsätzliche AkteurInnen-Perspektiven, sondern gleichermaßen deren praktische Umsetzung beinhaltet. Zum Verhältnis von Diskursforschung und Gouvernementalitätsstudien siehe die Beiträge in Angermüller/van Dyk (2010).

dabei die spezifische Aufgabe „[to] [focus] on identifying, developing, and transitioning technologies and capabilities to counter chemical, biological, explosive, and cyberterrorism threats, as well as protect our nation’s borders and infrastructure“ (DHS Science and Technology Directorate 2015). Laut „Homeland Security Act“ (US-Congress 2002, S. 2169) kommt der HSARPA konkret die Verantwortung zuteil,

„to (A) support basic and applied homeland security research to promote *revolutionary* changes in technologies that would promote homeland security; (B) advance the development, testing and evaluation, and deployment of critical homeland security technologies; and (C) accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities.“ (Hervorh. d. Verfasser)<sup>15</sup>

Die zuständigen Abteilungen des DHS haben demnach nicht weniger als die Entwicklung von „revolutionären“ Technologien zur Bekämpfung von nationalen Bedrohungen zum Ziel (s. a. DHS 2007b, S. 21). An anderer Stelle wird vom ehemals zuständigen Staatssekretär ähnlich auch von „game-changing technologies“ (Cohen 2007, S. 10) gesprochen, die es benötige, um zukünftige Anschläge zu verhindern, die – so die Antizipation – mit Sicherheit verübt würden. Denn, so abermals Cohen: „there will be another attack. Our terrorist enemies want to make it even more devastating than that of 9/11. And the question is not if, it is when“ (DHS 2008b). In diesem Sinne ist es eine der Grundaufgaben des DHS, als Innovationsinkubator von Sicherheitstechnologien zu fungieren.

Das FAST-Programm, welches von der HRSDPA federführend durchgeführt wird, sieht sich ebendiesen erklärten Sicherheitsinteressen verpflichtet, hat es doch zum Ziel – so steht es in der damaligen Ausschreibung für IndustriepartnerInnen –

„to host screening experiments as well as tests and evaluations to characterize the utility of behavioral, physical, and sensor based components of human screening to enhance the performance of security staff that is responsible for discerning intent to cause damage or harm.“(DHS 2007a, S. 2).

---

15 In einer Präsentation des damaligen Staatssekretärs für Wissenschaft und Technologie des DHS, Jay M. Cohen, ist diese Hervorhebung ebenfalls zu finden (s. Cohen 2007, S. 8).



Die Technologie korrespondiert damit unmittelbar mit einem „neuen Paradigma“ der Sicherheitstechnik – dem „behavioral profiling paradigm“: als zusätzliche Sicherheitsmaßnahme soll sie ermöglichen, die bisherigen „Unknowns“ aus der anonymen Menschenmasse herauszufiltern (Florence/Friedman 2010, S. 423; Hervorh. d. Verfasser): „FAST technologies focus on real-time physiological cues and behavior patterns in an attempt to prevent the unknown terrorist from gaining access to their target location.“ (Erickson o. J., S. 4) Diese präemptive<sup>16</sup> Interventionsstrategie implementierte sich im Sinne eines flächendeckenden Programms als Reaktion auf die Anschläge vom 11. September (s. Bush 2002), aus denen vor allem zweierlei sicherheitsarchitektonische Lehren für Flughäfen gezogen wurden: Erstens seien nicht gefährliche Gegenstände oder explosive Stoffe selbst das größte sicherheitsbezogene Problem, sondern es sind die Personen, die gefährlich seien. Zweitens reiche es nicht aus, lediglich die aus Datenbanken und Beobachtungslisten bereits bekannten ‚gefährlichen‘ Personen zu prüfen, vielmehr müssten *alle* Menschen, die an solch kritischen Orten verkehrten, als *potenzielle* AttentäterInnen angesehen, mithin ob ihrer (Un-)Gefährlichkeit kontrolliert werden. Beide Lehren integrierend merkt der ehemalige Direktor der TSA, Kip Hawley, an:

„[I]t is no longer sufficient to focus on finding weapons and common explosives; we must enhance our ability to recognize suspicious behavioral patterns and demeanors to identify people who may have devised a new means to attack our transportation systems or passengers“ (zitiert nach Armstrong et al. 2008, S. 26; vgl. auch Maccario 2013, S. 154).

---

16 Der Begriff der Präemption entstammt dem Militärvokabular und zielt auf die sich veränderte Rationalität des präventiven Eingriffs: War es bislang die Gefahrenvorbeugung, die als präventive Handlungsmaxime in der Sicherheitspolitik dominierte, ist es nun der Gefahrenvorgriff, der vorherrscht: ein Prinzip, das gänzlich von konkreten Verdachtsmomenten abstrahiert, sich auf diffuse Bedrohungslagen stützt und auf diese Weise Ereignisse zu verhüten gewillt ist, die hinsichtlich ihres Eintrittszeitpunkts und ihrer Erscheinungsformen nahezu durchweg unbekannt sind. Präemption repräsentiert damit eine eigenständige präventive Denklöge, die potenziell jedes Verhalten als möglicherweise bedrohlich ansieht, Verdächtigungen pro-aktiv zu generieren sucht, damit eine grundlegende Abkehr von der Unschuldsumutung beinhaltet und eine Umkehr der Beweislast impliziert, in deren Rahmen sich jede Person zunächst als unschuldig beweisen muss (Anderson 2010, S. 789 f.; Krasmann 2011, S. 54; Opitz 2012, S. 287 ff.).

Dieser, von Hawley konturierten Maxime kommt indes bereits das SPOT-Programm nach, indem es die BDO paarweise durch die Flughäfen nach auffälligen Personen Ausschau halten lässt. Allerdings gilt das Programm, insbesondere auf Grund des hohen Personalaufwands, als teuer und ressourcenraubend.<sup>17</sup> Deshalb und auch wegen der prinzipiellen Fehleranfälligkeit menschlicher Detektionskompetenzen wurde begonnen, an Systemen zu forschen, die ein automatisiertes Screening von unverdächtig erscheinenden ‚Risikosubjekten‘ erlauben (Burns 2007, S. 4). Und an ebendieser Stelle kommt das FAST-Projekt ins Spiel. Denn die Rationalitäten der US-Sicherheitsbehörden umfassen freilich nicht nur den schlichten Impetus, Sicherheit herzustellen, sondern ebenso die Frage, auf welchem, möglichst kostengünstigen, (datenschutz-)rechtlich akzeptablen und überhaupt praktikablen Wege dies möglich ist. Der treibende Impuls hinter den Innovationsbemühungen rund um das FAST-Verfahren ist demgemäß ein doppelter: einerseits soll das SPOT-Verfahren per maschineller Unterstützung an Validität gewinnen, also die Wahrscheinlichkeit erhöhen, gefährliche Personen korrekt als solche zu identifizieren; andererseits ist es das Ziel, den Detektionsprozess zu optimieren („to streamline“, DHS 2010, S. 2), um die Auswirkungen auf den Flughafenverkehr so gering wie möglich zu halten. Beide Punkte, die wichtige diskursive Bezugspunkte darstellen, sollen nun näher beleuchtet werden.

Zum einen ist das FAST-Projekt also mit der Intention verbunden, die detektorische *Validität* des SPOT-Programms zu verbessern und damit einen höheren Sicherheitsgewinn zu erzielen (Cohen 2007, S. 28). Einer der dafür wesentlichsten Schritte wird in der verstärkten Mechanisierung des psycho-physiologischen Screeningverfahrens gesehen, also in dem Austausch menschlicher mit technologischen Detektoren, der sich doppelt auf die Validität der Ergebnisse auswirken soll: einerseits durch eine erhöhte Reliabilität, andererseits durch eine gesteigerte Objektivität. Am SPOT-Verfahren wird die geringe Standardisierung des Detektionsprozesses bemängelt, der durch den menschlichen Faktor – die BDO – hervorgerufen werde (Burns 2007, S. 4). Menschen könnten schlichtweg nicht stets gleichermaßen aufmerksam beobachten und selektieren, seien ohnehin insgesamt sehr fehleranfällig in ihrer Beurteilungsverlässlichkeit (DHS o. J.b). Indem im Rahmen des FAST-Projekts die Detektionssensoren maschinell operierten, könnten demnach deutlich reliablere Ergebnisse erzielt werden (vgl. a. Kölbel/Selter 2010, S. 241). Die Objektivität wiederum könne im FAST-Pro-

---

17 Das Programm kostet jährlich rund 200 Mio. US-Dollar (Perry/Gilbey 2011).

gramm erhöht werden, indem zunächst deutlich mehr psychophysiologische Indikatoren erhoben werden könnten, insbesondere solche, die für die menschlichen Sinne unzugänglich sind (z. B. die Hautleitfähigkeit). Gleichmaßen könne die Technologie auf Basis ihres Malintent-Algorithmus einen ebenso wertfreien wie sachlichen Verdacht aussprechen (z. B. Cohen 2007, S. 28; Burns 2007, S. 4). Und nur unter Rückgriff auf die maschinelle Erhebung von psychophysiologischen Signalen kann schließlich die qualitative Verlagerung der Zielinformation gelingen: Das ultimative Ziel ist nicht mehr allein das Aufdecken verdächtiger Personen auf Basis ihres situativen Verhaltens, sondern auch auf Grund ihres Denkens, wozu nicht nur äußerlich, am Verhalten der Personen ablesbare Indikatoren herangezogen werden, sondern zusätzlich auch körperliche Parameter, die für menschliche BeobachterInnen unsichtbar sind (wie bspw. thermische Veränderungen der Gesichtshaut) und als Ausdruck von böswilligen Zukunftsgedanken interpretiert werden. Es wird nicht der Inhalt des Gedachten selbst auf verdächtigen Gehalt untersucht, sondern die somatischen Parameter einer Person kontrolliert, um auf bestimmte kognitive Inhalte rückzuschließen, womit die „Versicherheitlichung des Unbewussten“ (Weber 2005; Übers. d. Verfasser) konsequent und maschinell unterstützt vorangetrieben wird.

Zum anderen ist das FAST-Programm mit dem expliziten Ziel verbunden, den durch die erhöhte Validität erzielten Sicherheitszugewinn *auf möglichst rationale Weise* zu generieren. Dabei spielt neben den finanziellen Rahmenbedingungen insbesondere der Faktor Zeit eine wesentliche Rolle, da der ohnehin träge Flughafenbetrieb nicht noch weiter verlangsamt werden soll: „The ultimate goal is to allow people to move more freely and quickly through the screening process“ (DHS 2014). Um dies zu erreichen, wird angestrebt, das Screening automatisiert, aus der Distanz und per berührungsfreier Sensoren im Rahmen eines Durchgangsverfahrens („walk-through-proceeding“) ablaufen zu lassen und Ergebnisse in Echtzeit zu liefern (DHS 2008a). Damit soll der Personendurchlauf maximiert und die Auswirkungen auf die kontrollierten Personen minimiert werden (DHS 2008b, S. 23; Burns 2007, S. 4). Neben dem Faktor Zeit („rapid risk assessment“, Cohen o. J., S. 19) spielt dabei auch die Komponente Privatsphäre respektive Datenschutz und kulturelle Neutralität eine Rolle: „The FAST system is gender, culture and age-neutral and it does not use profiling techniques or collect personally identifiable information.“ (DHS 2014; s. a. Cohen o. J., S. 19) Es ist das Ziel, to „produce a tool that protects the public in the least intrusive manner possible“ (ebd.) und „to minimize the inconvenience of security hurdles“, indem z. B. Schuhe nicht mehr ausgezogen werden müssen und in Zukunft womöglich auf das Abtasten verzichtet

werden kann (DHS o. J.b). Und nicht zuletzt kommt es den Verantwortlichen bei der Entwicklung des FAST M<sup>2</sup> auf Mobilität und Flexibilität an, da intendiert ist, die Technologie nicht nur stationär an Flughäfen, sondern flexibel und temporär bei allen kritischen Großevents, aber auch in Einkaufszentren einsetzen zu können (DHS o. J.a, 2007a, S. 2).

Diese produktiv-diskursive Rolle der Sicherheitsbehörden erschöpft sich aber nicht nur in den jeweils in Auftrag gegebenen und demgemäß entwickelten Technologien, sondern ist durchaus weitreichender. Denn auch das *wissenschaftliche Fundament* des FAST-Verfahrens, die psychologische Malintent-Theorie, basiert grundlegend auf intellektuellen Bestrebungen der Sicherheitsbehörden (Buswell/Hallowell 2010, S. 15). In einer Projektvorstellung heißt es demgemäß: „The baseline for the project is the development and validation of the Theory of Malintent“ (DHS 2008a, S. 2). So spricht auch der bereits erwähnte ehemalige Staatssekretär für Wissenschaft und Technologie, Jay M. Cohen, diesbezüglich von „new science“ und er konstatiert: „We’ve gone to the National Academies of Science to help us define those sciences.“ (DHS 2008b, S. 19) Genuiner Bestandteil des FAST-Projektes ist folglich, ergänzend zur Entwicklung eines apparativen Prototyps und der dafür notwendigen Technologie, die Validierung von behavioralen Indikatoren für böse Absichten und die Entwicklung eines entsprechenden Algorithmus, der automatisch Personen mit „malintent“ identifiziert (Smith et al. 2008, S. 10). An anderer Stelle wird nun bereits von einem „growing body of the psycholegal study of true and false intentions“ (Granhag/Giolla 2014, S. 195) gesprochen und sogleich ergänzt: „it is only in recent years that focus has turned to statements concerning future, rather than past, events.“ (ebd.) Es ist anzunehmen, dass diese Perspektivverschiebung im Bereich der psychologischen Wissenschaft der „deception detection“ wesentlich auf die wissenschaftlichen Bestrebungen der US-Sicherheitsbehörden zurückgehen.

Auch wenn an der Umsetzung der neuen Lügendetektionsverfahren außerhalb experimenteller Kontexte noch Zweifel gehegt werden (z. B. Alder 2007, S. 252), zeigt das FAST-Beispiel, wie sich Sicherheitsbegehren an den neuen Lügendetektionsverfahren festmachen bzw. diese überhaupt erst hervorbringen und vorbilden, indem die finanziellen und gedanklichen – z. B. seitens der HerstellerInnen von notwendigen Hardware-Lösungen, im Sinne von Denkanstößen – Voraussetzungen für einen Innovationsprozess geschaffen werden. Indem durch einen ebenso expliziten wie detaillierten Ausschreibungstext spezifische Standards und materielle Kompositionen einer Technologie vorgegeben und mit den versprochenen finanziellen Ressourcen entsprechende Prototypen entwickelt werden, sind es gerade die

US-Sicherheitsbehörden, die im Rahmen der von ihnen als Reaktion auf die Anschläge vom 11. September verabschiedeten Programme zur Stärkung der nationalen Sicherheit die Weiterentwicklung der Lügentesttechnologie fördern und damit nicht nur das Einsatzfeld, sondern auch die späteren Konturen der Anwendung – auch auf Basis von bereits existierenden technologischen Gegebenheiten bzw. Paradigmen (vgl. z. B. Dosi 1982) – im Voraus präformieren (vgl. Littlefield 2011, S. 123; Alder 2007, S. 266). Mit Bezug auf Akrich (1992, S. 208) sind damit jene Inskriptionen angesprochen, die im Rahmen des Entwicklungs- und Herstellungsprozesses in technischen Artefakte eingeschrieben werden und sich auf eine spezifische Vision von der zukünftigen Rolle des Artefakts in der Welt seitens der InnovatorInnen beziehen. Durch die spezifischen behördlichen Anforderungen an die FAST inkorporiert diese neue Technologie spezifische Wissensbestände, Interessen und Sichtweisen, die sodann im Nutzungsprozess reproduziert und aktualisiert werden.

## **5. Materiale Intervention: (Rück-)Wirkungen der FAST auf den Sicherheitsdiskurs**

*„From Science and Technology... Security and Trust.“*  
(Motto des Science & Technology Directorate des DHS).

Technologien – hier: das FAST-System – sind stets das innovatorische Ergebnis von spezifischen Repertoires diskursiver Wissensbestände. Diese bleiben bei einer solch passiven Adressierungsrolle aber nicht stehen. Die materiale Eigenart einer Technologie ist mit einer Transformation der jeweils inskribierten Wissensbestände verbunden und mit einer Neu-Konstellation von Attribuierungen: der Technologie werden auf Grund ihrer Materialität spezifische Eigenschaften zugeschrieben, mit ihr werden neue Wissensbestände verknüpft und mitunter die von den InnovatorInnen intendierte unterdrückt. Gleichzeitig ist den Artefakten eine handfeste Widerständigkeit zu eigen, die nur bestimmte Verwendungsarten zulässt. Technologien treten in diesem Sinne als zusätzliche Diskursaktanten auf, als diskursive Referenzen und Partizipanten diskursiver Praktiken, die mit wirkmächtigen Diskurs-Effekten – direkter wie indirekter Art – verbunden sind. Im Folgenden wird es dabei vor allem um die indirekten, also über die

menschliche Wahrnehmung mediatisierte Auswirkungen gehen, da die Datenlage nur wenige Aussagen über die direkten Wirkungen erlaubt.<sup>18</sup>

Im Rahmen des FAST-Programms wird vornehmlich auf die Materialität und die mit ihr verbundenen bzw. die ihr zugeschriebenen Charakteristika (z. B. Reliabilität, Objektivität, Effizienz) der Technologien gesetzt. Das spärlich involvierte Personal dient eher als Wegweiser durch das Screening-Verfahren, zum Ablesen der Fragen<sup>19</sup> und zur Bedienung der Computer, welche die Daten schließlich zusammenführen und auswerten. Wie bereits betont, soll der menschliche Faktor in der FAST möglichst eliminiert und auf diese Weise die Validität der Detektionsergebnisse signifikant erhöht werden. Diese pauschale Priorisierung technologischer Verfahren gegenüber menschlichen AkteurInnen hinsichtlich ihrer Detektionsqualität lässt sich mit dem Konzept der *mechanischen Objektivität* (Daston/Galison 2007, S. 121 ff.) theoretisch rahmen. Gemäß diesem Attribuierungsmuster ist der adäquate Weg zur objektiven Erkenntnis, die Natur für sich selber sprechen zu lassen. Und diese ‚natürliche Abbildung‘ kann nur dann korrekt und unverzerrt hergestellt werden, wenn die menschliche Subjektivität möglichst in Gänze aus dem Erkennungsprozess getilgt werden kann (ebd., S. 126 f.). Einem »Maschinenideal« folgend, produzieren mechanisch-technologische Verfahren in dieser Perspektive nicht-interventionistische Repräsentationen der Natur und vollziehen diesen Dienst in unkorrupter Weise, indem die Maschine als „neutraler und transparenter Operateur“, als „interventionsloses Aufzeichnungsinstrument“ agiert (Galison 2003, S. 390). Pointiert aktualisiert das DHS diese Sichtweise in Bezug auf ihre AVATAR-Technologie: „Unlike humans who can become fatigued or distracted, the AVATAR conducts each interview with high vigilance and without bias.“ (DHS o. J.c). Diese Attribuierungen werden – durchaus ein wenig impliziter – auch dem Konglomerat an Scan-Verfahren der FAST zugeschrieben (s. a. DHS o. J.b; DHS 2008d, S. 2; Cohen 2007, S. 28):

„Security checkpoint officers currently use visual inspection techniques and devices (e.g., X-ray machines) to detect weapons or other items that can be used to cause harm. To identify individuals with malintent, how-

---

18 Wir beziehen uns hier allein auf Dokumente, die ja stets nur Deutungen über die Technologie und ihrer Materialität transportieren können. Um die direkten (Rück-)Wirkungen der FAST ausführlicher behandeln zu können, benötigt es z. B. das Hinzuziehen ethnografischer Fallstudien der FAST-Experimentierpraxis.

19 Dies wird im AVATAR-System des DHS bereits vom Computer übernommen (DHS o. J.c). Siehe dazu auch Fußnote 11.

ever, officers must rely on more *simplistic* techniques, including verifying credentials, randomly selecting individuals for questioning and observing individuals for visual cues. Often, screeners have insufficient time to evaluate individuals thoroughly, have limited access to supporting information or are not specially trained in detecting malintent indicators.“ (DHS 2008a; Hervorh. d. Verfasser)

Die FAST demgegenüber „inconspicuously and objectively selects individuals for secondary security screenings.“ (ebd.) Und DHS-Mitarbeiter Burns gibt wiederum sehr explizit als Ziel von FAST aus, (menschliche) Subjektivität aus dem Screeningprozess zu entfernen („remove subjectivity from the process“, 2007, S. 2). Diese Zuschreibungen von Objektivität und der allgemein verbesserten Performanz von FAST lassen sich mit ihrem auf sicherheitspolitisch-diskursiver Ebene besonders nachhaltigen Effekt im Sinne einer indirekten oder weichen materialen Rückwirkung konzeptualisieren. Der von FAST verkörperte technologische Fortschritt entkräftet somit (tendenziell) politische Gegenstimmen, die z. B. betonen, dass die sicherheitsarchitektonische Aufrüstung zu Lasten derer geht, die verdachtsunabhängig Grundrechtseingriffe hinnehmen müssen. Technologische Verfahren können auf diese Weise als Garant für die Legitimierung von Sicherheitsinterventionen dienen – und dies allein schon aufgrund ihrer materialen Verfasstheit und der damit verbundenen Zuschreibungen.

Als Subphänomen der mechanischen Objektivität kann jene empirisch zu beobachtende Haltung gelten, die als *datalogical objectivity* apostrophierbar ist: Die Erhebung und Analyse von Daten könne per se eine fehlerfreie und unverzerrte Beurteilung von Personen garantieren (vgl. McCulloch/Wilson 2016, S. 88). So äußert bereits der damalige US-Minister für Innere Sicherheit, Michael Chertoff, anlässlich eines Vortrags über die Notwendigkeit zur Übermittlung von Flugpassagierdaten an die USA zwecks Identifizierung von „unknown terrorists“:

„We use this data to focus on behaviour, not race and ethnicity. In fact, what it allows us to do is move beyond crude profiling based on prejudice, and look at conduct and communication and actual behaviour as a way of determining who we need to take a closer look at.“ (zitiert in Amoores 2009, S. 2)

In einem anderen Kontext, aber umso pointierter bringt Gary Wolf, Mitbegründer der Quantified Self-Bewegung, diese Attitüde gegenüber (digitalen) Daten auf den Punkt:

„Humans make errors. We make errors of fact and errors of judgment. We have blind spots in our field of vision and gaps in our stream of attention. Sometimes we can't even answer the simplest questions. [...] These weaknesses put us at a disadvantage. We make decisions with partial information. We are forced to steer by guesswork. We go with our gut. That is, some of us do. Others use data.“ (Wolf 2010)

Dabei ist nicht nur die naiv anmutende Objektivitätsanspruch gegenüber den Daten kritisch zu reflektieren – die ja keineswegs unabhängig von Raum und Zeit entstehen („raw data“ is an oxymoron“, Gitelman 2013) –, es gilt gleichermaßen zu berücksichtigen, dass solche Daten stets hochselektiv sind und sie die anvisierte Person in ein immer nur rudimentäres „data double“ verwandeln (Haggerty/Ericson 2000, S. 613), was nur noch aus den für die ProgrammiererInnen (bzw. deren AuftraggeberInnen) als wichtig erachteten Informationen besteht und keine ganzheitliche personelle Repräsentation beabsichtigt – und gerade dadurch die Interaktion besonders nachhaltig prägt.

Die vermeintliche Objektivität der technologischen Verfahren negiert dabei die auf gesellschaftlichen Wissensbeständen basierende Ausrichtung der Technologie. Dies gilt für die physische Präsenz und Verfahrensweise der technologischen Apparaturen ebenso wie für die Software. Die *Algorithmen*, welche die von den Sensoren erhobenen Daten verwerten, erhöhen den Anschein der Neutralität und Objektivität, da sie gänzlich selbstständig Ergebnisse produzieren. So schreibt das DHS:

„FAST offers security personnel an additional tool. The sensor technologies enable individuals' psychological and behavioral cues to be inputs to a malintent algorithm. The algorithm produces an *objective* recommendation for secondary screening and serves as a support tool.“ (DHS o. J.b; Hervorh. d. Verfasser)

Die pauschale Objektivitätszuschreibung gegenüber der automatisierten algorithmischen Arbeitsweise, die als finaler Wunsch auch den FAST-BefürworterInnen vorschwebt, blendet aus, dass die Konfiguration des Algorithmus von vornherein gesellschaftlich aufgeladen ist: Welche Personen als gefährlich angesehen und welche Indikatoren dafür wiederum als adäquat definiert werden, sind Fragen, die politisch verhandelt und nicht von der Technologie entschieden werden (Introna 2016, S. 20 ff.). Louise Amoore (2013, S. 163 f.) zeigt, dass bei automatisierten Entscheidungen daher auch nicht mehr von Sicherheits-Entscheidungen zu sprechen ist, sondern nur



noch von Wissensanwendung. Die Annahme, algorithmische Sicherheitsentscheidungen wären frei von politischen Wertungen, setzt sie entgegen: „automated decisions is equipped to make judgments but never to decide“ (ebd., S. 164). Aufgrund der Automatisierung gilt für die konkrete Kontrollinteraktion und damit der direkten situativen Wirkung der Aktanten, dass – anders als mit menschlichen SicherheitsakteurInnen – mit den beteiligten Apparaturen keine Verhandlung möglich ist und die Interaktion radikal auf die Detektionssituation reduziert wird; entweder ist ein Mensch qua algorithmischen Ergebnis autorisiert für den Zugang oder eben nicht – Diskussion ist dabei zwecklos (Lianos/Douglas 2000, S. 264 f.; Rammert 2008, S. 292).

Dabei wird gerade auch über den *visuellen Darstellungsmodus* der Daten – ob durch Kurvenbilder der Vermessungen oder durch die bildliche Darstellung der Gesichtsthermik – eine unvermittelte Quelle und die Unvoreingenommenheit der Messung nahelegt. Die Visualisierung suggeriert die Nicht-Intervention, die vermeintlich natürliche Repräsentation und agiert im Anschein des Fotorealismus. Die spezifische Darstellung der Daten des vermessenen Gesichtes, die in einem Bild zusammengefügt werden und verdächtige körperliche Parameter ebenso pointiert wie stilisiert auf den visuellen Punkt bringen, sollen Indikatoren für zukünftige Gefahren darstellen (Paul/Egbert 2014, S. 159 f.). Die Visualisierungen versprechen „unantastbare Zeugen“ zu sein, unterstellen eine Einfachheit, Widerspruchsfreiheit, Vollständigkeit und Zweifelsfreiheit, deren Akzeptanz bereits durch den bloßen Augenschein evoziert wird (Schwarte 2015, S. 168, 200). Bildlich mediatisiertes Wissen kann sich nicht selbst relativieren, geschweige denn negieren, womit es sich für den Existenzbeweis prädestiniert (Mersch 2006, S. 413).<sup>20</sup> Diese visuelle Evidenz operiert vor allem über das Fehlen einer absoluten Referenz, die zu repräsentieren das Verfahren für sich beansprucht (vgl. a. Fitsch 2014, S. 51 ff.) – im vorliegenden Fall somit der Lüge bzw. Gefährlichkeit. Nicht zuletzt agiert diese „preemptive visualization“ (Amoore 2013, S. 97) über das Versprechen, für Menschen unsichtbare Zeichen der antizipierten und noch unbekanntes Bedrohung technisch sichtbar zu machen, was von eminenter diskursiver Wirkmächtigkeit ist. Damit stellt die Visualisierung der Diskursivität (der antizipierten Gefahr übersetzt in körperliche Signale) eine Materialisierung *par excellence* dar: Der Computerbildschirm auf dem die Gefahr visuell abzulesen

---

20 Vgl. a. Egbert/Paul (2013) mit weiteren Verweisen. Dort wird am Beispiel von Drogentests die evidenzgenerierende Kraft visuellen Wissens ausführlicher analysiert.

ist, ist haptisch greifbar, das (technische) Bild der zukünftigen Gefahr ausdruck-, reproduzier- und mobilisierbar.<sup>21</sup>

Die Transformierung der erhobenen Daten in visuelle Resultate, die eine Theorie über die maschinelle Auslesbarkeit des lügenden Körpers und die Akzeptanz der psychophysiologischen Kernthese voraussetzt, bleibt dabei indessen unsichtbar. Der Prozess der Visualisierung ist, wie die gesamten technischen Vorgänge der Detektionsverfahren, Gegenstand von Intransparenz. Dabei geht der Materialisierungsprozess der FAST, die Überführung von Theorien, Annahmen und Wissensfragmenten in die materiale Komposition der Technologie, mit dem Prozess des „*black boxing*“ einher (Latour 2002, S. 373): Das Zusammenwirken der verschiedenen Komponenten des FAST-Prototypen und im Besonderen des eigentlichen Screening-Verfahrens innerhalb der FAST entzieht sich jeglichen Blickes; solange das System reibungslos läuft, sind höchstens Input (Was speise ich ein?) und Output (Welches Ergebnis wird ausgeworfen?) von Interesse und die eigentliche technische und wissenschaftliche Arbeit, die die tatsächliche Funktions- und Arbeitsweise der Technologie bedingt, bleibt opak. Diese unsichtbare Funktionsweise verstärkt aufs Neue das (Validitäts-)Vertrauen in die Technologie, da die eingeschriebenen gesellschaftlichen Relativitäten (Wissensbestände, Theorien, Praktikabilitätsanforderungen etc.) undurchdringbar bleiben und auf diese Weise im Sinne eines legitimatorischen Vorschusses auf den Sicherheitsdiskurs zurückwirken.

Das „*black boxing*“ bewirkt jedoch auch etwas Anderes. Es forciert die *visionäre Aura* der Technologie. Die FAST trägt diesen Zukunftsbezug nicht nur plakativ im Namen, das Programm stilisiert und pflegt auch die utopische Facette der Technologie. Dabei vereinen sich zwei nur scheinbar konträre Elemente: Zum einen wird bei nahezu jeder Vorstellung der Screening-Technologie zugleich erwähnt, welche weiteren Funktionen angestrebt werden und welche technologischen Visionen zukünftig realisiert werden sollen (z. B. Burns 2007, S. 11; Smith et al. 2008, S. 14). Zum anderen wird durch den Bau von Prototypen und ihrem experimentellen Einsatz, der Vorführung z. B. in Promotion-Videos, ein operatives Funktionieren suggeriert, dass die Vorstellung nährt, eine visionäre Technologie sei bereits im „Hier und Jetzt“ realisiert und einsetzbar.<sup>22</sup> Obschon die Technologien im

---

21 Zur Interferenz von Visualität und Materialität und damit einem expliziten Plädoyer für einen Praxisbezug in Abgrenzung zur rein auf der Repräsentationslogik setzenden Bedeutung von Visualität, siehe Rose/Tolia-Kelley (2012, S. 1 ff.).

22 Ähnlich dazu siehe Kirbys Konzept der diegetischen Technologien, wobei es bei ihm um kinematografische Prototypen geht, die im Anschluss ihrer filmischen Darstellung

Video selbst kaum sichtbar sind, wird ihre „Neuartigkeit“ (Lösch 2009, S. 260), zumindest verbal, integriert, in Form der Betonung des Innovationscharakters der Technologie. So beschreibt Burns die Kombination der verschiedenen Detektions-Verfahren als „revolutionary integration of screening moduls“ (2007, S. 4; s. a. DHS o. J.a). Das visionäre Element wird dabei genährt durch die Weiterentwicklung der Verfahren und vice versa. Die eigentlichen Technologien stützen den Zukunftsbezug – provozieren Wünsche der Machbarkeit und Anwendungskontexte, die dann im Diskurs weitergetragen werden. Dies greift den grundsätzlichen Symbolcharakter auf, der seit jeher mit Technologien der Lügendetektion einhergeht. Zentral ist dabei nicht, ob sie mit hundertprozentiger Zuverlässigkeit Menschen mit suspekten Absichten zu identifizieren vermögen, als vielmehr, dass sie das Versprechen tragen können, für Sicherheit zu sorgen: „it doesn't matter whether lie detection works, so long as it provides the promise of changing society for the better“ (Littlefield 2011, S. 10). Diese Versprechungen werden z. B. in der Kommentierung des Vorführungsvideos geleistet, obschon im Video nichts dergleichen konkret dargestellt wird (DHS o. J.a). Zugleich aber verkörpern die zum Großteil noch imaginativen Technologien eine reale Aktivität der Sicherheitsbehörden und signalisieren, dass das betreffende (Risiko-)Terrain im Fokus der Behörden steht. Moderne Verfahren der Lügendetektion, wie sie mit FAST in ihrem avancierten technologischen Gewand agieren, können somit bereits in ihrem Entwicklungsprozess eine per se symbolisch-politische Qualität perpetuieren, da sie auf Grund ihrer materialen Komposition detektorische Kompetenzen suggerieren (können) und gleichzeitig durch ihre Komplexität die Überprüfung des Herstellungsprozesse der detektorischen Ergebnisse intransparent machen, immer aber signalisieren: es wird aktiv gegen den Terror und für die Sicherheit der Bevölkerung gearbeitet.

Zusammenfassend ist zu konstatieren, dass die Transformation der Sicherheitsagenda der US-Behörden in die materiale Gestalt einer avancierten Technologie mit diskursiven Effekten verbunden ist, die nicht nur den Legitimitätsanspruch der damit zusammenhängenden Sicherheitsinterventionen und Grundrechtseingriffen per se zu erhöhen vermag. Den Behörden fällt es überdies leichter, die antizipierten Sicherheitsgewinne überzeugender in der Öffentlichkeit zu vertreten, da zum einen zahlreiche Objektivitätszuschreibungen eine leicht nutzbare, materiale Resonanzfläche bekommen und zum anderen die tatsächliche technologische Funktionsweise

---

eine reale Verwirklichung finden (2011, S. 193 ff.). Zu modernen Verfahren der Lügendetektion als diegetische Technologien siehe Egbert/Paul (2016).

weitestgehend opak bleibt. Gleichmaßen wird deutlich, inwieweit das diskursiv eingeschriebene Wissen durch den Einsatz der Technologien reproduziert und gleichsam gehärtet wird.

## **6. Fazit: Diskursanalytische Gegenwartsanalysen und die notwendige Integration techniksoziologischer und innovationstheoretischer Perspektiven**

Am Beispiel moderner Verfahren der Lügendetektion, allen voran der „Future Attribute Screening Technology“, haben wir empirisch fundiert aufgezeigt, wie die Innovationsprozesse technologisch mediatisierter Sicherheitsmaßnahmen wesentlich von den jeweiligen Sicherheitsbehörden und ihren Rationalitäten diskursiv gerahmt und gleichermaßen präformiert werden. Im Falle von der FAST ist es explizites Ziel des federführenden Department of Homeland Security, mit einer neuen, verbesserten Detektionstechnologie die nationale Sicherheit durch ein valides und praktikables Screeningverfahren zu erhöhen. Diese Ziele werden als dominante Referenzwünsche in den Innovationsprozess der Technologie integriert, schreiben sich demnach in das technologische System ein und werden somit in der praktischen Anwendung derselben reproduziert und aktualisiert. Gleichzeitig aber, so haben wir dargelegt, bildet die Technologie keineswegs allein eine materiale Manifestation und damit passive Adressatin der diskursiven Wissensbestände der InnovatorInnen. Vielmehr ist ihre Herstellung und Nutzung mit einer eigenlogischen Transformation der diskursiven Bedingungen verbunden, die sich auf ihren Status als materiale Technologie zurückführen lässt, indem Gedanken als Signale übersetzt und anhand einer material fundierten Visualität ausgelesen, interpretiert und in eine Risiko-Prognose überführt wurden. Die FAST kann und muss folglich als eigenständiger Aktant in diesem Sicherheitsdiskurs verstanden werden, der auf Grund seiner technologisch-materialen Eigenschaften der verschiedenen Messinstrumente einen relevanten (diskursiven) Unterschied macht. Dabei reicht es schon aus, dass die FAST als nicht-menschliches Gegenüber wahrgenommen wird, um ihr im Sinne der „mechanischen Objektivität“ entsprechende Attribuierungen der Wertneutralität zuzuschreiben, was wiederum zum einen die gesellschaftliche Legitimität dieser und ähnlicher Sicherheitsmaßnahmen erhöht, zum anderen die einschlägigen Entwicklungs-Bestrebungen der Sicherheitsbehörden noch zielstrebig werden lässt.

Das Beispiel der FAST zeigt gleichsam paradigmatisch, wie die gegenwärtige Sicherheitsgesellschaft und die damit zusammenhängenden Diskurse soziotechnische Kontexte herstellen. Insbesondere die für eine solche Sicherheitsgesellschaft typische politische Maxime, Sicherheitsrisiken bereits vor ihrer Entstehung eliminieren zu müssen, um potenziell katastrophalen Folgen präemptiv vorbeugen zu können, bedingt den zunehmenden Rückgriff der Sicherheitsbehörden auf technologische Instrumente und Systeme. Will sich die Diskursanalytik mit solchen und ähnlich gelagerten Fragen und Kontexten beschäftigen, müssen techniksoziologische und innovationstheoretische Kerngedanken – so unsere Schlussfolgerung – verstärkt in ihr konzeptuelles Repertoire integriert werden. Auf diese Weise kann eine konsequent symmetrische Berücksichtigung von Technologien in diskursiven Zusammenhängen erfolgen. Silke van Dyk (2013) folgend, ist es unseres Erachtens fruchtbar, hierbei auf den Begriff des Dispositivs zu rekurrieren, da dieser als übergeordnetes Konzept ermöglicht, gleichermaßen die diskursiv vermittelten Wissensbestände wie die materialen Eigenarten der Technologien gleichrangig und gegenstandssensibel in ein diskurstheoretisch-techniksoziologisches Analyseraster zu integrieren. Demgemäß versteht sich die vorliegende Analyse explizit als exemplarische Dispositivanalyse.

## Quellen

- Armstrong, N. J. et al. (2008): Securing America's Passenger Rails: Analyzing Current Challenges and Future Solutions, [www.insct.syr.edu/wp-content/uploads/2013/02/Securing-Americas-Passenger-Rails.pdf](http://www.insct.syr.edu/wp-content/uploads/2013/02/Securing-Americas-Passenger-Rails.pdf) (Abruf 21.6.2016).
- Burns, B. (2007): Future Attribute Screening Technology Mobile Module (FAST M<sup>2</sup>) Innovation/HSARPA HIP, [www.info.publicintelligence.net/DHS-FAST.pdf](http://www.info.publicintelligence.net/DHS-FAST.pdf) (Abruf 20.6.2016).
- Bush, G. W. (2002): Graduation Speech at West Point, United States Military Academy, New York. 1. Juni 2002, [www.georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020601-3.html](http://www.georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020601-3.html) (Abruf 15.6.2016).
- Buswell, B. I./Hallowell, S. (2010): Joint Prepared Statement of Bradley I. Buswell and Susan Hallowell. In: Hearing before the Subcommittee on Transportation Security and Infrastructure Protection of the Committee on Homeland Security, House of Representatives One Hundred Eleventh Congress. Second Session, March 17, 2010, S. 13–17.
- Cohen, J. M. (2007): DHS Science & Technology: Alignment for Success, [www.dtic.mil/ndia/2007pto/Tuesday/RADMJayCohen.pdf](http://www.dtic.mil/ndia/2007pto/Tuesday/RADMJayCohen.pdf) (Abruf 15.6.2016).
- Cohen, J. M. (o. J.): DHS Science & Technology Directorate Brief, [www.france-science.org/IMG/pdf/sdc\\_french\\_embassy\\_9-12-07.compressed.pdf](http://www.france-science.org/IMG/pdf/sdc_french_embassy_9-12-07.compressed.pdf) (Abruf 21.6.2016).

- DHS (Department of Homeland Security) (2007a): Broad Agency Announcement (BAA) Future Attribute Screening Technology (FAST) Demonstration Laboratory, [www.wired.com/images\\_blogs/threatlevel/files/001\\_BAA07-03A\\_FutureAttributeScreeningTechnologyFASTDemonstrationLaboratory.pdf](http://www.wired.com/images_blogs/threatlevel/files/001_BAA07-03A_FutureAttributeScreeningTechnologyFASTDemonstrationLaboratory.pdf) (Abruf 15.6.2016).
- DHS (Department of Homeland Security) (2007b): Science & Technology Strategy: to make the nation safer... [www.dhs.gov/xlibrary/assets/Science\\_and\\_Technology\\_Strategy.pdf](http://www.dhs.gov/xlibrary/assets/Science_and_Technology_Strategy.pdf) (Abruf 18.6.2016).
- DHS (Department of Homeland Security) (2008a): Privacy Impact Assessment for the Future Attribute Screening Technology (FAST) Project, [www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_st\\_fast.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf) (Abruf 15.6.2016).
- DHS (Department of Homeland Security) (2008b): Implementing Privacy Protections in Government Data Mining, [www.dhs.gov/xlibrary/assets/privacy/privacy\\_datamining\\_July24\\_2008\\_minutes.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_datamining_July24_2008_minutes.pdf) (Abruf 2.6.2016).
- DHS (Department of Homeland Security) (2008c): Privacy Impact Assessment for the Screening of Passengers by Observation (SPOT) Program, [www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_tsa\\_spot.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_spot.pdf) (Abruf 2.6.2016).
- DHS (Department of Homeland Security) (2008d): Experimental Testing of Hostile Intent Technology, [www.dhs.gov/sites/default/files/publications/privacy\\_pia\\_st\\_phi.pdf](http://www.dhs.gov/sites/default/files/publications/privacy_pia_st_phi.pdf) (Abruf 20.6.2016).
- DHS (Department of Homeland Security) (2010): Future Attribute Screening System, [www.epic.org/privacy/fastpresentation.pdf](http://www.epic.org/privacy/fastpresentation.pdf) (Abruf 15.6.2016).
- DHS (Department of Homeland Security) (2013): Transportation Security Administration's Screening of Passengers by Observation Technique, [www.oig.dhs.gov/assets/Mgmt/2013/OIG\\_13-91\\_May13.pdf](http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-91_May13.pdf) (Abruf 1.6.2016).
- DHS (Department of Homeland Security) (2014): Future Attribute Screening Technology, [www.dhs.gov/sites/default/files/publications/Future%20Attribute%20Screening%20Technology-FAST-508\\_0.pdf](http://www.dhs.gov/sites/default/files/publications/Future%20Attribute%20Screening%20Technology-FAST-508_0.pdf) (Abruf 15.6.2016).
- DHS (Department of Homeland Security) (o. J.a): Promotionvideo zum FAST-Programm, [www.youtube.com/watch?v=48FuWeF4m7U](http://www.youtube.com/watch?v=48FuWeF4m7U) (Abruf 15.6.2016).
- DHS (Department of Homeland Security) (o. J.b): Future Attribute Screening (FAST) System, [www.epic.org/privacy/fastinstallation.pdf](http://www.epic.org/privacy/fastinstallation.pdf) (Abruf: 2.6.2016).
- DHS (Department of Homeland Security) (o. J.c): Rapid Screening Tool: The AVATAR, [www.dhs.gov/sites/default/files/publications/Rapid%20Screening%20Tool-The%20AVITAR-NCBSI-AVATAR.pdf](http://www.dhs.gov/sites/default/files/publications/Rapid%20Screening%20Tool-The%20AVITAR-NCBSI-AVATAR.pdf) (Abruf: 18.6.2016).
- DHS Science and Technology Directorate (2015): Homeland Security Advanced Research Project Agency, [www.dhs.gov/sites/default/files/publications/HSARPA%20Fact%20Sheet-508.pdf](http://www.dhs.gov/sites/default/files/publications/HSARPA%20Fact%20Sheet-508.pdf) (Abruf 2.6.2016).
- Erickson, M. D. (o. J.): DHS Science & Technology Directorate Overview, [www.ct.gov/serc/lib/serc/commission\\_info/conferences/2009/dhs\\_science\\_technology.pdf](http://www.ct.gov/serc/lib/serc/commission_info/conferences/2009/dhs_science_technology.pdf) (Abruf 2.6.2016).
- Smith, A. et al. (2008): Human Factors Division: Social-Behavioral Threat Analysis, [www.dtic.mil/ndia/2008homest/behave.pdf](http://www.dtic.mil/ndia/2008homest/behave.pdf) (Abruf 20.6.2016).
- TSA (Transport Security Agency) (o. J.): SPOT Referral Report, [www.assets.documentcloud.org/documents/1697887/spot-referral.pdf](http://www.assets.documentcloud.org/documents/1697887/spot-referral.pdf) (Abruf 2.6.2016).
- US-Congress (2002): Public Law 107-296. An Act To establish the Department of Homeland Security, and for other purposes, [www.dhs.gov/xlibrary/assets/hr\\_5005\\_enr.pdf](http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf) (Abruf 2.6.2016).

## Literatur

- Adey, P. (2009): Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body. In: *Environment and Planning D: Society and Space* 27(2), S. 274–295.
- Akrich, M. (1992): The De-Description of Technical Objects. In: Bijker, W./Law, J. (Hrsg.): *Shaping Technology/Building Society*. Cambridge und London: MIT Press, S. 205–224.
- Alder, K. (2007): *The Lie Detectors. The History of an American Obsession*. New York und London: Free Press.
- Amoore, L. (2009): Lines of sight: on the visualization of unknown futures. In: *Citizenship Studies* 13(1), S. 17–30.
- Amoore, L. (2013): *The Politics of Possibility*. Durham und London: Duke University Press.
- Anderson, B. (2010): Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies. In: *Progress in Human Geography* 34(6), S. 777–798.
- Angermüller, J./van Dyk, S. (Hrsg.) (2010): *Diskursanalyse meets Gouvernementalitätsforschung*. Frankfurt am Main und New York: Campus.
- Baesler, J. P. (2013): Die Macht des Lügendetektors im amerikanischen Sicherheitssystem. In: Greiner, B./Müller, T. B./Voß, K. (Hrsg.): *Erbe des Kalten Krieges*. Hamburg: Hamburger Edition, S. 96–115.
- Baesler, J. P. (2015): From Detection to Surveillance: U.S. Lie Detection Regimes from the Cold War to the War on Terror. In: *Behemoth* 8(1), S. 46–66.
- Bijker, W. E. (1995): *Of Bicycles, Bakelites, and Bulbs. Towards a Theory of Sociotechnical Change*. Cambridge und London: MIT Press.
- Bijker, W. E. (2012\1987): *The Social Construction of Bakelite: Toward a Theory of Invention*. In: Bijker, W. E./Hughes, T. P./Pinch, T. (Hrsg.): *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Anniversary Edition. Cambridge und London: MIT Press, S. 155–182.
- Bijker, W. E./Pinch, T. J. (2012): Preface to the anniversary edition. In: Bijker, W. E./Hughes, T. P./Pinch, T. (Hrsg.): *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Anniversary Edition. Cambridge und London: MIT Press, S. xi–xxxiv.
- Bührmann, A./Schneider, W. (2008): *Vom Diskurs zum Dispositiv*. Bielefeld: transcript.
- Daston, L./Galison, P. (2007): *Objektivität*. Frankfurt am Main: Suhrkamp.
- Denninger, T./van Dyk, S./Lessenich, S./Richter, A. (2014): *Leben im Ruhestand*. Bielefeld: transcript.
- Dosi, G. (1982): Technological paradigms and technological trajectories. In: *Research Policy*, 11(3), S. 147–162.
- van Dyk, S. (2013): Was die Welt zusammenhält: Das Dispositiv als Assoziation und performative Handlungsmacht. In: *Zeitschrift für Diskursforschung* 1(1), S. 46–66.
- van Dyk, S./Langer, A./Macgilchrist, F./Wrana, D./Ziem, A. (2014): Discourse and beyond? Zum Verhältnis von Sprache, Materialität und Praxis. In: Angermüller, J. et al. (Hrsg.): *Diskursforschung. Ein interdisziplinäres Handbuch*. Band 1: Theorien, Methodologien und Kontroversen. Bielefeld: transcript, S. 347–363.
- Egbert, S./Paul, B. (2013): Augenscheinlich überführt: Drogentests als visuelle Selektionstechnologie. In: Dellwing, M./Harbusch, M. (Hrsg.): *Krankheitskonstruktionen und Krankheitstreiberi. Die Renaissance der soziologischen Psychiatriekritik*. Wiesbaden: VS, S. 233–270.

- Egbert, S./Paul, B. (2016): Devices of Lie Detection as Diegetic Technologies in the »War on Terror«. In: *Bulletin of Science, Technology & Society* 35(3-4), S. 84–92.
- Ekman, P./Rosenberg, E. L. (2005): *What the Face Reveals. Basic and Applied Studies of Spontaneous Expression Using the Facial Action Coding System (FACS)*. 2. Aufl. Oxford: Oxford University Press.
- Esposito, E. (2007): *Die Fiktion der wahrscheinlichen Realität*. Frankfurt am Main: Suhrkamp.
- Fitsch, H. (2014): *...dem Gehirn beim Denken zusehen?* Bielefeld: transcript
- Florence, J./Friedmann, R. (2010): Profiles in Terror: A Legal Framework for the Behavioral Profiling Paradigm. In: *George Mason Law Review* 17(2), S. 423–481.
- Foucault, M. (1978): *Dispositive der Macht*. Berlin: Merve.
- Galison, P. (2003): Urteil gegen Objektivität. In: Wolf, H. et al. (Hrsg.): *Diskurse der Fotografie*. Frankfurt am Main: Suhrkamp, S. 384–426.
- Gamer, M./Vossel, G. (2009): Psychophysiologische Aussagebeurteilung: Aktueller Stand und neuere Entwicklungen. In: *Zeitschrift für Neuropsychologie* 20(3), S. 207–218.
- Gitelman, L. (2013) (Hrsg.): *„Raw Data“ Is an Oxymoron*. Cambridge und London: MIT Press.
- Granhag, P. A./Giolla, E. M. (2014): Preventing Future Crimes. Identifying Markers of True and False Intent. In: *European Psychologist* 19(3), S. 195–206.
- Greimas, A. J./Courtés, J. (1982): *Semiotics and Language: An Analytical Dictionary*. Bloomington: Indiana University Press.
- Grubin, D./Madsen, L. (2005): Lie detection and the polygraph: A historical review. In: *The Journal of Forensic Psychiatry & Psychology* 16(2), S. 357–369.
- Haggerty, K. D./Ericson, R. V. (2000): The surveillant assemblage. In: *British Journal of Sociology* 51(4), S. 605–622.
- Honts, C. R./Hartwig, W. (2014): Credibility Assessment at Portals. In: Raskin, D./Honts, C./Kircher, J. (Hrsg.): *Credibility Assessment. Scientific Research and Applications*. Amsterdam und Boston: Academic Press, S. 37–61.
- Hutter, M./Knoblauch, H./Rammert, W./Windeler, A. (2016): Kommunikatives Handeln, das Neue und die Innovationsgesellschaft heute. Die reflexive Herstellung des Neuen. In: Rammert, W./Windeler, A./Knoblauch, H./Hutter, M. (Hrsg.): *Innovationsgesellschaft heute. Perspektiven, Felder und Fälle*. Wiesbaden: Springer VS, S. 15–35.
- Introna, L. D. (2016): Algorithms, Governance, and Governmentality: On Governing Academic Writing. In: *Science, Technology, & Human Values* 41(1), S. 17–49.
- Jäger, S. (2006): Diskurs und Wissen. In: Keller, Reiner et al. (Hrsg.): *Handbuch sozialwissenschaftliche Diskursanalyse*. 2., aktualisierte und erweiterte Auflage. Wiesbaden: VS, S. 83–114.
- Keller R. et al. (2015): Diskurse untersuchen – Ein Gespräch zwischen den Disziplinen. Teil 3a: Diskursive und nicht-diskursive Praktiken, Sprache und Wissen. In: *Zeitschrift für Diskursforschung* 3(3), S. 295–330.
- Keller, R. (2011): *Wissenssoziologische Diskursanalyse. Eine Grundlegung*. 3. Auflage. Wiesbaden: VS.
- Kirby, D. A. (2011): *Lab Coats in Hollywood. Science, Scientists, and Cinema*. Cambridge und London: MIT Press.
- Kölbel, R./Selter, S. (2010): Hostile Intent – the Terrorist’s Achilles Heel? Observations on Pre-Crime Surveillance by Means of Thought Recognition. In: *European Journal of Crime, Criminal Law and Criminal Justice* 18(3), S. 237–259.



- Kneer, G. (2010): Die Debatte über Konstruktivismus und Postkonstruktivismus. In: Kenner, G./Moebius, S. (Hrsg.): *Soziologische Kontroversen*. Frankfurt am Main: Suhrkamp, S. 314–341.
- Krasmann, S. (2003): *Die Kriminalität der Gesellschaft*. Konstanz: UVK.
- Krasmann, S. (2011): Der Präventionsstaat im Einvernehmen. Wie Sichtbarkeitsregime stillschweigend Akzeptanz produzieren. In: Hempel, L./Krasmann, S./Bröckling, U. (Hrsg.): *Sichtbarkeitsregime. Leviathan Sonderheft*. Wiesbaden: VS, S. 53–70.
- Laclau, E./Mouffe, C. (2012\1991): *Hegemonie und radikale Demokratie*. 4., durchgesehene Auflage. Wien: Passagen.
- Latour, B. (1998): Über technische Vermittlung. Philosophie, Soziologie, Genealogie. In: Rammert, W. (Hrsg.): *Technik und Sozialtheorie*. Frankfurt am Main und New York: Campus, S. 29–81.
- Latour, B. (2002): *Die Hoffnung der Pandora*. Frankfurt am Main: Suhrkamp.
- Latour, B. (2010): *Eine neue Soziologie für eine neue Gesellschaft*. Frankfurt am Main: Suhrkamp.
- Latour, B. (2012): *Das Parlament der Dinge*. 2. Auflage. Frankfurt am Main: Suhrkamp.
- Lemke, T. (2014): Die Regierung der Dinge. Politik, Diskurs und Materialität. In: *Zeitschrift für Diskursforschung* 2(3), S. 250–267.
- Lianos, M./Douglas, M. (2000): Dangerization and the End of Deviance. In: *British Journal of Criminology* 40(2), S. 261–278.
- Lindemann, G. (2014): *Weltzugänge: die mehrdimensionale Ordnung des Sozialen*. Weilerswist: Velbrück.
- Littlefield, M. M. (2011): *The Lying Brain: Lie Detection in Science and Science Fiction*. Ann Arbor: University of Michigan Press.
- Lösch, A. (2009): Visuelle Defuturisierung und Ökonomisierung populärer Diskurse in der Nanotechnologie. In: Hüppauf, B./Weingart, P. (Hrsg.): *Frosch und Frankenstein: Bilder als Medium der Popularisierung von Wissenschaft*. Bielefeld: transcript, S. 255–280.
- Luhmann, N. (1990): Die Zukunft kann nicht beginnen: Temporalstrukturen der modernen Gesellschaft. In: Sloterdijk, P. (Hrsg.): *Vor der Jahrtausendwende: Berichte zur Lage der Zukunft*. Frankfurt am Main: Suhrkamp, S. 119–150.
- Maccario, C. J. (2013): Aviation Security and Nonverbal Behavior. In: Matsumoto, D./Frank, M. G./Hwang, H. S. (Hrsg.): *Nonverbal Communication: Science and Applications*. Los Angeles und London: SAGE, S. 147–154.
- Maguire, M. (2015): Questioned by Machines. In: Wilmer, S. E./Žukauskaitė, A. (Hrsg.): *Resisting Biopolitics: Philosophical, Political, and Performative Strategies*. New York und London: Routledge, S. 159–172.
- Manderscheid, K. (2014): Formierung und Wandel hegemonialer Mobilitätsdispositive. In: *Zeitschrift für Diskursforschung* 2(1), S. 5–31.
- McCulloch, J./Wilson, D. (2016): *Pre-Crime. Pre-emption, precaution and the future*. London und New York: Routledge.
- Mersch, D. (2006): Naturwissenschaftliches Wissen und bildliche Logik. In: Heßler, M. (Hrsg.): *Konstruierte Sichtbarkeiten. Wissenschafts- und Technikbilder seit der Frühen Neuzeit*. München: Fink, S. 405–420.
- Opitz, S. (2012): *An der Grenze des Rechts*. Weilerswist: Velbrück.
- Paul, B./Egbert, S. (2014): Lügendetektion per Neuroimaging. Visuelle Verdachtstechnologien als soziotechnische Ensembles. In: *Kriminologisches Journal* 46(3), S. 153–167.

- Perry, M./Gilbey, A. (2011): The screening of passengers by observation techniques programme: analysing the issues. In: *Aviation Security International* 17(3), S. 12–13.
- Pinch, T./Bijker, W. E. (1984): The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. In: *Social Studies of Science* 14(3), S. 399–441.
- Putzke, H. (2013): Die Renaissance des „Lügendetektors“ in Straf- und Familiensachen. In: *Neue Juristische Wochenschrift-aktuell* 66(42), S. 14–15.
- Putzke, H. et al. (2009): Polygraphische Untersuchungen im Strafprozess. In: *Zeitschrift für die gesamte Strafrechtswissenschaft* 121(3), S. 607–644.
- Rammert, W. (2008): Technik und Innovation. In: Maurer, A. (Hrsg.): *Handbuch der Wirtschaftssoziologie*. Wiesbaden: VS, S. 291–319.
- Rammert, W. (2010): Die Innovationen der Gesellschaft. In: Howaldt, J./Jacobsen, H. (Hrsg.): *Soziale Innovation*. Wiesbaden: VS, S. 21–51.
- Rammert, W./Windeler, A./Knoblauch, H./Hutter, M. (2016): Die Ausweitung der Innovationszone. In: Dies. (Hrsg.): *Innovationsgesellschaft heute. Perspektiven, Felder und Fälle*, Wiesbaden: Springer VS, S. 3–13.
- Rose, G./Tolia-Kelley, D. P. (2012): *Visuality/Materiality: Introducing a Manifesto for Practice*. In: Dies. (Hrsg.): *Visuality/Materiality. Images, Objects and Practices*. Farnham und Burlington: Ashgate.
- Schneider, K./Merkle, C. (2007): „Minority Report“ – Fiction or reality? Legal questions raised by neuroscience with particular emphasis on German criminal law. In: *Journal of International Biotechnology Law*, 4, S. 227–232.
- Schwarte, L. (2015): *Pikturale Evidenz. Zur Wahrheitsfähigkeit der Bilder*. Paderborn: Wilhelm Fink.
- Seiterle, S. (2010): *Hirnbild und „Lügendetektion“*. Berlin: Duncker & Humblot.
- Singelstein, T./Stolle, P. (2012): *Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert*. 3., vollständig überarbeitete Auflage. Wiesbaden: VS.
- Waldenfels, B. (1991): Michel Foucault: Ordnung in Diskursen. In: Ewald, F./Waldenfels, B. (Hrsg.): *Spiel der Wahrheit*. Frankfurt am Main: Suhrkamp, S. 277–319.
- Weber, C. (2005): *Securitising the Unconscious: The Bush Doctrine of Preemption and Minority Report*. In: *Geopolitics* 10(3), S. 482–499.
- Weinberger, S. (2010): Intent to deceive? In: *Nature* 465(7297), S. 412–415.
- Weinberger, S. (2011): Terrorist „pre-crime“ detector field tested in United States. *Nature News*, 27. Mai 2011, [www.nature.com/news/2011/110527/full/news.2011.323.html](http://www.nature.com/news/2011/110527/full/news.2011.323.html) (Abruf 23.6.2016).
- Wolf, G. (2010): *The Data-Driven Life*. In: *New York Times Magazine*, [www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?\\_r=0](http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?_r=0) (Abruf 18.6.2016).
- Wrana, D. (2012): Diesseits von Diskursen und Praktiken. Methodologische Bemerkungen zu einem Verhältnis. In: Friebertshäuser, B./Seichter, S. (Hrsg.): *Qualitative Forschungsmethoden in der Erziehungswissenschaft*. Weinheim und Basel: Beltz Juventa, S. 185–200.
- Wrana, D./Langer, A. (2007): An den Rändern der Diskurse. In: *Jenseits der Unterscheidung diskursiver und nicht-diskursiver Praktiken*. In: *Forum: Qualitative Sozialforschung* 8(2), Art. 20, [www.qualitative-research.net/index.php/fqs/article/viewArticle/253/557](http://www.qualitative-research.net/index.php/fqs/article/viewArticle/253/557) (Abruf 07.12.2016).
- Zedner, L. (2009): *Security*. London und New York: Routledge.