INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG

manu:script

Gesellschaftliche Herausforderungen durch „intelligente Umgebungen“

Dunkle Szenarien als TA-Werkzeug

Ralf Lindner

Michael Friedewald

ÖAW
Österreichische Akademie der Wissenschaften

Wien, Sept./2007
ITA-07-07
ISSN 1681-9187

http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_07.pdf

September/2007
(ITA-07-07)

Gesellschaftliche Herausforderungen durch „intelligente Umgebungen“

Dunkle Szenarien als TA-Werkzeug

Ralf Lindner, Michael Friedewald

Fraunhofer Institut für System- und Innovationsforschung (Fraunhofer ISI), Karlsruhe

Keywords

Ambient Intelligence, Foresight, Risikoanalyse, Technikfolgenabschätzung, Szenarien-Methode, dunkle Szenarien

Abstract

Mit der umfassenden drahtlosen Vernetzung und Computerisierung von Alltagsgegenständen und Umgebungen werden nicht nur neuartige Anwendungen möglich, sondern auch zahlreiche Risiken erzeugt. Soll Ambient Intelligence (AmI) ein Erfolg werden, ist es erforderlich, angemessene Maßnahmen zu ergreifen, um Privatsphäre, Sicherheit oder Vertrauen in den jeweiligen Anwendungskontexten zu gewährleisten. Dabei besteht die Herausforderung darin, frühzeitig Vorkehrungen gegen Risiken zu entwickeln, die noch nicht manifest sind. Die im Rahmen des SWAMI-Projekts (Safeguards in a World of AMbient Intelligence) entwickelten „dunklen“ Szenarien werden als nützliches TA-Werkzeug vorgestellt, mit dessen Hilfe potenzielle Risiken in einer frühen Phase der Technikentwicklung identifiziert werden können. Nach einer Darstellung des methodischen Konzepts der dunklen Szenarien werden im Beitrag einige Beispielsituationen aus den Szenarien und die entsprechende systematische Analyse präsentiert sowie kurz die wichtigsten Empfehlungen des Projekts vorgestellt.

Inhalt

1 Einleitung ... 3

2 Der Szenarien-Ansatz von SWAMI ... 6
2.1 Dunkle Szenarien und Ambient Intelligence ... 6
2.2 Zur Methode der Szenarien-Entwicklung ... 7
2.3 Die vier SWAMI-Szenarien ... 10
2.4 Ergebnisse der Szenarien-Analyse ... 11

3 Schlussfolgerungen ... 14
3.1 Entwicklung geeigneter Schutzvorkehrungen ... 14
3.2 Methodische Aspekte ... 15

4 Literatur ... 16

Der Beitrag basiert auf dem gleichnamigen Vortrag, den die Autoren in Wien am 29. Mai 2006 im Rahmen der Sechsten Österreichischen TA-Konferenz „TA´06: Vermessen, codiert, entschlüsselt? Potenziale und Risken der zunehmenden Datenverfügbarkeit" gehalten haben.

IMPRESSUM

Medieninhaber:
Österreichische Akademie der Wissenschaften
Juristische Person öffentlichen Rechts (BGBl 569/1921 idF BGBl I 130/2003)
Dr. Ignaz Seipel-Platz 2, A-1010 Wien

Herausgeber:
Institut für Technikfolgen-Abschätzung (ITA)
Strohgasse 45/5, A-1030 Wien
http://www.oeaw.ac.at/ita

Die ITA-manu:scripts erscheinen unregelmäßig und dienen der Veröffentlichung von Arbeitspapieren und Vorträgen von Institutsangehörigen und Gästen.
Die manu:scripts werden ausschließlich über das Internetportal „epub.oeaw" der Öffentlichkeit zur Verfügung gestellt:
http://epub.oeaw.ac.at/ita/ita-manuscript

ITA-manuscript Nr.: ITA-07-07 (September/2007)
ISSN-online: 1818-6556
http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_07.pdf

1 Einleitung

Die Vision des Ambient Intelligence („intelligente Umgebungen“) postuliert eine künftige Gesellschaft, in der die Menschen von quasi autonomen und im Hintergrund agierenden Assistenzsystemen umgeben sind, die sich proaktiv auf die Bedürfnisse des Nutzers einstellen und dabei weitgehend ohne herkömmliche Mensch-Maschine-Schnittstellen auskommen. Angestrebt wird eine draht- und nahtlose Vernetzung von Alltagsgegenständen und Umgebungen, die mit rechnergestützten Sensoren und Aktuatoren versehen sind. Der Begriff Ambient Intelligence (AmI), der ursprünglich auf Emile Aarts von Philips Research zurück geht (vgl. Aarts und Appelo 1999), wurde bald von der Information Society Technologies Advisory Group der EU aufgegriffen (ISTAG 2001, 2003) und als ein Schwerpunkt in den Forschungsbereich „Künftige Technologien für die Informationsgesellschaft“ des Sechsten Forschungsrahmenprogramms integriert (vgl. Friedewald 2007). Wesentliche Elemente der Zukunftsvision AmI basieren auf Mark Weisers paradigmatischem Konzept des ubiquitous computing, das dieser Ende der 1980er Jahre als leitender Wissenschaftler am Xerox Palo Alto Research Center (Parc) zusammen mit seinen Forscherkollegen entwarf. In einem viel beachteten Zeitschriftenbeitrag beschreibt Weiser (1991) ubiquitous computing als dritte Generation von Computersystemen – nach Großrechnern und PCs –, die sich insbesondere dadurch auszeichne, dass Datenverarbeitung zu einem integralen und weitgehend unsichtbaren, aber für den Menschen leicht zugänglichen Bestandteil des Alltags wird (vgl. ebd., 92). Der Grundgedanke der unmerklichen Durchdringung der dinglichen Welt mit Informations- und Kommunikationstechnologien („Heinzelmännchen-Technologie“) ist seither in zahlreichen Varianten fortentwickelt worden, die durch jeweils spezifische Akzentuierungen, Reichweiten und Entstehungszusammenhänge charakterisiert sind. Zu den gebräuchlichsten Begriffen, die häufig synonym und uneinheitlich verwendet werden, zählen neben ubiquitous computing und AmI auch pervasive computing, nomadic computing, disappearing computing, sensor networks, embedded systems und neuerdings the internet of things bzw. das Internet der Dinge.

Der normative Gehalt der explizit nutzerzentrierten AmI-Vision (vgl. Punie 2005, 113) besteht in der Erwartung positiver Auswirkungen der Technologie auf die individuelle Lebensqualität – und zwar in nahezu sämtlichen lebensweltlichen Kontexten. In dem Maße jedoch, wie die allgegenwärtigen personalisierten Dienste und Anwendungen von AmI in das alltägliche Leben – in Beruf, Freizeit, in der Wohnung, unterwegs usw. – integriert werden, erhöht sich nicht nur der persönliche Komfort, die Kommunikations- und Leistungsfähigkeit, sondern es ergeben sich mit Blick auf Privatsphäre, Identität, Datenschutz und -sicherheit zahlreiche problematische Implikationen und potenzielle Gefahren. Die möglichen Risiken beruhen insbesondere darauf, dass

- ein Großteil der individuellen Alltagsaktivitäten erfasst, gespeichert, verarbeitet und innerhalb der allgegenwärtigen Netzwerke übermittelt wird, um die vorgesehenen personalisierten Dienste zu ermöglichen;
- sich somit die *Quantität* der in Umlauf befindlichen personenbezogenen Daten dramatisch steigern wird und die Daten zudem in wachsendem Maße miteinander verknüpft und ggf. zweit- und mehrfach verwertet werden können;
- sich die *Qualität* der personenbezogenen Daten aufgrund des Einsatzes von Kameras, Wahrnehmungssensoren und biometrischen Verfahren tiefgreifend wandeln wird.

Innerhalb der Forschungs- und Entwicklungsszene wächst das Bewusstsein über die systemimmanenten Herausforderungen von AmI, die sich aus unsichtbaren, vernetzten und weitgehend autonom agierenden Systemen für den Schutz von Privatsphäre, Identität und die Datensicherheit ergeben.[1] Obwohl davon auszugehen ist, dass die Entwicklung und Umsetzung von geeigneten Schutzmaßnahmen eine zentrale Voraussetzung für die breite Akzeptanz von AmI sein wird, sind bislang jedoch nur vereinzelt Anstrengungen unternommen worden, um die potenziellen Risiken zu benennen, zu analysieren und schließlich Wege aufzuzeigen, wie die problematischen Folgen von AmI verhindert werden können. Mit Blick auf die sozio-ökonomischen Auswirkungen von AmI stellt sich die gegenwärtige Forschungslandschaft wie folgt dar:

Die europäische „Information Society Technologies Advisory Group" (ISTAG) entwickelte vor einigen Jahren eine erste Reihe von Szenarien, mit denen die Potenziale von AmI beschrieben wurden und die die Grundlage für die Formulierung des AmI-Schwerpunktes im Sechsten Rahmenprogramm darstellen (ISTAG 2001; 2002). Obwohl diese Szenarien – zumindest teilweise – den Ansatz des Constructive Technology Assessment (CTA) verfolgten, um positiv auf die Prozesse der Technikentwicklung einzuwirken (vgl. Schot und Rip 1997), wurde die Vielzahl möglicher Implikationen für den Einzelnen und die Gesellschaft kaum thematisiert. Bedürfnis- bzw. nutzerorientierte Roadmaps (z. B. Friedewald und Da Costa 2003) folgen dem gleichen Ansatz, versuchen aber Technologieangebot und -nachfrage in Beziehung zu setzen. Hier spielen gesellschaftliche Bedarfe, Alltagsanforderungen und Akzeptanzfaktoren bereits eine bedeutende Rolle.

Fragestellungen der Innovations- und Technikanalyse im umfassenden Sinne haben vor allem die schweizerische Studie von Hilty et al. (2003) und das von der Gottlieb Daimler- und Karl Benz-Stiftung finanzierte Ladenburger Kolleg „Leben in einer smarten Umgebung – Auswirkungen des Ubiquitous Computing" (Mattern 2003, 2007) behandelt. Die Studie von Hilty et al. (2003) ist allerdings auf die Auswirkungen von AmI auf Gesundheit und Umwelt beschränkt und behandelt darüber hinausgehende gesellschaftliche und individuelle Auswirkungen (z. B. unkalkulierbares Verhalten der Technik, Reizüberflutung und Ablenkung der Aufmerksamkeit, Datenschutz und Datensicherheit) nur kursorisch im Zusammenhang mit den gesundheitlichen Aspekten. Im Rahmen des Ladenburger Kollegs „Leben in einer smarten Umgebung" wurden – allerdings überwiegend aus einer technologisch orientierten Sicht – ebenfalls mögliche Anwendungsszenarien entwickelt, die nur punktuell kritisch auf die Folgen für Individuum und Gesellschaft hinterfragt wurden (vgl. die Beiträge in Mattern 2003).

Ferner befassten sich auch zwei Projekte des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) mit Fragen des ubiquitären Computing. Das Projekt „Risiken und Chancen des Einsatzes von RFID-Systemen" betrachtete vorrangig die kurz- bis mittelfristigen Chancen und Risiken des Einsatzes von RFID-Systemen mit Fokus auf die IT-Sicherheit und den Einsatz im Bereich Handel, Identifizierung und Authentifizierung (vgl. Oertel et al. 2004). Das Projekt „Pervasive Computing – Entwicklungen und Auswirkungen" analysierte zwar einen längeren Zeithorizont, war allerdings ebenfalls auf Fragen der IT-Sicherheit und Anwendungen im Bereich von Identifikationssystemen begrenzt (vgl. Gabriel et al. 2006). Beide Studien verstehen sich nicht als Innovations- und Technikanalysen im umfassenderen Sinne, insbesondere fehlt ihnen die breite Betrachtung von gesellschaftlichen und individuellen Anforderungen jenseits der IT-Sicherheit.

[1] So wurde im November 2006 im Rahmen des EU-finanzierten F&E-Projekts Embedded WiSeNts (Cooperating Embedded Systems for Exploration and Control featuring Wireless Sensor Networks) ein internationaler Experten-Workshop zu den gesellschaftlichen Auswirkungen der Technologie abgehalten, in dessen Rahmen auch ein Teil der SWAMI-Ergebnisse vorgestellt wurde. (http://www.embedded-wisents.org/workshop/index.html; letzter Zugriff: 02.08.2007).

Aus dem Projekt TAUCIS (Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung), das vom deutschen Bundesministerium für Bildung und Forschung in Auftrag gegeben wurde, ist die bislang umfassendste deutschsprachige TA-Studie zum Thema AmI hervorgegangen (vgl. Bizer et al. 2006). Untersucht wurden die rechtlichen, technischen und gesellschaftlichen Rahmenbedingungen und Auswirkungen intelligenter Umgebungen; ein besonderer Schwerpunkt lag darauf, wie das Recht auf informationelle Selbstbestimmung der beteiligten Nutzer unter den Bedingungen von AmI gewährleistet werden kann. Teil der Studie sind sechs Szenarien, die exemplarisch das Leben mit AmI aufzeigen. Die TAUCIS-Szenarien haben dabei vorwiegend die Funktion, die mögliche AmI-Zukunft zu veranschaulichen; eine systematische Analyse der Auswirkungen der Technologie war damit nicht intendiert.

Das im August 2006 abgeschlossene Forschungsprojekt Safeguards in a World of AMbient Intelligence (SWAMI) befasste sich mit den potenziellen individuellen und gesellschaftlichen Folgen von künftigen AmI-Anwendungen.[2] Aufgabe des Projekts war es, politische Handlungsoptionen und Forschungserfordernisse zu identifizieren, um den gesellschaftlichen, rechtlichen und organisatorischen Implikationen von AmI angemessen zu begegnen. Der Fokus der Analyse lag auf den möglichen Auswirkungen künftiger AmI-Anwendungen auf die Privatsphäre, das Vertrauen der Nutzer in AmI-Dienste, die Sicherheit vernetzter AmI-Systeme sowie Fragen der sozio-strukturellen Selektivität von AmI-Angeboten. Wichtigstes methodisches Instrument des Projekts war die Entwicklung von sogenannten „dunklen“ Szenarien, anhand derer zentrale Schwachstellen und Risikobereiche künftiger AmI-Anwendungen möglichst realistisch herausgearbeitet werden sollten. Mit diesem spezifischen methodischen Zugang heben sich die SWAMI-Szenarien von bestehenden TA-Studien, die im Bereich von AmI durchgeführt wurden, deutlich ab.

Der Beitrag unterstreicht die Notwendigkeit, dass Szenarien über zukünftige Technikentwicklungen eine größere Realitätsnähe anstreben sollten, indem nicht nur die potenziell positiven Auswirkungen einer technologischen Innovation, sondern eben auch die denkbaren Schattenseiten systematisch herausgearbeitet werden. Im Folgenden wird ein solch realistischer Szenarien-Ansatz vorgestellt.

[2] Das Projekt SWAMI wurde vom Sechsten Forschungsrahmenprogramm der Europäischen Kommission finanziert und wurde von fünf Projektpartnern (Fraunhofer ISI, IPTS – JRC, Vrije Universiteit Brüssel, VTT, Trilateral Research and Consulting) durchgeführt. Die Projektergebnisse sind in Wright et al. (2008) zusammengefasst.

2 Der Szenarien-Ansatz von SWAMI

2.1 Dunkle Szenarien und Ambient Intelligence

Die Entwicklung von Szenarien zählt zu den wichtigsten Methoden, die im Bereich der Technikvorausschau und strategischen Technikplanung verwendet werden (vgl. Coates 2000; Miles et al. 2003; Maghiros et al. 2005, 85). Die Szenarien-Methode findet seit über 30 Jahren in unterschiedlichen Kontexten Anwendung (vgl. van Notten et al. 2003; Bradfield et al. 2005) und erfreut sich insbesondere in jüngster Zeit wieder reger Nachfrage (vgl. Heugens und van Oosterhout 2001; Chermack 2005, 60). Insgesamt ist das Feld gekennzeichnet von einer ausgeprägten Vielfalt und Koexistenz methodischer Varianten, Arbeitstechniken sowie einem Mangel an theoretischer Fundierung (vgl. Martelli 2001). Eingedenk dieser Unübersichtlichkeit sind in den letzten Jahren vermehrt Versuche unternommen worden, zumindest auf der Ebene von Terminologien und Ordnungsschemata einige dieser Defizite zu beheben.[3]

In diesem Zusammenhang haben van Notten et al. (2003) eine Typologie vorgeschlagen, die für sich in Anspruch nimmt, die in der Praxis bestehende große Bandbreite unterschiedlicher Szenarien-Ansätze systematisch zu erfassen und für vergleichende Analysen auf eine einheitliche Grundlage zu stellen. Um eine solche Typologie zu entwickeln, haben van Notten et al. eine breit angelegte Analyse der Szenarien-Literatur sowie von etwa 70 auf Szenarien basierenden Studien durchgeführt (2003, 424f.). Die auf dieser Basis entwickelte Typologie unterscheidet zunächst drei Hauptdimensionen, die zur Charakterisierung von Szenarien herangezogen werden können: (1) Das Ziel des Szenarien-Projekts, (2) den Szenarien-Entwicklungsprozess und (3) die Szenarien-Inhalte. Diese drei Hauptdimensionen stehen nicht unverbunden nebeneinander, sondern wirken aufeinander ein: So wird beispielsweise das gewählte Szenario-Ziel Einfluss auf den Entwicklungsprozess haben, und dieser wird wiederum die Inhalte eines Szenarios prägen. Jedes der drei Hauptdimensionen deckt ferner ein Möglichkeitsspektrum ab, das durch jeweils zwei Extrempunkte beschrieben wird. Mit Blick auf das (1) Szenario-Ziel bewegen sich Szenarien auf einem Kontinuum zwischen explorativen und beratenden Zielsetzungen. Das Design des (2) Szenarien-Entwicklungsprozesses lässt sich zwischen intuitiven und formalen Ansätzen ansiedeln. Und schließlich wird mit Blick auf die in einem Szenario verwendeten Variablen und deren Wechselwirkungen zwischen einfachen und komplexen (3) Szenario-Inhalten unterschieden.

In diese Typologie lassen sich sowohl der SWAMI-Szenarien-Entwicklungsprozess (hier: eher intuitiv statt formal) als auch die Szenario-Inhalte (hier: eher komplex statt einfach) einordnen. Mit Blick auf die Ziele der Szenarien – explorativ vs. beratend – ist jedoch keine klare Zuordnung möglich, da die SWAMI-Szenarien beide Charakteristika zu erfüllen suchen: Die Szenarien sind sowohl explorativ, da sie zum Nachdenken anregen und Problembewusstsein erhöhen möchten, als auch beratend, da sie explizit politisch-regulative Entscheidungsprozesse unterstützen sollen. Letztlich sind die SWAMI-Szenarien mit ihrem außergewöhnlichen Ansatz, der sich nur schwer in gängige Typologien einordnen lässt, auch Ausdruck des ausgeprägten Methodenpluralismus, der diese Form der Technikvorausschau nach wie vor charakterisiert.

Bekanntlich stellen Szenarien keine Vorhersagen dar, vielmehr werfen sie Schlaglichter auf mögliche künftige Entwicklungen bzw. zeigen Wege auf, wie diese realisiert werden können. Ihre primäre Funktion liegt dabei nicht nur in der Konkretion und Veranschaulichung von zunächst eher vagen Zukunftsbildern, sondern vor allem in der Stimulierung von Debatten, der Strukturierung

[3] Vgl. u. a. Technology Futures Analysis Methods Working Group (2004) und Bradfield et al. (2005).

von Denkfiguren und der Unterstützung bei der Synthetisierung möglichst realistischer Zukunftspläne in von großer Unsicherheit geprägten Entscheidungssituationen (vgl. Ringland 1998; Gavigan et al. 2000; Godet 2000).

Viele Szenarien-Prozesse und Foresight-Studien zielen darauf ab, möglichst erstrebenswerte Zukunftsbilder zu entwerfen. Folglich neigen sie dazu, nahezu ausschließlich optimistische Visionen zu präsentieren – eine Beobachtung, die gleichfalls für die Mehrzahl der Szenarien im Bereich von AmI gilt (vgl. Friedewald und Lindner 2007). Dieser positive Ansatz ist legitim und erfüllt zudem wichtige Funktionen bei der zielgerichteten Ausgestaltung von Forschungs- und Entwicklungsprozessen. Das SWAMI-Projekt hat dagegen bewusst einen alternativen Zugang gewählt. Die dort entwickelten Szenarien repräsentieren Zukunftsbilder, die sich aus einer normativen Perspektive grundsätzlich *nicht* realisieren sollten. Indem sich diese als „dark scenarios“[4] bezeichneten Zukunftsbilder auf die wahrscheinlichen, aber häufig nicht bedachten negativen Auswirkungen der Anwendung von AmI-Technologien konzentrieren, beschreiben sie eine Zukunft, die durchaus Realität werden könnte, sollten keine geeigneten Vorkehrungen ergriffen werden.

2.2 Zur Methode der Szenarien-Entwicklung

Am Beginn der eigentlichen Szenarien-Entwicklung von SWAMI stand die Identifizierung potenzieller Schwachstellen und Risiken von AmI. Dabei ist zu betonen, dass die dunklen Szenarien, die im Rahmen des Projekts konzipiert wurden, keineswegs sämtliche hypothetischen Fehlentwicklungen aufgreifen, die unter AmI aus heutiger Warte auftreten könnten. Auch sind die dunklen Szenarien nicht mit der Intention entworfen worden, Positionen zu stärken, die technologischen Fortschritt im Allgemeinen und AmI im Besonderen pauschal ablehnen. Im Gegenteil, explizites Ziel des Szenarien-Prozesses war es, frühzeitig auf mögliche Fehlentwicklungen aufmerksam zu machen und entsprechende Maßnahmen zu entwickeln und anzuregen, damit die dunklen Zukunftsbilder erst gar nicht eintreten. Ein weiterer zentraler Arbeitsschritt des SWAMI-Projekts bestand daher in der Identifizierung geeigneter Schutzmaßnahmen, um den zahlreichen Risiken von AmI wirksam begegnen zu können.

Diese Identifizierung von Gefährdungen und der entsprechenden Schutzvorkehrungen ähnelt Ansätzen, wie sie in der klassischen Risikoanalyse und -bewertung angewandt werden (vgl. Renn und Zwick 1997; Klinke und Renn 2001). Hier wie dort werden Gefahren und schützenswerte Güter identifiziert, Ausmaß und Wahrscheinlichkeit unerwünschter Folgen bestimmt und entschieden, welche Vorsichtsmaßnahmen zu ergreifen sind. Der eigentliche Unterschied zwischen dem Dark-Scenario-Ansatz und der klassischen technologischen Risikoanalyse liegt indessen darin begründet, dass die Art der Risiken, die gemeinhin mit den Technologien der Informationsgesellschaft in Verbindung gebracht werden, als erheblich weniger schwerwiegend betrachtet werden als beispielsweise nukleare Gefahren, Naturkatastrophen u. Ä., welche die traditionellen Gegenstände der Risikoanalyse darstellen. In diesen Bereichen wird das Vorsorgeprinzip als ein Instrument des Risikomanagements angewandt. Die in ihrem Risikopotenzial andersartigen Informations- und Kommunikationstechnologien werden dagegen nur selten mit diesem Instrumentarium betrachtet.[5] Die SWAMI-Szenarien legen jedoch nahe, dass die mit AmI verbundenen Bedrohungen durchaus er-

[4] Pearson und Anderson (2001) verwenden die Begrifflichkeit „dark-side scenarios“ für extrem pessimistische, zum Teil katastrophenartige Zukunftsbilder der Informationsgesellschaft. Ihre Szenarien sind indessen weder systematisch entwickelt noch analysiert worden.

[5] Zu den wenigen Ausnahmen vgl. Hilty et al. (2003).

heblich sein können, insbesondere wenn zunehmend zentrale gesellschaftliche Funktionen – etwa die Steuerung von Verkehrsströmen und anderen öffentlichen Infrastruktursystemen – von AmI-Systemen übernommen werden.

Um die Identifizierung der mit AmI verbundenen Risiken zu erleichtern, wird in den SWAMI-Szenarien eine weit fortgeschrittene Diffusion und nahezu flächendeckende Verfügbarkeit von AmI unterstellt. Entsprechend der gängigen AmI-Visionen wird ferner angenommen, dass die AmI-Systeme weitgehend im Hintergrund agieren, die verschiedenen Systeme miteinander vernetzt sind und autonom interagieren.

Der wesentliche Unterschied der SWAMI-Szenarien im Vergleich zu herkömmlichen Szenarien-Prozessen ist, dass sich das SWAMI-Projekt auf „dunkle" Situationen konzentrierte, um so potenzielle Schwachstellen und Bedrohungen stärker herausarbeiten zu können. Da hierfür jedoch keine spezielle Szenarien-Methode existiert, ist es zunächst erforderlich, die im SWAMI-Projekt angewandte Methode zu erläutern.[6]

Bei den SWAMI-Szenarien handelt es sich um so genannte Trendszenarien (vgl. Massini und Vasquez 2000).[7] Sie basieren auf Extrapolationen aktueller Entwicklungen; der eigentliche Szenarien-Prozess beginnt in der Gegenwart und tastet sich in eine möglichst realitätsnahe Zukunft vor. Extreme und damit ausgesprochen unwahrscheinliche Zukunftsentwürfe sollen damit nicht entwickelt werden.

Bereits zu Beginn des Projekts entschied man sich, insgesamt vier dunkle Szenarien zu entwickeln, um einen handhabbaren Kompromiss angesichts erwünschter Vielfalt und limitierter Ressourcen einzugehen. Der eigentliche Szenarien-Prozess bestand in einer Kombination aus Literaturanalysen und interaktiven Workshops, an denen sowohl das SWAMI-Konsortium als auch geladene Experten beteiligt waren. Tabelle 1 liefert einen Überblick über die Arbeitsschritte, die über eine Zeitspanne von etwa sechs Monaten durchgeführt wurden.

Tabelle 1: Arbeitsschritte des Szenarien-Prozesses

Arbeitsschritt	Instrument
Meta-Analyse bestehender Projekte, Studien und Szenarien zum Thema AmI (siehe Wright et al. 2008, 10-32)	• Literaturauswertung • systematische Analyse
Workshop mit 13 Experten; Validierung der Ergebnisse der Meta-Analyse sowie Brainstorming zur Vorbereitung des Szenarien-Prozesses	• Validierung in Workshop • Experteninterviews • Brainstorming
Interner Workshop zur Vorbereitung der Szenarien-Skripte und der späteren Analyse	• moderierte Diskussion
Ausbau und Verfeinerung der Szenarien und der entsprechenden Analyse innerhalb des Konsortiums	• zahlreiche Feedback-Schleifen
Workshop mit 15 externen Experten zur Validierung der Szenarien und der entsprechenden Analyse sowie Brainstorming zur Vorbereitung angemessener Schutzmaßnahmen	• Validierung in Workshop • Experteninterviews

[6] Für einen Überblick über gängige Foresightmethoden für die Informationsgesellschaft vgl. Miles et al. (2003).

[7] Für Beispiele von Trendszenarien vgl. Punie et al. (2002) oder Maghiros et al. (2005).

Statt der Entwicklung von umfang- und detailreichen Szenarien samt umfassender Analysen und Empfehlungen entschied man sich bei SWAMI für die Entwicklung von Szenarien, die sich auf die Darstellung von bestimmten Ausschnitten von Alltagssituationen beschränken, um sie insgesamt handhab- und lesbar zu halten.

Grundsätzlich ist zu betonen, dass die zu den Szenarien gehörigen „Geschichten“ keinen Selbstzweck darstellen. Den Szenario-Skripten wird zwar zumeist die größte Aufmerksamkeit zuteil, allerdings umfasst der Szenarien-Prozess darüber hinaus noch weitere zentrale Elemente. Im Falle von SWAMI waren insbesondere ein *reality check* sowie ein *technology check* prägend für die weitere Ausgestaltung der Skripte. Mit der Realitätsprüfung sollte sichergestellt werden, dass die in den Szenarien dargestellten Situationen in ihrer grundsätzlichen Ausprägung an tatsächliche Begebenheiten zurückgebunden sind. Dies wurde erreicht, indem Nachrichten und Pressemeldungen über bestimmte Ereignisse mit einem Bezug zu modernen Informations- und Kommunikationstechnologien – etwa Berichte über organisierten massenhaften Datendiebstahl – einen wichtigen Ausgangspunkt für die in den Szenarien dargestellten Situationen bildeten. Auch wurden die in den Szenarien angewandten Technologien und Applikationen von Experten aus dem Forschungs- und Entwicklungsbereich auf ihre technische Realisierungsfähigkeit hin überprüft.

Neben der eigentlichen Szenarien-*Entwicklung*, also dem kreativen und interaktiven Prozess der Gestaltung der in den Szenarien dargestellten Ereignisse, Kontexte und Akteure, stellt insbesondere die Szenarien-*Analyse* ein bedeutendes Element im Szenarien-Prozess dar. Für die Analyse der SWAMI-Szenarien wurde folgende Struktur entwickelt:

- Kurze Darstellung der wichtigsten „dunklen“ Situationen des Szenarios,
- Auflistung der wichtigsten AmI-Technologien und -Geräte, die zum Einsatz kommen,
- Auflistung der wichtigsten AmI-Anwendungen des Szenarios,
- Darstellung der zentralen Treiber oder Schlüsselparameter, die die Szenario-Situation prägen bzw. zur „dunklen“ Situation führen,
- Diskussion der wichtigsten Themen mit Blick auf Privatsphäre, Sicherheit, Identität, die im Szenario aufgeworfen werden,
- Diskussion der rechtlichen Fragen, die implizit in den Szenarien berührt werden,
- Formulierung vorläufiger Schlussfolgerungen.

Abbildung 1 gibt einen Überblick über den Szenarien-Ansatz von SWAMI:

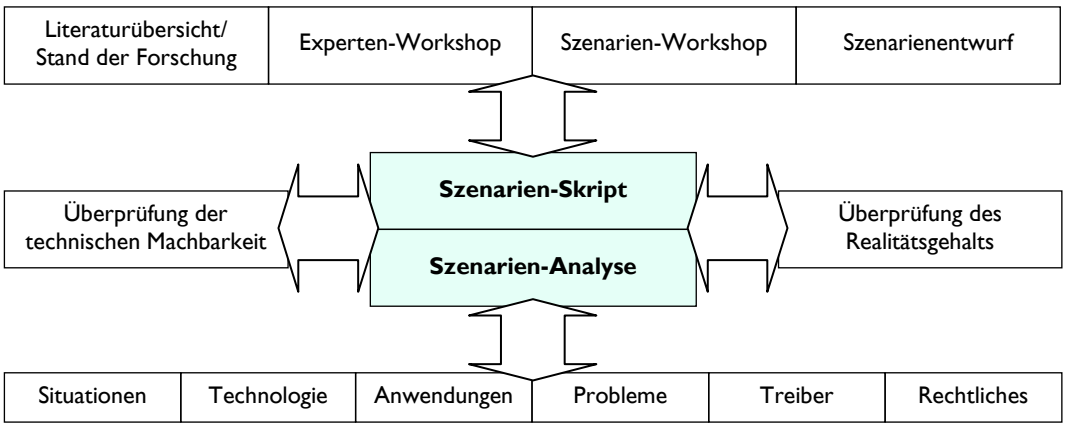

Abbildung 1: Szenarien-Ansatz von SWAMI. Quelle: Wright et al. (2008, 34)

2.3 Die vier SWAMI-Szenarien

Folgende Szenarien wurden im Rahmen des Projekts entwickelt:[8]

1. *Eine typische Familie mit Situationen in verschiedenen Kontexten*: Hier werden Schwachstellen von AmI veranschaulicht, die sich auf das Leben einer normalen Familie auswirken können. Die unerwünschten Situationen treten in unterschiedlichen Kontexten auf (im intelligenten Haus, am Arbeitsplatz, im öffentlichen Park).
2. *Senioren auf Reisen*: Durch eine illegale Manipulation an einem elektronischen Verkehrsleitsystem werden ältere Mitbürger in einen Unfall verwickelt, bei dem auch Mitglieder der Reisegruppe zu Schaden kommen. Verschiedene Situationen mit Blick auf Reisen, Kommunikation und Gesundheitsversorgung werden im Szenario behandelt.
3. *Vorstandssitzung eines internationalen Konzerns und gerichtliches Nachspiel*: Ein Unternehmen, dessen Geschäftsmodell auf der Sammlung, der Aggregation und dem Verkauf personenbezogener Daten basiert, wird Opfer eines großangelegten Datendiebstahls. Die Vertuschungsversuche der Unternehmensleitung werden in einem späteren Gerichtsverfahren aufgearbeitet.
4. *Facetten der Risikogesellschaft*: Aus der Perspektive einer Nachrichtensendung werden vier gesellschaftliche Problemfelder beleuchtet, in denen AmI eine Rolle spielt. Aufhänger sind die Forderungen einer Interessengruppe, die sich gegen personalisiertes Profiling wendet; die digitale Spaltung und Umweltprobleme im globalen Maßstab; die Schwachstellen von technischen Verkehrsüberwachungssystemen und schließlich nichtintendierte Wirkungen von AmI-Systemen zur Sicherung von Massenveranstaltungen.

Um mit lediglich vier Szenarien ein möglichst umfassendes und vielschichtiges Problemspektrum abdecken zu können, orientierte sich die Ausgestaltung von Situationen sowie die Bestimmung von Kontexten und handelnden Personen an einem zweidimensionalen Analysefeld (vgl. van't Klooster und van Asselt 2006). Die vertikale Achse differenziert zwischen Situationen, die eher auf der Makro- oder der Mikroebene angesiedelt sind, während die horizontale Achse zwischen Problemen unterscheidet, die eher einen Bezug zu privaten Belangen bzw. eine gesamtgesellschaftliche Relevanz aufweisen (siehe Abbildung 2).

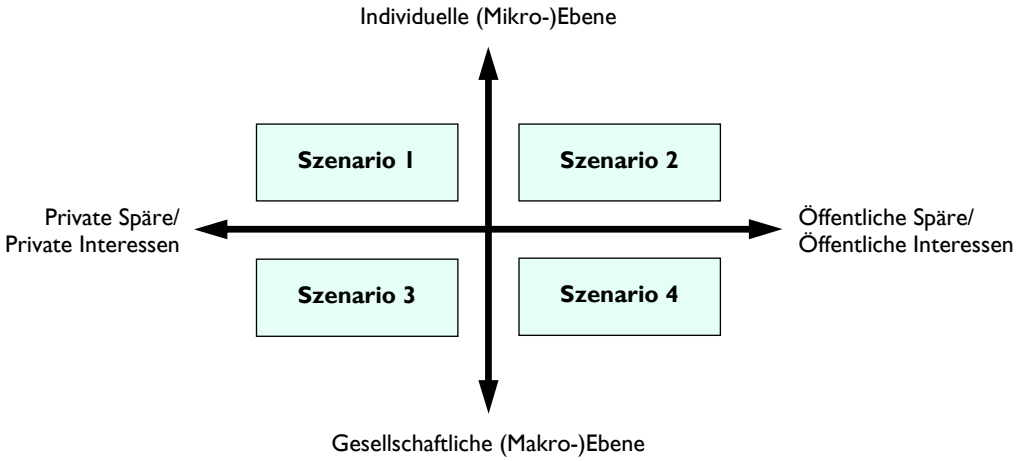

Abbildung 2: Positionierung der Szenarien

[8] Die vier SWAMI-Szenarien sind vollständig abgedruckt in Wright et al. (2008, 33-142).

Obwohl die Szenarien sowohl individuelle und gesellschaftliche als auch private wie öffentliche Belange thematisieren, wurde versucht, die Szenarien-Geschichten jeweils aus der Perspektive des Alltags eines individuellen Nutzers bzw. Betroffenen zu erzählen.

2.4 Ergebnisse der Szenarien-Analyse

Die Analyse der einzelnen Szenarien-Situationen förderte eine große Bandbreite an Themen und Problembereichen zutage. Unter Einbeziehung der Experten entschied sich das SWAMI-Team, die in den Szenarien identifizierten und herausgearbeiteten Schwachstellen entlang folgender Schlüsselthemen zu ordnen:

- *Privatsphäre:* Die Szenarien thematisieren verschiedene Formen von Eingriffen in die Privatsphäre, darunter Identitätsdiebstahl, Weitergabe privater Daten, Überwachung sowie die problematischen Wirkungen personalisierter Datenprofile.
- *Sicherheit:* Sicherheitsthemen werden in verschiedenen Kontexten und Anwendungszusammenhängen behandelt, u. a. in der Telearbeit, Nutzung biometrischer Daten zur Authentifizierung und Identifizierung, der „Störfaktor Mensch“, bösartige Attacken auf AmI-Systeme, Sicherheitsprüfungen, Sicherheitskopien von Datenbanken sowie Sicherheitsillusionen.
- *Identität:* In den Szenarien werden unterschiedliche Facetten von Identität beleuchtet und die Konsequenzen aufgezeigt, sollten identitätsbasierte Daten missbräuchlich, falsch oder unvollständig verarbeitet werden.
- *Vertrauen:* Verschiedene Aspekte von Vertrauen werden in den Szenarien aufgegriffen, u. a. der Mangel an Vertrauen gegenüber einer technischen Anwendung und der damit verbundene Widerwillen, persönliche Daten preis zu geben.
- *Kontrollverlust:* In den Szenarien wird Kontrollverlust durch unterschiedliche Faktoren ausgelöst, etwa wenn AmI-Anwendungen durch Fehlinterpretationen von Datenprofilen entgegen den eigentlichen Wünschen des Nutzers „technologiepaternalistisch“ im Sinne von Spiekermann und Pallas (2006) agieren.
- *Abhängigkeit:* Die Szenarien thematisieren die problematischen Folgen einer weitgehenden Abhängigkeit von umfassenden technischen Infrastrukturen sowie die Frustrationserlebnisse, sollten diese Dienste nicht zur Verfügung stehen.
- *Exklusion:* In den Szenarien werden auch Fragen des breiten gesellschaftlichen Zugangs zu den AmI-Diensten und -Infrastrukturen, Fragen der Technikgestaltung sowie der Einführungsbedingungen berührt.
- *Falsche Verdächtigung:* In den Szenarien werden Situationen beschrieben, in denen unverhältnismäßige Sanktionen aufgrund fehlinterpretierter Daten und irrtümlicher Verdächtigungen erlassen werden.

In den dunklen Szenarien werden über diese technologischen, organisatorischen und rechtlichen Schlüsselthemen hinaus noch die folgenden Probleme behandelt, die durch die gezielte Ausnutzung von Systemschwachstellen entstehen können:

- *Überwachung:* Jeder Nutzer von AmI-Diensten hinterlässt Datenspuren. Diese unvermeidbaren Nebenprodukte der Nutzung können verwendet werden, um detaillierte persönliche Verhaltensprofile anzulegen. Die besondere gesellschaftliche Herausforderung besteht darin, den legitimen aber widerstreitenden Ansprüchen von öffentlichen Sicherheitsinteressen einerseits und dem Schutz der Privatsphäre andererseits gerecht zu werden.

- *Identitätsdiebstahl:* Ohne hinreichende Datensicherung eröffnen AmI-Systeme vielfältige Gelegenheiten, identitätsbezogene Daten für illegale Zwecke zu nutzen. Solch neuartigen Verbrechensformen (z. B. „Datenwäsche“) werden auch in den Szenarien behandelt.
- *Bösartige Angriffe:* Bekanntlich hat jede neue Technologie Schwachstellen, die gewissermaßen „durch die Hintertür“ von Kriminellen ausgenutzt werden können. Einige denkbaren Folgen der Ausnutzung dieser Schwachstellen werden in den Szenarien aufgegriffen.
- *Spam:* Verschiedene Aspekte und Konsequenzen unerwünschter elektronischer Nachrichten werden in den Szenarien thematisiert, u. a. lästige Werbebotschaften oder falsche Benachrichtigungen.

Zur besseren Veranschaulichung werden im Folgenden vier der Schlüsselthemen anhand von Beispielsituationen aus den Szenarien kurz dargestellt:

Identität

Viele Internetnutzer verwenden dasselbe Passwort und/oder dieselbe Benutzerkennung für unterschiedliche Internetseiten und Systeme. Ob beabsichtigt oder nicht, die meisten NutzerInnen schützen ihre Identität(en) nur unzureichend. Zwar können bestimmte technische Lösungen, die bereits heute einen verbesserten Schutz privater Daten bieten, auch in einer AmI-Welt einige der Sicherheitsprobleme reduzieren – gänzlich verschwinden werden diese primär durch sorgloses Nutzerverhalten erzeugten Schwachstellen indessen nicht.

Ausschnitt aus Szenario 2, welches den „menschlichen Faktor“ bei AmI-Anwendungen thematisiert:

And thanks to the travel-assistance procedure of the AmI environment in our home in Murnau, this time we even thought of recharging our PWCs [personal wrist communicator] and HMDs [health monitoring device] early enough to avoid losing „our identity” like on our last trip (Wright et al. 2008, 73).

Stress aufgrund von Abhängigkeit

Massive Abhängigkeit von technischen Systemen kann Stress erzeugen. Sobald eine Technologie, die vollständig in das alltägliche Leben integriert ist, plötzlich nicht zur mehr Verfügung steht bzw. zeitweise ausfällt, werden gewohnte Abläufe und Routinen gestört. Stress entsteht insbesondere dann, wenn Unsicherheit darüber besteht, wann und ob überhaupt der ursprüngliche Zustand wiederhergestellt werden kann.

Ausschnitt aus Szenario 1:

Paul receives an alarm signal on his Personal Wrist Communicator (PWC). There is an intruder in the house. „How is that possible?” he asks himself. He knows that his son Ricardo is home. He had invited some friends to play a new virtual reality game (for which Ricardo has a licence) from the entertainment centre downstairs. Paul checks the home surveillance system remotely but only gets a still image from 30 minutes ago. There is no live image available from the front and back door cameras, nor is Paul able to play back who has passed in front of the doors today. Ricardo does not answer his calls. „What's happening? Where is he?” (Wright et al. 2008, 36).

Falsche Verdächtigung

Aufgrund von fehlerhaften Datenprofilen können unschuldige Personen fälschlicherweise als Verdächtige oder potenzielle Sicherheitsrisiken identifiziert werden. Neben technischen Ursachen, die dafür verantwortlich sein können, erhöht sich die Wahrscheinlichkeit falscher Verdächtigungen ins-

besondere dann, wenn die Spannung zwischen öffentlichen Sicherheitsbedürfnissen und privaten Schutzrechten einseitig zugunsten der ersteren aufgelöst wird. Zudem kann eine Kriminalisierung von Unschuldigen bereits durch unvollständige oder entkontextualisierte Datenprofile ausgelöst werden, wie im Folgenden Beispiel veranschaulicht:

Ausschnitt aus Szenario 1:

Paul is just leaving the office to return home when his boss calls, „Come in, Paul. I'm glad you are still at the office. It seems we have a small problem … I've just been contacted by the police who have asked for access to all the data we have on you. I understand this is just an informal request so we do not have to give them anything, but, as you know, as a security company, we cannot afford any suspicions of our staff."

Paul is astonished and does not understand what is happening. First the home problem, now this. „Surely, this must be some kind of mistake. I don't know why they'd want my data – although I have heard lately of cases where the police have been investigating innocent people based on inadequate profiling (Wright et al. 2008, 36).

Kontrollverlust und bösartiger Angriff

Der Verlust der Kontrolle über ein AmI-System bzw. bestimmte AmI-Anwendungen muss nicht zwingend auf den Voreinstellungen des Systems beruhen. Denkbar sind auch bösartige Angriffe durch Unbefugte auf ein System, die einen Kontrollverlust zur Folge haben können. Eine solche Situation wird ebenfalls in einem der Szenarien dargestellt. Nachdem die Hacker oder Angreifer die teilweise oder gar vollständige Kontrolle über das AmI-System erlangt haben, sind sie unter Umständen in der Lage, persönliche Profile zu verändern und/oder sensible Daten abzurufen, um diese für illegale Zwecke zu missbrauchen.

Ausschnitt aus Szenario 1:

Paul receives multiple messages on his PWC the moment he leaves his boss's office. He had all incoming communications on hold from the moment he entered her office. This is a company default setting. There is one message that immediately attracts his attention. „If you want your house systems to work again, click on the following link …" „What? I'm being blackmailed! So that's why I couldn't get access to my home systems, nor could the local security agent. That's why I got the intruder message," he thinks, slightly reassured, since that probably means that his children at home are OK (Wright et al. 2008, 37).

3 Schlussfolgerungen

3.1 Entwicklung geeigneter Schutzvorkehrungen

Im Zuge der Analyse der dunklen Szenarien wurde eine Vielzahl potenzieller Risiken identifiziert, die durch künftige AmI-Anwendungen hervorgerufen werden können. Entsprechend dieser Vielfalt wird eine große Bandbreite unterschiedlicher Maßnahmen benötigt, um den Risiken angemessen zu begegnen. Die zu entwickelnden Schutzvorkehrungen, so die Erkenntnisse aus der Szenarien-Analyse, sollten möglichst ganzheitlich und zugleich kontextabhängig sein, um ökonomische, rechtliche, soziale, ethische und technische Aspekte abdecken zu können sowie die Interessen von Anbietern wie Nutzern zu berücksichtigen. Eine weitere Herausforderung besteht darin, die unterschiedlichen, oft in verschiedenen Politikfeldern angesiedelten Maßnahmen so aufeinander abzustimmen, dass sie den größtmöglichen Schutz entfalten und nicht intendierte Wirkungen – etwa die Exklusion von Nutzern aufgrund fehlerhafter Identitätsdaten – begrenzen. Zudem ist davon auszugehen, dass aufgrund des raschen technologischen Fortschritts und der korrespondierenden sozio-technischen Entwicklungen abgewandelte und zum Teil neue Risiken entstehen, was wiederum die kontinuierliche Anpassung der Schutzvorkehrungen erforderlich macht. Die im Rahmen von SWAMI vorgeschlagenen Schutzmaßnahmen fallen in drei Hauptkategorien: technische, organisatorische und rechtliche Vorkehrungen.

(1) Die *technischen* Maßnahmen, die zum Schutz der Privatsphäre im Kontext von AmI beitragen sollen, basieren in aller Regel auf Anonymität, Pseudonymität und/oder Unverknüpfbarkeit verschiedener Datensätze. Grundsätzlich treten hierbei Konflikte auf zwischen dem Datensubjekt und den Anforderungen desjenigen, der die Daten sammelt und verarbeitet (vgl. Cas 2005, Vildjiounaite et. al 2007). Ein wichtiger Schutzmechanismus kann sich auf die Kontrolle der Datenzugangsprozeduren beziehen, die unaufdringlich und kontextabhängig sind sowie multimodale Authentifizierungsverfahren zur Verfügung stellen. Zudem können sichere Authentifizierungsmethoden, die auf Zero-knowledge-Techniken beruhen und einen minimalen Bedarf an Datenspeicherung vorsehen, dazu beitragen, die irrtümliche Protokollierung sensibler Daten zu vermeiden. Fortgeschrittene Techniken, die auf künstlicher Intelligenz basieren, können ferner Zugangskontrollen sicherer machen, indem ungewöhnliche Verhaltensmuster erkannt werden. Die öffentliche Forschungsförderung, so eine weitere Forderung von SWAMI, sollte künftig weitaus stärker die sicherheits- und datenschutzrelevanten Schlüsselthemen in F&E-Projekte integrieren.

(2) Zu den *organisatorischen* Schutzmaßnahmen, die von SWAMI vorgeschlagen wurden, zählen u. a.: Die Unterstützung offener Standards, um Interoperabilitätskonflikte zu minimieren; die breite Umsetzung von internationalen ISO-Standards im Bereich von Datenschutz und –sicherheit (z. B. ISO 17799); die Entwicklung und Verbreitung von datenschutzrechtlichen Qualitätssiegeln, um das Vertrauen in AmI-Dienste und -Infrastrukturen zu erhöhen; die Einführung von öffentlichen Reputationssystemen, um den Nutzern zusätzliche Orientierung über die Vertrauenswürdigkeit eines Anbieters zu geben. Eine wichtige Rolle bei der Verbreitung von Schutzvorkehrungen kann zudem ein entsprechendes Beschaffungsverhalten der öffentlichen Hand spielen. Letztendlich bleibt auch hier ein wesentliches Ziel, die Kompetenz der Nutzer im Umgang mit AmI-Anwendungen zu steigern sowie das öffentliche Bewusstsein über potenzielle Gefahren für Datenschutz und -sicherheit zu erhöhen.

(3) Die Analyse *rechtlicher* Regelungen hat aufgezeigt, dass bereits heute zahlreiche regulatorische und rechtliche Schutzvorkehrungen in Kraft sind, die auch in einem AmI-Kontext angewandt werden können. Zugleich ist aber deutlich geworden, dass AmI verschiedene neuartige rechtliche Fragen aufwirft – etwa, welchen Status Willenserklärungen haben, die im Namen des Nutzers im Rahmen eines automatisierten Identitätsmanagementverfahrens von technischen Assistenten abgegeben werden. Die Anpassung und Weiterentwicklung des gesetzlichen Rahmens sollte insbesondere Fragen des allgemeinen Zugangs und der Inklusion, der Zurechenbarkeit und der Haftung berücksichtigen.

3.2 Methodische Aspekte

Der Entstehungsprozess der dunklen Szenarien ähnelt überwiegend jenen Verfahren, die auch in herkömmlichen Szenarien-Prozessen angewandt werden. Hier wie dort besteht der Prozess aus iterativen Feedbackschleifen innerhalb der Forschergruppe, werden Erkenntnisse aus Metaanalysen bestehender Studien aufgegriffen sowie Expertengespräche und Workshops zur weiteren Validierung der (Zwischen-)Ergebnisse eingesetzt. Auch unterscheidet sich SWAMI nicht grundlegend von Mainstream-Szenarien in der Beschränkung der Szenarien-Zahl auf eine handhabbare Größe, die dennoch zugleich ein möglichst breites Spektrum abdecken sollte.

Zu betonen ist ferner, dass der eigentliche prospektive Gehalt der Szenarien sich nicht in der Erarbeitung interessanter und lesbarer „Geschichten“ erschöpft, sondern insbesondere in der Entwicklung eines analytischen Rahmens besteht, der auf alle Szenarien kohärent angewandt wird. Bei SWAMI bestand dieser Analyserahmen aus folgenden zentralen Elementen:

- den dunklen, also unerwünschten Situationen eines jeden Szenarios,
- den wichtigsten AmI-Technologien und -Anwendungen, die in den Szenarien zum Einsatz kommen,
- den wichtigsten Treibern bzw. Schlüsselparametern, die die problematischen Situationen hervorgerufen haben,
- der Erörterung der Szenarien mit Blick auf die SWAMI-Schlüsselthemen,
- der Diskussion der rechtlichen Fragen, die in den dunklen Situationen aufgeworfen werden,
- sowie vorläufigen Schlussfolgerungen.

Um die letztlich fiktionalen Szenarien möglichst wirklichkeitsnah auszugestalten und unrealistische Situationen zu vermeiden, wurden sie sowohl einem technology check als auch einem reality check unterzogen. Insofern beruhen die SWAMI-Szenarien auf in die Zukunft gerichteten Extrapolationen gegenwärtiger Trends. Die Bemühungen, keine extremen, unrealistischen Szenarien zu entwickeln, sollten insbesondere dazu beitragen, dass der gesamte Szenarien-Prozess nicht als irrelevant verworfen wird.

Der Hauptunterschied zwischen dem SWAMI-Ansatz und der Mehrzahl der Szenarien-Prozesse liegt darin, dass durch den SWAMI-Fokus auf dunkle, unerwünschte Situationen zentrale Risiken von AmI identifiziert werden konnten, die wiederum den Ausgangspunkt für die Entwicklung von risikovermindernden Schutzvorkehrungen bilden. Damit heben sie sich ab von den meisten technischen Szenarien und deren inhärenter Neigung zur Entwicklung betont optimistischer Zukunftsbilder. Die dunklen SWAMI-Szenarien verstehen sich jedoch ausdrücklich als konstruktiver Beitrag, eine sichere und somit erfolgreiche AmI-Zukunft entstehen zu lassen. Indem die negativen Potenziale von AmI frühzeitig erkannt werden, erhöhen sich die Chancen, dass problematische Entwicklungen antizipiert und somit auch vermieden werden können.

Die Herausforderung für SWAMI bestand darin, die Risiken, die mit AmI verbunden sein können, zu identifizieren, ohne zugleich die potenziellen Stärken dieser Technologie zu negieren. Dementsprechend wurde versucht, sich bei der Szenarien-Entwicklung nicht von „Schwarzmalerei" leiten zu lassen. Dabei kann man durchaus behaupten, dass es sich eher um „graue" Bilder handelt. Da die Szenarien sowohl negative als auch positive Aspekte einer Zukunftstechnologie aufgreifen, könnte man sie auch schlicht als „realistisch" bezeichnen. Für eine zukunftsorientierte Technikfolgenabschätzung ist ein solcher Szenarien-Prozess weitaus zielführender, als die ausschließliche Beschränkung auf die positiven oder rein negativen Aspekte neuer Technologien. Während positive Szenarien als Hilfsmittel der Technikentwicklung durchaus einen Sinn machen, in dem sie ein die Entwicklung leitendes Bild entwerfen (eben ein Leit-Bild), das dabei helfen kann, die Kommunikation in großen und heterogenen Entwicklergruppen zu erleichtern und auf eine gemeinsame Grundlage zu stellen (vgl. dazu Dierkes et al. 1992; Sturken und Thomas 2004), verkörpern diese Szenarien häufig ein technophiles Weltbild, das mit der Realität wenig gemein hat. Aber auch „Weltuntergangsszenarien", die zur Verdeutlichung der Risiken von Großtechnologien wie der Kerntechnik für einige Zeit sehr beliebt waren und auch gewiss ihre Berechtigung hatten, zeichnen nur ein verzerrtes Bild der Alltagswelt, in die sich neue Technologien mit all ihren Unzulänglichkeiten einfügen (müssen). Die Entwicklung dunkler Szenarien ist unserer Auffassung nach ein probates Mittel, Entscheidungsträger mit einem hinreichend realistischen Bild neuer Technologien mit seinen Licht- und Schattenseiten zu vermitteln, das für die Bewertung bzw. als Unterstützung für die Planung und Steuerung der Entwicklung notwendig ist.

4 Literatur

Aarts, E., Appelo, L., 1999, Ambient Intelligence: thuisomgevingen van de toekomst, IT Monitor 9/1999, 7-11.

Bizer, J., Dingel, K., Fabian, B., Günther, O., Hansen, M. et al., 2006, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung. Studie im Auftrag des Bundesministeriums für Bildung und Forschung, Kiel/Berlin: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin.

Bradfield, R., Wright, G., Burt, G., Cairns, G., Van Der Heijden, K., 2005, The Origins and Evolution of Scenario Techniques in Long Range Business Planing, Futures 37(8), 795-812.

Čas, J., 2005, Privacy in Pervasive Computing Environments – A Contradiction in Terms? IEEE Technology and Society Magazine 24(1), 24-33.

Chermack, T., 2005, Studying Scenario Planning: Theory, Research Suggestions, and Hypotheses, Technological Forecasting and Social Change 72(1), 59-73.

Coates, J., 2000, Scenario Planning, Technology Forecasting and Social Change 65(1), 115-123.

Dierkes, M., Hoffmann, U., Marz, L., 1992, Leitbild und Technik: Zur Entstehung und Steuerung technischer Innovationen, Berlin: Sigma.

Friedewald, M., Da Costa, O., 2003, Science and Technology Roadmapping: Ambient Intelligence in Everyday Life (AmI@Life), Karlsruhe: Fraunhofer-Institut für System- und Innovationsforschung (FhG-ISI).

Friedewald, M., Lindner, R., 2007, Datenschutz, Privatsphäre und Identität in intelligenten Umgebungen: Eine Szenario-Analyse, in: Mattern, F. (Hg.), Die Informatisierung des Alltags. Leben in smarten Umgebungen, Berlin und Heidelberg: Springer, 207-231.

Friedewald, M., 2007, Ubiquitous Computing: Ein neues Konzept der Mensch-Computer-Interaktion und seine Folgen, in: Hellige, H. D. (Hg.), Das Mensch-Computer-Interface: Geschichte, Gegenwart und Zukunft, Bielefeld: Transcript Verlag (i.E.).

Gabriel, P., Bovenschulte, M., Hartmann, E., 2006, Pervasive Computing: Entwicklungen und Auswirkungen, Ingelheim: SecuMedia.

Gavigan, J.P., Scapolo, F., Keenan, M., Miles, I., Fahrl, F. et al. (Hg.), 2001, A Practical Guide to Regional Foresight, EUR 20128 EN, December, Seville: Institute for Prospective Technological Studies (IPTS).

Godet, M., 2000, The Art of Scenario and Strategic Planning: Tools and Pitfalls, Technological Forecasting and Social Change 65(1), 3-22.

Heugens, P., van Oosterhout, J., 2001, To Boldly Go Where No Man Has Gone Before: Integrating Cognitive and Physical Features in Scenario Studies, Futures 33(10), 861-872.

Hilty, L., Behrendt, S., Binswanger, M., Bruinink, A., Erdmann, L. et al., 2003, Das Vorsorgeprinzip in der Informationsgesellschaft. Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt, Bern: TA-Swiss, Zentrum für Technologiefolgen-Abschätzung.

ISTAG (Information Society Technologies Advisory Group), 2001, Scenarios for Ambient Intelligence in 2010, Luxembourg: Office for Official Publications of the European Communities.

ISTAG (Information Society Technologies Advisory Group), 2003, Ambient Intelligence: From Vision to Reality. For Participation – in Society and Business, Luxembourg: Office for Official Publications of the European Communities.

Klinke, A., Renn, O., 2001, Precautionary Principle and Discursive Strategies: Classifying and Managing Risks, Journal of Risk Research 4(2), 159-173.

Maghiros, I., Punie, Y., Delaitre, S., Lignos, E, Rodríguez, C. et al., 2005, Biometrics at the Frontiers: Assessing the Impact on Society, Technical Report EUR 21585 EN, Seville: Institute for Prospective Technological Studies (IPTS).

Martelli, A., 2001, Scenario Building and Scenario Planning: State of the Art and Prospects of Evolution, Futures Research Quarterly 3(2), 57-70.

Massini, E., Vasquez, J., 2000, Scenarios as Seen from a Human and Social Perspective, Technological Forecasting and Social Change 65(1), 49-66.

Mattern, F. (Hg.) 2003, Total vernetzt: Szenarien einer informatisierten Welt, Berlin und Heidelberg: Springer.

Mattern, F. (Hg.), 2007, Die Informatisierung des Alltags. Leben in smarten Umgebungen, Berlin und Heidelberg: Springer.

Miles, I., Keenan, M., Kaivo-Oja, J., 2003, Handbook of Knowledge Society Foresight, European Foundation for the Improvement of Living and Working Conditions, Dublin, <http://www.eurofound.eu.int/pubdocs/2003/50/en/1/ef0350en.pdf>.

Oertel, B., Wölk, M., Hilty, L., Köhler, A., Kelter, H. et al., 2004, Risiken und Chancen des Einsatzes von RFID-Systemen: Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit, Ingelheim: SecuMedia.

Pearson, I., Anderson, R., 2001, The „Dark Side" of the Information Revolution. The Future of the Information Revolution in Europe: Proceedings of an International Conference, April 2001, Limelette, Belgium, Santa Monica, CA: RAND, 71-74.

Punie, Y., Burgelman, J.-C., Bogdanowicz, M., 2002, The Future of Online Media Industries. Scenarios for 2005 and Beyond, The IPTS Report 64, 35-42.

Punie, Y., 2005, The Future of Ambient Intelligence in Europe: The Need for More Everyday Life, Communications & Strategies 57(1), 141-165.

Renn, O., Zwick, M., 1997, Risiko- und Technikakzeptanz, Heidelberg und Berlin: Springer.

Ringland, G., 1998, Scenario Planning. Managing for the Future, Chichester: John Wiley & Sons.

Schot, J., Rip, A., 1997, The Past and Future of Constructive Technology Assessment, Technological Forecasting and Social Change 54(2-3), 251-268.

Spiekermann, S., Pallas, F., 2006, Technology Paternalism – Wider Implications of Ubiquitous Computing, Poiesis & Praxis 4(1), 6-18.

Sturken, M., Thomas, D., 2004, Introduction. Technological Visions and the Rhetoric of the New, in: Sturken, M., Thomas, D., Ball-Rokeach, S. (Hg.), Technological Visions. The Hopes and Fears that Shape New Technologies, Philadelphia: Temple University Press, 1-18.

Technology Futures Analysis Methods Working Group, 2004, Technology Futures Analysis: Toward Integration of the Field and New Methods, Technological Forecasting and Social Change 71(3), 287-303.

van Notten, P., Rotmans, J., van Asselt, M., Rothman, D., 2003, An Updated Scenario Typology, Futures 35(5), 423-443.

van't Hof, C., 2006, RFID and Identity Management in Everyday Life: Striking the Balance between Convenience, Choice and Control, Report IPOL/A/STOA/2006-22, Luxembourg: European Parliament.

van't Klooster, S.A., van Asselt, M.B.A., 2006, Practising the Scenario-axes Technique, Futures 38(1), 15-30.

Vildjiounaite, E., Rantakokko, T., Alahuhta, P. et al., 2007: Privacy Threats in Emerging Ubicomp Applications: Analysis and Safeguarding, in: Mostéfaoui, S. K., Maamar, Z., Giaglis, G. (Hg.), Advances in Ubiquitous Computing: Future Paradigms and Directions, Hershey, PA: Idea Group Publishing (i.E.).

Weiser, M., 1991, The Computer for the 21st Century, Scientific American 265(3), 94-104.

Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E., Punie, Y. (Hg.), 2008, Safeguards in a World of Ambient Intelligence, Dordrecht: Springer (i.E.).

Bisher erschienene manu:scripte

ITA-01-01 Gunther Tichy, Walter Peissl (12/2001): Beeinträchtigung der Privatsphäre in der Informationsgesellschaft. <http://www.oeaw.ac.at/ita/pdf/ita_01_01.pdf>

ITA-01-02 Georg Aichholzer(12/2001): Delphi Austria: An Example of Tailoring Foresight to the Needs of a Small Country. <http://www.oeaw.ac.at/ita/pdf/ita_01_02.pdf>

ITA-01-03 Helge Torgersen, Jürgen Hampel (12/2001): The Gate-Resonance Model: The Interface of Policy, Media and the Public in Technology Conflicts. <http://www.oeaw.ac.at/ita/pdf/ita_01_03.pdf>

ITA-02-01 Georg Aichholzer (01/2002): Das ExpertInnen-Delphi: Methodische Grundlagen und Anwendungsfeld „Technology Foresight". <http://www.oeaw.ac.at/ita/pdf/ita_02_01.pdf>

ITA-02-02 Walter Peissl (01/2002): Surveillance and Security – A Dodgy Relationship. <http://www.oeaw.ac.at/ita/pdf/ita_02_02.pdf>

ITA-02-03 Gunther Tichy (02/2002): Informationsgesellschaft und flexiblere Arbeitsmärkte. <http://www.oeaw.ac.at/ita/pdf/ita_02_03.pdf>

ITA-02-04 Andreas Diekmann (06/2002): Diagnose von Fehlerquellen und methodische Qualität in der sozialwissenschaftlichen Forschung. <http://www.oeaw.ac.at/ita/pdf/ita_02_04.pdf>

ITA-02-05 Gunther Tichy (10/2002): Over-optimism Among Experts in Assessment and Foresight. <http://www.oeaw.ac.at/ita/pdf/ita_02_05.pdf>

ITA-02-06 Hilmar Westholm (12/2002): Mit eDemocracy zu deliberativer Politik? Zur Praxis und Anschlussfähigkeit eines neuen Mediums. <http://www.oeaw.ac.at/ita/pdf/ita_02_06.pdf>

ITA-03-01 Jörg Flecker und Sabine Kirschenhofer (01/2003): IT verleiht Flügel? Aktuelle Tendenzen der räumlichen Verlagerung von Arbeit. <http://www.oeaw.ac.at/ita/pdf/ita_03_01.pdf>

ITA-03-02 Gunther Tichy (11/2003): Die Risikogesellschaft – Ein vernachlässigtes Konzept in der europäischen Stagnationsdiskussion. <http://www.oeaw.ac.at/ita/pdf/ita_03_02.pdf>

ITA-03-03 Michael Nentwich (11/2003): Neue Kommunikationstechnologien und Wissenschaft – Veränderungspotentiale und Handlungsoptionen auf dem Weg zur Cyber-Wissenschaft. <http://www.oeaw.ac.at/ita/pdf/ita_03_03.pdf>

ITA-04-01 Gerd Schienstock (1/2004): Finnland auf dem Weg zur Wissensökonomie – Von Pfadabhängigkeit zu Pfadentwicklung. <http://www.oeaw.ac.at/ita/pdf/ita_04_01.pdf>

ITA-04-02 Gunther Tichy (6/2004): Technikfolgen-Abschätzung: Entscheidungshilfe in einer komplexen Welt. <http://www.oeaw.ac.at/ita/pdf/ita_04_02.pdf>

ITA-04-03 Johannes M. Bauer (11/2004): Governing the Networks of the Information Society – Prospects and limits of policy in a complex technical system. <http://www.oeaw.ac.at/ita/pdf/ita_04_03.pdf>

ITA-04-04 Ronald Leenes (12/2004): Local e-Government in the Netherlands: From Ambitious Policy Goals to Harsh Reality. <http://www.oeaw.ac.at/ita/pdf/ita_04_04.pdf>

ITA-05-01 Andreas Krisch (01/2005): Die Veröffentlichung des Privaten – Mit intelligenten Etiketten vom grundsätzlichen Schutz der Privatsphäre zum Selbstschutz-Prinzip. <http://www.oeaw.ac.at/ita/pdf/ita_05_01.pdf>

ITA-05-02 Petra Grabner (12/2005): Ein Subsidiaritätstest – Die Errichtung gentechnikfreier Regionen in Österreich zwischen Anspruch und Wirklichkeit. <http://www.oeaw.ac.at/ita/pdf/ita_05_02.pdf>

ITA-05-03 Eva Buchinger (12/2005): Innovationspolitik aus systemtheoretischer Sicht – Ein zyklisches Modell der politischen Steuerung technologischer Innovation. <http://www.oeaw.ac.at/ita/pdf/ita_05_03.pdf>

ITA-06-01 Michael Latzer (06/2006): Medien- und Telekommunikationspolitik: Unordnung durch Konvergenz – Ordnung durch Mediamatikpolitik. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_01.pdf>

ITA-06-02 Natascha Just, Michael Latzer, Florian Saurwein (09/2006): Communications Governance: Entscheidungshilfe für die Wahl des Regulierungsarrangements am Beispiel Spam. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_02.pdf>

ITA-06-03 Veronika Gaube, Helmut Haberl (10/2006): Sozial-ökologische Konzepte, Modelle und Indikatoren nachhaltiger Entwicklung: Trends im Ressourcenverbrauch in Österreich. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_03.pdf>

ITA-06-04 Maximilian Fochler, Annina Müller (11/2006): Vom Defizit zum Dialog? Zum Verhältnis von Wissenschaft und Öffentlichkeit in der europäischen und österreichischen Forschungspolitik. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_04.pdf>

ITA-06-05 Holger Floeting (11/2006): Sicherheitstechnologien und neue urbane Sicherheitsregimes. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_05.pdf>

ITA-06-06 Armin Spök (12/2006): From Farming to „Pharming" – Risks and Policy Challenges of Third Generation GM Crops. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_06.pdf>

ITA-07-01 Volker Stelzer, Christine Rösch, Konrad Raab (3/2007): Ein integratives Konzept zur Messung von Nachhaltigkeit – das Beispiel Energiegewinnung aus Grünland. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_01.pdf>

ITA-07-02 Elisabeth Katzlinger (3/2007): Big Brother beim Lernen: Privatsphäre und Datenschutz in Lernplattformen. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_02.pdf>

ITA-07-03 Astrid Engel, Martina Erlemann (4/2007): Kartierte Risikokonflikte als Instrument reflexiver Wissenspolitik. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_03.pdf>

ITA-07-04 Peter Parycek (5/2007): Gläserne Bürger − transparenter Staat? Risiken und Reformpotenziale des öffentlichen Sektors in der Wissensgesellschaft. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_04.pdf>

ITA-07-05 Helge Torgersen (7/2007): Sicherheitsansprüche an neue Technologien – das Beispiel Nanotechnologie. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_05.pdf>

ITA-07-06 Karen Kastenhofer (9/2007): Zwischen „schwacher" und „starker" Interdisziplinarität. Die Notwendigkeit der Balance epistemischer Kulturen in der Sicherheitsforschung zu neuen Technologien. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_06.pdf>

ITA-07-07 Ralf Lindner, Michael Friedewald (9/2007): Gesellschaftliche Herausforderungen durch „intelligente Umgebungen. Dunkle Szenarien als TA-Werkzeug. <http://epub.oeaw.ac.at/ita/ita-manuscript/ita_07_07.pdf>