Barometer Sicherheit Deutschland

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Verbundprojekt: Sicherheiten, Wahrnehmungen, Lagebilder, Bedingungen und Erwartungen – Ein Monitoring zum Thema Sicherheit in Deutschland (BaSiD)

Modul 6.2 – Interaktive Technikgestaltung

Förderkennzeichen: 13N11149

Abschlussbericht

Bruno Gransche, Ina Jacoby, Philine Warnke, Peter Zoche

Fraunhofer-Institut für System- und Innovationsforschung ISI

Karlsruhe, Dezember 2013

1 EINLEITUNG 1

1.1 Theoretische Vorüberlegungen 2

1.2 Vorgehen 5

2 AUSWERTUNGSERGEBNISSE 13

2.1 Technisierungsgrad 13

2.1.1 Beurteilung von Mensch-Technik-Anteilen 14

2.1.2 Beurteilung technischer Merkmale 20

2.2 Rahmenbedingungen/ Einsatzsituation 26

2.3 Gesellschaftliche Effekte und allgemeine Lebensqualität 31

2.4 Kriminalitätseffekte 32

2.5 Fazit 33

3 ANHANG 37

3.1 Anhang 1: Teilauszüge der Transkripte der partizipativen Workshops 37

3.2 Anhang 2: Auszug aus dem Arbeitspapier 1 – Technisierung und Sicherheitswahrnehmung 44

3.3 Anhang 3: Auszug aus dem Arbeitspapier 2 – Methodensichtung 55

LITERATURVERZEICHNIS 69

1 Einleitung

Ziel des Teilvorhabens des ISI war es, Mechanismen der ***Wechselwirkung von Technisierung von Sicherheit und Sicherheitswahrnehmung*** zu untersuchen. Im Fokus stehen in der Entwicklung befindliche oder zukünftig mögliche Sicherheitslösungen. Die Perspektive ist also eine der Technikgeneseforschung und der prospektiven Technikfolgenabschätzung.[1] Da das Teilvorhaben einen dezidiert subjektiven Sicherheitsbegriff (nämlich primär Sicherheitswahrnehmung) zugrundelegt, wurden Methoden gewählt, die es erlauben, Grundeinstellungen und Werthaltungen von Bürgern[2] zu erfassen und bezüglich verschiedener möglicher Sicherheitslösungen zu beurteilen. Als methodisches Ziel sollten die angewandten Verfahren zur partizipativen Bewertung im Entstehen befindlicher Sicherheitslösungen durch Bürger für die Untersuchungsfrage zugeschnitten, getestet und weiterentwickelt werden.

Der vorliegende Bericht gliedert sich wie folgt:

Zunächst werden zum besseren Verständnis der Ergebnisse einige theoretische Vorüberlegungen wiederholt, die die Untersuchung theoretisch verorten (1.1).[3] Dann wird das gewählte Vorgehen zur Erfassung der Einschätzungen der Bürger und zur Auswertung des so gewonnen Materials beschrieben (1.2).

Die eigentlichen Ergebnisse schließlich werden in Abschnitt 2 dargelegt, gegliedert nach den Aspekten des *Technisierungs-*

---

1 Vgl. Decker et al. 2012.

2 Im Sinne der Lesbarkeit wird im Folgenden für Nomen verallgemeinernd und ohne Absicht der Diskriminierung das generische Maskulinum verwandt. Mit z.B. *Bürger* im generischen Maskulinum sind dann Bürgerinnen und Bürger gemeint.

3 Die Vorüberlegungen wurden in Zwischenergebnissen in einer frühen Phase des Projektes detailliert beschrieben (Gransche/Warnke/Zoche: Technisierung und Sicherheitswahrnehmung, Arbeitspapier 1, Fraunhofer ISI 2011, 22 S.; Warnke/Jacoby/Zoche/Gransche: Methodensichtung, Arbeitspapier 2, Fraunhofer ISI 2011, 24 S.).

grades (→ 2.1), der *Einsatzsituation* (→ 2.2), der *gesellschaftlichen Wirksamkeit* (→ 2.3) sowie der seitens der Nutzer *perzipierten Handlungsmöglichkeiten* der Sicherheitslösungen.

1.1 Theoretische Vorüberlegungen

Unter ***Technisierung*** wird die *Etablierung bestimmter soziotechnischer Ensembles* verstanden. Die sozialwissenschaftliche Technikforschung hat „Ko-Evolutionsprozesse“ (Rip, Schot 2002) von Technik und Gesellschaft vielfach untersucht. So haben Forscher aus Technikgeneseforschung (Dierkes 1992), Technikgeschichte (Hard, Jamison 2005), Innovationsforschung (Geels 2005a) und den internationalen Science and Technology Studies (Jasanoff et al. 1997) an aktuellen und historischen Beispielen Technisierungsprozesse empirisch untersucht und verschiedene Konzepte zu deren Beschreibung und Verständnis vorgeschlagen wie etwa der prominent gewordene „Social Construction of Technology (SCOT)“ Ansatz (Bijker, Law 1997), der Technisierung als sozialen Aushandlungsprozess beschreibt oder die Actor-Network-Theory, die eher auf die gleichzeitige Formation materieller und sozialer Strukturen in Netzwerken fokussiert (Latour 2005). Andere Ansätze beschreiben insbesondere die kulturellen und symbolischen Aneignungsprozesse von Technik (Rammert 2002).

Bei der Implementierung neuer Sicherheitstechniken wird versucht, Routinen und Artefakte in eine stabile Einheit zusammenzubinden. In einer solchen „**soziotechnischen Konstellation**“[4] ist die Aktivität dann auf viele technische und nichttechnische Elemente verteilt. Jede solche „Technisierung“ eröffnet bestimmte Handlungsmöglichkeiten und verschließt gleichzeitig andere.[5] Die Betrachtung soziotechnischer Konstellationen mit verteilten Rollen erlaubt es, einen konstruktiven gestaltungsorientierten Blick auf den Einsatz von Sicherheitstechnik zu werfen. So kann etwa für Videoüberwachung gefragt werden, welche Konstellationen eine symmetrische Blickinteraktion erlauben (Rammert). Die Bewertung der Bestimmt-

4 Rammert 2002a; Hempel, Metelmann 2005, S. 355.

5 Bijker, Law 1997.

heit der Situation und damit das resultierende Sicherheitsempfinden hängen von der soziotechnischen Konstellation ab.

Ausgegangen wird von einem **subjektiven Sicherheitsbegriff**[6], also davon, was Individuen *subjektiv als (un-)sicher empfinden*.[7] Basis für die Untersuchung der Sicherheitswahrnehmung ist also das subjektive Sicherheitsempfinden bzw. Sicherheitsgefühl. Dieses wird über Beurteilungen der Angemessenheit von Handlungsmöglichkeiten adressiert, da ein starker Zusammenhang von Sicherheitswahrnehmung und perzipierter Angemessenheit der Handlungsmöglichkeiten angenommen wird. In der Risikoforschung wird etwa die Möglichkeit der persönlichen Risikosteuerung als maßgebliches Kriterium für die Bewertung eines Risikos angesehen.[8]

Entscheidend für die Sicherheitswahrnehmung ist demnach die Einschätzung der eigenen Handlungsmöglichkeiten und Handlungsfähigkeiten, die individuelle Handlungssicherheit[9]. Da der Mensch in der neuzeitlichen Gesellschaft als handelndes Wesen begriffen wird[10], ist Handlungssicherheit entscheidend für die Empfindung von Sicherheit. Sicherheitsgefühl ist dann ein Bewusstseinszustand, in dem *Situation* (Erwartungen hinsichtlich der externen Umstände/ anderer Akteure und ihrer Entwicklung) und Handlungsmöglichkeiten (Erwartungen

---

6 Vgl. für eine semantisch ansetzende Systematisierung des Sicherheitsbegriffes: Kaufmann 1973.

7 Im Folgenden wird Sicherheit und Unsicherheit je nach zu betonender Perspektive gebraucht und die sperrige Schreibweise (Un-)Sicherheit vermieden. Wenn von Sicherheit und Sicherheitswahrnehmung, Sicherheitsempfunden etc. die Rede ist kann stets auch Unsicherheitswahrnehmung etc. mitgedacht werden. In der Mehrheit der Fälle wird Sicherheit darüber verhandelt, was als unsicher empfunden wird, etwa wenn Sicherheit als die Abwesenheit von Gefahr oder Bedrohung definiert wird.

8 Vgl. Renn 2007, S.42. Weitere Kriterien sind Gewöhnung an die Risikoquelle, Fairness der Risikoübernahme und Freiwilligkeit. Diese werden hier nicht weiter verfolgt, da hier der Technikeinfluss deutlich geringer ist.

9 Handlungssicherheit kann mehrere Bedeutungen annehmen; hier ist mit dem Begriff eine als einer Situation angemessen empfundene Handlungsmöglichkeit gemeint.

10 Vgl. Kaufmann 1970, Kap. 5.3, S. 285 ff.

an das eigene Verhalten, perzipierte Handlungsmöglichkeiten in dieser Situation) als in angemessenem Verhältnis stehend empfunden werden.

> „Es geht beim ‚Sicherheitsgefühl' um die Wahrnehmung eines Gleichgewichts zwischen äußeren Risiken oder Ungewissheiten und inneren Möglichkeiten."[11]

Sicherheitswahrnehmung weist damit eine Komponente der Erwartung an die Person und eine Komponente der Erwartung an die Situation auf.

Die *Komponente der Erwartung an die Person* umfasst das innere Orientierungs- und Koordinationssystem, das in Abhängigkeit von Angst und Furcht[12] bestimmte Aktionszustände hervorruft (Leistung, Hemmung, Reagibilität, Desorientierung[13]) sowie die gelernten Überzeugungen und Erwartungsmuster an die Situation und das eigene Verhalten (Selbstvertrauen, Selbstsicherheit).

Die *Komponente der Erwartung an die Situation* wird von der Bestimmtheit der Situation[14] und dem situationsspezifischen

---

11 Kaufmann 1970, S. 299.

12 Die Begriffe Furcht und Angst – alltagssprachlich oft synonym verwendet – werden in der Philosophie und Psychologie stark getrennt. Seit v.a. Hegel, Kierkegaard, Heidegger und Sartre werden Angst und Furcht durch ihren Objektbezug und ihre Konkretheit unterschieden. Dabei richtet sich die Furcht auf ein konkretes Objekt, eine identifizierbare Bedrohung und hat also ein reales Wovor des Fürchtens, weshalb Furcht auch als Realangst (Freud) bezeichnet wird. Angst hingegen ist ein unspezifisches, objektloses Gefühl des allgemeinen Bedrohtseins. In der Psychologie und Psychiatrie gilt die Angst auch als die pathologische Dimension der Furcht. Kurz: bestimmte Gefahr = Furcht, unbestimmte Gefahr = Angst (s. Kaufmann 1970, S. 288. Vgl. Hegel 1986, Heidegger 1979, Kierkegaard 1984, Sartre 1991.)

13 Kaufmann 1970, S. 288f.

14 Der handlungstheoretische Begriff der Situation bezeichnet „nicht den Zustand der Umgebung eines Subjekts schlechthin, sondern die vom Subjekt erfahrene und zugleich definierte Zuständlichkeit seiner Umwelt. […] Die Definition der Situation geht der Diagnose von Gefahr voran, ja sie bestimmt weitgehend den Bereich möglicher Gefahren." (Kaufmann 1970, S. 271) „„Situation" und „Umwelt" […] bezeichnen somit stets eine Beziehung zwischen Subjekt und „Welt" und nicht einen unabhängig von einem Subjekt objektivierbaren Zustand." (Kaufmann 1970, S. 358)

Geschick im Umgang mit Ungewissheit charakterisiert. Das höchste Unsicherheitsgefühl geht von einem „Bewusstsein der Unfähigkeit, die äußeren Gegebenheiten richtig einschätzen zu können“[15] aus (existentielle Angst).

So ergibt sich für die Untersuchung von Mechanismen der *Wechselwirkung von Technisierung von Sicherheit und Sicherheitswahrnehmung* folgende **Forschungsfrage**:

Welche Merkmale soziotechnischer Konstellationen haben Einfluss darauf, wie involvierte Bürger den Umfang und die Qualität ihrer Handlungsmöglichkeiten bewerten?

Auf den theoretischen Vorüberlegungen aufsetzend, kann die Schlussfolgerung abgeleitet werden, dass als angemessen perzipierte Handlungsmöglichkeiten mit einem hohen Sicherheitsgefühl einhergehen und umgekehrt. Um das empirisch nicht unmittelbar messbare Sicherheitsempfinden zugänglich zu machen, wurden daher in spezifischen partizipativen Verfahren grundlegende Werteinstellungen und Grundhaltungen von Bürgern gegenüber Technisierung von Sicherheit und Beurteilungen definierter Arrangements ausgewählter, zukünftig denkbarer Sicherheitslösungen erfasst und der Auswertungsfokus auf den Zusammenhang von Technikgestalt und Sicherheitswahrnehmung, vermittelt über die subjektiven Handlungseinschätzungen, gelegt. Dazu wurde ein dreistufiges Vorgehen entwickelt.

1.2 Vorgehen

Die inhaltliche thematische Auswahl fand mit der Entwicklung dreier sogenannter *Brennpunkte* statt. Unter Brennpunkte werden die thematischen Zuschnitte verstanden, die eine besondere Kombination relevanter Sicherheitstechnologien einerseits und Bezüge zu aktuellen gesellschaftlichen Sicherheitsthemen andererseits aufweisen. In den „Brennpunkten“ bündeln sich Aspekte von Technologiedynamiken und medialgesellschaftlicher Aufmerksamkeit, wodurch ein besonderer Fokus entsteht.

15 Kaufmann 1970, S. 298.

Es wurde auf der Basis einschlägiger aktueller Literatur eine Zusammenstellung wesentlicher Sicherheitstechnologien und ihrer Einsatzbereiche vorgenommen sowie eine erste Charakterisierung des Reifegrads der Technologien mit Experten diskutiert; Beispiele sind Mustererkennungssysteme, vernetzte Mikrodrohnen, neuere Biosensortechnologie, (semi-)autonome robotische Technologie, Data-Mining- und Big Data-Technologien etc. Gleichzeitig wurden in jüngster Zeit[16] geführte öffentliche Debatten zu Fragen der Sicherheitslösungen und -technik berücksichtigt; Beispiele sind der Terroranschlag am Moskauer Flughafen, Debatten um U- und S-Bahn Schläger, der Stuxnet-Virus in iranischen Kernkraftwerken, die Panik der Love Parade in Duisburg etc. Eine Gegenüberstellung der beiden Bestandsaufnahmen ergab die ersten Brennpunkte in denen aktuelle Technologieentwicklungen und öffentliches Interesse zusammenfallen. Nach folgenden Kriterien wurden drei dieser Brennpunkte für die Bearbeitung im Projekt ausgewählt:

- Vermutete Relevanz für breite Sicherheitswahrnehmung und damit als Beitrag zum BaSiD-Gesamtvorhaben
- Vorhandensein aktueller, noch offener Gestaltungsfragen in der Entwicklungs- oder Einführungsphase
- Relevanz für BMBF Förderpolitik
- Eignung des Brennpunkts für die Bearbeitung mit partizipativen Verfahren:
    - Der Brennpunkt sollte für breite Gruppen von Bürgern interessant sein – nicht nur für spezielle Organisationen oder Kleingruppen
    - Hohe Anschaulichkeit bzw. gute Handhabbarkeit des Brennpunktes
    - Es sollte eine Möglichkeit bestehen, die erarbeiteten Ergebnisse im Rahmen von bzw. An-

16 Einbezogen wurden Fälle, die im Zeitraum zwischen den Jahren Mitte 2009 und Frühjahr 2011 öffentlich diskutiert wurden. Die zugrunde liegenden Anlässe reichten teilweise länger zurück.

schluss an BaSiD zu Gestaltungskriterien zu verdichten

Schließlich noch liegt es im Interesse der Projektziele, verschieden gelagerte Problemstellungen zu bearbeiten, um möglichst breite Erfahrungen sammeln zu können.

Unter Anwendung dieser Kriterien wurde folgende Auswahl getroffen:

- Brennpunkt 1: Intelligente Videoüberwachung öffentlicher Räume
- Brennpunkt 2: UAVs (Unmanned Aerial Vehicle; Drohnen) – Sicherheit von Oben
- Brennpunkt 3: Web2.0-Dienste als Medium der sozialen Kontrolle

Brennpunkt 1: Intelligente Videoüberwachung öffentlicher Räume

> „Ein Videoüberwachungssystem stellt… eine in ständiger Veränderung begriffene, komplexe soziotechnische Verbindung von Instrumenten und sozialen Akteuren dar.“[17]

Videoüberwachung (CCTV) gehört international zu den verbreiteten und intensiv eingesetzten Überwachungssystemen. Die technologische Entwicklung führt diese Überwachungssysteme jedoch auf ein anderes Niveau, das es rechtfertigt vom Entstehen ***intelligenter* Videoüberwachungssysteme** zu sprechen. Dazu führt eine Kombination der qualitativen Verbesserung der Systemkomponenten (höhere Auflösung bei sinkenden Preisen; höhere Störungs-/ Täuschungstoleranz; bessere/ schnellere/ robustere Datenübertragung, zunehmend drahtlos; Miniaturisierung; höhere Rechenleistung) mit weiteren technischen Innovationen, die Umsetzungsreife erreichen bzw. erreicht haben und die die Komplexität und Vernetzung der Technologie vorantreiben (leistungsfähigere Algorithmen zur automatischen Mustererkennung, automatisierten Personenverfolgung, automatischen Situations-/ Verhaltensanalyse, automatisierte Kombination mit umfassenden Datenbanken;

---

17 Klauser 2006, S. 117.

Fortschritte bei der 3D-Technik; Erkennung einer Vielzahl biometrischer Merkmale).

Der Fokus auf **öffentliche Räume** wurde in diesem Brennpunkt gewählt, um eine möglichst hohe Relevanz für das Gesamtvorhaben von BaSiD, die breite Sicherheitswahrnehmung in Deutschland, zu gewährleisten. Öffentliche Räume betreffen jeden Bürger, der diese alltäglich nutzt und keine Möglichkeit hat sie zu meiden, daher fassen wir darunter öffentliche Plätze, Straßen, Wege, (Park-)Anlagen, aber auch Kaufhäuser und Bahnhöfe, die nicht zugangsbeschränkter Teil der öffentlichen Sphäre sind. Flughäfen betrachten wir nicht darunter, da hier teilweise Zugangsbeschränkungen bestehen und sie nur von einem bestimmten Personenkreis zu bestimmten Zwecken freiwillig aufgesucht werden; Bahnhöfe weisen dagegen eine größere Offenheit und Öffentlichkeit auf, als Flughäfen.

Brennpunkt 2: UAVs (Drohnen) – Sicherheit von Oben?

Drohnen, auch *unmanned arial vehicles* (UAV), sind unbemannte (semi-)autonome robotische Fluggeräte, die als Plattform für eine Vielzahl von Sensoren und Manipulatoren genutzt werden können. Dabei reichen die UAV-Varianten von 19 Gramm leichten Roboterkolibris wie dem *Nano Hummingbird* (siehe Bild rechts[18]) bis zum hochfliegenden Langstreckenaufklärer *Global Hawk* mit fast 40m Spannweite. Mit entsprechenden Kameras bestückt, können UAVs mobile intelligente Videoüberwachungssysteme darstellen, womit sie eine andere Dimension etwa in Personenverfolgungs-, Spionage- oder Aufklärungsfunktionen der Videoüberwachung bringen. Multisensorische UAVs können aber auch Teile anderer intelligenter Überwachungskonzepte sein, die über Kamerasysteme weit hinausgehen.

18 Aufklärungs-UAV der DARPA : Quelle: http://www.kurzweilai.net/nano-hummingbird-uav.

Brennpunkt 3: Web2.0 Dienste als Medium der sozialen Kontrolle

Ein weiteres Setting des Bereichs intelligente Überwachung, das untersucht werden soll, ist die Entwicklung von **Web2.0 Diensten** zur sozialen Kontrolle, bei der Bürger – im Gegensatz zur öffentlichen Videoüberwachung – nicht nur Überwachte sondern auch Überwacher sind. In Diskussion sind etwa Onlineplattformen als Meldeportale für beobachtete Straftaten, suspekte Objekte und dergleichen. Als Überwachungssystem gefasst fungieren die Bürger hier quasi als Sensoren mit integrierter Auswertungs-/ Interpretationskompetenz. Weiter angedacht ist ein allgemeiner Zugriff auf Videokameras über das Internet, bei der jeder Bürger Auffälligkeiten oder gar Straftaten an privaten Bildschirmen beobachten und melden kann – damit wäre ein gängiges Problem der Videoüberwachung, nämlich dass (zu) wenige Beobachter mannigfaltige Videosequenzen auf (zu) vielen Bildschirmen überblicken, umgekehrt.

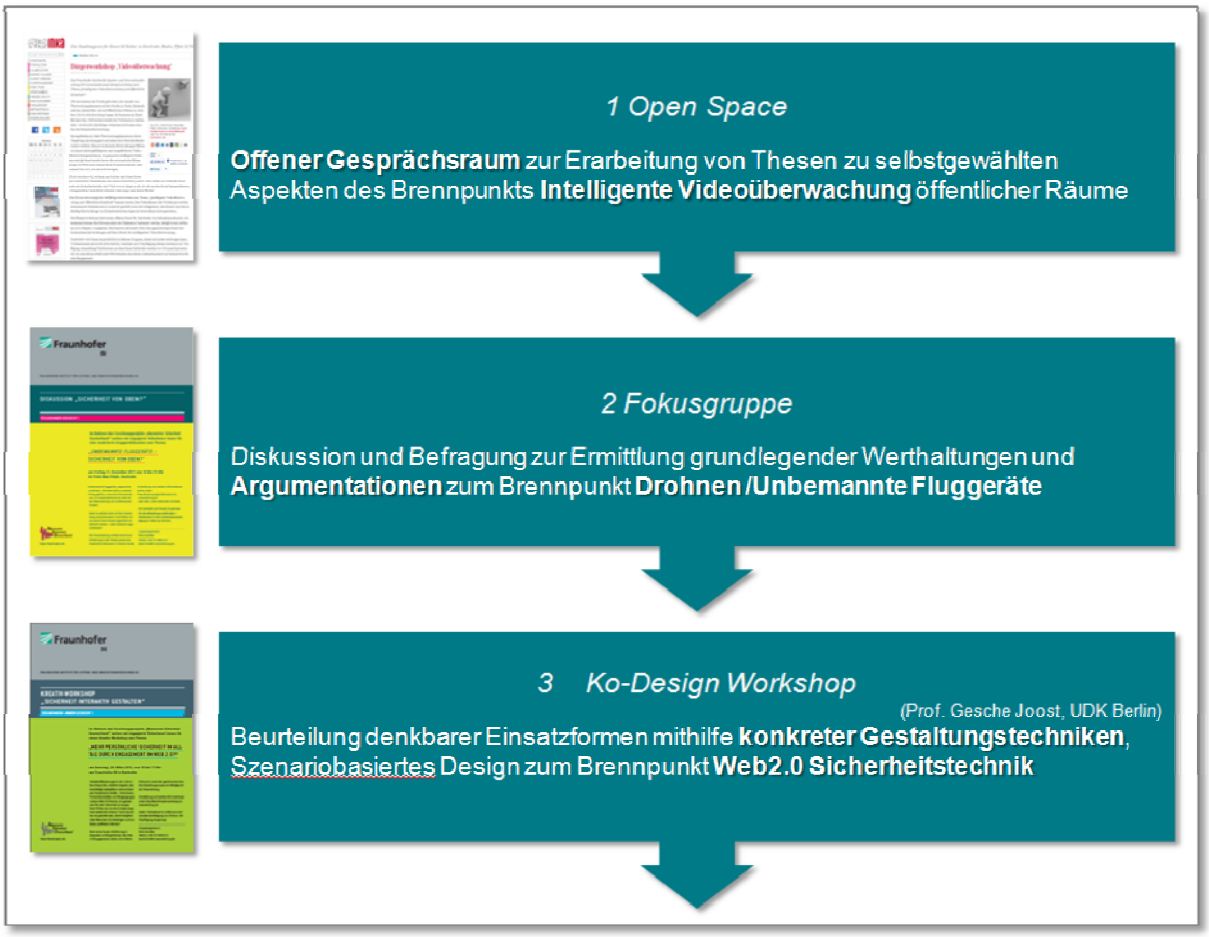

Abbildung 1 - Vorgehen[19]

Die Wahl der verwendeten Verfahren der Workshops richtete sich nach den jeweils identifizierten methodischen Stärken in Bezug auf die formulierten Fragestellungen. [20] So eignet sich das Open Space Verfahren insbesondere dafür, einen Zugang zum Alltagswissen und damit auch zum Wertekanon der Beteiligten zu gewinnen, da das Verfahren als ideal gilt, um eine offene Kommunikation innerhalb einer heterogenen Gruppe zu befördern. Ergänzend eignet sich die Fokusgruppe in beson-

19 Links abgebildet sind drei Bekanntmachungen, mit denen die Laien auf die Veranstaltung aufmerksam gemacht und für die Beteiligung gewonnen wurden, z.B. über Anzeigen in Online-Veranstaltungskalendern der Stadt Karlsruhe, Plakate, Flyer etc.

20 Vgl. für einen Überblick Steyaert et al. 2006.

derer Weise dafür, konkrete Einschätzungen von Bürgerinnen und Bürgern in Bezug auf im Entstehen begriffene Sicherheitstechnologien einzuholen. In einem teilstrukturierten Prozess werden hier Meinungen zu denkbaren Einsatzformen von Drohnen ausgetauscht und gegenseitig begründet. Das dritte Workshopformat hat schließlich zum Ziel, in einem kreativen Prozess zwischen Designern, Forschern und Teilnehmern konkrete Gestaltungsmerkmale von Sicherheitstechnologien zu identifizieren, die einen Einfluss auf das Sicherheitsempfinden ausüben. Der Ko-Design Workshop wurde in Zusammenarbeit mit Prof. Gesche Joost von der UDK Berlin für die Fragestellung der Gestaltung von Web2.0-Diensten als Sicherheitstechnologien entwickelt.

Für die Teilnahme an den unterschiedlichen Workshopformaten wurde eine möglichst heterogene Gruppe von Personen rekrutiert. Die Bürger wurden dabei als „Experten ihres Alltags“ befragt.

In allen Workshops wurde, wie bei partizipativen Verfahren üblich, mit kurzen inhaltlichen Experteninputs gearbeitet, da bezüglich der Brennpunkte bei den Teilnehmern kein einheitlicher Informationsstand vorausgesetzt werden kann. Die Inputs enthielten jeweils einen Überblick über neuste Entwicklungen im Bereich intelligente Videoüberwachung, unbemannte Fluggeräte und Web 2.0 Sicherheitsanwendungen. Dabei wurde darauf geachtet möglichst neutral zu informieren. Während im ersten wie auch im dritten Workshop die selbst gewählten Themen (im Rahmen der Brennpunkte) der Teilnehmer im Mittelpunkt standen, wurde die Vorgehensweise im zweiten Workshop durch einen Gesprächsleitfaden teilstrukturiert.[21]

Der **Auswertung** liegen die schriftlichen Transskripte der Ergebnispräsentationen und diskursiven Abschnitte der drei Workshops sowie die präsentierten Materialien der Teilnehmer zugrunde. Das Material wurde mit Hilfe des Computerprogramms MAXQDA 10 codiert und ausgewertet. Die Aus-

21 Eine detaillierte Beschreibung des methodischen Vorgehens und eine methodenbezogene Dokumentation der Workshops wurden im Projekt separat erstellt.

wertung orientierte sich an der Verfahrensweise der zusammenfassenden Inhaltsanalyse (nach Mayring[22]), wobei eine im Kern induktive Vorgehensweise angewendet wurde. Mit Hilfe von Paraphrasierung, Generalisierung und Reduktion konnten gemeinsame Aspekte und Themen der drei Workshops identifiziert werden.

22 Vgl. Mayring 2010.

2 Auswertungsergebnisse

2.1 Technisierungsgrad

Eine Vielzahl der zentral diskutierten Aspekte zukünftiger Sicherheitslösungen lassen sich als Merkmale des Technisierungsgrades der jeweiligen Lösung fassen. Wird mit Technisierung die *Etablierung bestimmter soziotechnischer Ensembles* verstanden (vgl. 1.1, S. 2), so soll mit dem Technisierungsgrad das *Maß der Fixierung der beteiligten technischen und nicht-technischen Elemente zu einer bestimmten soziotechnischen Konstellation* verstanden werden. In Konstellationen mit hohem Technisierungsgrad werden zunehmend Handlungsanteile, die zuvor als Konsequenz freier Entscheidung in situativer menschlicher Aktion lagen, auf automatisierte, fixe Systemteile verlagert. Mit zunehmender Technisierung verschiebt sich so Handeln zu bloßem Verhalten oder gar Funktionieren, wobei in solchen Konstellationen sowohl Menschen durchaus nur noch quasi-technisch „funktionieren" als auch Technik mit zunehmender „Intelligenz", „Autonomie" und zunehmenden Leistungsmöglichkeiten bereits quasi-menschlich „handeln".[23] Technik selbst kann als Prozess der Technisierung, also über den Mitteleinsatz hinaus als Sicherung des Gelingens des Mitteleinsatzes[24], als Fixierung von Handlungsvorgängen gesehen werden, die so wiederholbar bis automatisierbar werden.

> „Aus technikgenetischer Perspektive erscheint Technik als sozialer Prozeß der graduellen Technisierung von Wahrnehmungs- und Handlungsvorgängen, in dem aus der praktischen Erfahrung Schemata des Wirkens herausgebildet, diese unter funktionalen Gesichtspunkten zu komplexen technischen Gebilden kombiniert und zur Steigerung von Leistungen dauerhaft und anerkannt genutzt werden."[25]

Technisierungsprozesse sind stets sozialen Aushandlungsprozessen unterworfen. Im Rahmen der partizipativen Verfah-

---

23 Vgl. Rammert und Schulz-Schaeffer 2002.

24 Vgl. Hubig 2002.

25 Rammert 1999, S. 4.

ren, die in den Workshops verwendet wurden, können gewisse Dynamiken solcher sozialen Aushandlungsprozesse teilweise nachvollzogen werden. So wurden beispielsweise zum Brennpunkt der „intelligenten Videoüberwachung“ die verschiedensten Konstellationen von rein personaler Überwachung selbst ohne Kamera (z.B. Wachmann), über Mischkonzepte verschiedener CCTV-Systeme[26] mit unterschiedlichsten Kamera-Überwacher-Verhältnissen[27] bis hin zu reinen „vollautonomen“ „intelligenten“ CCTV-Systemen diskutiert. Vollautonome Überwachung wurde – technisches Funktionieren einmal vorausgesetzt – dabei zwar als möglicherweise leistungsfähiger bei der jeweiligen Überwachungsaufgabe, der zu überwachenden Räume oder der Kostenbilanz beurteilt, was aber nicht zur Einschätzung angemessenerer eigener Handlungsmöglichkeiten und damit nicht zu einer perzipierten Erhöhung des Sicherheitsgefühls beitrug und insofern auch als Sicherheitsparadox gefasst werden kann.

2.1.1 Beurteilung von Mensch-Technik-Anteilen

Bei der Beurteilung von verschiedenen Konstellationen mit unterschiedlichem Mensch-Technik-Verhältnis hat sich in allen drei Workshops eine deutliche Tendenz zur Skepsis gegenüber „autonomer“ Technik und zur Befürwortung menschlicher Letztkontrolle in den Sicherheitslösungen gezeigt. Die deutlich dominante Haltung in allen Gruppen lehnte vollautonome Systeme ab. Wenigstens eine menschliche Letztinstanz in hybriden Systemen wurde als ein Minimum angesehen, damit eine

Anmerkung zu den Zitaten

In den Textfeldern am rechten Rand werden jeweils Originalzitate aus den Workshops zur Verdeutlichung der im Text erwähnten Aussagen angeführt. Da es sich um Transskripte von Audioaufnahmen handelt, stellt die Verschriftlichung, v.a. die Interpunktion, bereits eine gewisse Interpretation der Autoren dar, die dabei jedoch um Neutralität bemüht sind. Um die Lesbarkeit zu erhöhen, werden kleine nicht sinnverändernde Korrekturen in der Grammatik und Satzstellung der gesprochenen Sprache vorgenommen, ohne diese wie üblich extra in eckigen Klammern anzuzeigen. Alles Sonstige in eckigen Klammern sind ergänzende Einfügungen der Autoren.

26 CCTV: Überwachungskamerasysteme, engl. Closed Circuit Television.

27 Dabei reichen die Varianten von „eine Kamera - ein Überwacher“ wie bei dem Türspion bzw. bei der kameraunterstützen Türklingelanlage über „viele Kameras – wenige Überwacher“ wie bei den meisten gegenwärtigen CCTV-Systemen, in denen wenige Beobachter eine Vielzahl von Kameras im Blick behalten müssen und dabei wiederum graduell von Technik mittels Hinweisen und Alarmen unterstützt werden, bis hin zu „wenige Kameras – viele Überwacher“ wie etwa wenn über online Webcams öffentliche Plätze von einer großen Menge potenzieller Beobachter überwacht werden.

Sicherheitslösung als Sicherheitsgewinn wahrgenommen werden könne. Es wurden vielfach Pro- und Contra-Argumente bezüglich menschlicher und technischer Handlungsanteile in Sicherheitslösungen diskutiert, wobei trotz großer Perspektivenvielfalt eine allgemeine Bevorzugung von Personen im System gesehen wurde. Im Folgenden werden Argumente zum Mensch-Technik-Verhältnis von hybriden Sicherheitslösungen aus allen drei Workshops dargestellt. Die genannten Positionen repräsentieren immer Momentaufnahmen aus den Diskussionen. Es kann als großer Vorteil der partizipativen diskursiven Methoden gelten, dass sich die Teilnehmer im interaktiven Austausch wechselseitig in ihren Einschätzungen ergänzen, widersprechen oder relativieren. Für die Analyse ergibt sich daraus der methodische Vorteil, dass – anders als in Umfragen möglich - diskursive Prozesse der Meinungsfindung abgebildet und die Begründungen der unterschiedlichen Einschätzungen unmittelbar erkennbar werden.

Einschätzungen zu Personen[28];

Personen im Sicherheitssystem wurde tendenziell deutlich mehr *vertraut*, als technischen Elementen.

Das Vertrauen in Personen gegenüber technischen Elementen wurde damit begründet, dass Personen eine Situation je am „**gesunden Menschenverstand**“ auf Situationsadäquatheit und Verhältnismäßigkeit prüften, statt technisch vorimplementierte Regeln zu prozessieren. Personen wird zugetraut, wo nötig und opportun „ein Auge zudrücken zu können“, nicht unter eine Bagatellgrenze zu sanktionieren und v.a. auf den jeweiligen Fall individuell eingehen und notfalls die eigenen Regeln suspendieren zu können. Die 100%ige Regeltreue von Systemen mit algorithmischer Mustererkennung wird mitunter als technikinduzierter Totalitarismus empfunden und die

Gesunder Menschenverstand

„Wenn jetzt zum Beispiel eine Kamera [filmt] wie jemand ein Kaugummi irgendwohin klebt, dann meldet vielleicht dieses System einem Polizisten: ‚Okay, der tut was‘. Aber ich glaube, kein Polizist auf der Welt wird sich dann auf den Weg machen, um jemandem einen Zettel über 20 Euro Strafe in die Hand zu geben, weil der irgendwo in der Bahn einen Kaugummi rein geklebt hat.“

Misstrauen gegenüber Technik

„Wenn das eine materiale, also eine künstliche Intelligenz ist, die uns überwacht, trauen wir ihr einfach nicht.“

28 Da der Personenbegriff hier nicht als Fachbegriff in Anschlag gebracht wird, wird bei der Differenzierung der Elemente sozio-technischer Konstellationen statt von „Menschen“ von Personen gesprochen, da dies weniger biologistisch gattungsbegrifflich konnotiert ist.

Intransparenz algorithmischer „Entscheidung“ sorgt für generelles **Misstrauen** gegenüber solchermaßen technisch usurpierten eigentlich menschlichen „Hoheitsgebieten“ wie Entscheiden, Intelligenz usw. Technik – obwohl gesellschaftlich-kulturelles Produkt wird demnach klar von kulturgeprägt gesellschaftlichem Handeln unterschieden.

Schließlich rührt die Präferenz von Personen im System von der Möglichkeit zur aktiven **Interaktion** mit Ihnen über die ein Regelverstoß etwa erklärt werden könnte oder über die direkt Hilfe angefordert werden kann, welche Personen im Gegensatz zu technischen Systemen dann auch direkt leisten könnten.

Interaktion

„Im Zweifelsfall, haben wir uns gesagt, setzten wir uns lieber in die Nähe des Straßenbahnführers, als in die Nähe von so ‘ner Kamera, weil der im Zweifelsfall dann doch noch direkt eingreifen kann.“

Das geäußerte Vertrauen in Personen ist nicht zwingend vernünftig, schließlich gehen eine Vielzahl von Gefahren gerade auf menschliche Fehler und Versagen zurück und haben Personen auch Vorurteile, sind mitunter bestechlich, diskriminierend, stimmungsvolatil und können ihre Macht auch missbrauchen. Auch diese Punkte wurden diskutiert, was zu einem gewissen Grad Aspekte von ***Checks and Balances*** zwischen Mensch und Technik thematisierte, jedoch nicht zur Befürwortung rein technischer Lösungen geriet.
So wurden nicht nur Anteile von Personen und Technik in der Konstellation bewertet, sondern auch welche Personen und welche Technik welchen Einfluss auf die Sicherheitswahrnehmung haben. Bei der Technik wurde dies unter entsprechenden *Safety*-Aspekten diskutiert (vgl. dazu auch 2.1.2), nach denen technische Komponenten auf sicheren Betreib geprüft, abgenommen (z.B. TÜV) und zugelassen werden müssen. Es wird von den Teilnehmern mehrheitlich auf das deutsche Rechts- und Prüfsystem diesbezüglich vertraut. Eine ähnliche sicherheitsfördernde Vertrauensgrundlage durch „Prüfung“ wurde in Bezug auf beteiligte Personen in der Sicherheitslösung diskutiert: Damit Personen eine Erhöhung des Sicherheitsempfindens bewirken, dürfen dies nicht irgendwelche Personen sein, sondern besonders qualifizierte, autorisierte etc. So genießen Sicherheitsbeamte wie Polizei (mit guter Ausbildung, staatlicher Autorisierung, richterlichem Beschluss, besonderer Kompetenz, ausreichender Ausstat-

Menschen als Sicherheitslücke

„Menschen die vorhaben zum Beispiel eine Bank auszurauben, werden Wege und Mittel finden diese Überwachung [z.B. durch CCTV/Drohnen] zu umgehen. Sie werden vielleicht Sicherheitsleute bestechen die mit der Überwachung zusammenhängen, dass zu dem Zeitpunkt die Drohne zufällig irgendwo anders hinguckt.“

tung, Pausen etc.) tendenziell größeres Vertrauen, als private Sicherheitsdienste. Um „normale“ Bürger in diskutierten Web2.0-Anwendungen „prüfen“ bzw. sie als Sicherheitsgewinn statt –risiko wahrnehmen zu können wurden technisch unterstütze Formen der sozialen Kontrolle bedacht, wie z.B. die Community-Bewertungen mittels Zufriedenheitspunkten wie sie von eBay oder Amazon bekannt sind. Zusammenfassend lässt sich also sagen, dass neben der grundsätzlichen Befürwortung von menschlicher Restinstanz in möglichen Sicherheitslösungen qualifizierende, vertrauensbildende Aspekte sowohl auf Seiten der Technik, als auch auf Seiten der Personen hinzukommen müssen, um als Sicherheitsgewinn wahrgenommen zu werden. Der Nexus von Vertrauen und Sicherheitsempfinden verweist wiederum auf den von Handlungskompetenz und Sicherheitsempfinden, da Vertrauen als eine Art pauschalisierte delegierte Kontrolle aufgefasst werden kann. Wo ich keine Möglichkeit habe, Sicherungs- und Gefährdungspotenziale von Personen und Technik *selbst zu überprüfen* (Handlungsmöglichkeit), da kann diese Möglichkeit durch das Vertrauen in prüfende Institutionen (Staat, Gerichte, Kollektive) teils ersetzt werden. Dementsprechend wirken Entwicklungen, die diese Vertrauensaspekte bzw. Kontrolldelegationen untergraben negativ auf das Sicherheitsempfinden (z.B. wenn nicht mehr plausibel ist, dass Prüfinstanzen wie der TÜV aufgrund der Komplexität der Technik noch in der Lage sind, verlässliche Funktionsbürgschaften auszusprechen).

Einschätzungen zu Technik

Als Vorteile der technischen Elemente wurde zwar die **vermeintliche Neutralität** (z.B. Vorurteilsfreiheit) der Technik angesprochen, jedoch in der Diskussion als „Mythos“, da z.B. Mustererkennungssoftware lediglich „neutral“ die ihr inskribierten „Vorurteile“ prozessiert und, im Falle fehlender menschlicher Letztkontrolle, gar verabsolutiert.

Als durchgehend präsupponierter Vorteil der zunehmenden Verlagerung von Aufgaben bzw. Funktionen der Sicherheitslö-

Kosten

„A: Wenn einfach wirklich Personal da wäre, das im Zweifelsfall dann auch eingreifen kann. Würde natürlich entsprechend Geld kosten. Aber das wär‘ eben in unserer Meinung eben eine Alternative [zur intelligenten Videoüberwachung].“

„Also im Zweifelsfall: beides wird Geld kosten und die Frage ist halt dann, was nützt im Zweifelsfall mehr oder inwieweit sind halt die Kosten dann gerechtfertigt.“

sung von Personen auf technische Elemente wurden deren (vermuteten) **niedrigere Kosten** angeführt.[29]

Als Vorteil gewendet kann die im Vergleich zu Personen geringe situative Flexibilität technischer Systeme als technikseitige **Fehlerkompensation** von menschlichen Fehlern verstanden werden. Dass Personen in jeder Situation anders reagieren können, ist nicht immer ein Vorteil, da sie so auch immer neue Fehlermöglichkeiten entwickeln. Das sichernde Kompensationspotenzial von Technik (z.B. das kurze Lösen der Bremse bei ABS) wird jedoch als auf vergleichsweise einfache „Aufgaben" beschränkt gesehen; in komplexen soziotechnischen Systemen mit komplexen Aufgaben wie der Erkennung von „auffälligem/aggressivem Verhalten" gewinnt die situative Flexibilität von Personen gegenüber der Sicherung durch Technik an Wert.[30]

Durch diese Eigenart der Technik, *Normal Accidents* zu produzieren, denen Personen insofern machtlos ausgeliefert sind, als die verunfallende Technik nicht wie Personen robuste Interaktionsmöglichkeiten bietet, schlägt der intendierte Sicherungseffekt v.a. komplexer technikintensiver Konstellation in der Sicherheitswahrnehmung beteiligter Personen in sein Gegenteil um. Zur technischen „Eigenrationalität" kommt der zunehmende Eindruck einer eigenmächtigen künstlichen Intelligenz, was als erschreckend empfunden wird. So kann komplexe Sicherheitstechnik in zukünftigen Konstellationen nicht nur Sicherheit nicht erhöhen, sondern massiv zur Unsicherheit beitragen. Ähnliches gilt aber für Sicherheitslösungen, mit niedrigem Technisierungsgrad, so kann die erhöhte personelle Polizeipräsenz ebenfalls eher verunsichern, als zu versichern, wobei Polizeibeamten dennoch einerseits der „gesunde Menschenverstand" im angemessenen Handeln, andererseits ein

Unbeherrschbare Technik

„Technik ist immer auf gewisse Weise unbeherrschbar, bzw. was, wenn sie auf einmal ausfällt, bzw. nicht funktioniert?' [...] Wir würden dann natürlich bei sicherheitsrelevanten Sachen, wenn es jetzt darum geht, einen Notruf abzusetzen, das versuchen doppelt und dreifach abzusichern. Aber hundertprozentige Sicherheit wird sich da vermutlich leider nicht gewähren lassen. Das ist vermutlich ein allgemeines technisches Problem."

Erschreckende Technik

„Was ich echt erschreckend fand war, dass die Vereinigten Staaten versuchen, mehrere Drohnen zu koppeln, um wirklich etwas größere Gelände abzudecken. […] Und dass das alles über Maschinen gesteuert wird, und das – muss ich sagen – habe ich ehrlich mit Erschrecken zur Kenntnis genommen, dass daran geforscht wird. […] dass die auch noch anfangen sollen, alleine zu ‚denken'. Das fand ich doch schon sehr erschreckend."

Legitimität von Polizei

„Dass die Polizei nicht einfach im Verdachtsfall diese Drohne einsetzen kann, dass sich jetzt gerade mal jemand denkt: ‚Ja, machen wir das mal.' Sondern dass es einen begründeten Verdacht geben muss und das auch durch einen Richter legitimiert werden muss."

29 Es wurden in allen drei Workshops in zahlreichen Varianten Kosten-Nutzen-Abwägungen argumentiert, vgl. dazu die weiteren Ausführungen.

30 Mit anderen Worten: Die Fehleranfälligkeit der Technik steigt mit zunehmender Komplexität, weshalb für komplexe Systeme mit eng gekoppelten technischen Elementen *Unfälle normal* sind, was Charles Perrow bereits 1984 unter dem Titel *Normal Accidents* prominent machte; vgl. Perrow 1984.

höheres Vertrauen aufgrund ihrer legitimierten formalen Exekutivfunktion zugesprochen wird; auf private Sicherheitsdienstleister trifft schon nur noch ersteres und dies evtl. auch in geringerem Maße zu.

Zwischenfazit

Diese Einschätzungen stützen die These vom Einfluss der perzipierten Angemessenheit der eigenen Handlungsmöglichkeiten auf das Sicherheitsempfinden: Konstellationen werden umso negativer in ihrem Sicherheitseffekt beurteilt, je weniger sie Möglichkeiten zu Handeln, zur Intervention und Interaktion lassen. Das reicht von hochtechnisierten Konstellationen, die Bagatelldelikte rigide ahnden, „nicht mit sich reden lassen", keine unmittelbare Hilfe leisten können bis zu gänzlich opaken „mysteriösen" Systemen, deren „Handeln" und Urteilen nicht einmal mehr Experten nachvollziehen können.[31] Verunsicherung entsteht durch das technische vorformulieren (implementierte Routinen) bzw. das Etablieren „technischer Sachzwänge"[32]. Eine durch Sicherheitssysteme kontrollierte Situation, in der „nichts schief gehen" kann, würde deshalb dennoch nicht als sicher wahrgenommen, da die Situation gänzlich dem Einfluss von Personen entzogen wäre, was gemäß der hier überprüften These das Unsicherheitsempfinden erhöht (etwa weil man so den systemeigenen *Normal Accidents* ausgeliefert wäre).

Stark komprimiert könnte man resümieren: Personen in der Konstellation möglicher Sicherheitslösungen wird zugetraut i.d.R. mit gesundem Menschenverstand urteilen, zur Not aktiv

---

31 Wie etwa bei Systemen, die auf evolutionären Algorithmen basieren, was durchaus bei intelligenten CCTV-Systemen zum Einsatz kommen kann, die dann etwa „lernen" was normales bzw. auffälliges Verhalten ist und so u.U. die Alarmschwellen eigenständig justieren könnten.

32 Wobei der Begriff *Sachzwang* nicht missverstanden werden sollte, da diese Zwänge z.B. sozial oder mindestens in soziotechnischer Wechselwirkung verursacht werden. Technik entsteht nicht aus dem Nichts und deshalb sind Sachzwänge immer auch ein Stück weit als sozial zumindest hingenommen (wenn nicht als bewusst hergestellt) zu sehen.

eingreifen, in zwischenmenschlicher Interaktion individuell und fallspezifisch angesprochen werden zu können, weshalb sie so insgesamt eher für ein höheres Sicherheitsempfinden sorgen – Technik wird demgegenüber als pauschaler (totalitärer) aufgefasst, als nicht in der Interpretation, sondern in der Reichweite von Überwachung überlegen und als billiger.

In Nuce:
Personen könnten helfen, seien aber teuer –
Technik sei billiger, nutze aber nur bedingt.

2.1.2 Beurteilung technischer Merkmale

Bezüglich des Technisierungsgrades der im Entstehen befindlichen Sicherheitslösungen waren neben Aspekten des Mensch-Technik-Verhältnisses konkrete Gestaltungs- und Funktionsmerkmale der beteiligten technischen Elemente von zentralem Interesse der Teilnehmer. Die Einschätzung einzelner Merkmale – wie etwa biometrischer Erkennungssoftware, Kameraauflösung etc. – lassen sich wiederum anhand ihres Effektes auf die perzipierten Handlungsmöglichkeiten eher mit einem höheren bzw. niedrigeren Sicherheitsempfinden korrelieren.

2.1.2.1 Sichtbarkeit technischer Elemente

Das Standarditem zur Messung von Kriminalitätsfurcht aus den 1960ern[33] fragt nach dem Sicherheitsempfinden bei Bewegung (spazieren) im öffentlichen Raum (Straße) bei Dunkelheit, also z.B. „Wie sicher fühlen Sie sich, wenn Sie nachts alleine nach Hause gehen?“ Die Straßenbeleuchtung hat einen Einfluss auf die Sichtdistanz, in der potenzielle Gefahren wahrgenommen werden könnten und damit auf den Zeitraum und also die Möglichkeit adäquat auf eine solche reagieren zu können, sei es durch Vermeidung (Wechseln der Straßenseite) oder sonstige Vorbereitungen. Die Sicht und Sichtbarkeit

33 Vgl. etwa Kreuter 2002, S. 47.

ist also direkt korreliert mit der eigenen Handlungsmöglichkeit, weshalb Dunkelheit meist als verunsichernd empfunden wird und das erwähnte Item nach einer Situation in relativer Dunkelheit fragt.

Wie sich in den Workshops gezeigt hat, kann der Konnex von Sicht und Sicherheitsempfinden erweitert werden auf Information und Sicherheitsempfinden, was nahe liegt, ist Sichtbarkeit doch das Vorhandensein von (visuellen) Informationen. So wurden viele Merkmale bezüglich Gestalt und Funktionalität der Elemente möglicher Sicherheitslösungen in zweifacher Hinsicht bezüglich ihres Verhältnisses zu Informationen bewertet; a) – wie im o.g. Itembeispiel – bezüglich der Sichtbarkeit von potenziellen Gefahren und b) bezüglich der eigenen Sichtbarkeit für das jeweilige Sicherheitssystem.

Dabei scheint zunächst im Fall von a) zu gelten, *je höher Sichtbarkeit bzw. je besser die Informationsbasis ist, desto höher ist das Sicherheitsempfinden*. Hierauf Verweisen geäußerte Forderungen, wie nach der prinzipiellen Sichtbarkeit, gute Erkennbarkeit und Identifizierbarkeit von Drohnen, aber auch die Forderung nach adäquaten Hinweisen von überwachten Zonen wie die bekannten Zeichen der Videoüberwachung. Hinzu kam jedoch die Forderung entweder nach zusätzlicher oder bei Bedarf zusätzlich abrufbarer Information über Zweck, Betreiber, Speicherdauer usw. des Überwachungseinsatzes, sei es bei fester (CCTV) oder mobiler (UAV) Videoüberwachung. Bezüglich der Gestalt der technischen Elemente ergibt sich so eine Tendenz zur Ablehnung gegenüber unsichtbarer Überwachungstechnik wie **biomimetische Drohnen**, versteckte oder nicht hinreichend ausgewiesene Kameras und erst recht gegen jegliche Form von Spionagetechnik, wie Knopflochkameras etc. Minimalbedingung für die Akzeptanz von zivilen Drohnen waren auf der Gestaltungsebene entsprechend Sichtbarkeit/ Hörbarkeit und Identifizierbarkeit etwa durch klare Kennzeichnung mit Nummernschildern, Warngeräuschen, Blaulicht (im Falle von Polizeidrohnen) etc. An die Forderung der **Identifizierbarkeit** wurde die Hoffnung geknüpft, sich an offizieller Stelle (Betreiberwebsite o.ä.) über Autorisierung, Zweck etc. jeweiliger

Sichtbarkeit von Kameras

„Bei der Überwachungstechnik ist auch schon die Pflicht da, dass das angekündigt ist im öffentlichen Raum, dass das auch wirklich nur im öffentlichen Raum stattfindet. Weil es mittlerweile schlecht markiert ist. Wenn ich jetzt auf einen Platz gehe, sehe ich nicht sofort: Okay, da ist Videoüberwachung. Da hängt irgendwo in fünf Meter Höhe ein Schild "Vorsicht Videoüberwachung mit Drohneneinsatz". Privat geht so etwas überhaupt nicht und wenn es der Staat einsetzt, dann muss das eine Zweckgebundenheit haben.“

Drohnen informieren und gegebenenfalls Beschwerde einlegen zu können. Beides kann als Mindesthandlungsspielraum gegenüber Überwachungstechnologien angesehen werden, denen man prinzipiell passiv ausgesetzt ist. Sollte selbst eine Identifizierbarkeit nicht gewährleistet werden können, bleibt als Letzthandlungsmöglichkeit die Meidung der überwachten Zonen (bei CCTV) oder das aktive Umgehen bzw. Ausweichen vor Drohnen. Bedingung für letzteres ist mithin die **grundsätzliche Wahrnehmungsmöglichkeit** von Kameras an Gebäuden und Drohnen. Fehlt es an erkennbaren Informationen über die eingesetzte Technik bzw. an Transparenz über den Einsatzzweck und den geplanten Umgang mit den erhobenen Daten oder auch nur an der Möglichkeit, eine überwachungstechnische Einrichtung als solche zu erkennen, so wird dies als ein Verlust an informiertem Handlungsvermögen wahrgenommen.
Angesichts der technologischen Entwicklungen wie Nanodrohnen (allg. Miniaturisierungstendenzen) und die Massenverfügbarkeit von Kamera- bzw. Drohnentechnologie (iPhone steuerbare Spielzeugdrohnen/ Modellflugzeug-Drohnen Bausätze etc.) wird der Gewährleistung der grundsätzlichen Sichtbarkeit und Identifizierbarkeit von Überwachungstechnologien nicht vertraut. Die Konsequenz aus diesem **prinzipiellen Misstrauen**, das sich in der Diskussion schließlich durchsetzte war die Forderung eines prinzipiellen Verbots von z.B. Drohnentechnologie zumindest für private, also nicht staatlich/richterlich autorisierte Zwecke.

Resümierend lässt sich sagen, dass daher nichtsichtbare aber als vorhanden angenommene, sichtbare aber nicht identifizierbare und identifizierbare aber nicht zu „entkommende“ Sicherheitstechnik nicht nur keine Erhöhung des Sicherheitsempfindens bewirken, sondern im Gegenteil ihrerseits verunsichernd wirken und zwar nicht zuletzt deshalb, weil sie keine adäquaten Handlungsmöglichkeiten der überwachten Subjekte zulassen. Andersherum: wenn die Elemente möglicher Sicherheitslösungen so gestaltet werden, dass sie betroffenen Bürgern adäquate Handlungsmöglichkeiten eröffnen (oder zumindest suggerieren) – z.B. Verhaltensanpassung, Be-

Sichtbarkeit und Handlungsmöglichkeit

„In dem Fall, wenn ich sehe, über mir fliegt etwas, das könnte jetzt ein Bild von mir beispielsweise erfassen, dann könnte ich mich eigentlich sogar noch schützen im Sinne von vermummt sein, sage ich jetzt mal. Ich könnte meine Handlungen so darauf abstimmen, dass nichts von mir erfasst wird, was ich nicht möchte. Aber in dem Fall, in dem ich dann nicht merke, dass da eine Drohne fliegt und es wird irgendwas von mir erfasst, da finde ich den Gedanken daran sogar viel, viel schlimmer, weil ich dann eben nicht dementsprechend handeln kann.“

Ablehnung privater Drohnen

„Wenn die [Drohne] von einer Privatperson gestartet worden ist, habe ich keine reelle Chance denjenigen zu finden, der dahinter steckt. Im Umkehrschluss – Sie haben das gerade schon mal zwischendurch eingeworfen – heißt das für mich, dass Drohnen im privaten Sektor nichts verloren haben. Das ist jetzt so eine Meinung, die sich bei mir innerhalb der Diskussion gebildet hat – [dass die] komplett verboten werden [sollten]. Dass Drohnen frei erhältlich sind für solche [private] Zwecke. Über Polizeieinsatz, über solche Veranstaltungen [hier: Stadtfestivals] kann man reden, das sind Institutionen, die das machen können. Aber dass sich jede Privatperson so eine Drohne kaufen kann und damit Informationen sammelt, das finde ich gefährlich.“

schwerde, Vermeidung –, dann werden sie tendenziell weniger als Sicherheitsrisiko bzw. Quelle der Verunsicherung wahrgenommen; ob sie zu mehr Sicherheit beitragen, ist damit nicht gesagt.

Die Geltung des mit dem Standarditem angesprochenen „höhere Sichtbarkeit möglicher Gefahren = höheres Sicherheitsempfinden“ ist vor dem Hintergrund der Ergebnisse der Workshops zweifach zu relativieren: erstens bezog sich die Sichtbarkeit nicht auf potenzielle „Übertäter“, sondern auf die technischen Elemente selbst, die als Sicherheits*lösung* proklamiert werden. Sicherer fühle ich mich demnach nicht, wenn ich durch Drohnen die dunkle Straße vor mir weiter und besser einsehen kann, sondern wenn ich die Drohne selbst sehen und identifizieren kann. So ist im Fall von Videoüberwachung durch CCTV oder Drohnen einerseits nicht die *Sichtbarkeit potenzieller Gefahren* im Fokus, sondern die *Sichtbarkeit der technischen Elemente als potenzielle Gefahr.* Dieser Fokuswechsel lässt den Nutzen sowie die Akzeptabilität besagter Sicherheitslösungen äußerst fragwürdig erscheinen. Es bleibt das angenommene und auch in den Workshops breit diskutierte Kostenargument (für Technik), wonach jedoch die sogenannten Sicherheitssysteme eher als Kostensenkungssysteme verhandelt werden müssten.[34]

2.1.2.2 Sichtbarkeit betroffener Bürger

Andererseits wurde verstärkt die Perspektive b) eingenommen, bei der die eigene Sichtbarkeit *für* das Überwachungssystem im Fokus steht. Hier scheint das Gegenteil zu gelten, nämlich: *je geringer die eigene Sichtbarkeit für ein System eingeschätzt wird, desto größer scheint das perzipierte Sicherheitsempfinden*. Unter dem Aspekt der „Sichtbarkeit für

---

34 Ähnliches legt eine Untersuchung von Karsten Weber et al. über die Einführung von eHealth-Pflegesystemen (Health-Monitoring-Systeme) nahe, die als Sicherheitserhöhung propagiert werden, allerdings vermehrt Unsicherheiten erzeugen und so schließlich als Kostensenkungs- bzw. als (nach ökonomischen Kriterien gesehen) Effizienzerhöhungssysteme erscheinen. Vgl. Weber et al. 2012.

das Überwachungssystem“ wurden Gestaltungs- und Funktionsmerkmale angesprochen, die sich auf die Bereiche Datenschutz, Reichweite und Eindringtiefe beziehen.

So ergeben sich in Zusammenhang mit der Forderung, keine Individuen, Menschen nur in der anonymen Masse und am besten nur Objekte und Infrastrukturen zu überwachen (mehr dazu → 2.2) auch konkrete Anforderungen an Gestalt und Funktionsumfang entsprechender Elemente.

Überwachungstechnik könnte nach Meinung der beteiligten Bürger mit hochgeschätzten Grundrechten und Rechtsprinzipien von Demokratien kollidieren. So wurden Bedenken geäußert, der (vermehrte) Einsatz von Überwachungstechnik – selbst im autorisierten Falle durch den Staat – könne zu Einschränkungen des Rechts auf **Versammlungsfreiheit** nach Artikel 8 GG, zu Verletzungen der Unverletzlichkeit der Wohnung (Artikel 13, (1) GG) oder zu einer schleichenden Erosion der grundsätzlichen Unschuldsvermutung (Artikel 11, (1), Allg. Erklärung der Menschenrechte) führen. Zumindest dem Anspruch nach wurde in den Workshops mit dem Recht auf Versammlungsfreiheit die Forderung nach theoretischer Anonymität bzw. Schutz vor unbegründeter Überwachung und Erfassung durch den Staat verknüpft, da – so der Gedankengang – die individuelle Identifikation und Speicherung der Verknüpfung von Person und Versammlung als Einschränkung dieser Versammlungsfreiheit gesehen werden kann. Hier kommt die Annahme einer Unverträglichkeit von Freiheit mit Überwachung zum Ausdruck. Entsprechend wurde gefordert, Überwachungskameras (v.a. von Drohnen) dürften keine Einzelpersonen identifizieren. Diesbezüglich wurde auch ein gewisses Misstrauen selbst staatlichen Betreibern gegenüber geäußert, was in der Forderung von ***privacy by design*** mündete, der Forderung also, dass Drohnen rein technisch nicht in der Lage sein dürften, auf individueller Ebene Personen zu erkennen. Dahinter stand der implizite Verdacht, dass Videoaufnahmen die dies zuließen u.U. doch oder „heimlich“ oder von Nichtautorisierten (Hackern) auf individueller Ebene ausgewertet würden.

Versammlungs- als Überwachungsfreiheit

„In der Studie [nicht genauer benannt] wird sogar gegeneinander diskutiert, dass das Grundrecht auf zum Beispiel Versammlungsfreiheit unüberwacht, also im Vertrauen auf nicht überwachte Versammlung, stattfinden muss. Der Staat hätte sogar die Pflicht, das Recht zu garantieren, dass sich die Leute im Vertrauen auf Nicht-überwacht-Werden versammeln können.“

Privacy by design

„Überall wo es unbedenklich für Menschen ist, kann man das [Drohnen] einsetzen. Bei Großveranstaltungen, wo keiner mehr erkennbar ist, muss [das] aber auch technisch gewährleistet sein, durch schlechte Kameras zum Beispiel, das wäre was anderes.“

Die Forderung nach „Privacy durch schlechte Kameras“ verweist auf einen grundsätzlichen technikphilosophischen Aspekt, der als das *Überschießen der Mittel*[35] angesprochen werden kann, die Tatsache nämlich, dass Technik immer zu mehr taugt, als wozu sie hergestellt wurde.[36] Daraus resultiert (bei teuren Systemen auch aus Amortisationsgründen) ein Druck, die vorhandenen Möglichkeiten zunehmend auch auszunutzen. Zu den „vorhandenen Möglichkeiten“ zählen nicht nur gegenwärtige, sondern auch angelegte und zukünftig mögliche. So können gesammelte Daten nicht damit „unkritisch“ gemacht werden, dass fehlende Auswertungsmöglichkeiten in Anschlag gebracht werden. Dies zeigt deutlich die enormen Massen an Bildern im Internet, bei denen es bislang unmöglich war (nicht manuell vertaggte) Personen gezielt zu finden; mit der Möglichkeit von Gesichtserkennungssoftware werden *alle* Bilder individuell durchsuchbar, nicht nur diejenigen, die im Bewusstsein der Möglichkeit von Gesichtserkennung aufgenommen wurden.[37] Damit gehören die Aspekte der Datenerhebung, gegenwärtigen sowie potenziellen zukünftigen Datenverarbeitung und –auswertung auch in der Einschätzung betroffener Bürger zum integralen, akzeptabilitätsrelevanten Bestandteil von Sicherheitslösungen. Diese Einsicht geht über die Forderung bloßer Datensparsamkeit kate-

---

35 Vgl. Hubig 2002.

36 So kann auf einem Amboss freilich geschmiedet werden, er kann aber auch klingen, etwa in Wagners Rheingold oder Parlowschen Polka für Solo-Amboss.

37 Ähnliches gilt für unzählige „Geruchsproben“, die die Grenzsicherung der ehemaligen DDR für den Einsatz von Spürhunden in den 1970er Jahren gesammelt hat (vgl. DIE ZEIT unter http://www.zeit.de/wissen/2010-12/stasi-duftarchiv, DER SPIEGEL 23/1991 sowie SPIEGEL SPECIAL 1/1996 unter http://www.spiegel.de/spiegel/print/d-13487518.html bzw. http://www.spiegel.de/spiegel/spiegelspecial/d-8870325.html). Unter veränderten technologischen Bedingungen, wie beispielsweise der Genanalyse, können in solchen Proben vorhandene „Überschussinformationen“ zu weiteren Zwecken, quasi als Genprobendatenbank, genutzt werden, als ursprünglich beabsichtigt. Der Dresdner Informatiker Pfitzmann (2006) benennt weitere Beispiele für grundsätzliche Sicherheits- und Datenschutzprobleme durch Biometrie.

gorial wie zeitlich weit hinaus. Relevant ist nämlich nicht nur die Sichtbarkeit für jetzige, sondern auch für zukünftige Systeme.

Vor dem Hintergrund des Gesagten ist direkt ersichtlich, dass und warum sich die Bürger in den Workshops **gegen** die Implementierung von **biometrischen Funktionen** ausgesprochen haben, da diese dezidiert der Identifizierung von Individuen dienen.

2.2 Rahmenbedingungen/ Einsatzsituation

Die Bewertung verschiedener Sicherheitslösungen hing neben dem Technisierungsgrad, der konkreten Gestalt und den Funktionsmerkmalen besonders vom Verhältnis von Sicherheitslösung und Einsatzbedingungen bzw. von Konstellation und Situation ab.

Wurden nicht sichtbare Kameras/ Drohnen mit biometrischen Erkennungsfunktionen von den Bürgern mehrheitlich als verunsichernd abgelehnt, was sich gemäß der hier in den Vordergrund gerückten Hypothese, aus einer damit einhergehenden Einschränkung der Handlungsmöglichkeiten verstehen lässt, so wurde der Einsatz von Drohnen in anderen Situationen als durchaus akzeptabel und als Sicherheitsgewinn bewertet. Ebenfalls gemäß der zu prüfenden Hypothese waren dies vornehmlich Bereiche, in denen zunächst keine Menschen betroffen und wenige Handlungsmöglichkeiten eingeschränkt werden.

So stellte sich ein gewisses Akzeptanzgefälle bezüglich des **Überwachungsgegenstandes** heraus: am ehesten akzeptiert waren die Überwachung von technischen Infrastrukturen wie Strom- oder Gasleitungen, Industrieanlagen, Deichanlagen etc. Anonyme Menschenmassen wie Publikumsströme bei Großveranstaltungen zu überwachen, um diese ordnend zu lenken (Steuerung von Menschenströmen, Vermeidung von Personenstaus und „Stampedes“, Hinleiten von Notärzten zu Unfallstellen) galt unter Umständen (keine/kurze Speicherzei-

Überwachung von Infrastruktur vs. Personen

„C: Wenn ich als Energieunternehmen meine Stromleitungen mit dem Teil abfahre oder meine Gasleitungen mit irgendwelchen Gassensoren, solange diese Zweckgebundenheit [einer Drohne] da ist, interessiert es ja keinen. Wenn ein Gassensor dran ist, dann kann mir das ja egal sein.
A: Und zur Sicherheitsgewährleistung in der Nachbarschaft? Wenn ein Schmetterling [eine biomimetische Drohne dieser Form] im Vorgarten…
C: Nein. Das sollte auch juristisch unterbunden werden.
A: Würden Sie darauf vertrauen, dass man Sie darüber aufklären würde?
C: Ja, ich vertraue darauf, dass der Staat entsprechend Gesetze macht.“

„Man beurteilt es vielleicht auch aus der Vogelperspektive ein bisschen objektiver. Auch das Hinleiten von Rettungskräften ist natürlich ungleich einfacher. Ich kenne keine Veranstaltung, wo es ohne diese Luftaufnahmen überhaupt noch geht – nicht ab einer gewissen Größe.“

ten, Safety der technischen Elemente, Transparenz des Einsatzes) als akzeptabel. Keine Akzeptanz fand die Überwachung von Einzelpersonen.[38]

Die negativen Effekte auf das Sicherheitsempfinden von Überwachungstechnologie wurden in bestimmten Fällen gegen anderen Schaden abgewogen; so galt der Einsatz von Drohnen zur Verletztensuche und Lageanalyse bei konkreten Katastrophenfällen durchaus als akzeptabel wie allgemein in Fällen konkreter Notfälle oder bei Gefahr im Verzug. Jeglicher Form gegenüber antizipativer Überwachung – wie sie beispielsweise unter dem Stichwort **Precrime** bekannt wurde – wurde starke Ablehnung entgegengebracht. Dies wurde u.a. mit langfristigen gesamtgesellschaftlichen Effekten eines verbreiteten Einsatzes von Überwachungstechnologie begründet (→ Abschnitt 2.3).

Auch die grundsätzlich eher positive Einschätzung der Nutzung von Drohnen und anderen Technologien zur Überwachung von Objekten und Infrastrukturen wurde im Laufe der Diskussionen in Frage gestellt und im Ergebnis entscheidend relativiert bzw. an Forderungen nach Einbettung in eine solide Rechtslage und klare Rahmenbedingungen für einen „Wenn-überhaupt-Einsatz“ solcher Technologien gebunden.
Da Drohnen, die mit einem Gassensor ausgerüstet sind, sehr leicht und schwer kontrollierbar mit anderen Sensoren und Kameras ausgestattet werden können, liegt der Verdacht der Funktionserweiterung, der Zweckentfremdung, der Nutzung des Mittelüberschusses nahe, der die prinzipielle Akzeptanz der Nutzung zu einer Frage des Vertrauens macht. Privaten Anwendern und Unternehmen wurde hier kaum vertraut, weshalb die Regulierung und Kontrolle durch einen demokrati-

---

38 Als abschreckendes Negativbeispiel wurden die Vorhaben des EU-Forschungsprojektes INDECT angeführt. In einem Projektvorstellungsvideo zeigten Forscher von INDECT ein Szenario, in dem mittels mustererkennender „intelligenter“, vernetzter Überwachung in/an Gebäuden, von Drohnen etc. eine Person sogar (EU)grenzübergreifend identifiziert, verfolgt und schließlich in martialischer Manier gestellt wird. Vgl. hierzu mit weiteren Quellenangaben zu INDECT: http://de.wikipedia.org/wiki/Indect.

schen Rechtsstaat als zentral angesehen wurde. Selbst hier wurde ein grundsätzliches **Vollzugsdefizit** gesehen, also die Möglichkeit und Wirksamkeit staatlicher Kontrolle.
Nicht nur der Wechsel des *Was* der Kontrolle (Objekte, Menschen) wurde problematisiert, sondern auch der Wechsel des *Wer*: Selbst wenn die Rahmenbedingungen z.B. in Deutschland „vertrauenswürdig" seien, sei nicht auszuschließen, dass die „technischen Meisterwerke" nicht auch in **totalitären Regimen** gegen die Bevölkerung oder zur Unterdrückung von Minderheiten eingesetzt würden. Das ‚Wer' der Überwachung ist, aus Gründen fehlender Kontrollmöglichkeit, also Gegenstand des Vertrauens, das über delegierte Kontrolle durch eine vertrauenswürdige Instanz (Rechtsstaat) gewonnen wird. Dieses Vertrauen ist individuell sehr unterschiedlich ausgeprägt. Einige Teilnehmer äußerten ein grundlegendes Misstrauen in die Exekutivorgane selbst des deutschen Rechtsstaates, weshalb sie konsequenterweise *jeglicher* Überwachungstechnologie ablehnend gegenüberstanden.

Als Minimalkriterien für einen „Wenn-überhaupt-Einsatz" von zukünftigen Sicherheitslösungen bezüglich der Rahmenbedingungen und Einsatzsituation wurden genannt:

- der Anlass eines konkreten Schadens-/ Notfalles wie z.B. MANV-Fälle[39]/ Katastrophen[40]
- Datenminimalismus, Transparenz im Umgang mit Daten
- Datensicherheit (Einhaltung von Datenschutzgesetze[41], sichere Löschvorgänge und eingeschränkte Datenaufbewahrung, Hackerschutz etc.)
- autorisierte Instanzen (Polizei unter Einbeziehung eines Richters)

Vollzugsdefizite

„Ich bin auch eher deiner Meinung zu sagen: Nein, überhaupt gar nicht. [...] Oder, dass die ein Peilsignal aussenden müssen, dass sie sich identifizieren, sage ich jetzt mal, entweder durch ein Piepgeräusch oder irgendwie so was. Aber ich befürchte, das ist nicht umsetzbar…"

„Da ist dann auch fraglich, wie kontrolliert man den privaten Einsatz. Also, es ist sehr schwer überprüfbar."

Missbrauch der Technik

„Ich persönlich finde, in solchen praktischen Fällen wie Feuer ausbrechen ist es ja ganz okay. Aber ich befürchte natürlich auch, dass solche technischen Meisterwerke auch in irgendwelche Länder ausgeführt werden, Syrien oder sonst irgendwie, die damit ganz andere Dinge im Sinn haben wie Feuerausbruch oder sonst was, also, die das ganz anders einsetzen. Diese Befürchtung habe ich natürlich auch."

---

39 MANV steht für Massenanfall von Verletzten.

40 Vgl. etwa das Schwarmdrohnen-Projekt zum „Schutz kritischer Infrastrukturen" (etwa zur Aufklärung bei Chemieunfällen) "AirShield": vgl. Website: www.bmbf.de/pubRD/AirShield_Daniel_Auftakt_IPF_SuRvM.pdf.

41 Gleichwohl ist das AirShield-Projekt nicht unumstritten und bei einer Präsentation bei der Langen Nacht der Wissenschaft an der TU Berlin am 13.06.2009 fand eine Protestaktion von Bürgern als „antimilitaristische Aktion" statt: vgl. Website: http://lndw.tu-berlin.de/lndw09/course/view.php?id=1187.

- Transparenz des Anlasses[42] sowie Zweckgebundenheit des Einsatzes
- minimale Vernetzung verschiedener Daten und Überwachungskanäle (zur Verhinderung von flächendeckender Rasterfahndung mit daraus resultierendem „Generalverdacht“)

Zu den beiden oben genannten Verhältnissen von Sicherheitsempfinden und Information (bspw. unter der Metapher der Sichtbarkeit) ist der Sichtbarkeit von möglichen Gefahren (a) und der eigenen Sichtbarkeit für das jeweilige Sicherheitssystem (b) noch die Sichtbarkeit des Systems für den Bürger (c) zu nennen. Viele Forderungen an zukünftige Sicherheitslösungen lassen sich unter dem Aspekt der Sichtbarkeit (c) subsummieren: Hinweisschilder, „Drohnennummernschilder“ in Verbindung mit Auskunftsstellen über betreibende und steuernde Instanz, Datenerhebung, -verarbeitung und -speicherung, Legitimität, Zweck, Ausmaß und Anlass der Überwachung, dies sind alles Informationsaspekte der Sichtbarkeit (Transparenz) des jeweiligen Systems. Bei der Sichtbarkeit des Systems gilt nicht: je sichtbarer, desto höher das perzipierte Sicherheitsgefühl. Denn sichtbare Sicherheitsmaßnahmen (seien es Wachpersonal, Videokameras, Stacheldrahtzäune, Drohnen oder gar Polizeiaufmärsche) *ohne* gleichzeitige Information über Zweck und Anlass der Maßnahmen führt nicht zu einem höheren, sondern zu einem geringeren Sicherheitsgefühl, da die Sicherheitsmaßnahmen ihre eigene Notwendigkeit suggerieren. Wird über diese Notwendigkeit nicht sachbezogen informiert, wird der Informationsmangel mit einer diffusen Bedrohung ersetzt. Sichtbare Sicherheitstechnik etwa, verweist nicht nur als Zeichen auf eine nicht sichtbare Gefahr, sondern stellt ihrerseits wieder ein eigenes Sicherheitsrisiko dar (z.B. durch Fehlfunktionen oder Fehlsteuerung).

---

42 Die recht hohe Akzeptanz von Überwachung bei Großveranstaltungen rührt wohl von der (zumindest präsumierten) großen Transparenz des Einsatzzweckes wie Leitung von Rettungskräften, Vermeidung von Publikumsstaus und Prävention vor Massenpaniken.

In der Summe lassen sich diese Forderungen der Teilnehmer auf die einfache Formel des ***Sehens, ohne gesehen zu werden*** bringen, eine Situation, die nicht zuletzt in militärischen Kontexten schon immer als sicher empfunden worden sein dürfte. Die Formel im hiesigen Kontext expliziert hieße: Überwachungstechnik muss erkennbar sein (keine Nanodrohnen und Knopflochkameras), sie muss auf sich aufmerksam machen (Hinweisschilder), sich ausweisen (Nummernschilder), sich erklären (zumindest auf Nachfrage) – d.i. *Sehen* –, während die Bürger ein Recht auf unüberwachte Versammlung geltend machen und sich jederzeit den überwachten Bereichen entziehen können müssen – *ohne gesehen zu werden*. Entsprechend wurden etwa in Workshop 3 zu Sicherheitsanwendungen im Web2.0 im Kern unterschiedlichste „**Informationsdienste**“ entworfen, die ebenfalls dieser Formel folgen.

Auf Aspekte dieser Formel wird jedoch umso mehr beharrt, je technisierter die diskutierten Sicherheitssysteme sind. Menschen gegenüber gilt das Gesehen-, das Wahrgenommen- und Berücksichtigt-, vielleicht sogar Gegrüßt-Werden als Teil der soziokulturellen Anerkennung und Selbstvergewisserung, die im sozialen Umgang erheblich zur Erhöhung des Sicherheitsempfindens beitragen. Menschen fühlen sich bei prinzipieller Symmetrie des Blickes wohler[43], weil das gesehen werden wiederum gesehen werden kann[44], was die Möglichkeit eröffnet, adäquat zu handeln. Asymmetrie des Blickes, der Beobachtung oder Überwachung, nimmt dem einseitig Beobachteten Handlungsmöglichkeiten und senkt somit dessen Sicherheitsempfinden; das diffuse Gefühl, beobachtet zu werden verunsichert.[45]

Sehen, ohne gesehen zu werden

„Das ist auch eine, ich sage mal, Option des Internets. Nämlich das Gefühl der Sicherheit in der Anonymität. Wenn ich meinen Wunsch äußere, dann äußere ich ihn erst mal anonym gegenüber einer Vermittlerstelle. Das ist positiv, es kann aber auch negative Auswirkungen haben. Zum Beispiel die ganzen Mobbingdiskussionen, die aus der Anonymität heraus entstehen. Aber der erste Schritt ist getan, für mich; das persönliche Sicherheitsgefühl: „Ich muss erst mal nicht so viel preisgeben“. Jedenfalls nicht aktiv preisgeben. Was ich passiv preisgebe, allein durch die technische Kontaktaufnahme mit der Stelle, das realisiere ich ja erst gar nicht mal so.“

„Und da ist mir aufgefallen, es wird gut aufgenommen, dass man von sich wenig Infos preisgeben muss, also niederschwellig, und bleibt relativ anonym oder eigentlich überhaupt anonym und kriegt aber konkret Informationen, also bedarfsorientiert.“

43 Vgl. Rammert 2002.

44 Vgl. zu dieser Beobachtung zweiter Ordnung etwa: Luhmann 1997.

45 Für dieses Gefühl stehen Topoi der allessehende und später oder auch sofort strafende Gott, seine literarische maligne Variante Sauron (Lord of the Rings) oder Orwells überwachungstechnischer „Big Brother“.

2.3 Gesellschaftliche Effekte und allgemeine Lebensqualität

Entsprechend der verunsichernden Wirkung einer anzunehmenden aber nicht wahrnehmbaren und nicht identifizierbaren Beobachtung bzw. Überwachung machten die Teilnehmer für den präsumierten Fall heimlicher und v.a. hochtechnisierter Überwachung eine Reihe von negativen gesellschaftlichen Wirkungen geltend.

Da technische Mustererkennung nicht neutral „tatsächliche Notsituationen“ oder „auffälliges Verhalten“ erkennen kann, denn Auffälligkeit ergibt sich stets in Relation zur jeweiligen Normalitätsauffassung, instanziieren technische Systeme mit „intelligenter Mustererkennung“ die ihnen zuvor eingeschriebenen Konzepte. Wenn also intelligente Überwachungssysteme mit technischer Mustererkennung automatisiert „Auffälliges“ detektieren, dann führe dies auf lange Sicht dazu, dass sich eine Verhaltensangleichung der Bürger an die Normalitätskonzepte des Systems entwickelt, was zu einer „fürchterlichen Einheitsgesellschaft“ führe.

Andererseits wird eine **Verhaltensschere** befürchtet, dass also neben der zunehmenden Normalisierung, um nicht ‚sicherheitssystemrelevant‘ zu werden, sich eine Tendenz zu extremeren Verhaltensweisen zeigt, wie sie teilweise vor Videoüberwachungskameras stattfindet. Die Kamera erzeugt, so die Ansicht, einen gewissen performativen Druck, bei ohnehin gegebenem Gesehen-Werden wenigstens auch sehenswürdig zu sein.

Durch diese Spreizung von Verhaltensweisen wird angepasstes und "normales" Verhalten tendenziell in seinen Aktionsmöglichkeiten weiter eingegrenzt, was wiederum als Indiz für eher niedrigeres Sicherheitsempfinden verstanden werden kann. Weiter vermuteten die Teilnehmer vor diesem Hintergrund, dass die Verhaltensnormierung, die wenigstens als Verbrechensvermeidung noch positiv geltend gemacht werden könnte, gerade nur auf „Normalbürger“ wirkt und Kriminelle so oder so mit Gegentechnik, Umgehungsstrategien, Verbre-

Fürchterliche Einheitsgesellschaft

„‘Ich habe mir nichts vorzuwerfen‘ – dieses Argument zählt insofern nicht, denn wer definiert denn, wann ich mir was vorzuwerfen habe und wann nicht, also es wär‘ ja schrecklich, wenn es immer so gelaufen wär‘, wir wären dann noch im Kaiserreich oder sonst was, oder in irgendwelchen anderen Sachen hängengeblieben wenn es immer so fortlaufen würde. Es käme niemals zu neuen Ideen es wär‘ ja eine fürchterliche Einheitsgesellschaft. Es wär fürchterlich.“

„Genau, es geht eigentlich wirklich mehr darum, dass man halt Sachen, die egal sind, macht, die aber auffällig sind, weil sie außergewöhnlich sind. Und wenn ich auf der Straße anfange zu tanzen, diese Freiheit will ich halt haben, aber es wird halt für ein intelligentes Überwachungssystem, immer auffällig sein.“

Verhaltensschere durch Überwachungstechnik

„U: Die, die nichts getan haben, die machen weiterhin nichts, und die, die meinen, sie müssen immer den Kasper spielen, die machen weiterhin den Kasper und zwar noch extremer. Also...
G: Aber die anderen nehmen sich noch mehr zurück, obwohl sie ein bisschen aus sich rausgehen können.“

„Also ich persönlich hab‘ auch eher den Eindruck, bei den Leuten, die sich eher sowieso normal verhalten, bei denen hat es wahrscheinlich einen größeren Einfluss, wenn da jetzt noch Kameras sind. Die verhalten sich vielleicht noch angepasster. Dagegen, wenn jetzt jemand wirklich vorhat, irgendwie was Kriminelles zu begehen, dann findet der auch Wege so Sachen zu umgehen und lässt sich dadurch dann auch nicht unbedingt so beeinflussen.“

chensverlagerung oder gar mit einer gesteigerten Radikalisierung ihrer Handlungen agieren.

Neben dieser Normierung bzw. Radikalisierung von Verhalten auf gesamtgesellschaftlichem Niveau wird die Sorge geäußert, dass durch die Präsenz von hochtechnisierten und weitverbreiteten Sicherheitssystemen die persönliche Verantwortung als Mitglied der Gesellschaft und Bürger im öffentlichen Raum an die Sicherheitslösungen delegiert wird. Dies ist für eine schnelle und aktive Hilfe im konkreten Notfall fatal, da wie oben erwähnt, den diskutierten Sicherheitslösungen nur eine passive Funktion zugesprochen wird. Ähnlich dem bekannten Effekt, bei dem Personen in einer Notsituation umso weniger helfen, je mehr Personen anwesend sind[46], wird so befürchtet, dass die Verantwortungsdelegation an technische Systeme (die dieser Delegation in keinster Weise gerecht werden können) etwa zum zunehmenden Verschwinden von Zivilcourage führe.[47] Sicherheitstechnologie stellt keine Alternative zu individueller sozialer Verantwortung dar und wird dort zum Problem, wo sie die soziale Kohäsion erodiert. Im Notfall ist der Mitbürger immer schneller an der Unfallstelle als jede noch so intelligent zum Unfallort geleitete Rettungseinheit.[48]

Sicherheitstechnik vs. Zivilcourage

„So Kameras führen aber jetzt unserer Meinung nach zu dem Problem, dass die Verantwortung abgegeben wird. Wurde vorhin auch schon erwähnt. Sprich, die Zivilcourage lässt nach. Also vor lauter Kameras denkt sich jeder, naja, ich muss jetzt nicht mal handeln. Irgendjemand wird‘s schon sehen, irgendjemand wird schon was tun. Außerdem besteht ein scheinbares Sicherheitsgefühl, was letztendlich dazu führt, dass der Staat sich denkt, naja, wir können uns Personal einsparen.“

2.4 Kriminalitätseffekte

Die Wirksamkeit von sicherheitstechnischen Anwendungen, bezogen auf ihre proklamierte Funktion zur Abwehr von Gefahren und Aufklärung von Verbrechen wurde ambivalent bewertet. So wird die Tätermittlung und Fallaufklärung mit Hilfe von (intelligenter) Videoüberwachung für möglich und im Einzelfall nützlich gehalten, jedoch als nachrangig betrachtet, angesichts technischer und organisatorischer Schwierigkeiten wie fehfehlendem Personal, Überwachungslücken oder tech-

Kriminalitätsverlagerung und -radikalisierung

„Ja die Tat wird eigentlich meiner Meinung nach, also unserer Meinung nach, nicht unbedingt verhindert, sondern irgendwie verschoben. Also wenn ich jetzt dealen will, dann werde ich das nicht vor einer Kamera machen, sondern vielleicht irgendwo zu Hause oder um die nächste dunkle Ecke rum. Dann führt das vielleicht psychologisch gesehen noch dazu, dass der Täter gesehen werden will. Also es wird auch ganz toll in den Medien angezeigt. Das ist vielleicht auch eine Verantwortung, die Medien übernehmen sollten.“

46 Vgl. etwa Milgram 1970.

47 Als weiterer befürchteter gesellschaftlicher Effekt von verbreiteter Überwachungstechnologie wird die Erosion des Rechtprinzips der Unschuldsvermutung genannt. Vgl. dazu oben Abschnitt 2.1.2.2.

48 Vgl. zu dem daraus folgenden Nothilfe-Bildungsimperativ etwa: Ripley 2010.

nische Unzulänglichkeiten. Zu ersterem wird vermutet, dass sogenannte Sicherheitstechnik eigentlich Rationalisierungstechnik ist und der Kostenreduzierung v.a. bei Personal dient. Die Überwachungslücken wurden einerseits auf gegenwärtige Überwachung bezogen als Mangel angesehen, da sie es ermögliche, Kriminalität in diese Lücken zu verlagern. Andererseits wurden diese Lücken mit zukünftiger Perspektive auf hypothetisch lückenlose Überwachung als Refugien von Privatheit und Freiheit gesehen. Die technischen Unzulänglichkeiten sind ein irreduzibles Moment jeder, insbesondere komplexer Technikkonstellationen und somit nicht durch „bessere“ Technik vollends zu beheben (Normal Accidents).

2.5 Fazit

Die Teilnehmer ziehen zu ihrer Bewertung möglicher Sicherheitslösungen mit im Entstehen befindlicher Technologie sowohl die konkret beteiligten Elemente, als auch die Einsatzsituation und die jeweiligen Rahmenbedingungen der beabsichtigten oder zur Diskussion stehenden Sicherheitslösung heran. Dazu gehört konkret der Überwachungsgegenstand, die erhobenen Daten, deren Verarbeitung, Weiterleitung, Vernetzung und Speicherung, die überwachende Instanz bzw. der Betreiber der Systeme und die Eigenschaften der Person bzw. des Algorithmus „am Monitor“. Somit bestätigt sich der theoretische Ansatz, der Sicherheitstechnik als komplexe soziotechnische Konstellation auffasst, die über technische Aspekte hinaus, menschliche und vor allem auch organisationelle und andere gesellschaftlich-kulturelle Dimensionen einbezieht.

Neben diesen vielschichtigen und eher synchronen Aspekten wurden ebenso Perspektiven möglicher zukünftiger – durchaus langfristiger, über mehrere Innovationszyklen verlaufende – Entwicklungen berücksichtigt. Eine Beurteilung wird zwar primär aus selbst erfahrenen oder durch nahe Freunde, Familienangehörige o.dgl. berichteten Anwendungssituationen, die meist in lokale politische Kontexte eingebunden sind, ausgebildet. Doch lassen die Gruppendiskussionen auch erkennen, dass die Beurteilung von sicherheitstechnischen Anwendungen zudem an globalen politischen Ereignissen bzw. Problem-

lagen ausgerichtet ist. Diese werden meist in irgendeiner Form als medienvermittelte Information an das Individuum herangetragen, sie sind also seltener durch eigene Erlebnisse oder durch Berichte des nahen sozialen Umfelds qualifiziert. Viele ambivalente Bewertungen sicherheitstechnischer Konstellationen stützen sich insbesondere auf Berichte über sicherheits- und freiheitsgefährdende Technikeinsätze in nicht demokratischen Staaten, die vor allem kritische, ambivalente Einstellungen nähren und die abschließende Beurteilung einer Sicherheitslösung eher als einen offenen Prozess, denn als abgeschlossene Haltung erkennen lassen. In den partizipativen Workshops konnte miterlebt werden, mit welcher Wucht einzelne unmittelbaren Erfahrungen oder Argumente Einzelner, einen radikalen Einstellungswandel im Hinblick auf bestimmte Positionen bei anderen Teilnehmern hervorrufen könnten.

Die ausgiebigen Diskurse der Workshopteilnehmer zu den thematisierten Sicherheitslösungen – mit intelligenter Videokommunikation, Drohnen, Web 2.0-Techniken – gelangen insgesamt zu der Einschätzung, dass diese zumindest ambivalent, meist ehr als problematisch und mit Unsicherheitspotenzial behaftet angesehen wurden. Es ließen sich jedoch einige Bedingungen identifizieren, die „Wenn-überhaupt-Kriterien“ denkbarer Einsatzszenarien pointiert zusammenfassen (vgl. nachstehende Übersicht):

I. Was wird überwacht?	1. Objekte/ Infrastrukturen	Eher akzeptabel, wenn unter rechtsstaatlicher Kontrolle. Problem des Vollzugsdefizits und des Wechsels der Einsatzsituation (bspw. Diktaturen).
	2. Menschenmassen	Wie I.1., wenn keine persönliche Erkennung stattfinden kann, v.a. bei konkreten Anlässen (z.B. Loveparade) und unter vorauszusetzender Safety der technischen Elemente.
	3. Individuen	Nicht akzeptabel.

II. Wer überwacht?	1. Individuen (Privatpersonen)	Nicht akzeptabel (Paparazzi, Nachbarschafts-Späher usw.), außer u.U. in einem totalitären Regime als Gegenmittel gegen staatliche Repressionen bzw. Menschenrechtsverletzungen.[49]
	2. Private Institutionen (Firmen, Flughafenbetreiber,…)	Wenig akzeptabel. Nicht im öffentlichen Raum, nur in prinzipiell meidbaren Bereichen (Kaufhäuser, Bahnhöfe, …).
	3. staatliche Instanzen	Am ehesten akzeptiert, wenn Vertrauen in die delegierte Kontrolle hergestellt werden kann (richterlicher Beschluss, strenge Datenschutzgesetze, minimale Speicherdauer, rechtstaatliche Überwachung der Überwacher, Schutz vor Missbrauch etc.).
III. Wie wird überwacht?	1. rein technisch	Keine Akzeptanz (autonomer Technik), wegen des Problems technischer Eigenrationalität und fehlendem „gesunden Menschenverstand“ sowie der „Normal Accidents“ von Technik allgemein.
	2. menschliche Kontrolle im System	Menschen mit mindestens Letztentscheidungskompetenz im System sind ein Minimalkriterium („Wenn-überhaupt-Kriterium“), um Sicherheitslösungen mit einem solchen System überhaupt als Sicherheitsgewinn bewerten zu können.

49 Vgl. z.B. Witness: “Witness uses video to open the eyes of the world to human rights violations.” Witness.

So kann das Resümee gezogen werden, dass im Rahmen der durchgeführten Workshops die Lösung der Ursachen von Sicherheitsproblemen in den Vordergrund gerückt und als gesamtgesellschaftliche Aufgabe angesehen wurde. Der unmittelbare Umgang mit Sicherheitsproblemen erfordert nach Ansicht vieler Teilnehmer vor allem neue, alternative organisationelle Formen der Sicherheitsgewährleistung bzw. der Vermeidung von Unsicherheiten. Eine kritische Begleitung von Technisierungsprozessen wäre hierfür eine wichtige Maßnahme, mit der systematisch die Frage nach der Notwendigkeit und konkreten Ausgestaltung von Sicherheitskonstellationen und deren Folgewirkungen erwogen werden könnten. In diesem Kontext sollten auch Rechtsfragen in Bezug auf neue, im Entstehen begriffene Technologien frühzeitig geklärt und quasi „rechtsfreie Räume“ vermieden werden. Erhöhte Rechtssicherheit ist eine Voraussetzung für Handlungskompetenz der Beteiligten, die in den Untersuchungen als essentielle Rahmensetzung bestätigt wurde.

Nicht zuletzt sollte die Frage nach der gesamtgesellschaftlichen Relevanz der jeweiligen Sicherheitstechnik – unter Berücksichtigung möglicher gesellschaftlicher Kosten und Nutzen, d.h. langfristiger Folgewirkungen und nicht von möglicherweise nur kurzfristig auftretender Effekte Beantwortung finden.[50]

---

50 Vgl. hierzu auch Bornewasser, Manfred: Evaluation der Videoüberwachung: Ein Praxisbericht. Ergebnisse einer wissenschaftlichen Begleituntersuchung. In: Hempel/Metelmann 2005, S. 251 f.

3 Anhang

3.1 Anhang 1: Teilauszüge der Transkripte der partizipativen Workshops[51]

Bez.	*Stelle*	*Beispiel*
A1	WS 1; 162	„Mir ging es auch um den Punkt (..) Menschen die vorhaben zum Beispiel eine Bank auszurauben, werden Wege und Mittel finden diese Überwachung zu umgehen. Sie werden vielleicht Sicherheitsleute bestechen die mit der Überwachung zusammenhängen, dass zu dem Zeitpunkt die Drohne zufällig irgendwo anders hinguckt (..)
A2	WS 1; 192	„Wenn das eine materiale, also eine künstliche Intelligenz ist, die überwacht uns, wir trauen ihr einfach nicht.“
A3	WS 1; 17	„Nächster Punkt: Sicherheitsempfinden. Also, da war bei uns so die Meinung, naja, so richtig gesteigert wird das nicht durch die Kamera. Im Zweifelsfall haben wir uns gesagt, setzten wir uns lieber in die Nähe des Straßenbahnführers, als in die Nähe von so ner Kamera, weil der im Zweifelsfall dann doch noch direkt eingreifen kann. Mein, das ist eben auch so ein Punkt, so wie das momentan organisiert ist. Man kann ja nur rückwirkend irgendwie sich Sachen angucken, man kann nicht sozusagen in der unmittelbaren Situation eingreifen.“
A4	WS1; 14	„Diese Live-Auswertung, da muss man halt sagen, da ist das nicht der Fall. Also Ich meine, der Mensch der die Straßenbahn da steuert, der hat da nicht noch die Kontrolle von diesen ganzen Live-Bildern, sondern es wird halt irgendwie aufgezeichnet. Das wär dann mehr sowas, wenn man es anders organisieren würde. Ermittlung von Straftätern, da wäre es mal interessant mal wirklich konkrete Zahlen zu hören. Ich glaub mit der momentanen Technik sind halt viele Bilder dann doch zu schlecht um da wirklich Leute zu ermitteln.“
A5	WS1; 94	„Dann, das nächste ist, Aufklärung von Verbrechen. Hatte man ganz am Anfang einmal in der Straßenbahn und zwischendrin auch nochmal. Für nach der Tat, wobei da das System auch noch nicht komplett ausgereift ist, weil ich nicht immer die Kameraeinstellung so habe, dass ich die Täter erkennen oder identifizieren kann.“

51 Buchstaben und Nummern Spalten eins und zwei bezeichnen interne Codierungen; WS1,2,3 steht für Workshop 1, 2 oder 3

A6	WS1; 199	J: (wieder einen Kaugummi-Witz, mehrere lachen) „Genau, es geht eigentlich wirklich mehr darum, dass man halt Sachen, die egal sind macht, die aber auffällig sind, weil sie außergewöhnlich sind, Und wenn ich auf der Straße anfange zu tanzen, diese Freiheit will ich halt haben, aber es wird halt für ein intelligentes Überwachungssystem, immer auffällig sein. Und sowas geht halt einfach weg. Ob man es jetzt toll findet, dass es Leute machen oder nicht, darüber kann man...es mag sicher Leute geben, die finden es ist auch blöd, und das sollen die Leute nicht machen. Aber ich leb in einer Welt, wo ich halt nicht, wenn ich einfach irgendetwas Außergewöhnliches mache, pauschal verdächtigt werden will.“
A7	WS 1, 197	„Dass immer schrittchenweise kleine Dinge eingeführt werden, damit sich der Bürger nicht so sehr daran aufstößt. Zum Beispiel, ok, da hängt jetzt ne Kamera, die zeichnet nur Koffer auf, die über 20 Minuten an einem Fleck stehen, und nach zwei, drei Jahren, wenn sich jeder daran gewöhnt hat, kommt der nächste Politiker und sagt, wir haben da jetzt schon Kameras hängen, wir könnten die jetzt eigentlich so erweitern, dass der auch Menschen aufzeichnet, die sich irgendwie besonders verhalten. Und irgendwann geht‘s dazu, dass man generell einfach alles aufnimmt und dass dann auch mehr Kameras dazu kommen, an anderen Orten, bis ans eigene Haus dann.“
A8	WS1; 95	„Und weiter zu diesem Punkt, das ist einfach diese falsche Interpretation der Auswertung. Weil zum Beispiel mit unser heutige Technik und ich denk auch in der Zukunft, wird es immer schwer sein zu entscheiden welche Intensität von dieser Aktion bringt Gefahr und welche nicht. Wenn zum Beispiel zwei Kumpel miteinander irgendwie aufeinander losgehen und dann die Kamera überwacht und es sieht aus wie eine Schlägerei, es ist aber total anders (..) ihre Bewegungen, Körperbewegungen einfach ähnlich sind wie mit einer Gefahr möglichen Aktion, dann kommt einfach die Polizei und nimmt diese zwei Leute fest und das ist ein bisschen blöd.“
A9	WS1; 197	„Punkte. Erstens, zur Verhaltensänderung durch Videoüberwachung. Ehm, dazu ein ganz schlimmes Beispiel: Großbritannien, London. Und zwar ist das so, dass dort auch schon etwas intelligenter in Echtzeit überwacht wird. Wenn z.B. vor bestimmten Gebäuden, wie zum Beispiel Polizeireviere, Leute mit einen Fotoapparat erscheinen, dann ist sofort ein Polizist in der Nähe: He, was machen sie mit dem Fotoapparat hier? Sie könnten ja irgendwie was fotografieren was wichtig ist und sie planen einen Terroranschlag auf dieses Polizeirevier. Da kommt dann wieder dieser Generalverdacht auf, dieses anti-pre-crime sozusagen, um zu verhindern dass etwas passiert.“
A10	WS1; 94	„Das andere ist, war auch ein Thema, diese Vorverurteilung. Eine Gefühlsüberwachung vor einer Tat. Da sind wir draufgekommen, zum Bei-

		spiel irgend so ein Amoklauf in einer Schule. Was löst das aus? Wenn ich jetzt ein Jahr lang einen Schüler mobbe, kann ich eine Kameraüberwachung haben, jeden Morgen wird er von zwei Schülern angelacht. Das Lächeln sagt aber nicht die Wortwahl. Ich kann auch lächelnd zu einen sagen „du bist das größte Arschloch", auf Deutsch gesagt. Sag das jeden Morgen einem Schüler, jahrelang, irgendwann rastet der aus. Das krieg ich nicht mit einer Überwachung hin wenn ich keine Gefühlsüberwachung habe.“
A12	WS 1; 29	Sprecher O: „Aber, sollen nur die Kosten Gedanken machen? Oder wirklich was beibringen, das oder jenes? Wenn man nur über die Kosten denkt, dann geht‘s nun mal nicht vorwärts!?“ E: „Wenn es nur um Kosten geht, dann dürft‘ man gar nichts machen ... „.
B1	WS 2 217	**„**(..) Um ganz ehrlich zu sein: Ich fühle mich in Deutschland nicht unsicher. Hier in Karlsruhe schon gar nicht. Das ist so ein kleines, gemütliches Städtchen. Ich habe hier keine Angst und brauche keine Überwachung von außen. Weil, ich kenne hier Leute oder wenn ich auf der Straße bin und mir kommt irgendetwas komisch vor, dann würde ich laut um Hilfe rufen und gezielt Personen ansprechen, die mir helfen sollen. Aber diese Kameras sorgen bei mir nicht für ein Sicherheitsgefühl. “
B2	*WS 2; 138*	„Ich habe das Recht darauf … eigentlich meines Erachtens, es ist mein Recht zu wissen, was macht dieses Ding da? (...)“
B3	WS 2; 136	„Zur Frage, weil Sie gesagt haben: "Positive Argumente". Ich habe vorher einen Punkt versucht zu betonen, der mir in diesem Zusammenhang wichtig scheint, das ist nicht die eigentliche Technologie an sich, ob jetzt Bilder erhoben werden oder nicht, sondern auf welche Weise sie verarbeitet werden.“
B4	WS2; 72	„Da sind zum Schluss diese beiden grünen Punkte aufgeschrieben: das eine ist Verkehrsdatenerfassung und das andere sind Großveranstaltungen. Das heißt zum Beispiel, große Demonstrationen sollten videoüberwacht werden.“ K : „Aber nur mit ausreichend Abstand. Also dass nur eine Bewegungsanalyse quasi erfolgen kann, keine Gesichter und Personen dann.“
B5	WS2; 187	„Also kann sich jemand ein Modellflugzeug nehmen, dann eine Kamera drankonstruieren und wahrscheinlich kommt man sogar mit weniger als 200 Dollar weg. (...) Wie wollen Sie das verhindern?“ **A: „**Abschießen.“ **C: „**Das heißt noch lange nicht, dass das durch den Staat legitimiert sein muss. Nur weil ich W-LAN Netze abhören kann, ist das ja auch nicht legal. Und deswegen muss der Staat immer gucken, dass zu verbieten.“

		J: „Unterbinden mit Strafe im Notfall." (…) „dass Drohnen für mich [wegen mangelnder Zuordenbarkeit] im privaten Sektor nichts verloren haben. Das ist jetzt so eine Meinung, die sich bei mir innerhalb der Diskussion gebildet hat − komplett verboten werden. Dass Drohnen frei erhältlich sind für solche Zwecke. Über Polizeieinsatz, über solche Veranstaltungen kann man reden, das sind Institutionen, die das machen können. Aber dass sich jede Privatperson so eine Drohne kaufen kann und damit Informationen sammelt, das finde ich gefährlich."
B6	WS 2; 151	„Ich hätte noch eine kurze Nachfrage an Sie. Sie haben vorhin gesagt: Das Informiert-Werden über den Einsatz. Meinen Sie damit, dass es den Einsatz einer Drohne gibt? Oder was mit Drohneninformationen passiert, die dadurch erhoben werden, wer sie verarbeitet, auf welche Weise sie verarbeitet werden? Und denken Sie, wenn es ein Gesetz gäbe, dass das vorschreibt, dass Sie tatsächlich darüber aufgeklärt würden?" „Mir ging es einfach darum, wenn so etwas überhaupt eingeführt wird, ganz subjektiv, dann ist das für meinen Geschmack das Minimum, dass ich weiß, was mir da über den Kopf kreist." **B: „**Nein, das denke ich nicht wirklich."
B7		„Ich habe mal eine Gegenfrage. Wir haben eine Aufklärungsquote bei Haus- und Wohnungseinbrüchen von, glaube ich, zehn Prozent. Angenommen man würde Drohnen einsetzen und wir hätten plötzlich eine Aufklärungsquote von 50 Prozent, weil nur dann, wenn ein Einbruch war, die Polizei als Möglichkeit hat zu gucken, wer ist da rein- und rausgegangen. Das wäre doch eine tolle Sache." (WS 2, 163)
B9	WS 2; 136	„(...) In dem Maße, in dem diese Technologie eingeführt wird, wird diese Unschuldsvermutung durch das Vorhandensein dieser Technologie auf den Müllhaufen der Geschichte geworfen. Und das ist eine Frage, die ich durchaus für brisant finde, und das habe ich ganz in meinem allerersten Statement gesagt, was sind die Motivationen des Auftraggebers dieser Studie? Ich würde sagen, und da lege ich jetzt wirklich sehr viel in die Runde, es sind zunächst einmal Verwertungsinteressen. Es muss keine böse Motivation sein, aber zum Beispiel im Rahmenvertrag der Europäischen Union, der diese Zukunftsprogramme allgemein beschreibt, mit dem Rahmenvertrag ist auch beschrieben, das war eine Frage, die auch vorher aufgetaucht ist, dass man auch im Bereich Sicherheitstechnologie ein maßgeblicher Akteur auf dem Weltmarkt werden möchte. Das heißt, man möchte deutsche Firmen stärken damit sie das im Ausland auch verkaufen. Natürlich unter demokratischer Kontrolle. (...)"
B10	WS 2; 115	„Wir hatten bis jetzt eigentlich nur Deutschland oder den europäischen Raum betrachtet. Denken sie mal an andere Länder, totalitäre Staaten.

		Wenn zum Beispiel Syrien oder Iran die Kameradichte von Großbritannien hätte, dann sähe das glaub ich schon wieder ganz anders aus, weil die Oppositionsbewegung hat da ein Problem, die können sich jetzt nicht irgendwo treffen. Und dann würden auch wahrschlich die Kameras ausgewertet werden. Die Infrastruktur die damit möglich ist, die birgt Gefahren für die Gesellschaft. Nicht unbedingt bei uns, jedenfalls nicht heute bei uns, aber sowas mag man sich dann nicht ausdenken.“
B11	WS2; 20	„Ich bin ein Kind der Achtziger, George Orwell war natürlich ganz großes Kino für uns. Nach dem Film gab es auch wilde Diskussionen, viele können das nachvollziehen. Als die ersten Kameras auf den Platz kamen, hatte ich schon irgendwie so ein Kribbeln und war schon sehr kritisch und dachte auch: "Will ich das, will ich das wirklich?".
B12		„eine Kamera, die dort installiert ist, würde ein gutes Bild haben wollen. Das heißt, es ist ein Scheinwerfer dran, Sie können nicht erkennen, was das für ein Objekt ist. In vielen Fällen könnten Sie das gar nicht mehr verfolgen. Das wäre so, wie wenn jemand das Nummernschild von seinem Auto weg macht. Die Problematik wäre nicht nur in der Gesetzgebung, sondern auch in diesem rechtsfreien Raum, den das eröffnet, weil es kann ja faktisch nicht verfolgt werden, weil das Objekt“ …
B13	WS 2; 215-216	„Man könnte das sicherheitstechnisch erst quantifizieren. Ich habe mir sagen lassen, die Straßenbahnen haben alle vor, Kameras einzubauen. Dann hat man gerechnet, ohne Kameras, wie viel Schaden haben wir dann. Und dann hat man die Kameras ein Jahr später ausgewertet, wie ist der Schaden jetzt und es waren tolle Ergebnisse.“ (…) **B: „**Aber Rechte und Freiheiten können Sie nicht quantifizieren. Das ist ein Terminus den können Sie nicht quantifizieren.“
B14	WS 2; 138	„(..) es ist mein Recht zu wissen, was macht dieses Ding da? Das geht mir auch schon bei Helikoptern so, teilweise. Warum steht dieser Helikopter jetzt schon seit einer halben Stunde über diesem Stadtzentrum, in dem ich mich gerade aufhalte? Es ist keine Demonstration, was ist das? Und ich glaube, je weiter die weg sind, also je höher sie fliegen oder je kleiner sie werden, also je schwerer erkennbar sie werden, desto schwerer kann der- oder diejenige, ich will ja nicht sagen (die) Beobachteten/Getrackten, das irgendwie einschätzen und das finde ich einfach bedenklich.“
B15	WS 2; 138	„(..) zum Beispiel denke ich an diese Drohne und wie auch immer, dieses unbemannte Flugobjekt von der Polizei. Da steht dann zwar drauf "Polizei", aber ganz viele andere waren eigentlich nicht erkennbar. Und wenn dieses Ding in einer entsprechenden Höhe fliegt, weiß ich doch, sehe ich das doch vielleicht gar nicht. Keine Ahnung, vielleicht habe ich meine Brille nicht auf oder das Ding ist einfach zu hoch, ich sehe es nicht. Ich kann nicht einordnen, zu wem und welcher Funktion und welchem Zweck dieses

		Ding konkret jetzt gerade Einsätze über meinem Kopf fliegt.“
B16	WS 2; 177	**A: „**Und Sie vertrauen darauf, dass der Staat Sie über Ihre Spionagetechnik aufklärt?“ **B: „**Nein, ich vertraue ihm überhaupt nicht. Das ist eine Minimalforderung. Und wenn ich das nicht verhindern kann, dass das eingeführt wird, ist dass das, was ich sozusagen als Rechtssubjekt mindestens fordere. Wenn ein Konzern, eine Firma, ein Produkt auf den Markt bringt, das gekauft werden kann um an meinem Balkon vorbeizufliegen abends um 22 Uhr, dann vertraue ich überhaupt auf gar nichts und ich will nur, dass das verschwindet. Und wenn es nicht verschwindet, müsste ich die Möglichkeit haben zu erkennen, wo das herkommt, um mich dort zu erkundigen, was die hier gefälligst machen. Und dass man von Information spricht und nicht von Einwilligung. Ich willige nicht ein, ich will nur die Möglichkeit haben nachzufragen, was das war.“
C1	WS1; 197	„Punkt Zwei war zur intelligenten Videoüberwachung überhaupt, und zwar das allgemein in Politik und Sicherheitsfragen immer so eine sogenannte Salamitaktik verfolgt wird, (...). Dass immer schrittchenweise kleine Dinge eingeführt werden, damit sich der Bürger nicht so sehr daran aufstößt. Zum Beispiel, ok, da hängt jetzt ne Kamera, die zeichnet nur Koffer auf, die über 20 Minuten an einem Fleck stehen, und nach zwei, drei Jahren, wenn sich jeder daran gewöhnt hat, kommt der nächste Politiker und sagt, wir haben da jetzt schon Kameras hängen, wir könnten die jetzt eigentlich so erweitern, dass der auch Menschen aufzeichnet, die sich irgendwie besonders verhalten. Und irgendwann geht‘s dazu, dass man generell einfach alles aufnimmt und dass dann auch mehr Kameras dazu kommen, an anderen Orten, bis ans eigene Haus dann.“
C2	WS 3; 180	„Das ist auch eine, ich sage mal, Option des Internets. Nämlich das Gefühl der Sicherheit in der Anonymität. Wenn ich meinen Wunsch äußere, dann äußere ich ihn erst mal anonym gegenüber einer Vermittlerstelle. Das ist positiv, es kann aber auch negative Auswirkungen haben. Zum Beispiel die ganzen Mobbingdiskussionen, die aus der Anonymität heraus entstehen. Aber der erste Schritt getan ist, für mich, das persönliche Sicherheitsgefühl, „ich muss erst mal nicht so viel preisgeben“. Jedenfalls nicht aktiv preisgeben. Was ich passiv preisgebe, allein durch die technische Kontaktaufnahme mit der Stelle, das realisiere ich ja erst gar nicht mal so. Aber die Überwindung direkt jemanden anzusprechen, den direkten Kontakt zu suchen, ist immer noch größer als den Verdacht, „hm, unter Umständen könnte ich jetzt eigentlich doch mehr preisgeben, als ich preisgeben möchte“
	WS 22-28	**A: „**Wie ich Sie verstanden habe, haben Sie nicht unbedingt Angst vor einzelnen Personen, sondern dass zu viele Menschen auf einem Platz

		sind?“ **D: „**Es geht um diese Massen. Besucherströme zu eliminieren.“ **A: „**Also, das ist Ihre konkrete Angst?“ **D: „**Angst ist es überhaupt gar keine, es ist die konkrete Aufgabe.“ **A: „**Aufgabe. Also nicht vor einzelnen Personen?“ **D: „**Nein. Wir haben sicherlich die Möglichkeit aufgrund von anderen Kamerasituationen reinzuzoomen, ins Detail zu gehen. Wir können uns natürlich nicht das Weiße im Auge des Betrachters angucken − es ist auch völlig uninteressant. Wir haben die Möglichkeit reinzuzoomen, tun dies aber nur im Schadensfall. Das heißt, wir kriegen eine Meldung: Es ist ein Mensch umgekippt, er ist bewusstlos, wo liegt er? Wir versuchen erst mal diesen Punkt mit der Kamera zu finden, das zu lokalisieren, dann die Meldung an die Sanitätskräfte weiterzugeben und dann zu sehen: Okay, wir können in die Wege leiten, was zu tun ist.“ "Es ist ein Mensch umgekippt, er ist bewusstlos, wo liegt er? Wir versuchen erst mal diesen Punkt mit der Kamera zu finden, das zu lokalisieren, dann die Meldung an die Sanitätskräfte weiterzugeben und dann zu sehen: Okay, wir können in die Wege leiten was zu tun ist"
C4	WS 3, 207	„Also mir hat das gezeigt, dass die Lebensumstände doch ganz unterschiedlich sind. Wir leben alle im selben Land, in derselben Stadt, aber unsere täglichen Erfahrungswelten sind offenbar ganz unterschiedlich. Also wenn ich höre, „ich fühle mich nachts unsicher“. Bei mir ist das nicht so. Da habe ich offenbar irgendwie andere Erfahrungen. Und das könnte man jetzt wer weiß wie aufdröseln. Es atomisieren sich sozusagen die Lebenswelten und damit kann man auch, glaube ich, nur ganz schwer einheitliche Sicherheitsgeschichten definieren.“
C5	WS 3; 207	„Ich hatte fast den gegensätzlichen Eindruck, dass die Leute als Unsicherheitsfaktoren ziemlich ähnliche Sachen nennen. Also selbst jetzt von den männlichen Teilnehmern war dieses „Abend oder allein oder Gruppen angetrunkener“ oder so, trotzdem eher immer eine unsichere Situation. Bei den Frauen sowieso. Aber das fand ich gar nicht so unterschiedlich. Und auch, dass Großstädte eigentlich von den meisten als unsichere Orte eher wahrgenommen werden. Also ich fand das eher relativ homogen.“

3.2 Anhang 2: Auszug aus dem Arbeitspapier 1 – Technisierung und Sicherheitswahrnehmung[52]

Sicherheitstechnik als Element von Sicherheitskultur

Als Sicherheitskultur bezeichnen wir die Art und Weise der Herstellung, Bewahrung und Wiedergewinnung von Handlungssicherheit.[53]

Sicherheitstechnik - als Teil von Sicherheitskultur - ist dann zunächst der Versuch technischer Unterstützung der Produktion von Handlungssicherheit. Darunter fallen einerseits der Einsatz von physischen Techniken wie Werkzeugen und andererseits die Ausbildung von bestimmten Verhaltensweisen (operative Techniken). Diese Untergliederung in „Sachen“ (Artefakte, physikalische/substanzielle Technik) und „Verfahren“ (Routinen, operative/prozessuale Technik) ist lediglich eine Ausdifferenzierung der Technik zu Analysezwecken. Beide Seiten müssen immer als „dialektische Einheit“ von Prozess und Substanz gedacht werden. „Tatsächlich sind das Verfahren und die Sache, der Prozess und die Substanz auf einander bezogene Erscheinungen einer dialektischen Einheit: Prozesse sind nichts Anderes als die Verhaltensweisen von Substanzen, und Substanzen sind die Träger von Prozessen.“[54]

Beides, Werkzeugeinsatz und Ausbildung von Verhaltensweisen, kann auf verschiedenen Ebenen stattfinden: Der individuellen Handlungsebene, der Mesoebene von Organisationen wie etwa der Polizei und der Makroebene der Gesellschaft insgesamt. Dabei erscheinen die Dimensionen nicht als strikt abgrenzbare Größen, sondern als Punkte einer kontinuierlichen Achse mit vielen möglichen Zwischenpositionen.

52 Gransche/Warnke/Zoche, Fraunhofer ISI, 2011.

53 Vgl. Rusch 2010.

54 G. Ropohl in: Banse, Reher 2004, S. 28.

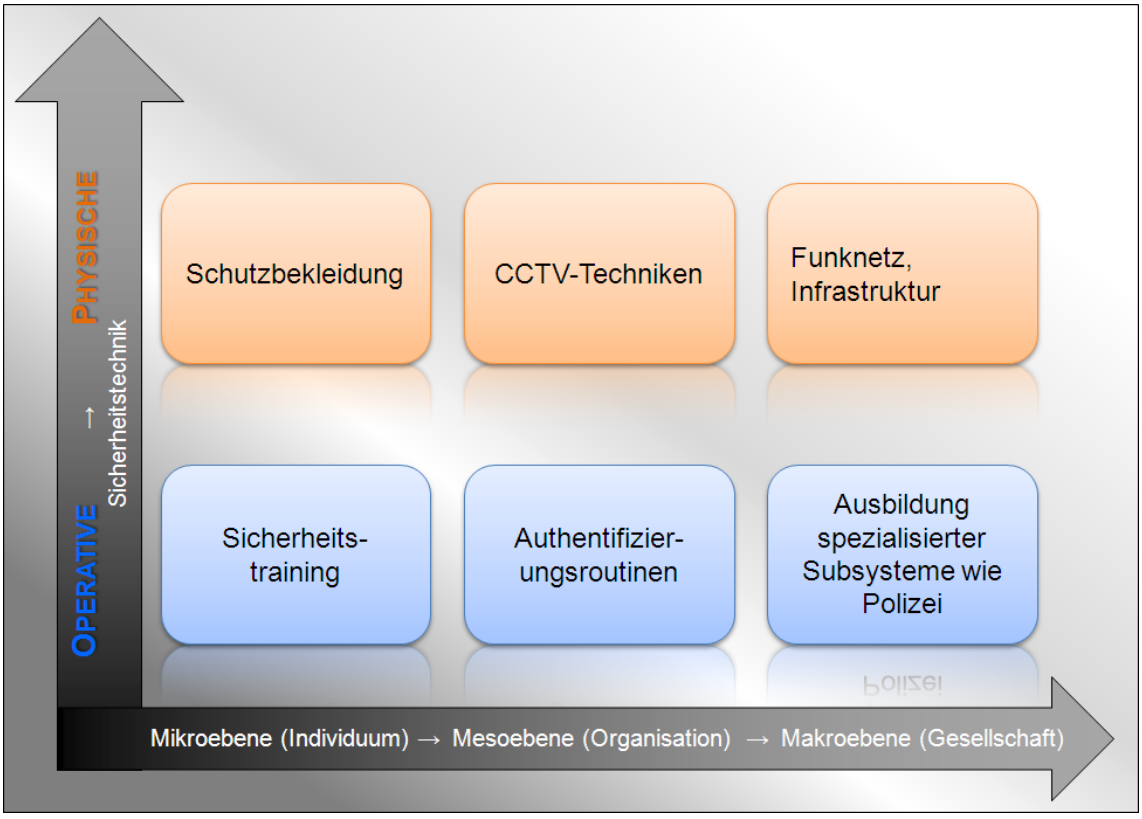

Abbildung 2: Beispiele für verschiedene Typen von Sicherheitstechnik[55]

55 Zu dieser Einteilung vgl. Rusch 2010.

Ermittlung der Brennpunkte

Als **Brennpunkte** werden im Folgenden die thematischen Zuschnitte bezeichnet, die eine besondere Kombination relevanter Sicherheitstechnologien einerseits und Bezüge zu aktuellen gesellschaftlichen Sicherheitsthemen andererseits aufweisen. In den „Brennpunkten" bündeln sich die „Strahlen" der Technologiedynamiken und der medial-gesellschaftlichen Aufmerksamkeit, wodurch ein besonderer Fokus entsteht.

Im Rahmen von Arbeitspaket 1 wurde auf der Basis einschlägiger aktueller Literatur eine Zusammenstellung wesentlicher Sicherheitstechnologien und ihrer Einsatzbereiche vorgenommen sowie eine erste Charakterisierung des Reifegrads mit Experten diskutiert (vgl. Anhang A). Gleichzeitig wurden in jüngster Zeit[56] geführte öffentliche Debatten zu Fragen der Sicherheitstechnik berücksichtigt (Vgl. Anhang B). Eine Gegenüberstellung der beiden Bestandsaufnahmen ergab die ersten Brennpunkte in denen aktuelle Technologieentwicklungen und öffentliches Interesse zusammenfallen (Vgl. Abbildung 3 Ermittlung der Brennpunkte).

56 Einbezogen wurden Fälle, die im Zeitraum zwischen den Jahren Mitte 2009 und Frühjahr 2011 öffentlich diskutiert wurden. Die zugrunde liegenden Anlässe reichten teilweise länger zurück.

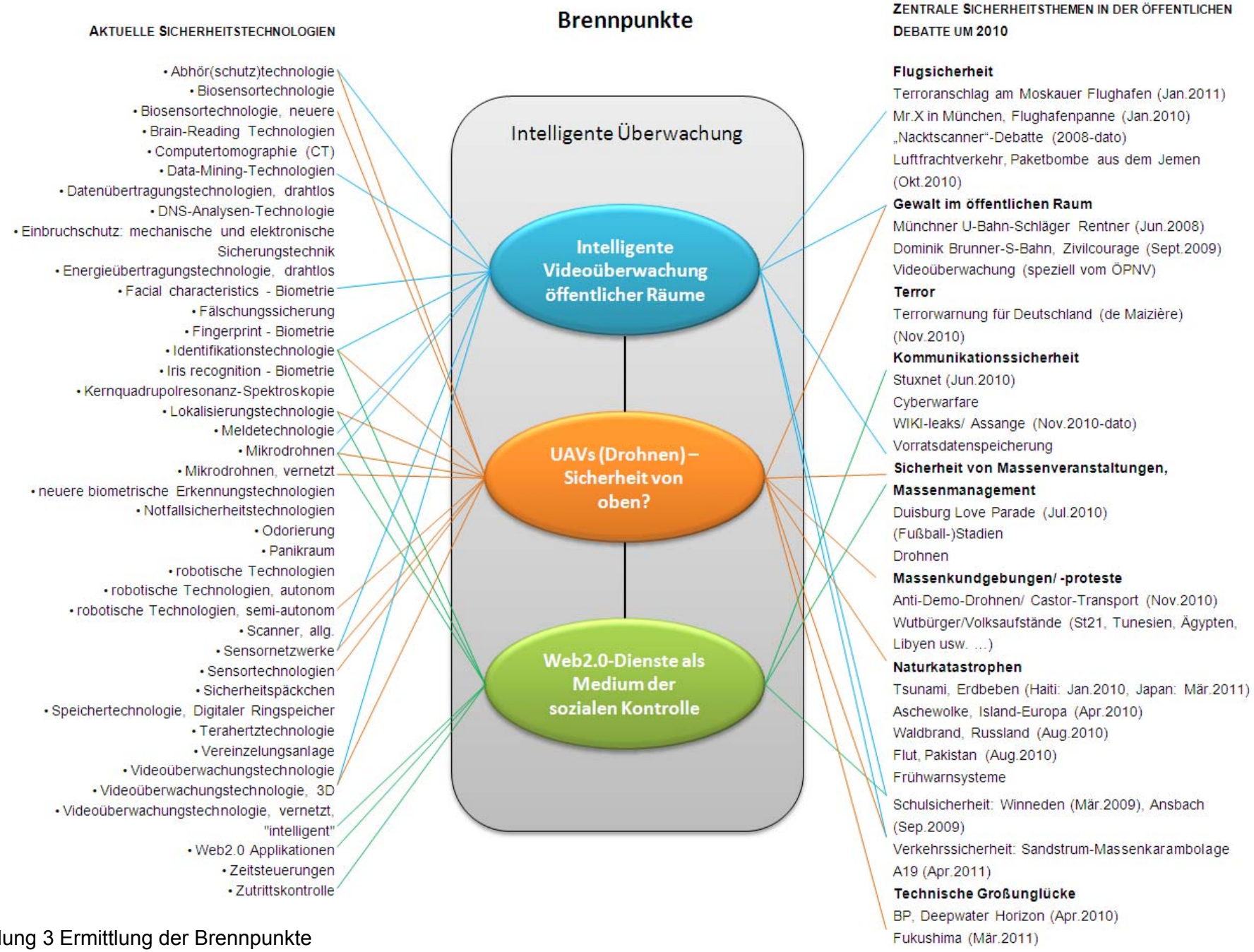

Abbildung 3 Ermittlung der Brennpunkte

Auswahl der Brennpunkte

Für die Auswahl der in BaSiD Modul 6 zu bearbeitenden Brennpunkte *gesellschaftliche Dimensionen von Sicherheit* wurden folgende **Kriterien** erarbeitet:

- Vermutete Relevanz für breite Sicherheitswahrnehmung und damit Beitrag zu BaSiD Gesamtvorhaben
- Vorhandensein aktueller, noch offener Gestaltungsfragen in der Entwicklungs- oder Einführungsphase
- Relevanz für BMBF Förderpolitik
- Eignung des Brennpunkts für die Bearbeitung mit **partizipativen Verfahren**:
    - Der Brennpunkt sollte für **breite Gruppen von Bürgern** interessant sein – nicht nur für spezielle Organisationen oder Kleingruppen
    - Hohe **Anschaulichkeit** bzw. gute **Handhabbarkeit** des Brennpunktes
    - Es sollte eine Möglichkeit bestehen die erarbeiteten Ergebnisse im Rahmen von BaSiD zu Gestaltungskriterien zu verdichten

Schließlich noch liegt es im Interesse der Projektziele verschieden gelagerte Problemstellungen zu bearbeiten, um möglichst breite Erfahrungen sammeln zu können.

Unter Anwendung dieser Kriterien wurde folgende Auswahl getroffen:

Brennpunkt 1: Intelligente Videoüberwachung öffentlicher Räum

Begründung:
hohes öffentliches Interesse; neue Phase „intelligente Videoüberwachung“; Integration verschiedener Sicherheitstechnologien; breiter Einsatz ähnlicher Systeme, hoher Bekanntheitsgrad, „allgegenwärtig“; hohe Aktualität in der gesellschaftlichen Debatte; hohe Relevanz für das BMBF

Brennpunkt 2: UAVs (Drohnen) – Sicherheit von Oben

Begründung:
steigendes öffentliches Interesse; Integration verschiedener Sicherheitstechnologien; breites mögliches Einsatzfeld; hohe Aktualität in der gesellschaftlichen Wahrnehmung; hohe Anschaulichkeit; hohe Relevanz für das BMBF

Brennpunkt 3: Web2.0-Dienste als Medium der sozialen Kontrolle

Begründung:
hohes Beteiligungspotenzial, Eignung für partizipative Behandlung; Anschluss an das bekannte aktuelle Phänomen der Sozialen Netzwerke; großer offener Gestaltungsspielraum

Skizzierung der Brennpunkte

Brennpunkte übergreifende Überlegungen

Die drei ausgewählten Brennpunkte stellen unterschiedliche Konstellationen verschiedener Anwendungsbereiche, Technologien und soziotechnischer Handlungsverteilung dar, lassen sich aber alle dem Feld der *Intelligenten Überwachung* zuordnen. In diesem Bereich können sowohl ein Großteil der wesentlichen Sicherheitstechnologien, als auch eine Vielzahl der aktuellen gesellschaftlichen Sicherheitsthemen zueinander in Beziehung gesetzt werden (vgl. Abbildung 3). *Intelligent* ist ein Überwachungssystem dann, wenn maßgebliche Anteile von Prozessen wie Auswertung, Erkennung, Interpretation oder Verfolgung zumindest teilweise automatisiert sind, also vom physikalischen Teil einer Sicherheitstechnik übernommen werden. *Intelligent* hat sich als spezifisches Prädikat im technischen Kontext etabliert und meint nicht wie auch immer definierte menschliche Intelligenz.[57]

Am Beispiel der intelligenten Videoüberwachung bedeutet dies eine Verlagerung der Handlungsverteilung bei der Realisierung des Überwachungsaktes von menschlichen Anteilen hin zu physikalischen Technikteilen des Systems. Demnach wäre ein Videoüberwachungssystem *intelligent*, wenn es statt der reinen Aufnahme, Übertragung und Ausgabe visueller Informationen von der Straße auf einen Bildschirm auch eine Kenntnis geltender Regeln und damit erlaubter Routinen in interpretierenden Abgleich mit der aufgenommenen Szene bringen und adäquate Folgeroutinen autonom einleiten könnte.

Mikroebene – Individuum

Auf dieser Ebene lässt sich im Bereich der physikalischen Sicherheitstechnik intelligenter Überwachung beliebig kleinteilig beginnen; etwa bei einzelnen technischen Komponenten wie Sensoren, z.B. hochauflösende und Infrarot-Kameras, aber auch einzelne Systemkomponenten wie Einzelkameras, Bildschirme, Datenbanken, Server- und Netzwerktechnik, verschiedene Speicher usw. Dem korreliert auf operativer Seite die Ausbildung und Schulung von Individuen in ihren jeweiligen Funktionen, etwa als Wachpersonal vor den Monitoren, als ergänzende Patrouilleeinheit für „tote Winkel“

---

57 Auch nicht intendiert ist eine Verwendung des Intelligenzbegriffes, wie er in der „starken“ Künstlichen-Intelligenz-Forschung verhandelt wird. Wie unter anderen Acatech (acatech 2009) im Fall der „Intelligenten Objekte“ vorführt, wird das Prädikat „intelligent“ im technischen Kontext oft nicht weiter abgegrenzt, aber meist im Sinne einer „schwachen“ Definition der künstlichen Intelligenz verwendet. „Von einem „Intelligenten Objekt“ kann die Rede sein, wenn mindestens ein Prozessor und ein Programm vorhanden sind, […].“(acatech 2009, S. 9)

oder zur Verifizierung von Warnmeldungen und Fehlalarmen. Zu dieser Schulung und Ausbildung des Personals, also der Herausbildung der je spezifischen Kompetenzen des Wahrnehmens, Interpretierens und (Re-)Agierens, kommen die Kompetenzen anderer beteiligter Personen aus dem Bereich der Systementwicklung, -installation, -wartung, etc.

Am Übergang zur Mesoebene ist hier die physikalische Sicherheitstechnik kleinerer Areale bzw. kleinerer Entitäten zu nennen. Dies ist von Individuen privat genutzte Sicherheitstechnik, wie der Gegensprechanlage, dem Türspion[58], einzelne, meist nicht vernetzte Kameras am Hauseingang oder auch Anwesenheitssimulationen[59], Brandmelder, Bewegungsmelder etc. Auch Kfz-Einbruchmeldeanlagen (EMA), Wegfahrsperren und dergleichen wären hierzu zu zählen. Zugehörige operative Technik wäre hier etwa vorstrukturiertes Verhalten im Not- bzw. Meldefall, also Routinen wie den abzusetzenden Notruf an die Feuerwehr/Polizei, das Einleiten von Gegenmaßnahmen[60] oder Flucht usw.

Mesoebene – Organisation

Auf der Mesoebene befinden sich auf physikalischer Seite etwa die *Closed Circuit TeleVision* (CCTV) Systeme mit analogen oder IP-Kameras sowie Drohnen im Überwachungseinsatz oder das *ganze physikalische Ensemble vernetzter Einzelgeräte einer Organisation* wie der Polizei, der Verkehrsbehörden, einer Stadt etc. Ein Beispiel wäre die Gesamtheit verwendeter Hardware zur Verkehrsüberwachung einer Stadt, also die Summe der Kameras, Bildschirme, Leitungen, Überwachungszentralen, mobilen Endgeräte usw. Auf operativer Seite kommen neben den Funktionen und Kompetenzen der Mikroebene hier vor allem die Ausdifferenzierung in spezielle Bereiche der Überwachung mit je eigenen Routinen, Regeln, Zielen und Vorgaben hinzu; also etwa Kaufhausüberwachung, Verkehrsüberwachung, Personenverfolgung, Überwachung öffentlicher/halböffentlicher Orte wie Einkaufszentren, Banken, Flughäfen, Bahnhöfe oder zutrittsbeschränkter Areale und Gebäudekomplexe wie Firmengelände, Regierungsgebäude, etc. Die Routinen unterscheiden sich in diesen Bereichen je nach ihrem primären Ziel, also der Überwachung von Diebstählen, Regelverstößen und

---

58 ein nicht elektronischer Vorläufer der Video(=ich sehe)Überwachung

59 Anwesenheitssimulationen sollen dem Einbruchschutz dienen, indem sie die Anwesenheit von Personen simulieren, etwa durch zeitgesteuertes Ein- und Ausfahren der Jalousien oder Rollläden, durch Schalten von Licht, Radio, TV, etc.

60 Die Gegenmaßnahme im Brandfall wäre der Einsatz eines Feuerlöschers; dieser ist zwar ein Artefakt der physikalischen Sicherheitstechnik, jedoch nicht mehr des Bereiches *Überwachung*, sondern bereits des Bereiches *Intervention/Bekämpfung* und daher – wie entsprechend eine Vielzahl anderer Sicherheitstechnik – hier nicht im Fokus.

(Verkehrs-)Gefährdungen, Gewalttaten und Sachbeschädigung oder unbefugtem Zutritt und sind daher je nachdem Kontroll-, Identifikations-, Authentifizierungs-, Detektionsroutinen usw. Ebenfalls zur operativen Sicherheitstechnik der Mesoebene zählen kodifizierte Prozess- und Ablaufstandards also Routinevorgehen bei Kontrollen, Unfällen, usw.

Ebenfalls Teil operativer Sicherheitstechnik, ist der Umgang mit und die Geltung von Inhalten der physikalischen Überwachungstechnik; ein Beispiel dafür wäre die Nutzung von Videomaterial als Beweis vor Gericht und etwa dessen Gewicht gegenüber Zeugenaussagen. Hier wird die Grenze zur Makroebene operativer Sicherheitstechnik berührt, auf der schließlich für ein ganzes Rechtssystem einheitlich die Grenzen der Geltung etwa von „Videobeweisen" als gesellschaftlich-rechtlich anerkannte Routine festgelegt werden muss.

Makroebene – Gesellschaft

Auf physikalischer Seite dieser Ebene wären die gesellschaftlichen Dimensionen der Gesamtheit sicherheitstechnischer Hardware zu fassen, also z.B. sämtliche beteiligten Komponenten einer nationalen Videoüberwachungs(infra)struktur oder das Sensor-Netzwerk-Ensemble eines internationalen (Erdbeben-)Frühwarnsystems sowie die damit einhergehende Allokation von Personen und Ressourcen (qualifiziertes Personal, also etwa Entwicklung-, Bedien- und Wachpersonal, Finanzmittel, Geräte, Ausstattung,…) zu ausdifferenzierten Subsystemen des Sicherheitssektors. Diese Ausdifferenzierung ist wiederum Teil der operativen Sicherheitstechnik auf gesellschaftlicher Ebene, also die Spezialisierung in Landes- und Bundespolizei, Sondereinheiten, Bundeswehr aber auch die nationale Sicherheitsforschung, gesellschaftlich-politische Sicherheitsdebatten und Sicherheitsgesetze wie etwa die Vorratsdatenspeicherung, Begrenzung von Untersuchungshaftdauer oder die Kompetenzgrenzen der Exekutivorgane. Ebenso Teil der operativen Sicherheitstechnik auf Makroebene sind etwa die nationalen CCTV-Strategien (etwa der Unterschied von England und Deutschland) oder die unterschiedlichen Präsenzstrategien der Landespolizeien (etwa Rheinland-Pfalz und Baden-Württemberg im Vergleich).

Brennpunkt 1:
Intelligente Videoüberwachung öffentlicher Räume

Videoüberwachung (CCTV) gehört international zu den verbreiteten und intensiv eingesetzten Überwachungssystemen. Die technologische Entwicklung führt diese Überwachungssysteme jedoch auf ein anderes Niveau, das es rechtfertigt vom Entstehen

intelligenter Videoüberwachungssysteme zu sprechen. Dazu führt eine Kombination der qualitativen Verbesserung der Systemkomponenten (höhere Auflösung bei sinkenden Preisen; höhere Störungs-/ Täuschungstoleranz; bessere/ schnellere/ robustere Datenübertragung, zunehmend drahtlos; Miniaturisierung; höhere Rechenleistung) mit Innovationen, die Umsetzungsreife erreichen bzw. erreicht haben (leistungsfähigere Algorithmen zur automatischen Mustererkennung, Personenverfolgung, automatischen Situations-/ Verhaltensanalyse, Kombination mit umfassenden Datenbanken; Fortschritte bei der 3D-Technik; Erkennung einer Vielzahl biometrischer Merkmale).

Der Fokus auf **öffentliche Räume** wurde in diesem Brennpunkt gewählt, um eine möglichst hohe Relevanz für das Gesamtvorhaben von BaSiD, die breite Sicherheitswahrnehmung in Deutschland, zu gewährleisten. Öffentliche Räume betreffen jeden Bürger, der diese alltäglich nutzt und keine Möglichkeit hat sie zu meiden, daher fassen wir darunter öffentliche Plätze, Straßen, Wege, (Park-)Anlagen, aber auch Kaufhäuser und Bahnhöfe, die nicht zugangsbeschränkter Teil der öffentlichen Sphäre sind. Flughäfen betrachten wir nicht darunter, da hier teilweise Zugangsbeschränkungen bestehen und sie nur von einem bestimmten Personenkreis zu bestimmten Zwecken freiwillig aufgesucht werden; Bahnhöfe weisen dagegen eine größere Offenheit und Öffentlichkeit auf als Flughäfen.

Brennpunkt 2: UAVs (Drohnen) – Sicherheit von Oben?

Drohnen, auch *unmanned arial vehicles* (UAV), sind unbemannte (semi-)autonome robotische Fluggeräte, die als Plattform für eine Vielzahl von Sensoren und Manipulatoren genutzt werden können. Dabei reichen die UAV-Varianten von 19 Gramm leichten Roboterkolibris wie dem *Nano Hummingbird* bis zum hochfliegenden Langstreckenaufklärer *Global Hawk* mit fast 40m Spannweite. Mit entsprechenden Kameras bestückt, können UAVs mobile intelligente Videoüberwachungssysteme darstellen, womit sie eine andere Dimension etwa in Personenverfolgungs-, Spionage- oder Aufklärungsfunktionen der Videoüberwachung bringen. Multisensorische UAVs können aber auch Teile anderer intelligenter Überwachungskonzepte sein, die über Kamerasysteme weit hinausgehen.

Brennpunkt 3: Web2.0-Dienste als Medium der sozialen Kontrolle

Ein weiteres Setting des Bereichs intelligente Überwachung, das untersucht werden soll, ist die Entwicklung von **Web2.0 Diensten** zur sozialen Kontrolle, bei der Bürger – im Gegensatz zur öffentlichen Videoüberwachung – nicht nur Überwachte sondern auch Überwacher sind. In Diskussion sind etwa Onlineplattformen als Meldeportale für

beobachtete Straftaten, suspekte Objekte und dergleichen. Als Überwachungssystem gefasst fungieren die Bürger hier quasi als Sensoren mit integrierter Auswertungs-/ Interpretationskompetenz. Weiter angedacht ist ein allgemeiner Zugriff auf Videokameras über das Internet, bei der jeder Bürger Auffälligkeiten oder gar Straftaten an privaten Bildschirmen beobachten und melden kann – damit wäre ein gängiges Problem der Videoüberwachung, nämlich dass (zu) wenige Beobachter (zu) viele Bildschirme überblicken, umgekehrt.

Anhang A: Aktuelle gesellschaftliche Sicherheitsthemen

Zentrale Sicherheitsthemen in der öffentlichen Debatte um 2010[61]

Flugsicherheit	Terroranschlag am Moskauer Flughafen (Jan.2011) Mr.X in München, Flughafenpanne (Jan.2010) „Nacktscanner"-Debatte (2008-dato) Luftfrachtverkehr, Paketbombe aus dem Jemen (Okt.2010)
Gewalt im öffentlichen Raum	Münchner U-Bahn-Schläger Rentner (Jun.2008) Gesetzesverschärfung-Debatte Warnschussarrest für jugendliche Gewalttäter (Apr.2011) Dominik Brunner-S-Bahn, Zivilcourage (Sept.2009) Videoüberwachung (speziell vom ÖPNV)
Terror	Terrorwarnung für Deutschland (de Maizière) (Nov.2010)
Kommunikations-sicherheit	Stuxnet (Jun.2010) Cyberwarfare WIKI-leaks/ Assange (Nov.2010-dato) Vorratsdatenspeicherung

61 Quelle: Pressedatenbank LexisNexis® GmbH, berücksichtigter Zeitraum war 2010

Sicherheit von Massen-veranstaltungen, Massenmanagement	Duisburg Love Parade (Jul.2010) (Fußball-)Stadien Drohnen Massenkundgebungen/ -proteste Anti-Demo-Drohnen/ Castor-Transport (Nov.2010) Wutbürger/Volksaufstände (St21, Tunesien, Ägypten, Libyen usw. …)
Naturkatastrophen	Tsunami, Erdbeben (Haiti: Jan.2010, Japan: Mär.2011) Aschewolke, Island-Europa (Apr.2010) Waldbrand, Russland (Aug.2010) Flut, Pakistan (Aug.2010) Frühwarnsysteme
Schulsicherheit	Winnenden (Mär.2009), Ansbach (Sep.2009)
Verkehrssicherheit	Sandsturm-Massenkarambolage A19 (Apr.2011)
Technische Groß-unglücke	BP, Deepwater Horizon (Apr.2010) Fukushima (Mär.2011)

3.3 Anhang 3: Auszug aus dem Arbeitspapier 2 – Methodensichtung[62]

1. Bestandsaufnahme partizipativer Verfahren - Überblick

Die Bestandsaufnahme der Verfahren, die eine partizipative Auseinandersetzung mit Technik ermöglichen, ergab vier Typen von Ansätzen, die jeweils unterschiedliche Einsatzbereiche abdecken und verschiedenen wissenschaftlichen Traditionen entstammen:

Bürgerdiskurse, Stakeholderverfahren, interaktive Wertschöpfung und partizipatives Design (vgl. S. 57).

Bürgerdiskurse zielen auf die Auseinandersetzung mit Werten oder die Bewertung von Wissen (Chancen und Risiken) als Grundlage von politischen Entscheidungen und involvieren Bürgerinnen und Bürger als Repräsentanten einer breiten Öffentlichkeit. Diese Verfahren stammen aus der Tradition der partizipativen Technikfolgenabschätzung (TA).[63] **Stakeholderverfahren** legen demgegenüber den Schwerpunkt auf Interessenausgleich, Verhandlung, Strategieentwicklung und -umsetzung und beteiligen organisierte Interessenvertreter (Stakeholder) oder Bürgerinnen und Bürger als Vertreter betroffener Gruppen. Diese Ansätze werden vor allem im Kontext neuer Formen politischer Aushandlungsprozesse (Governance) diskutiert und sind insbesondere im Bereich der Innovationspolitik in den letzten zehn Jahren populär geworden.

Bürgerdiskurse und Stakeholderverfahren fokussieren auf Technik*bewertung* - ein Einfluss auf die Technikgestaltung erfolgt lediglich über die politische Rahmensetzung.

Demgegenüber etablieren sich neuerdings auch im Umfeld der TA Verfahren die auf die auf ein **partizipatives Design** von Technik zielen[64]. Konkrete Umsetzungen finden sich in der Roboterentwicklung[65] oder im Baubereich.[66] Solche Ansätze sind in der TA

---

62 Warnke/Jacoby/Zoche/Gransche, Fraunhofer ISI, 2011.

63 Diese lassen sich unterscheiden nach den Kriterien „Art der Repräsentation“ (Laien/Interessenvertreter), der „Thematisierungsweise“ (Werte/Wissen/Interessen) und „Politische Handlungsform“ (Auslotend (explorativ), Rahmensetzend (formativ)); vgl Nentwich et al. 2006; Steyaert et al. 2006.

64 Compagna et al. 2009 bezeichnen solche Ansätze, die sich unmittelbar auf die zu entwickelnde Technik richten, als „funktionale Verfahren“ im Gegensatz zu den normativen d. h. bewertenden der klassischen partizipativen TA

65 Compagna et al. 2009

schon früh als „Constructive Technology Assessment (CTA)“ diskutiert worden, haben aber bisher nur in den Niederlanden Anwendung gefunden.[67] Ganz ähnliche Verfahren werden von Unternehmen und Organisationen eingesetzt, um Produkte und Arbeitsumgebungen den Bedürfnissen der Anwender anzupassen. Diese Ansätze stehen in der Tradition der „Humanisierung der Arbeit“ und des „nutzerzentrierten Designs“ von Informations- und Kommunikationstechnologie.

Schließlich ermöglichen es Verfahren der **interaktiven Wertschöpfung**, dass Nutzerinnen und Nutzer unmittelbar an bestimmten Phasen der Erstellung von Produkten und Dienstleistungen, etwa der Ideengenerierung oder der Personalisierung, beteiligt sind. diese Verfahren stammen aus dem Innovationsmanagement.

Die Methoden und insbesondere Moderationsverfahren, die in den verschiedenen Verfahren bei der Strukturierung der Interaktionen der Teilnehmer eingesetzt werden, sind oft ähnlich. Wegen der Unterschiede in übergeordneten Zielsetzung, dem Fokus der Aktivitäten und der Art der Partizipation des Teilnehmerkreises gestaltet sich jedoch deren konkrete Umsetzung durchaus. Tabelle 1 gibt einen Überblick über die vier identifizierten Ansätze und ihre wesentlichen Merkmale.

---

66 Rohracher, Ornetzeder 2008

67 Schot, Rip 2002

	Übergeordnetes Ziel	Fokus der Aktivitäten	Art der Partizipation	Typische Methoden und Techniken
Bürgerdiskurse	Verbreiterung der Wissens- und Wertebasis von Technologiepolitik und dadurch: • Verbesserung • Demokratisierung, Steigerung von Akzeptanz und Legitimität	a) Bewertungen, Entscheidungen b) Ermittlung von Werthaltungen	Bürger als Repräsentanten der allgemeinen Öffentlichkeit	Konsensuskonferenz, Bürgerkonferenz, Fokusgruppen, Planungszelle, Interview-Meeting, Citizens Jury, Open-Space
Stakeholderprozesse	• Demokratisierung, Steigerung von Akzeptanz und Legitimität • Gemeinsame robuste und resiliente Strategien mit hoher Wirkung	Kollektive Entwicklung von Visionen, Strategien und Aktionsplänen	• Organisierte Interessenvertreter für alle relevanten Stakeholder-gruppen („whole system in the room“) oder • Unmittelbar von einem Vorhaben betroffene Bürgerinnen und Bürger (z. B. Anwohner)	Zukunftskonferenz, Szenariowork-shops, Future Search, Deliberative Visioning, Roadmapping, Deliberation, Delphi-Umfragen, Causal Layered Analysis
Interaktive Wertschöpfung	Produktoptimierung und dadurch Markterschließung	Generierung von Ideen, Gestaltung	Nutzer a) mit speziellen Anforderungen b) als Repräsentanten einer möglichst breiten Spannweite	Lead-user-Workshop, Innovationsbaukasten, Prototypen-Workshop
Partizipatives Design/ Constructive technology Assessment (CTA)	Optimale Anpassung eines technischen Systems an die Bedürfnisse der Anwender	Gestaltung eines technischen Systems	Personenkreis, der von einer Systemgestaltung betroffen ist	Zukunftswerkstatt, Fokusgruppen, ethnographische Methoden[68]: Kontextanalyse, Visioning, Situative Interviews, Szenariobasiertes Design, Storyboards, Kartenspiele, Archetypische Personen (Persona)

68 Vgl. Blomberg et al. 1993.

2. Die Ansätze im Einzelnen

Im Folgenden werden die vier Typen partizipativer Technikgestaltung jeweils kurz umrissen und anhand ihrer charakteristischen Methoden und ausgewählter Anwendungsbeispiele exemplarisch vorgestellt.

2.1. Bürgerdiskurse

Ein Teil der Bürgerdiskurse zielt auf die Beteiligung von Bürgerinnen und Bürgern an Entscheidungen über Technologiefragen. Häufig werden Empfehlungen zu Gesetzgebungsverfahren oder Technikprojekten erarbeitet. In anderen Fällen steht die Erfassung der Werthaltungen und Beurteilungen der am Diskurs beteiligten Personen im Mittelpunkt, um diese dann an die Politik zu übermitteln. Ein wichtiger Bestandteil dieser Verfahren ist in der Regel die gründliche, neutrale Information der Teilnehmenden über die betreffenden Technologien, oft ist eine Befragung von Expertinnen und Experten durch die Bürgerinnen und Bürger Bestandteil der Prozesse. Bürgerdiskurse richten sich nicht auf konkrete Technikgestaltung oder Entwicklung, sondern eher auf Bewertung vorhandener Technologien oder Technologievisionen.

Verfahren der Bürgerbeteiligung sind im Kontext der partizipativen Technikfolgenabschätzung seit Jahrzehnten weiterentwickelt worden. Aktuelle Veröffentlichungen mit ausführlicher Methodenreflexion und Zusammenstellungen der gängigen Methoden liegen vor.[69]

Typische Methoden und Techniken der Bürgerdiskurse sind Konsensuskonferenz, Bürgerkonferenz, Planungszelle, Fokusgruppen, Interview-Meeting, Citizens Jury, Open Space.

2.1.1. Methodenbeispiele Bürgerdiskurse

Konsensus-Konferenz[70] Bei einer Konsensus-Konferenz erarbeiten ausgewählte heterogen zusammengesetzte Personengruppen in intensivem Dialog mit Fachleuten eine konsensuale Antwort auf eine politisch oder gesellschaftlich kontrovers diskutierte Frage. Einbezogen werden rund 10 bis 30 interessierte Bürgerinnen und Bürger, die in Bezug auf Alter, Geschlecht, Bildungsgrad und Berufsspektrum einen möglichst repräsentativen Querschnitt der Bevölkerung

69 Vgl. Nentwich et al. 2006, Steyaert et al. 2006 (Strategiegruppe Partizipation ÖGUT 2002b).

70 Vgl. Steyaert et al. 2006, S.67-82.

darstellen. Sie arbeiten sich mithilfe von Hintergrundberichten, Zeitungsartikeln, Stellungnahmen etc. in die Fragestellung ein und treffen sich zwei Mal zu vorbereitenden Sitzungen. Die Konsensus-Konferenz selbst findet an drei aufeinanderfolgenden Tagen statt. Dabei wird das Thema durch Sachverständige umfassend dargestellt, die Teilnehmerinnen und Teilnehmer haben die Möglichkeit, diese Fachleute zu befragen und das Thema (umfassend) zu diskutieren. Schließlich erstellen die Bürgerinnen und Bürger einen schriftlichen Bericht mit ihren im Konsens erzielten Stellungnahmen, Empfehlungen und deren Begründung. Der Bericht wird Entscheidungsträgern präsentiert.

Planungszelle[71]
Die von Peter C. Dienel entwickelte „Planungszelle ist eine Gruppe von BürgerInnen, die nach einem Zufallsverfahren ausgewählt und für begrenzte Zeit von ihren arbeitstäglichen Verpflichtungen vergütet freigestellt worden sind, um, assistiert von ProzeßbegleiterInnen, Lösungen für vorgegebene, lösbare Planungsprobleme zu erarbeiten“.[72] Die erforderlichen Informationen erhalten die beteiligten Bürgerinnen und Bürger durch Ortsbegehungen, Impulsreferate und Expertenanhörungen aber auch in Hearings mit betroffenen Personen und Verbänden.
In wechselnden Kleingruppen werden sodann konkrete Aufträge bearbeitet und anschließend die jeweiligen Resultate im Plenum präsentiert und zur Diskussion gestellt. Die Resultate einzelner Arbeitseinheiten stellen lediglich Zwischenergebnisse dar; sie münden schließlich in ein möglichst konsensuales Bürgergutachten. Planungszellen umfassen in der Regel rund 25 (aber auch bis zu 250) nichtorganisierte Personen. Die Veranstaltung selbst dauert im Durchschnitt 5 Tage.

Interview Meeting[73]
Das Interview Meeting ist eine Kombination von Gruppeninterview und schriftlicher Befragung. Eine Gruppe von ca. 30 Personen wird zunächst durch Experten über die zur Debatte stehende Technologiefrage informiert und diskutiert dann in Kleingruppen. Anschließend wird individuell ein Fragebogen ausgefüllt. Ziel ist die Ermittlung von Einstellungen, Werten und Begründungszusammenhängen rund um die Technologie. Das Meeting dauert insgesamt ca. 3 Stunden und wird abends nach der Arbeit abgehalten. Es ist keine Repräsentation der Bevölkerung angestrebt.

71 Nentwich et al. 2006. S. 35-36 (Strategiegruppe Partizipation ÖGUT 2002a), s.a. Steyaert et al. 2006, S. 67ff.

72 Dienel 2002

73 Vgl. The Danish Board of Technology

2.1.2. Anwendungsbeispiele Bürgerdiskurse

Konsensus Konferenz "Energieversorgung der Zukunft in Deutschland?", Essen März 2010[74]
23 Bürgerinnen und Bürger aus Essen und Umgebung im Alter von 29 bis 77 Jahren diskutierten im Rahmen einer „Konsensuskonferenz“ an drei aufeinander folgenden Wochenenden die Energieversorgung der Zukunft in Deutschland. Nach einem intensiven Austausch mit 13 Energie-Experten entwickelten sie im Konsens ein Bürgergutachten mit Empfehlungen an Forschung und Politik darüber, wie Deutschland in Zukunft seine Energie gewinnen sollte. Das Gutachten enthält Empfehlungen zu verschiedenen Bereichen wie Strom und Mobilität. Dabei berücksichtigten die Bürger Wirtschaftlichkeit, Umweltverträglichkeit und Versorgungssicherheit als gängige Kriterien der Energieversorgung und fügten die Komponente der Sozialverträglichkeit hinzu. Die Diskussion soll mit möglichst vielen verschiedenen Akteuren aus dem Energiesektor fortgeführt werden. Die Konferenz war Teil des Forschungsprojektes "Wissenschaft debattieren!", in dem die Initiative Wissenschaft im Dialog (WiD) gemeinsam mit Sozialwissenschaftlern des Forschungsinstituts ZIRN der Universität Stuttgart untersucht, mit welchen Mitteln und mithilfe welcher Veranstaltungsformate sich Bürger am besten am Diskurs über Forschungsthemen beteiligen.

Prise Interview Meeting[75]
Im Jahr 2007 fanden im Rahmen des EU-geförderten Prepatory Action for Security (PRISE)-Projektes in sechs europäischen Ländern Interview-Meetings statt. Erklärtes Ziel war es, Meinungen und Argumente aus der Bevölkerung zum Themenfeld „Privacy versus Security“ zusammenzutragen, um Präferenzen und Werturteile beim Ausgestaltungsprozess zukünftiger Sicherheitstechnologien berücksichtigen zu können.
Im Vorfeld der Veranstaltungen wurden verschiedene Zukunftsszenarien über das Zusammenspiel von Sicherheitstechnologien und Datenschutz- bzw. persönlichkeitsrechtlichen Anforderungen, beispielsweise beim Einsatz von biometrischen Verfahren, Videoüberwachung oder Ortungstechnologien an die Teilnehmer ausgegeben. Diese Szenarien wurden eingangs durch ergänzende Experteninformationen näher erläutert. Einstellungen in Bezug auf Sicherheitstechnologien und Zukunftsszenarien wurden anschließend mithilfe eines standardisierten Fragebogens erhoben. In moderierten Kleingruppeninterviews wurden schließlich vertiefende Fragestellungen zu prononcierten, die öffentliche Debatte bestimmenden Themen diskursiv erarbeitet und abschließend im Plenum zusammengetragen.

2.2. Stakeholderprozesse

Stakeholderprozesse unterstützen eine Gruppe von Akteuren bei der Entwicklung von Strategien, angefangen von der Einschätzung der Situation über die Bildung von Ziel-

74 Vgl. http://www.wissenschaft-debattieren.de/konsensuskonferenz.html

75 Vgl. Danish Board of Technology 2007.

vorstellungen bis hin zur Entwicklung und Implementierung von Strategien. Die Akteure gehören einer gemeinsamen „Arena“ an, etwa in räumlicher Hinsicht (Nachbarschaft, Stadt, Region, Land) oder organisatorisch (Einrichtung, Firma, Sektor, Innovationssystem). Wichtig für erfolgreiche Stakeholderprozesse ist die Berücksichtigung sämtlicher relevanter Perspektiven für den betreffenden Bereich durch die Einbeziehung von Repräsentanten aller relevanten Akteure (Stakeholder). Im Mittelpunkt der Prozesse steht das Ausloten von Gemeinsamkeiten zwischen verschiedenen Interessen und Positionen und die Aushandlung von für alle akzeptablen Strategien. Häufig werden Ideen oder Visionen generiert und konkrete Handlungsoptionen erarbeitet. Technische Entwicklungen kommen in der Regel als einer von mehreren Aspekten des Wandels zum Tragen, können aber auch im Mittelpunkt der Strategieentwicklung stehen.

Typische Methoden und Techniken von Stakeholderprozessen sind: Visioning, World-Cafe, SWOT Analyse, System Mapping, Szenarioworkshops, Roadmapping, Delphi Umfragen, Causal Layered Analysis, Deliberative Visioning, Future Search/Zukunftskonferenz;

2.2.1. Methodenbeispiele Stakeholderprozesse

Szenarioworkshop
In Szenarioworkshops entwickelt eine Gruppe von Stakeholdern gemeinsam konsistente, plausible Zukunftsbilder – die Szenarien. Dabei wird ein komplexes System zunächst in Einzelfaktoren zerlegt und deren mögliche Entwicklung diskutiert. Die systematische und strukturierte Vorgehensweise stellt sicher, dass Kenntnisse und Einschätzungen aus verschiedenen Perspektiven in die Szenarioentwicklung eingehen („kollektive Intelligenz“) und systematisch die Bereiche möglicher Veränderungen bedacht werden. Szenarioworkshops können ein gemeinsames Verständnis der Dynamik des Gesamtsystems fördern und damit eine Grundlage für eine robuste, resiliente Strategieentwicklung sowie eine normative Debatte von Zielvorstellungen darstellen.

Future Search[76]/Zukunftskonferenz
Die Future Search Zukunftskonferenz zielt auf die Entwicklung einer Vision und eines Aktionsplans zu deren Umsetzung. Die Erarbeitung wird in einem gemeinsamen Verfahren mit allen maßgeblichen Stakeholdern eines Systems vorgenommen. Dabei wird stets in folgenden Schritten vorgegangen: Gemeinsame Bewertung der Vergangenheit, Stellungnahmen der Einzelgruppen zur Bewertung der Situation („Prouds and Sorrys“), Festhalten von Gemeinsamkeiten, Erstellung eines Vision-Statement, Entwicklung konkreter Visionen zu Einzelbereichen in Kleingruppen, Entwicklung eines Aktionsplans. Der dreitägige

76 Weisbord, Janoff 2000

Prozess läuft nach genauen Regeln ab, die durch einen Prozessbegleiter umgesetzt werden.

2.2.2. Anwendungsbeispiele Stakeholderprozesse

Foresight Irland 2025[77]
In Irland wurde nach der ökonomischen Krise 2008 im Jahr 2009 ein Foresight Prozess durchgeführt, um die Grundlagen für eine neue wirtschaftspolitische Strategie zu erarbeiten. Unter der Leitung des irischen Rats für Forschungs- und Technologiepolitik Forfas wurden nicht nur eine Reihe von Unternehmen und Unternehmensverbänden, sondern auch Vertreter anderer relevanter Stakeholdergruppen wie Verbraucher, Kirchen, internationale Organisationen und Einwanderer einbezogen. In Interviews und gruppenspezifischen Workshops wurden elf Treiber von Veränderung sowie vier besonders kritische Bereiche sozio-ökonomischen Wandels identifiziert, auf deren Grundlage vier Szenarien zu den Perspektiven Irlands unter Berücksichtigung weltweiten Wandels generiert wurden. Dies diente der Ableitung strategischer Maßnahmen zur Förderung einer langfristigen, wettbewerbsfähigen Unternehmenslandschaft und gleichzeitig der Absicherung hoher Lebensqualität in Irland. Die technologiepolitischen Maßnahmen konzentrierten sich auf die Bereiche Informations- und Kommunikationstechnologie, Energie und Verkehr.

Zukunftskonferenz Wasser Vision Naxos (Future Search Conference)[78]
Auf der griechischen Insel Naxos wurde 2003 eine Future Search Conference abgehalten, um Lösungsansätze für die strittige Wasserallokation für verschiedene Zwecke und Regionen zu erarbeiten. Geleitet von einem Moderationsteam generierten 36 eingeladene Stakeholder, darunter Landwirte, Wissenschaftler, Anwohner aus verschiedenen Regionen, Unternehmer, Hoteliers, NGOs, die gemeinsame Vision eines nachhaltigen Wassermanagements. Dabei entwickelte zunächst jede Stakeholdergruppe vor dem Hintergrund vorab entwickelter Umfeldszenarien eine eigene Zukunftsvorstellung. Basierend auf den Gemeinsamkeiten der verschiedenen Sichtweisen wurde dann eine gemeinsame Zukunftsvorstellung erarbeitet. Im nächsten Schritt wurden in gemischten Gruppen Ideen und Maßnahmen zur Umsetzung der gemeinsamen Vision diskutiert. Während die erzielten Ergebnisse (Vision und Aktionsplan) sich als zu allgemein zur direkten Umsetzung herausstellten, wurde die Entwicklung einer gemeinsamen Basis der verschiedenen Gruppen als wichtige Voraussetzung für die Entwicklung einer künftigen Strategie für die nachhaltige Wasserbewirtschaftung der Insel Naxos bewertet.

77 Forfás 2009

78 Kallis et al. 2009

2.3. Interaktive Wertschöpfung

Verfahren aus dem Bereich der interaktiven Wertschöpfung[79] werden vor allem von Unternehmen mit dem Ziel der Produktoptimierung eingesetzt. Die Verfahren zielen darauf, Nutzerinnen und Nutzer zu einem frühen Zeitpunkt in die Entwicklung von Produkten einzubeziehen. Hintergrund ist die Beobachtung der Innovationsforschung, dass das Wissen über den Anwendungskontext, über das häufig Techniknutzer eher als Hersteller verfügen, oft maßgeblich für bahnbrechende Innovationen ist.[80] Diese Verfahren zielen in der Regel auf Nutzer mit besonders ausgeprägten Anforderungen (Lead-user) und konzentrieren sich meist auf die Ideengenerierung oder die Poduktgestaltung in einer sehr frühen Phase des Innovationsprozesses.[81]
Andere Verfahren wiederum zielen auf Personalisierung von Produkten, um der immer höheren Vielfalt individueller Anforderungen gerecht zu werden. In diesen Fällen werden Nutzer in die Lage versetzt, innerhalb eines vorgegebenen Rahmens ihr eigenes Produkt individuell zu gestalten, zu personalisieren. Einige Firmen setzen Software-Plattformen als „Toolkits“ ein, um die Interaktion mit den Nutzern in verschiedenen Phasen zu realisieren.[82]

Typische Methoden und Techniken der interaktiven Wertschöpfung sind: Lead-user-Workshop unter Anwendung von Kreativitätstechniken, Innovationsbaukasten, Prototypen Workshop

2.3.1. Methodenbeispiele interaktive Wertschöpfung

Lead-user-Workshop[83]
Mithilfe von Trendanalysen, Screening-Verfahren, Ideenwettbewerben o.ä. erfolgt zunächst die Auswahl der Teilnehmer des Workshops, der sogenannten Lead-user. Anschließend erarbeiten die ca. zehn Lead-user und Experten aus verschiedenen Unternehmensbereichen an ein bis drei Tagen unter der Anleitung eines Moderators Ideen und Konzepte für ein genau umrissenes Innovationsvorhaben. Nach einer Einleitung in den Produktbereich und die zugrunde liegende Fragestellung erfolgt der Einstieg in den Prozess der Ideenfindung und die Konzeptionierung einer Problemlösung. Hierfür stehen verschiedene Kreativitätstechniken wie Brainstorming-Techniken oder Verfahren zur Prozessvisualisierung zur Verfügung. Eine anschließende Prototypisierung mithilfe von *Rapid-Prototyping* ist denkbar.

---

79 Reichwald, Piller 2006

80 von Hippel 2005, S.19-31. Von Hippel nennt Beispiele für relevante Nutzerinnovationen aus den Bereichen Maschinenbau, Elektronik-Schaltkreise, Medizintechnik, Sportartikel und Software.

81 Herstatt, Henkel 1992.

82 Vgl. Reichwald, Piller 2006, S. 163 ff.

83 Vgl. Reichwald, Piller 2006, S. 156 ff.

Innovations-Toolkit[84]
Toolkit-Systeme zur interaktiven Wertschöpfung bilden, unter der Voraussetzung entsprechender technischer Möglichkeiten, eine Alternative zum Lead-user-Workshop. Es wird vom Hersteller eine Entwicklungsumgebung zur Verfügung gestellt, die es dem Nutzer ermöglichen soll, seine Bedürfnisse direkt in konkrete Lösungen zu überführen. Diese Bedürfnisse und Lösungen werden dem Hersteller anschließend zur Verfügung gestellt. Um einen möglichst hohen Grad an Innovation sicher zu stellen, sollte der Spielraum für den Nutzer sowie die Benutzerfreundlichkeit, ähnlich einem „Chemiebaukasten", möglichst groß sein. Zielgruppe sind wiederum vor allem Lead-user, da von diesen großes technisches Know-how verbunden mit kreativem Potenzial erwartet werden kann.

2.3.2. Anwendungsbeispiele interaktive Wertschöpfung

3M Lead-user-Workshop[85]
1996 wurde eine Abteilung des internationalen Technologiekonzerns 3M, zuständig für die Steuerung des Marktbereiches medizinisch-chirurgischer Produkte, zu einer der ersten Abteilungen, die den Lead-user-Prozess für den Konzern praktisch umsetzten. Nach einer gründlichen mehrmonatigen Recherche- und Sondierungsphase, bei der es vor allem darum ging, mithilfe von Management, Experten und potenziellen Nutzern mögliche Trends im Bereich der Infektionskontrolle zu identifizieren, wurde, basierend auf den gewonnenen Erkenntnissen, ein Lead-user-Workshop ausgerichtet. Ziel des Workshops war es, einen vollkommen neuen Ansatz zur Infektionskontrolle zu entwickeln und dies mit möglichst geringen Kosten und unter Einsatz verfügbarer Technologien. Über zweieinhalb Tage hinweg trafen sich die Teilnehmer - Lead-user, Mitarbeiter aus Technik und Marketing bzw. des Organisationsteams - in Kleingruppen mit wechselnder Zusammensetzung. Dabei lag die Herausforderung vor allem darin, kreative Ideen mit dem technisch Machbaren übereinzubringen. Anschließend wurden die Ergebnisse im Plenum zu Konzepten ausgearbeitet. Resultat waren sechs ausgearbeitete Vorschläge für neue Produktlinien die u.a. einen innovativen Ansatz zur Infektionskontrolle beinhalteten und damit dem Unternehmen zusätzliche Absatzmöglichkeiten eröffneten. Drei der ausgearbeiteten Konzepte wurden in der Folge dem Management vorgestellt.

D.tools – open Innovation Toolkit[86]
D.tools basiert auf einem Interface aus mobilen, greif- und fühlbaren Bestandteilen und ist ein computerbasierter „Gerätebaukasten", der speziell zur Unterstützung der Designentwicklung eingesetzt wird, z.B. zur Entwicklung von Produkt- oder Interaktionsdesigns. Der Gerätebaukasten unterstützt erfahrene Nutzer ohne besonderes Spezialwissen elektronische Bestandteile zu einfachen Prototypen zusammenfügen, ohne dass dabei ein Schaltungsaufbau oder Pro-

84 Vgl. Reichwald, Piller 2006, S. 163 ff.

85 Vgl. von Hippel et al. 1999, S.8.

86 Vgl. Hartmann et al. 2006.

grammierkenntnisse erforderlich wären. Zunächst lassen sich Geräte wie beispielsweise ein MP3-Player grob aus einer schaumstoffartigen Masse formen, um dann durch d.tools-Komponenten wie Schalter, Tasten oder LCD-Bildschirme vervollständigt zu werden. Eine PC-Editor-Software wird über ein Kabel und eine Kontrollbox mit dem Prototypen verbunden. Am Computer können nun die physischen d.tools-Komponenten des Prototypen als virtuelle Repräsentationen bearbeitet werden. So können Graphiken, Klänge oder andere spezielle Konfigurationen zusammengestellt und miteinander verbunden werden.

Nestle FoodServices Toolkit[87]
Wenn es bei Nestle FoodServices darum geht, Rezepturen für Fertiggerichte für Franchise-Restaurantunternehmen und Schnellrestaurants zu entwickeln, spielen die Chefköche der betroffenen Restaurantketten eine herausragende Rolle. Sie entwickeln mit Hilfe verfügbarer Zutaten die Rezepte und übermitteln diese anschließend an Nestle FoodServices zur Produktion. Die so kreierten Rezeptideen lassen sich allerdings in der Regel nicht unmittelbar auf eine industrielle Produktion übertragen, da beispielsweise die Lebensmittel nicht in der erforderlichen Menge und in konstant hoher Qualität beschafft werden können. Und auch die ursprünglich von den Köchen verwendete Produktionsausrüstung kann nicht immer auf Massenherstellung ausgerichtet werden. Der Prozess zur Rezepturfindung erfordert daher häufig einen genauen, langwierigen und somit teuren Abstimmungsprozess zwischen Nestle und den Restaurantköchen. Um die Geschwindigkeit dieses Verfahrens zu erhöhen und die Kosten zu senken, wurde ein Werkzeugkasten aus genau auf den Produktionsprozess abgestimmten Komponenten erstellt, die von den Köchen in der Phase der Produktenwicklung verwendet werden können. Im Falle einer Sauce besteht ein Komponentenset beispielsweise aus 20 bis 30 einzeln verpackten Komponenten, zusammen mit einer Gebrauchsanweisung. In einem Trial-and-Error Prozess wird mithilfe dieser Komponenten nun ein Rezept entwickelt, das eins zu eins von Nestle FoodServices reproduziert werden kann.

2.4. Partizipatives Design

Das Verfahren des partizipativen Designs ist auf die gemeinsame Gestaltung eines bestimmten Systems mit den unmittelbar involvierten Personen (co-design)[88] gerichtet. Das partizipative Design entwickelte sich aus der skandinavischen Tradition der nutzerzentrierten Gestaltung von Arbeitsprozessen und Arbeitsumgebungen, angelehnt an den Leitgedanken einer Humanisierung der Arbeit. Populär wurde das Verfahren vor allem aufgrund seiner Erfolge im Softwarebereich, es wird mittlerweile in ganz verschiedenen Bereichen so etwa im Rahmen der technischen Kommunikation genutzt.[89]

87 Vgl. von Hippel 2001.

88 Buur, Matthews 2008.

89 Spinuzzi 2005

Einschlägige Forschungsinstitute wie das „Participatory Innovation Research Centre“ der University of South Denmark SPIRE[90] treiben die Methodenentwicklung ebenso voran wie professionelle Designteams großer Unternehmen wie Philips[91] und IBM. Im Gegensatz zum Lead-user-Ansatz geht es bei dem partizipativen Design nicht um besondere Vorreiter, sondern gerade um das Verstehen gewöhnlicher Nutzerinnen und Nutzer. Das partizipative Design hat eine große Vielzahl von Methoden hervorgebracht, die immer wieder auf den jeweiligen Fall angepasst werden. Sie beruhen auf Erkenntnissen aus der qualitativen Sozialforschung, der Psychologie sowie aus Design-, Markt- und Konsumforschung. Insbesondere die Design-Anthropologie hat – in Analogie zur ethnographischen Beobachtung anderer Kulturen – Methoden entwickelt, um Nutzungsweisen und Nutzungskontexte zu verstehen.[92] In neuerer Zeit wird von verschiedenen Seiten vorgeschlagen, partizipative Verfahren auch im Rahmen einer öffentlich geförderten Technikgestaltung einzusetzen.[93] Für solche Bedarfsanalysen eignen sich die Verfahren des partizipativen Designs in hohem Maße. So setzt etwa das Forschungsprojekt „WiMi Care“ unter der Leitung von Sozialwissenschaftlern der Universität Duisburg-Essen Verfahren der qualitativen Sozialforschung bei der Entwicklung von Pflegerobotern ein.[94] Ähnliche Ansätze sind auch in der Technikfolgenabschätzung unter dem Label „Constructive Technology Assessment (CTA)“ schon früh gefordert[95] aber bisher im Bereich der staatlich geförderten Technikfolgenabschätzung nur selten umgesetzt worden.

Typische Methoden und Techniken des partizipativen Designs sind[96]:
Kontextanalyse, Situative Interviews, Problemzentrierte Interviews, Storyboard Prototyping, Video-Games, Card Games, Shared Language Games, Persona, Rollenspiele, Prototyping (Papier, Schaumstoff), Begehungen, Szenario Scripting/Szenariobasiertes Design, Zukunftswerkstatt, Fokusgruppen, Visioning.

2.4.1. Methodenbeispiele partizipatives Design

Szenariobasiertes Design[97]

90 http://www.sdu.dk/Om_SDU/Institutter_centre/C_SPIRE

91 Rameckers, Un 2005

92 Blomberg et al. 1993

93 Compagna et al. 2009; Compagna et al. 2010; Rohracher, Ornetzeder 2008; Schachtner, Roth-Ebner 2009

94 Compagna et al. 2009; Compagna et al. 2010

95 Schot, Rip 2002

96 Vgl. etwa Schuler, Naioka 1993

Grundlegend für diese Methode ist die Verwendung sogenannter Szenarien zur Darstellung bestehender oder zukünftiger Nutzungen. Aus dem Blickwinkel des Nutzers, seinen Emotionen, seiner Motivation und seinem Hintergrund heraus werden in kleinen Geschichten Anwendungssituationen, sogenannte Szenarien, anschaulich dargestellt. Zentrales Element der Darstellung ist der Umgang der handelnden Personen mit bestimmten Objekten bzw. technischen Werkzeugen. Abstraktionstiefe und Detaillierungsgrad der Szenarien werden schrittweise angepasst und begleiten so die gesamte Konzeptionsphase eines Produktes. Durchführung: Nach der ausführlichen Analyse des Nutzungskontextes findet eine Gewichtung der verschiedenen Daten und Themen statt. Die ermittelten Themen werden anschließend mithilfe verschiedener Personas (archetypischer Nutzerpersönlichkeiten) in Texten, Zeichnungen oder anderen Medien als Szenarien verdeutlicht. Die Szenarien fungieren als Grundlage für die Ermittlung von Anforderungen für eine ideale Nutzung.

Cooperative Prototyping[98]
Hier steht der Prozess der gemeinsamen Entwicklung eines oder mehrerer Prototypen, beispielsweise von Softwareanwendungen zur Erleichterung bzw. Verbesserung von Arbeitsabläufen, im Mittelpunkt. In einer ersten Untersuchungsphase werden zunächst die betreffenden Mitarbeiter zu Arbeitsabläufen und Problembereichen befragt, ihre Antworten ausgewertet und an die Befragten zurückübermittelt. Die Mitarbeiter bestimmen nun aus ihren Reihen die Teilnehmer an den anschließenden Zukunftsworkshops. Diese erarbeiten im Rahmen der Workshops zentrale Problemstellungen und einigen sich auf konkrete Schwerpunkte. Eine Expertengruppe, die selbst am Workshop teilgenommen hat, entwirft nun einen oder mehrere Prototypen zu den ermittelten Schwerpunktfragestellungen, die anschließend von den Mitarbeitern beurteilt und wiederum von den Experten angepasst werden. In einer weiteren Phase wird der Prototyp in der Anwendung erprobt und Ablauf und Ergebnisse wissenschaftlich dokumentiert und bewertet.

2.4.2. Anwendungsbeispiele partizipatives Design

Partizipative Entwicklung von Steuerungsgeräten bei Danfoss[99]
Zur nutzergerechten Entwicklung von Steuerungsgeräten für Klärwerke führte die Firma Danfoss an mehreren Klärwerken partizipative Feldstudien durch. Dabei wurden die Klärwerker zunächst beobachtet, gefilmt und interviewt. Aus Filmausschnitten wurden Karten generiert, anhand derer die Prozesse im Klärwerk in Gruppen diskutiert werden konnten. Mit Schaummodellen wurden verschiedene denkbare Prozessvarianten dargestellt und fiktive Situationen in Videos festgehalten. Als Resultat wurden verschiedene neue Steuerungsgeräte vorgeschlagen, die den tatsächlichen Bedarfen der Klärwerker angepasst sind.

---

97 Compagna et al. 2010

98 Bødeker, Grønbæk 1991

99 Buur, Matthews 2008

Szenariobasiertes partizipatives Design im Rahmen von WIMI Care[100]
Im Rahmen des Ende 2008 angelaufenen, mit Bundesforschungsmitteln geförderten Projektes „Wissenstransfers für eine aktive Mitgestaltung des Pflegesektors durch Mikrosystemtechnik“ wurden die Einsatzmöglichkeiten von Servicerobotik im stationären Pflegebereich analysiert und anschließend getestet. Zunächst wurde mithilfe ethnographischer Beobachtung, Ad-hoc- und Problemzentrierten Interviews eine Analyse von Arbeitsabläufen und Arbeitsorganisation und deren Alltagspraxis durchgeführt sowie relevante Personengruppen wie Patienten und Pflegepersonal identifiziert und befragt. Anschließend wurde eine Fokusgruppe aus Pflegekräften gebildet. Mithilfe leitfadengestützter Einzel- und Gruppeninterviews wurden nun die erarbeiteten Informationen im Rahmen der Fokusgruppe konkretisiert und vertieft. Die gesammelten Ergebnisse wurden in einem Gespräch an die Technikentwickler und Produktdesigner übermittelt, die daraus Skizzen, Pläne und Szenarien erarbeiten, um den ermittelten Bedarf mit den technischen Möglichkeiten abzugleichen. In einem iterativen Prozess wurden nun die erarbeiteten Szenarien dem Pflegepersonal präsentiert, deren Ausgestaltung gemeinsam diskutiert und entsprechend modifiziert Basierend auf den vom Pflegepersonal geäußerten Wunsch der Erleichterung von täglichen Routinetätigkeiten und logistischen Aufgaben wurden schließlich konkrete, technisch umsetzbare Szenarien für den Einsatz von Servicerobotern in der stationären Pflege erarbeitet.

100 Compagna et al. 2009; Derpmann, Compagna 2009

Literaturverzeichnis

acatech (2009): Intelligente Objekte – klein, vernetzt, sensitiv. Eine neue Technologie verändert die Gesellschaft und fordert zur Gestaltung heraus, acatech BEZIEHT POSITION – Nr. 5.

AirShield. Schutz von Mensch und Umwelt. Online verfügbar unter http://www.airshield.de/, zuletzt geprüft am 08.07.2013.

Aktion gegen Airshield an der TU-Berlin. Bildungsstreik 2009 - Technik kann Begeistern, Schützen, Töten! Online verfügbar unter http://www.youtube.com/watch?v=3gHx04OT554, zuletzt geprüft am 08.07.2013.

Banse, G.; Reher, E.-O. (Hrsg.) (2004): Fortschritte bei der Herausbildung der Allgemeinen Technologie: Symposium der Leibniz-Sozietät und des Instituts für Technikfolgenabschätzung und Systemanalyse des Forschungszentrums Karlsruhe in der Helmholtz-Gemeinschaft am 14. Mai 2004 in Berlin / Herausgegeben von Gerhard Banse & Ernst-Otto Reher; Bd. 75, Sitzungsberichte der Leibniz-Sozietät. Berlin: Leibniz-Sozietät.

Bijker, W.E.; Law, J. (1997): Shaping technology / building society. Studies in sociotechnical change, Inside technology, Cambridge/Mass.: MIT Press.

Blomberg, J.; Giacomi, J.; Mosher, A.; Swenton-Wall, P. (1993): Ethnographic Field Methods and Their Relations To Design. In: Schuler, D.; Naioka, A. (eds.): Par-ticipatory Design: Principles and Practices. pp. 123-155.

Bødeker, S.; Grønbæk, K. (1991): Cooperative Prototyping: users and designers in mutual activity. In: International Journal of Man-Machine Studies, 34 (3), pp. 453-478.

Bornewasser, M. (2005): Evaluation der Videoüberwachung: Ein Praxisbericht. Ergebnisse einer wissenschaftlichen Begleituntersuchung. In: Hempel, L.; Metelmann, J. (Hrsg.) (2005): Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. Frankfurt am Main: Suhrkamp (Suhrkamp Taschenbuch Wissenschaft, 1738).

Buur, J.; Matthews, B. (2008): Participatory Innovation. In: International Journal of In-novation Management, 12 (3), pp. 255-273.

Compagna, D.; Derpmann, S.; Graf, B.; Hartmann, C.; Jacobs, T.; Klein, P.; Luz, J.; Mauz, K.; Shire, K. (2010): Anwenderorientierte Technikentwicklung im Pflege-Bereich: Instrumente für den Wissenstransfer zur partizipativen Gestaltung von Mikrosystemtechnik. In: VDI/VDE/IT (ed.): Ambient Assisted Living 2010 : 3. Deutscher AAL-Kongress mit Ausstellung, Assistenzsysteme im Dienste des Menschen - zuhause und unterwegs. Berlin: Bundesministerium für Bildung und Forschung.

Compagna, D.; Derpmann, S.; Mauz, K.; Shire, K.A. (2009): Methoden für eine Be-darfsanalyse zum Zweck einer nutzerzentrierten Technikentwicklung, Working Brief No. 4.

The Danish Board of Technology (2007): PRISE Annexes to D 5.8 Synthesis Report - Interview Meeting on Security Technology and Privacy.

The Danish Board of Technology Methods: Interview Meeting. Online: http://www.tekno.dk/subpage.php3?article=1234&toppic=kategori12&language=uk (accessed: 05.04.2011).

Decker, M.; Grunwald, A.; Knapp, M. (Hrsg.) (2012): Der Systemblick auf Innovation. Technikfolgenabschätzung in der Technikgestaltung. 1. Auflage, Berlin: Edition Sigma (Gesellschaft - Technik - Umwelt, 16).

Derpmann, S.; Compagna, D. (2009): Erste Befunde der Bedarfsanalyse für eine partizipative Technikentwicklung im Bereich stationärer Pflegeeinrichtungen, Working Papers kultur- und techniksoziologische Studien No. 5.

Dienel, P.C. (2002): Die Planungszelle - Der Bürger als Chance, 5. Auflage, mit Statusreport 2002, Wiesbaden: Westdeutscher Verlag.

Dierkes, M. (1992): Leitbild und Technik: zur Entstehung und Steuerung technischer Innovationen, Berlin: Ed. Sigma.

Elzen, B.; Geels, F.W.; Green, K.E. (2004): System innovation and the transition to sustainability: Theory, evidence and policy. In: Elgar Publ. Ltd.

Forfás (2009): Sharing our Future: Ireland 2025, Dublin: Forfás.

Geels, F.W. (2005a): Processes and patterns in transitions and system innovations: Refining the co-evolutionary multi-level perspective. In: Technological Forecasting and Social Change, 72 (6), S. 681-696.

Geels, F.W. (2005b): Technological transitions and system innovations: a co-evolutionary and socio-technical analysis: Edward Elgar Publishing.

Geels, F.W.; Schot, J. (2007): Typology of sociotechnical transition pathways. In: Research Policy, 36 (3), S. 399-417.

Hard, M.; Jamison, A. (2005): Hubris and hybrids: a cultural history of technology and science, New York [u.a.]: Routledge.

Hartmann, B.; Klemmer, S.R.; Bernstein, M.; Abdulla, L.; Burr, B.; Robinson-Mosher, A.; Gee, J. (2006): Reflective physical prototyping through integrated design, test, and analysis. Proceedings of UIST 2006, Montreux.

Hegel, G.W.F. (1986): Phänomenologie des Geistes, 1, Moldenhauer, E.; Michel, K.M. (Hrsg.), Frankfurt am Main: Suhrkamp.

Heidegger, M. (1979): Sein und Zeit, 15., durchges. Auflage mit d. Randbemerkungen aus d. Handex. d. Autors im Anh., Tübingen: Niemeyer.

Hempel, L.; Metelmann, J. (2005): Bild - Raum - Kontrolle : Videoüberwachung als Zeichen gesellschaftlichen Wandels, Hempel, L.; Metelmann, J. (Hrsg.), Suhrkamp Taschenbuch Wissenschaft, 1738: Suhrkamp, Frankfurt am Main.

Herstatt, C.; Henkel, J. (1992): From Experience: Developing New Product Concepts via the Lead User Method. In: Journal of Product Innovation Management, 9 (3), pp. 213-222.

Hubig, Ch. (2002): Mittel. Bielefeld: Transcript (Edition panta rei, 1).

INDECT. For the Security of Citizens. Online verfügbar unter http://www.indect-project.eu/, zuletzt geprüft am 08.07.2013.

Jasanoff, S.; Markle, G.E.; Petersen, J.C.; Pinch, T. (Hrsg.) (1997): Handbook of science and technology studies. Thousand Oaks [u.a.]: Sage.

Kallis, G.; Hatzilacou, D.; Mexa, A.; Coccossis, H.; Svoronou, E. (2009): Beyond the manual: Practicing deliberative visioning in a Greek island. In: Ecological Economics, 68 (4), pp. 979-989.

Kaufmann, F.-X. (1970): Sicherheit als soziologisches und sozialpolitisches Problem - Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften, Stuttgart: Enke.

Kaufmann, F.-X. (1973): Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften. 2. Aufl. Stuttgart: Enke.

Kemp, R.; Schot, J.; Hoogma, R. (1998): Regime Shifts to Sustainability through Processes of Niche Formation: The Approach of Strategic Niche Management. In: Technology Analysis and Strategic Management, Vol. 10, S. 175-195.

Kierkegaard, S. (1984): Der Begriff Angst, Hamburg: F. Meiner.

Klauser, F.R. (2006): Die Videoüberwachung öffentlicher Räume - Zur Ambivalenz eines Instruments sozialer Kontrolle, Campus Forschung; Bd. 902, Diss., Freiburg (Schweiz), Univ., 2006 (zugl.), Frankfurt, New York, N.Y.: Campus Verl.

Kreuter, F. (2002): Kriminalitätsfurcht: Messung und methodische Probleme. Univ, Opladen, Konstanz.

Latour, B. (2005): Reassembling the social : An introduction to actor-network-theory: Oxford Univ. Press, New York.

Luhmann, N. (1997): Die Kunst der Gesellschaft. 1. Aufl. Frankfurt am Main: Suhrkamp (Suhrkamp Taschenbuch Wissenschaft, 1303).

Milgram, S. (1970): Das Erleben der Großstadt. Eine sozialpsychologische Analyse. In: Zeitschrift für Sozialpsychologie 1/1970, S. 149 f.

Nentwich, M.; Bogner, A.; Peissel, W.; Sotoudeh, M.; Torgersen, H. (Hrsg.) (2006): TECHPOL 2.0. Awareness, Partizipation und Legitimität. Endbericht. Wien.

Perrow, C. (1984): Normal Accidents. Living with high-risk technologies. New York: Basic Books.

Pfitzmann, A. (2006): Biometrie – wie einsetzen und wie keinesfalls? In: Informatik_Spektrum_29_5_2006, S. 353-356.

Rameckers, L.; Un, S. (2005): People insights at the fuzzy front of innovation. How to achieve human centred innovation?, ESOMAR Qualitative 2005 Conference.

Rammert, W. (1999): Technik. Stichwort für eine Enzyklopädie. Institute for Social Schiences, Technische Universität Berlin (TUTS-WP, 1). Online verfügbar unter http://www.ts.tu-berlin.de/fileadmin/fg226/TUTS/TUTS_WP_1_1999.pdf.

Rammert, W.; Schulz-Schaeffer, I. (2002a): Technik und Handeln. Wenn soziales Handeln sich auf menschliches Verhalten und technische Artefakte verteilt. Institut für Soziologie (TUTS-WP, 4). Online verfügbar unter http://www.ts.tu-berlin.de/fileadmin/fg226/TUTS/TUTS_WP_4_2002.pdf.

Rammert, W. (2002b): Gestörter Blickwechsel durch Videoüberwachung. Ambivalenzen und Asymmetrien soziotechnischer Beobachtungsordnungen. Institut für Soziologie Berlin. Berlin (Technical University Technology Studies Working Papers, TUTS-WP-9-2002). Online verfügbar unter http://www.ts.tu-berlin.de/fileadmin/fg226/TUTS/TUTS_WP_9_2002.pdf, zuletzt aktualisiert am 28.04.2003, zuletzt geprüft am 27.06.2012.

Rammert, W. (2002c): The Cultural Shaping of Technologies and the Politics of Technodiversity. In: Sorensen, K.; Williams, R. (Hrsg.): Shaping technology, guiding policy: Concepts, spaces and tools. Elgar Publ. Ltd., Cheltenham, UK; Northampton, MA,USA, S. 173-194.

Reichwald, R.; Piller, F. (2006): Interaktive Wertschöpfung : Open Innovation, Individualisierung und neue Formen der Arbeitsteilung, Wiesbaden: Gabler.

Renn, O. (2007): Risiko: Über den gesellschaftlichen Umgang mit Unsicherheit. Oekom-Verlag.

Rip, A.; Schot, J.W. (2002): Identifying loci for influencing the dynamics of technological development. In: Sorensen, K.; Williams, R. (Hrsg.): Shaping technology, guiding policy: Concepts, spaces and tools. Elgar Publ. Ltd., Cheltenham, UK; Northampton, MA,USA, S. 155-172.

Ripley, A. (2010): Survive. Katastrophen - wer sie überlebt und warum. Frankfurt, M: Fischer-Taschenbuch-Verlag

Rohracher, H.; Ornetzeder, M. (2008): Wohnen im "Haus der Zukunft". Eine Bestandsaufnahme sozio-ökonomischer Projekte im Rahmen der Projektlinie "Haus der Zukunft", Berichte aus Energie- und Umweltforschung 8/2008, Graz: Bundesministerium für Verkehr, Innovation und Technologie.

Rusch, G. (2010): Sicherheit, Sicherheitskultur, Sicherheitstechnik - Vortrag auf der Tagung: „Sicherheitskulturelle Dynamiken" der Forschungsgruppe Sicherheitskommunikation SiKomm am 14.07.2010 in Jena. Jena: (Stand: 28.04.2011).

Sartre, J.-P. (1991): Das Sein und das Nichts, 1. Aufl. der Neuübersetzung., König, T.; Schöneberg, H. (Hrsg.), Reinbek bei Hamburg: Rowohlt.

Schachtner, C.; Roth-Ebner, C. (2009): Konstruktivistisch-partizipative Technikentwicklung. In: Kommunikation@Gesellschaft - Journal für alte und neue Medien aus soziologischer, kulturanthropologischer und kommunikationswissenschaftlicher Perspektive, 10 (1).

Schot, J.; Rip, A. (2002): The past and future of constructive technology assessment. In: Technological Forecasting and Social Change, 54 (2-3), pp. 251-268.

Schuler, D.; Naioka, A. (eds.) (1993): Participatory Design: Principles and Practices.

Spinuzzi, C. (2005): The Methodology of Participatory Design. In: Technical Communi-cation, 52 (2), pp. 163-174.

Steyaert, S.; Lisoir, H.; Nentwich, M. (Hrsg.) (2006): Leitfaden partizipativer Verfahren. Ein Handbuch für die Praxis. Österreichische Akademie der Wissenschaften. Brüssel, Wien, Online: http://epub.oeaw.ac.at/ita/ebooks/Leitfaden_pTA_DE_Feb06.pdf (accessed 20.06.2013)

Strategiegruppe Partizipation ÖGUT (2002a): Methoden: Konsensus Konferenz. Online: http://www.partizipation.at/konsensus-konferenz.html (accessed: 08.04.2011a).

Strategiegruppe Partizipation ÖGUT (2002b): Partizipation: Alle Methoden. Online: http://www.partizipation.at/alle-methoden.html (accessed: 08.04.2011b).

von Hippel, E.; Thomke, S.H.; Sonnack, M. (1999): Creating Breakthroughs at 3M. In: Harvard Business Review, 77 (5), pp. 47-57.

von Hippel, E. (2001): Perspective: User Toolkits for Innovation. In: Journal of Product Innovation Management, 18, pp. 247-257.

von Hippel, E. (2005): Democratizing innovation, Cambridge und London: MIT Press.

Weber, K.; Bittner, U.; Manzeschke, A.; Rother, E.; Quack, F.; Dengler, K.; Fangerau, H. (2012): Taking Patient Privacy and Autonomy More Seriously: Why an Orwellian Account Is Not Sufficient. In: *The American Journal of Bioethics* 12 (9), S. 51–53.

Weisbord, M.R.; Janoff, S. (2000): Future search: an action guide to finding common ground in organizations and communities, San Francisco: Berrett-Koehler.

Witness. See it. Film it. Change it. Online verfügbar unter http://www.witness.org/, zuletzt geprüft am 08.07.2013.