Mehrseitige IT-Sicherheit als politisches Projekt der digitalen Informationsgesellschaft

Von Olaf Winkel und Ulrich Klose*

Nr. 224 / November 2002

Arbeitsbericht

ISBN 3-934629-86-5
ISSN 0945-9553

* Ulrich Klose ist Journalist und studiert Politikwissenschaft, Kommunikationswissenschaften und Soziologie an der Westfälischen Wilhelms-Universität in Münster. 2001 war er als studentischer Mitarbeiter der Forschungsstelle IT-Innovation und IT-Sicherheit am Institut für Politikwissenschaft der Westfälischen Wilhelms-Universität tätig.
Prof. Dr. Olaf Winkel lehrt Politik- und Verwaltungswissenschaft an der Fachhochschule für Verwaltung und Recht Berlin. Er ist Privatdozent am Institut für Politikwissenschaft der Westfälischen Wilhelms-Universität Münster, wo er als Mitglied im Forschungsverbund Datensicherheit NRW die Forschungsstelle für IT-Innovation und IT-Sicherheit gleitet hat.

Akademie für Technikfolgenabschätzung
in Baden-Württemberg

Industriestr. 5, 70565 Stuttgart
Tel.: 0711 • 9063-0, Fax: 0711 • 9063-299
E-Mail: info@ta-akademie.de
Internet: http://www.ta-akademie.de

Ansprechpartner:
Dr. Gerhard Fuchs Tel. 0711 • 9063-199
E-Mail: gerhard.fuchs@ta-akademie.de

Die *Akademie für Technikfolgenabschätzung in Baden-Württemberg* gibt in loser Folge Aufsätze und Vorträge von Mitarbeitern sowie ausgewählte Zwischen- und Abschlussberichte von durchgeführten Forschungsprojekten als *Arbeitsberichte der TA-Akademie* heraus. Diese Reihe hat das Ziel, der jeweils interessierten Fachöffentlichkeit und dem breiten Publikum Gelegenheit zu kritischer Würdigung und Begleitung der Arbeit der TA-Akademie zu geben. Anregungen und Kommentare zu den publizierten Arbeiten sind deshalb jederzeit willkommen.

Zusammenfassung

Können Verfahren aus dem Bereich der partizipativen Technikfolgenabschätzung einen Beitrag zur Realisierung von mehrseitiger Sicherheit in elektronischen Netzwerken liefern? Ein fachwissenschaftlicher Diskurs zu dieser Frage ist dringend geboten.

Inhaltsverzeichnis

1 Einführung[1]

Die moderne Gesellschaft wandelt sich zu einer Informationsgesellschaft. Ein zentrales Charakteristikum dieses Wandels ist die Abwicklung von immer mehr sozialen Funktionen mittels interaktiver Informationstechnologien (IT), sodass es durchaus Sinn macht, von einer digitalen Informationsgesellschaft zu sprechen. Für die vielfältigen Hoffnungen, die unterschiedliche Seiten mit dieser Entwicklung verbinden, stehen Begriffe wie *Electronic Commerce* und *Electronic Government*. Gleichzeitig treten aber auch die Risiken und Gefahren, welche die Kehrseite der Medaille bilden, immer deutlicher hervor. Für ein griffiges Verständnis der schädigenden Funktion, die den elektronischen Massenmedien und den interaktiven Informationstechnologien gemeinhin zugeschrieben wird, stehen der abgestumpfte *Couch Potato* und der bindungslose *Cyberfreak* als Gesellschaftsmitglieder, die die Umwandlung herkömmlicher Kommunikation in technikgestützte Formen mental und sozial nicht unbeschadet überstanden haben.

Bei näherer Betrachtung sind daneben aber auch Probleme gänzlich anderer Art zu erkennen, die sich auf die Dauer als noch wesentlich gravierender erweisen könnten. Gemeint sind die Probleme, die daraus erwachsen, dass die Frage der IT-Sicherheit – in einer ersten Annäherung zu verstehen als Sicherheit von Informationen und Informationstechnologien – unter den veränderten Vorzeichen des elektronischen Zeitalters eine völlig neue Bedeutung gewinnt, weil die Verletzlichkeit der Netzwerke mit der zunehmenden Digitalisierung von Kommunikations- und Kooperationsbeziehungen zur Verletzlichkeit der Gesellschaft selbst wird.

Dass sich die Sozialwissenschaften in der Vergangenheit noch nicht ausführlicher mit diesem Thema auseinandergesetzt haben, ist in Anbetracht seiner gesellschaftlichen Bedeutung überraschend. Dies gilt insbesondere angesichts der Tatsache, dass Ingenieure und Informatiker, die sich professionell mit der Verbesserung der Sicherheitslage in Unternehmen oder anderen Organisationen befassen, heute einhellig davon ausgehen, dass die Förderung von IT-Sicherheit in erster Linie ein Problem der sozialen Organisation und der Kultur und erst in zweiter Linie ein technisches Problem ist.

Dieser Paradigmawechsel, der nun auch schon einige Jahre zurückliegt, ist vor allem auf drei Gründe zurückzuführen: Der erste besteht darin, dass Netzwerksicherheit kein statisches, sondern ein dynamisches Phänomen darstellt, der zweite darin, dass die Vertrauenswürdigkeit in diesem Bereich eine ebenso große Rolle spielt wie die

[1] Die Arbeiten, die zu der vorliegenden Publikation geführt haben, wurden vom MSWF NRW finanziell gefördert.

faktische Zuverlässigkeit von technischen Systemen, und der dritte darin, dass IT-Sicherheit für unterschiedliche Seiten Unterschiedliches bedeuten kann, was Interessenkonflikte unvermeidbar macht. Hier erscheint die Informationsgesellschaft als Risikogesellschaft.

Der Satz, dass sich die technische Entwicklung an den politisch-administrativen Einrichtungen moderner Staaten weitgehend vorbei vollzieht und daher keiner wirksamen demokratischen Kontrolle oder Beeinflussung unterworfen ist, scheint für den Bereich der IT-Sicherheit in ganz besonderem Maße zu gelten. Die Konflikte, die hier entstehen können, scheinen die überkommenen gesellschaftlichen und politischen Konfliktbearbeitungsstrukturen und –kulturen in vielerlei Hinsicht zu überfordern. Wie groß diese Überforderung sein kann, wurde insbesondere im Laufe der so genannten Kryptokontroverse deutlich. Gegenstand dieser Kontroverse, die 1993 in den USA ihren Ausgang nahm und danach in abgeschwächter Form auch auf Europa übergriff, war die Suche nach einem rationalen gesellschaftlichen Umgang mit der vertraulichkeitsschützenden Verschlüsselung als einer Anwendungsvariante der elektronischen Kryptographie, welche die zentrale Sicherheitstechnologie der digitalen Informationsgesellschaft darstellt.

Das sich immer deutlicher abzeichnende Unvermögen der primär repräsentativ und korporatistisch ausgerichteten Demokratie zur Bewältigung der im Bereich der IT-Sicherheit auftretenden Probleme macht die Auseinandersetzung mit der Frage, ob bzw. inwieweit Verfahren der partizipativen Technikfolgenabschätzung (PTA) hier eine sinnvolle Ergänzung bieten können, zu einem lohnenswerten Unterfangen. Allerdings kann diese Auseinandersetzung nur in einem breiten fachwissenschaftlichen Diskurs erfolgen. Als normativer Bezugspunkt eines solchen Diskurses bietet sich das Leitbild der mehrseitigen Sicherheit an, d.h. der Gedanke, dass auch im Bereich der IT-Sicherheit nur Lösungen sinnvoll und dauerhaft tragfähig sein können, die darauf angelegt sind, eine möglichst breite Palette von Interessen zu integrieren.

Die Verfasser erheben nicht den Anspruch, mit ihrer Arbeit einen maßgeblichen Beitrag zur Klärung der Frage nach den Möglichkeiten und Grenzen von Verfahren aus dem Bereich der PTA zur Förderung mehrseitiger IT-Sicherheit zu leisten. Es geht ihnen lediglich darum, die Fachwelt für die wachsende Bedeutung des Themas zu sensibilisieren, einige Ansatzpunkte zur analytischen Durchdringung des Untersuchungsgegenstands zu markieren und auf diese Weise an der Schaffung der Voraussetzungen für einen umfassenden Diskurs mitzuwirken.

Abgesehen von den einführenden und abschließenden Bemerkungen gliedert sich die Arbeit in drei Teile. Im ersten wird die Frage erörtert, was die zentralen Merkmale von IT-Sicherheit sind, und wie IT-Sicherheit in sozialen Einheiten hergestellt werden kann. Der zweite Teil widmet sich unterschiedlichen Komponenten von PTA und ihren Möglichkeiten und Grenzen. Im dritten Teil werden die bis dahin angestellten Überlegungen miteinander verknüpft, sodass ein erster Eindruck davon ent-

steht, wo ein Diskurs zur Rolle von PTA-Komponenten bei der Förderung von mehrseitiger IT-Sicherheit ansetzen könnte und welche Aspekte er abdecken sollte.

2 IT-Sicherheit als Phänomen mit vielen Facetten

Sicherheit ist ein menschliches Grundbedürfnis.[2] Der Kern dessen, was Sicherheit in der virtuellen Welt der Netze bedeutet, lässt sich nach einer weitgehend akzeptierten Auffassung unter die Kategorien der Verfügbarkeit, der Integrität, der Verbindlichkeit und der Vertraulichkeit von Informationen und Kommunikationsbeziehungen fassen.

2.1 IT-Sicherheit als Verfügbarkeit, Integrität, Verbindlichkeit und Vertraulichkeit

Verfügbar sind Informationen und Kommunikationsbeziehungen, wenn ein berechtigter Anwender im Bedarfsfall auf sie zugreifen kann. Verfügbarkeitsverluste treten ein, wenn die Funktionsfähigkeit der Systeme beeinträchtigt ist, die der Verarbeitung, Speicherung und Übermittlung von Informationen dienen. Dieser Aspekt von Sicherheit ist es, der den Gegenstand der Diskussion um die so genannten kritischen Infrastrukturen bildet, d.h. um den Umstand, dass die Sicherheit der informationstechnischen Infrastruktur zunehmend zur Voraussetzung der Sicherheit anderer wesentlicher Infrastrukturen wird, etwa der Energieversorgung, der Gesundheitsversorgung, des Rettungswesens und des Verkehrswesens. Dabei werden die unterschied-

[2] Weil sich einer der Autoren in der Vergangenheit bereits intensiv mit Fragen der IT-Sicherheit auseinandergesetzt hat, rekurrieren die Ausführungen in den entsprechenden Kapiteln vorwiegend auf dessen einschlägige Arbeiten: Eine umfassende Übersicht über den Gegenstandsbereich der IT-Sicherheit findet sich bei Winkel 2000c. Aus Interessenkonflikten resultierende Probleme werden erörtert bei Winkel 1997b/1998/2000a/2000d. Anmerkungen zum Prozesscharakter von IT-Sicherheit sowie zu den Anforderungen eines effektiven Sicherheitsmanagements, das sich am Leitbild der mehrseitigen Sicherheit orientiert und in einer adäquaten Sicherheitskultur verankert ist, finden sich bei Winkel 1997a/2000b/2001. Die Frage der Herausbildung von Vertrauen als subjektives Moment der Herstellung von IT-Sicherheit wird ausführlich behandelt bei Winkel 1999. Die Anforderungen, die sich aus den Problemen der IT-Sicherheit für die sozialwissenschaftliche und insbesondere die politikwissenschaftliche Forschung ergeben, werden bei Winkel 2000b erörtert. Natürlich finden sich in den aufgeführten Arbeiten auch zahlreiche Hinweise auf weiterführende Literatur und URLs.

lichsten Bedrohungsszenarien entworfen. In der Zeitschrift ‚Der Spiegel' wurde sogar die Behauptungen aufgestellt, dass "statt einer hochgerüsteten Armee" heute "dreißig Computervirtuosen" ausreichen, "um die Vereinigten Staaten lahm zu legen" (so Deckstein/Dworschak/Kerbusk/ Mascolo/Müller/Ulrich 2000: 60 f.). Ausgestattet "mit einem Budget von weniger als zehn Millionen Dollar" und "geschickt auf die Knotenpunkte des weltweiten Rechnernetzes verteilt" könne ein solches virtuelles Einsatzkommando "Stromversorger abschalten, Flughafenkontrollsysteme außer Kraft setzen und ein landesweites Chaos inszenieren".

Integrität steht für die unverfälschte Übertragung von Informationen zwischen berechtigten Partnern. Integritätsverluste treten ein, wenn Nachrichten auf ihrem Weg im Netz oder beim Adressaten verändert werden. Möglich wird ein solcher Angriff etwa in der Form der so genannten *Man-in-the-Middle-Attack*. Dabei täuscht ein Angreifer einen freien Weg im Netz vor, um Datenpakete auf den eigenen Rechner zu locken, sie dort zu manipulieren und dann weiterzuleiten.

Verbindlich sind Kommunikationsprozesse, wenn sie sich den Kommunikationspartnern verlässlich zuordnen lassen. Wo keine rechtsverbindlichen Willenserklärungen ausgetauscht werden können, ist die Abwicklung von Rechtsgeschäften und Verwaltungsakten unmöglich. Während dies in Intranets – also in geschlossenen Netzwerken – bereits seit vielen Jahren an der Tagesordnung ist, befindet sich die Infrastruktur für die verbindliche Kommunikation im Internet als einem offenen Netzwerk noch in ihren Kinderschuhen.[3]

Als vertraulich gelten Informationen und Kommunikationsbeziehungen, die nur ausgewählten Teilnehmern bekannt sein sollen. Vertraulichkeitsverluste können durch einen unberechtigten Zugriff auf Informationen entstehen, etwa wenn der Inhalt einer E-Mail von einem unberechtigten Dritten mittels entsprechender Software – so genannter *Hackertools* – ausgespäht wird. Aber auch schon allein das Wissen darum, dass ein Teilnehmer bestimmte Kommunikationsakte durchgeführt hat, kann eine kompromittierende Verletzung des Vertraulichkeitsschutzes darstellen und für den Betroffenen negative Folgen haben. Man denke hier etwa an eine telefonische Kontaktaufnahme mit den Anonymen Alkoholikern oder mit einer Schuldnerberatungsstelle. Das Leitbild der Vertraulichkeit integriert neben dem Fernmeldegeheimnis auch den Datenschutz in den Kontext der IT-Sicherheit. (vgl. Winkel 1998: 288).

[3] Gerade hier sehen die führenden Politiker und Unternehmer diesseits und jenseits des Atlantik aber die größten ökonomischen Entwicklungschancen. So ließ schon Al Gore in seiner Zeit als US-Vizepräsident verlauten, dass sich im Internet "eine neue Welt wirtschaftlicher Möglichkeiten und ökonomischen Fortschritts" eröffne. Der damalige US-Präsident Bill Clinton stellte sogar Bezüge zur Pionierzeit der Vereinigten Staaten her, als er erklärte, der elektronische Handel sei "wie der wilde Westen der Wirtschaft" (vgl. Winkel 1998: 288).

2.2 IT-Sicherheit als Verlässlichkeit und Vertrauen

Wie alle Fragen der Sicherheit sind auch die abstrakten Sicherheitswerte der Verfügbarkeit, der Integrität, der Verbindlichkeit und der Vertraulichkeit von Informationen und Kommunikationsbeziehungen nicht nur unter Gesichtspunkten der faktischen Zuverlässigkeit, sondern ebenso unter Vertrauensaspekten zu betrachten. Wenn informationstechnische Systeme die ihnen zugedachten Aufgaben erfüllen und auf Akzeptanz stoßen sollen, müssen sie nicht nur eine hohe Verlässlichkeit aufweisen, sondern auch ein entsprechendes Maß an Vertrauenskapital auf sich vereinigen. Vertrauen kann dabei definiert werden als "riskante Vorleistung von Akteuren im Spannungsfeld zwischen Wissen und Nichtwissen" (so Braczyk/Barthel/Fuchs/Konrad 1999: 121). Neben den Wirkungen einer vorrangig mit Expertisen operierenden Öffentlichkeitsarbeit und der Möglichkeit, Analogien zwischen der "realen" Welt und der virtuellen Welt der Netze zur Förderung von Vertrauen produktiv zu machen[4], ist für die Entstehung von Vertrauen vor allem die gesellschaftliche Einbindung der interaktiven Informationstechnologien von Bedeutung. Dies kann durch die Schaffung von Institutionen geschehen, die den Umgang mit der Technik regeln. So kommt immateriellen Institutionen wie dem Telekommunikationsgesetz und materiellen Institutionen wie der Regulierungsbehörde für Telekommunikation unter anderem auch die Funktion zu, das Vertrauen in die Sicherheit von informationstechnischen Anwendungen zu stützen, indem sie etwa Aufgaben der „Handlungsregulierung, Zugangsregulierung, Konfliktregulierung, Versicherung und Bürgschaft" wahrnehmen (so Barthel/Braczyk/Fuchs 1999: 120). Auf dem Wege der institutionellen Einbindung von Technik kann es auch gelingen, im Sinne von Luhmanns "Soziologie des Risikos" (Luhmann 1992) zur Förderung von Vertrauen und Akzeptanz Abwehr hervorrufende Gefahren über das Mittel der Beteiligung in tolerierte Risiken zu verwandeln.

Auf der anderen Seite existiert das Vertrauen in die Technik aber auch hier nicht unabhängig von ihrer Zuverlässigkeit. Maßnahmen, die der Erhöhung der Verlässlichkeit von informationstechnischen Systemen dienen, sind daher auch prinzipiell geeignet, einen Beitrag zur Erhöhung ihrer Vertrauenswürdigkeit zu leisten.

[4] Dies ist etwa dann der Fall, wenn mit Bezeichnungen wie virtuelle Gemeinschaft, Online-Mall oder Online-Party Begriffe aus der "realen" Welt auf den Cyberspace übertragen werden, oder dann, wenn eine Firma, die sich bereits als herkömmliches Versandhaus einen Namen gemacht hat, mit identischen Logos und Slogans als Internethändler auftritt.

2.3 IT-Sicherheit als knappes Gut

Wie alle anderen Formen von Sicherheit – etwa von Sicherheit im Straßenverkehr oder von wirtschaftlicher Sicherheit – kann auch IT-Sicherheit niemals schrankenlos, sondern immer nur in einem begrenzten Umfang gewährleistet werden. Verschärft wird die Lage dadurch, das sich in der jüngsten Zeit die Bedrohungen für sensible Informationen und Kommunikationsbeziehungen in der virtuellen Welt der Netze potenziert haben, weil Angriffssoftware aller Art im Internet frei erhältlich ist, und weil für ihren Einsatz keine besonderen technischen Kenntnisse mehr erforderlich sind. So hat prinzipiell jeder Teilnehmer die Möglichkeit, spezielle Websites aufzusuchen, um dort Viren oder Würmer herunter zu laden und sie in der Anlage einer E-Mail an missliebige Personen zu versenden. Vor diesem Hintergrund stellt sich im konkreten Einzelfall die Frage, welches Maß an Sicherheit für welchen Bereich angemessen und finanzierbar ist.

2.4 IT-Sicherheit als Prozess

Schon weil sich die Gefahren stetig wandeln, die durch Viren, Würmer, E-Mail-Bomben, Spionageprogramme oder andere destruktive Software verursacht werden, ist IT-Sicherheit nicht statischer, sondern dynamischer Natur. Um ein bestimmtes Maß an IT-Sicherheit aufrecht erhalten zu können, muss ein System in der Lage sein, immer wieder neu und ohne schädliche Zeitverluste auf die Veränderung von Umweltbedingungen zu reagieren. Daher hat sich unter Sicherheitsingenieuren und –informatikern ein Denken durchgesetzt, das Sicherheit als einen Prozess versteht, der nach dem Prinzip des kybernetischen Regelkreises abläuft.
Nach den *Guidelines* des *Joint Technical Committees (*JTC) der *International Standardization Organization (*ISO) und der *International Electronical Commission* (IEC) lässt sich der Sicherheitsprozess idealtypisch in vier Phasen einteilen, wobei die vierte Phase wiederum in die erste einmündet (vgl. Plate 1997):

- (1) Analyse der Sicherheitslage
- (2) Auswahl von Maßnahmen, um die erkannten Bedrohungen zu reduzieren
- (3) Umsetzung der Maßnahmen und
- (4) Aufrechterhaltung eines spezifischen Sicherheitsniveaus im laufenden Betrieb.

Die letztgenannte Phase gliedert sich wiederum in drei Stufen:

- (1) Überprüfung, ob die Maßnahmen durchgehalten werden und Wirkung entfalten
- (2) Nachbesserungen, wenn Maßnahmen nicht wie geplant greifen sowie

- (3) Reaktion auf Umweltveränderungen (insbesondere auf eine Änderung der Bedrohungslage).

2.5 IT-Sicherheit als Konfliktpotenzial

Bereits die oberflächliche Betrachtung zeigt, dass die Beziehungen zwischen den IT-Sicherheitswerten der Verfügbarkeit, der Integrität, der Verbindlichkeit und der Vertraulichkeit schon auf der abstrakten Ebene teilweise durch Zielkonkurrenzen geprägt sind. Wechselt man auf die Ebene der konkreten Sicherheitsinteressen, treten die Spannungen noch deutlicher hervor. Man denke etwa daran, dass viele Teilnehmer großen Wert darauf legen, dass ihre Kommunikationsakten vertraulich bleiben – d.h. nicht protokolliert und insbesondere nicht zur Anfertigung von Persönlichkeitsprofilen oder Kundenprofilen genutzt werden – während die Netzbetreiber und Dienstanbieter in dieser Hinsicht auf Verbindlichkeit angewiesen sind, weil sie entsprechende Daten zu Abrechnungszwecken benötigen. Ähnliche Konflikte finden sich in den unterschiedlichsten anderen Bereichen, etwa zwischen Arbeitnehmern und Arbeitgebern am Arbeitsplatz oder zwischen Käufern und Verkäufern im Internethandel.
Was Konflikte der geschilderten Art so brisant macht, ist einerseits die Tatsache, dass es sich dabei im Gegensatz zu verbreiteten anderen Auffassungen nicht nur um primär medienpolitische, technologiepolitische, telekommunikationspolitische oder sicherheitspolitische Konflikte handelt, sondern um Konflikte, die fast alle Bereiche des menschlichen Zusammenlebens unmittelbar betreffen und daher genuin gesellschaftspolitischer Natur sind. Andererseits ist es der Umstand, dass bei der Gestaltung informationstechnischer Systeme und damit auch bei der Gestaltung der Informationsgesellschaft selbst prinzipiell die Möglichkeit besteht, die unterschiedlichsten Ziele in deren Software hineinzuschreiben. Dass bei der Entscheidung der Frage, welche Sicherheitsinteressen bei der Ausgestaltung der Infrastruktur der Informationsgesellschaft Beachtung finden und welche an den Rand gedrängt werden, die gesellschaftlichen Kräfteverhältnisse eine ausschlaggebende Rolle spielen, steht angesichts entsprechender Erfahrungen aus anderen Bereichen zu vermuten.

2.6 IT-Sicherheit als mehrseitige Sicherheit

Um den neuen Herausforderungen zu begegnen, die in den unterschiedlichsten Bereichen aus der Konkurrenz unterschiedlicher Sicherheitsbilder und Sicherheitsinteressen erwachsen, wurde das Konzept der mehrseitigen Sicherheit erarbeitet als „eine sich mit der Technik fortentwickelnde Handlungsanleitung, die einerseits die Gestaltung neuer Technik für Kommunikationssysteme leiten soll und andererseits als

Grundlage für eine technikgestaltende Gesetzgebung dienen kann“ (so Müller/Pfitzmann 1997: 13). Seine Urheber sind nicht Sozialwissenschaftler, sondern Ingenieure und Informatiker. Nach diesem Ansatz gilt es, die Sicherheitsbelange aller an einem Kommunikationsvorgang Beteiligten über Kompromisse so weit wie möglich zu berücksichtigen und die verbleibenden Restrisiken in einer allgemein akzeptablen Weise zu verteilen. Auf diesem Wege soll nicht nur die Verlässlichkeit, sondern auch die Vertrauenswürdigkeit und Akzeptanz der interaktiven Informationstechnologien gesteigert werden. Letztlich kann die Orientierung am Leitbild der mehrseitigen Sicherheit auch als Versuch einer Erhöhung der Qualität von IT-Sicherheit interpretiert werden, denn eine Lösung, die eine breite Palette von Sicherheitsinteressen berücksichtigt, impliziert gegenüber einer einseitigen Berücksichtigung der Sicherheitsinteressen durchsetzungsstarker Akteure eine “bessere” Sicherheit. Auch für durchsetzungsstarke Akteure können mehrseitig akzeptable Sicherheitslösungen Vorteile bringen. Dies ist etwa dann der Fall, wenn sich auf diese Weise aufwendige Konflikte vermeiden lassen, oder dann, wenn es darum geht, Teilnehmer, den herkömmliche Verfahren als Alternativen zur Verfügung stehen, für vertrauenskritische Anwendungen wie Homebanking zu gewinnen.

Was die Realisierung des Leitbilds der mehrseitigen Sicherheit betrifft, setzen die Begründer dieses Konzeptes verstärkt auf Regulierung durch Codes, d.h. auf eine unter sozialen und politischen Aspekten gezielt vorgenommene Gestaltung von technischen Systemen. Eine Software, die entsprechende Aushandlungsprozesse im Rahmen konkreter Kommunikations- und Kooperationsvorfälle ermöglicht, steht als Prototyp schon seit geraumer Zeit zur Verfügung. Ihre praktische Anwendung beschränkt sich bis heute aber weitgehend auf Präsentationsveranstaltungen. Aus sozialwissenschaftlicher und insbesondere politikwissenschaftlicher Sicht interessant wäre die Ermittlung der Faktoren, die dafür ursächlich sind, dass eine Software, die einem zentralen neuen gesellschaftlichen Bedarf Rechnung trägt, nicht diffundiert. Noch weitaus bedeutsamer erscheint hier aber die Klärung der Frage nach neuen Konfliktlösungsstrukturen und Konfliktlösungskulturen, die dazu dienen können, auf der Ebene gesellschaftlicher Aushandlungsprozesse einen Beitrag zur Umsetzung des Leitbilds der mehrseitigen Sicherheit zu leisten.

Der oben unter Bezugnahme auf das JTC skizzierte Sicherheitsprozess bedarf aus einem Blickwinkel, der die Förderung von mehrseitiger Sicherheit zur Notwendigkeit erhebt und dieses Unterfangen gleichzeitig weniger als ingenieurtechnisches denn als sozialtechnisches Projekt versteht, einer Erweiterung und Modifikation. Danach stellt sich der Sicherheitsprozess folgendermaßen dar:

- (1) Identifizierung und Kommunikation von Sicherheitsbedrohungen (unter Beachtung des Umstands, dass ein technisches System unter Aspekten der faktischen Verlässlichkeit und der Vertrauenszuschreibung gleichermaßen angreifbar ist),

- (2) Abgleich von divergierenden Sicherheitsbildern und Sicherheitsinteressen zur Herausarbeitung von Lösungen, die Kompromisse und Kompensationen beinhalten können,
- (3) Auswahl von Strategien und Maßnahmen, um erkannte Bedrohungen zu reduzieren und die Restrisiken allgemein akzeptabel zu verteilen
- (4) Umsetzung der Strategien und Maßnahmen sowie
- (5) Aufrechterhaltung des Sicherheitsniveaus durch Kontrolle, Nachbesserung und Umweltbeobachtung.

Unabhängig davon, ob es um die Verbesserung des IT-Sicherheitsniveaus in einem Unternehmen, in einer Behörde oder auf gesamtgesellschaftlicher Ebene geht, ist ein funktionierender Sicherheitsprozess an unterschiedliche Voraussetzungen gebunden. Zu den wichtigsten zählen die Verfügbarkeit von anwenderfreundlicher, kostengünstiger und zuverlässiger Sicherheitstechnik sowie die Etablierung eines Sicherheitsmanagements und die Entwicklung einer Sicherheitskultur.

2.7 IT-Sicherheit als Ergebnis technischer Maßnahmen

Wie die neuen Technologien neue Gefahren mit sich gebracht haben, haben sie auch zur Entwicklung und Verbreitung neuer Schutzmechanismen geführt. So können *Firewalls* dazu dienen, die Schnittstellen zwischen Intranets und Internet in einer Weise zu gestalten, die externe Angriffe aller Art verhindern oder zumindest nachhaltig erschweren. So bieten Zugangskontrollsysteme und Zugriffsregelungssysteme die Möglichkeit, unberechtigten Dritten den Zugang zu sensiblen Informationen und technischen Systemen zu verwehren. So gibt die vertraulichkeitsschützende Verschlüsselung den Anwendern die Möglichkeit, ihre sensiblen Informationen auf Speichermedien und im Netz zuverlässig vor einer unberechtigten Kenntnisnahme Dritter abzuschotten. Und so können digitale Signaturen dazu dienen, zurechenbare und unverfälschte Willenserklärungen nicht nur in geschlossenen, sondern auch in offenen Netzwerken auszutauschen.

Die Grundlage technischer Sicherheitsmaßnahmen ist die elektronische Kryptographie. Diese Verfahren eröffnen prinzipiell die Möglichkeit, die Sicherheit von Informationen und Kommunikationsbeziehungen im Hinblick auf drei der vier abstrakten Sicherheitswerte – nämlich auf die der Vertraulichkeit, der Integrität und der Verbindlichkeit – unmittelbar zu gewährleisten. Was das Ziel der Verfügbarkeit betrifft, ist die elektronische Kryptographie zwar nicht unmittelbar, aber zumindest mittelbar von Bedeutung. So basieren Zugangskontrollsysteme, Zugriffsregelungssysteme und andere Maßnahmen zur Verhinderung von Sabotageakten in vielen Fällen auf dieser Technologie.

2.8 IT-Sicherheit als Ergebnis von Sicherheitsmanagement und Sicherheitskultur

Aber auch die elektronische Kryptographie bietet natürlich kein Allheilmittel zur Bewältigung der vielfältigen neuen Sicherheitsprobleme, die in einer sich zunehmend digitalisierenden Gesellschaft auftreten. Es müssen unter anderem organisatorische Maßnahmen, wie die sicherheitsspezifische Optimierung von Arbeitsprozessen, und personalbezogene Maßnahmen, wie die Sensibilisierung und Schulung von Anwendern in Fragen der IT-Sicherheit, hinzukommen. Weil Netzwerksicherheit kein statisches, sondern ein dynamisches Phänomen ist, weil sie unter sich stetig verändernden Umweltweltbedingungen immer wieder neu erzeugt und zugeteilt werden muss, weil sie niemals unbeschränkt, sondern immer nur in begrenztem Umfang bereitgestellt werden kann, und nicht zuletzt, weil Sicherheit nicht nur "objektive" Verlässlichkeit, sondern auch "subjektives" Vertrauen bedeutet, erscheint es sogar angeraten, den Ansatzpunkt für die Förderung von IT-Sicherheit nicht im technischen Bereich, sondern im Bereich der sozialen Organisation und der Kultur zu wählen.
Gefordert ist die rationale Gestaltung von Sicherheitsprozessen durch ein effektives Sicherheitsmanagement, das in einer tragfähigen Sicherheitskultur wurzelt. Sicherheitsprozess steht dabei für die auf Dauer angelegten Formen und Verfahren, in denen in einer sozialen Einheit Risiken und Gefahren bewältigt werden. Als Sicherheitsmanagement lässt sich die Art und Weise bezeichnen, in der der Sicherheitsprozess – von der Förderung der Problemwahrnehmung über die Gestaltung der internen und externen Problemkommunikation bis hin zur Organisation der Problembearbeitung – in einer sozialen Einheit institutionell und funktionell organisiert wird. Eine effektive Problembearbeitung kann sich dabei nicht nur in der Entschärfung von Bedrohungen durch technische und personalbezogene Maßnahmen äußern, sondern auch in einem rationalen Umgang mit verbleibenden Restrisiken, etwa durch die Vorhaltung von Notfallkonzepten, die Anbindung an Computernotfallteams oder den Abschluss von Versicherungen. Sicherheitskultur steht wiederum für das im Selbstverständnis einer sozialen Einheit verankerten Systems von kollektiven Wertvorstellungen, Denkweisen und Handlungsmustern, das deren Mitglieder im Umgang mit Sicherheitsbedrohungen anleitet, und das daher gleichermaßen als Basis und Resultat des Sicherheitsmanagements anzusehen ist.

3 Mehrseitige Sicherheit als Überforderung der repräsentativ-korporatistischen Demokratie

Aus der normativen Perspektive erscheint die Bundesrepublik Deutschland in erster Linie als repräsentative Demokratie, aus der empirischen Perspektive verstärkt als korporatistische Demokratie. Auch was die Formulierung und Vertretung von Interessen im Bereich der IT-Sicherheit betrifft, spielen neben Parlamenten, Regierungen, Verwaltungsbürokratien und anderen dem politisch-administrativen System zugehörigen Einrichtungen unter anderem auch Verbände, Vereine und zivilgesellschaftliche Initiativen eine wichtige Rolle. Durch die Fremdorganisation von Interessen – hier ist insbesondere das differenzierte System der Datenschutzbeauftragten zu nennen – wird der Versuch unternommen, die Folgen der aus Korporatismus und Lobbyismus erwachsenden Asymmetrien bei der Ausübung von Definitionsmacht und Durchsetzungsmacht im Hinblick auf den Vertraulichkeitsschutz in akzeptablen Grenzen zu halten (vgl. etwa Der Bundesbeauftragte für den Datenschutz 1999 oder Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen 1999). Einrichtungen wie die vom Bundesinnenministerium initiierte Internet-Taskforce und der Arbeitskreis Schutz Kritischer Infrastrukturen (AKSIS), in dem unter anderem Energieversorger, Telekommunikationsanbieter, die Bahn AG, Luftverkehrsgesellschaften, Banken, Forschungseinrichtungen, Kommunalverwaltungen, Bundesministerien, das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Sicherheitsdienste vertreten sind (vgl. Geiger 2000: 130 und Hutter 2000: 35), stehen dagegen für Sicherheitsinteressen, die mit den durch die Datenschützer vertretenen Belangen in vielerlei Hinsicht konfligieren.

Die in diesem Beitrag angestellten Überlegungen basieren auf der Prämisse, dass die Einrichtungen, Akteure und Netzwerke, die im repräsentativ-korporatistischen System der Bundesrepublik Deutschland und in grenzüberschreitenden Kontexten auf dem Feld der IT-Sicherheit eine Rolle spielen, nicht in der Lage sind, einen entscheidenden Beitrag zur Realisierung des Leitbilds der mehrseitigen Sicherheit zu leisten. Weil wir uns heute noch in einer Phase befinden, in der sich die immensen Dimensionen und die große Brisanz der neuartigen Sicherheitsprobleme der Informationsgesellschaft erst andeuten, kann derzeit noch nicht der letzte Beweis zur Untermauerung dieser These angetreten werden. Vieles spricht aber dafür, das sie tatsächlich zutrifft: Man denke etwa daran, dass Software zur Gewährleistung mehrseitiger Sicherheit trotz ihrer sozialen Wünschbarkeit bis heute kaum Verbreitung gefunden hat (vgl. Müller/Pfitzmann 1997: 11 ff und Winkel 2001: 56). Man denke auch daran, dass die Kryptokontroverse in der Bundesrepublik Deutschland wie in den USA nicht auf dem Wege der Verständigung, sondern durch die normative Kraft des Faktischen entschieden worden ist – nämlich durch die zuletzt für keine Seite mehr übersehbare Tatsache, dass technische Umgehungsmöglichkeiten und die globale

Ausdehnung der Netzwerke jede Form der Kryptoregulierung zu einer Farce gemacht hätten (vgl. Winkel 1997b:582 f./2000a: 73 ff/2001: 54 ff). Oder man denke an die Art und Weise, wie nicht nur hierzulande sondern auch in der politischen und diplomatischen Kommunikation im europäischen und transatlantischen Rahmen der Umstand behandelt bzw. eben nicht behandelt worden ist, dass mit *Echelon* ein unter der Federführung Washingtons und unter Beteiligung der Briten arbeitendes Lauschsystem existiert, das sich auch gegen Mitgliedsstaaten der Europäischen Union richtet (vgl. Mascolo/Schreiber/Thielke 2000: 216 ff, Winkel/Kösemen 2002: 1227 ff und Woolsey 2000: 10).
Folgt man der These, dass die derzeit gegebenen Problembearbeitungsstrukturen und -kulturen durch das Erfordernis, die elektronischen Kommunikations- und Kooperationsbeziehungen auf das Leitbild der mehrseitigen Sicherheit auszurichten, überfordert werden, weil es unter anderem an den dazu erforderlichen Einrichtungen, Arenen und Netzwerken fehlt, stellt sich die Frage nach möglichen Alternativen und Ergänzungen. Im Folgenden werden unterschiedliche diskursive Verfahren aus dem Bereich der PTA vorgestellt, mit deren Hilfe es vielleicht möglich sein kann, einen wesentlichen Beitrag zu Schließung der entsprechenden Lücken zu leisten.

4 Partizipative Technikfolgenabschätzung als erweiterte Form von TA, die in unterschiedlichen Varianten realisiert werden kann

Technikfolgenabschätzung (TA) und PTA lassen sich bekanntlich nicht trennscharf voneinander abgrenzen. Zum Verhältnis von TA und PTA ist zu sagen, dass PTA eine Sonderform bzw. eine insbesondere um spezifische Bewertungsaspekte erweiterte Form von TA darstellt, und dass es unmöglich ist, PTA ohne den Kontext der TA zu verstehen.

4.1 TA als exklusives Projekt

Eine umfassende Definition von TA, in der sich auch zentrale Leitlinien für die Arbeit des Büros für Technikfolgenabschätzung des Deutschen Bundestags (TAB) wiederfinden, liefern Wilgart Schuchardt und Rainer Wolf. Danach erhebt das "Idealkonzept der Technikfolgenabschätzung" den Anspruch, "neben der Früherkennung technologieinduzierter Risiken eine umfassende Analyse des Spektrums möglicher sozialer, wirtschaftlicher, rechtlicher, politischer, kultureller und ökologischer Auswirkungen zu leisten, in der problemorientierten Aufbereitung der Untersuchungsergebnisse alternative Handlungsoptionen entscheidungsorientiert aufzuzeigen und

zugleich unterschiedliche gesellschaftliche Interessen und Werturteile, die sich an die Entwicklung und Nutzung neuer Technologien knüpfen, offen zu legen" (so Schuchardt/Wolf 90: 19).
Komponenten eines Technikfolgenabschätzungsprojektes herkömmlicher Art, das in erster Linie auf einer Kooperation von Wissenschaftlern und Politkern beruht, sind die technologische Prognose der zukünftigen Entwicklungen, die technologische Wirkungsanalyse und die Politikanalyse mit der Ermittlung von Handlungsoptionen. In diesem Rahmen wird mit unterschiedlichen Untersuchungsmethoden gearbeitet, unter anderem mit der Delphitechnik, der Kosten-Nutzen-Analyse und der Simulationsstudie. Ein verbindliches Technikfolgenabschätzungsverfahren kann es schon wegen der Heterogenität der Technikfolgenabschätzungsaufgaben nicht geben.[5]

4.2 TA als inklusives Projekt

In der Vergangenheit wurden die in der Bundesrepublik Deutschland in exklusiven Kreisen von Wissenschaftlern und Politikern praktizierten Formen der Technikfolgenabschätzung bekanntlich zunehmend zum Gegenstand der Kritik. In der sozialwissenschaftlichen Diskussion favorisiert man seit geraumer Zeit Technikfolgenabschätzungskonzepte, die als „Kombination aus Sachverstand und öffentlichem Diskurs" (so Renn 2002: 32) Merkmale partizipativer Systemgestaltung aufweisen (vgl. Bechmann 1997: 159 ff, Renn 2002: 32 und Saretzki 1997a: 277 ff).
PTA, die von vielen als eine – wenn auch unvollständige – Antwort auf die Defizite einer exklusiven TA angesehen wird, "geschieht prozedural, indem neben der Wissenschaft Entscheidungsträger und von Entscheidungen direkt oder indirekt Betroffene in den Analyse- und Bewertungsprozess eingebunden werden" und "auf den Untersuchungsprozess Einfluss" erhalten (so Baron 1995: 233). Die Funktion von PTA liegt vor allem darin, einen Beitrag zur Bannung der Gefahr zu leisten, dass sich Technik "am Bedarf, an den Interessen, an den gesellschaftlichen Werten vorbei" entwickelt und auf diese Weise den gesellschaftlichen Konsens gefährdet und Widerstand provoziert (so Simonis 1989: 197). Durch eine breite Beteiligung an den Prozessen der Technikabschätzung im Sinne einer Technikbewertung soll den pluralen Einstellungen und Interessen in der Gesellschaft besser Rechnung getragen, eine öffentliche Debatte angeregt und soziales Lernen ermöglicht werden (dies und das Folgende nach Baron 1995: 194 f., Bechmann 1997: 157 und Renn 1996: 3 ff). Zugleich gehen die Verfechter von PTA davon aus, dass diese weitaus besser als herkömmliche TA geeignet ist, die Akzeptanz für politische Entscheidungen zu verbessern. Da-

[5] Es existieren aber immerhin erprobte Verfahrensschemata wie das der MITRE-Corporation (vgl. Böhret/Franz 1986: 356).

bei mache die Beteiligung von Laien die Experten-TA jedoch keineswegs obsolet. Die letztere sei vor allem dort sinnvoll, wo Probleme auftreten, die nicht über die individuelle Lebenserfahrung lösbar sind, deren Politisierungsgrad gering ist, und deren Lösung sich in Form einer eindeutigen Handlungsregel darstellen lässt. Eine breite Partizipation sei hingegen bei komplexeren Probleme mit hohem Konfliktpotenzial angebracht, denn nur sie eröffne die Möglichkeit, zunächst die Konflikte aufzudecken und dann in weiteren Schritten auf eine Annäherung der divergierenden Positionen hinzuwirken.[6]

4.3 TA und PTA als informelle und institutionalisierte Projekte

TA und PTA können sowohl sporadisch und informell zu aktuell auftretenden Problemen als auch über längere Zeiträume und institutionalisiert praktiziert werden. Beide Varianten haben ihre Berechtigung. Wenn TA und PTA eine nachhaltige politische Bedeutung gewinnen sollen, müssen sie aber zumindest in einem gewissen Ausmaß im bestehenden repräsentativ-demokratischen Gefüge verankert werden.
Die Diskussion um die Institutionalisierung von TA in der Bundesrepublik Deutschland rankte sich auch darum, wie unabhängig eine entsprechende Einrichtung sein durfte. Zur Auswahl standen eine tendenziell vom Parlament abhängige Amtslösung, wie sie bei der Einrichtung des Büros für Technikfolgenabschätzung des Deutschen Bundestags (TAB) gewählt wurde (Petermann 2000: 96 f), und eine ausgegliederte Lösung, wie sie im Falle der als Stiftung organisierten Akademie für Technikfolgenabschätzung in Baden-Württemberg zum Tragen kam (vgl. Baron 1995: 178 ff und Mohr 1997: 410 ff). Im Unterschied zu anderen Einrichtung hat die letztgenannte bekanntlich einen über die rein parlamentarische Beratung hinaus gehenden Auftrag. Sie soll zur technologischen Erneuerung und Entwicklung Baden-Württembergs beitragen und ist zudem auf die Initiierung und Koordinierung eines gesellschaftlichen TA-Diskurses verpflichtet. So ist es auch die Akademie für Technikfolgenabschätzung in Baden-Württemberg, die in der Vergangenheit besonders häufig PTA-Projekte angestoßen hat (vgl. insb. Akademie für Technikfolgenabschätzung in Baden-Württemberg 2000, aber auch Guston 1998: 3 und Westphalen 1997: 12).
Betrachtet man die Technikfolgenabschätzungslandschaft aus der Sicht der Bundesrepublik Deutschland, gelangt man zu der Erkenntnis, dass sich auf allen Ebenen – von der Landesebene (vgl. Baron 1995: 178 ff, Guston 1998: 3 und Mohr 1997: 410 ff) über die Bundesebene (vgl. Meyer 1997: 340 ff und Petermann 2000: 96 f.) und

[6] Es liegt in der Natur der Sache, dass PTA-Projekte tendenziell eine komplexere Struktur aufweisen als herkömmliche Formen von TA (Näheres dazu bei Ott/Skopurinski 2000: 177 ff).

die europäische Ebene (vgl. Rader 1998: 13 ff, Uhl/Thiele 2000: 98 ff und Wunrich 1997: 287 ff)[7] bis hin zur globalen Ebene (vgl. Andersen 1997, Coenen 1998: 44 f. und König 1997: 281 ff) – Einrichtungen finden, in denen gegebenenfalls TA und PTA zur Bearbeitung von Problemen der IT-Sicherheit betrieben werden kann.

4.4 Partizipationsverfahren als Komponenten von PTA

In den folgenden Kapiteln werden unterschiedliche Verfahren dargestellt, mit denen eine stärkere Beteiligung von Bürgerinnen und Bürgern an der politischen Entscheidungsfindung erreicht werden kann.[8] Die verschiedenen partizipativen Methoden haben eine gemeinsame Grundmotivation: Erreicht werden soll eine Verständigung der Akteure durch direkte Kommunikation. Auf der Basis eines so entwickelten Konsenses sollen anstehende Entscheidungen rationaler gestaltet und besser legitimiert werden. Hervorzuheben ist, dass die Partizipationsmethoden auf der Ebene der Politikberatung angesiedelt sind. Sie zielen entweder auf das politische System, um beispielsweise eine Themensetzungsfunktion zu erfüllen, oder auf die Öffentlichkeit mit dem Ziel der Information, der Anregung einer öffentlichen Debatte oder der Weiterentwicklung des demokratischen Systems (vgl. EUROPTA 2000: 36 ff und Hennen 1997: 14).

4.4.1 Die Planungszelle als Korrektiv korporatistischer Entscheidungsfindung mit Legitimationsanspruch

Das Planungszellenverfahren wird in der Bundesrepublik Deutschland vor allem mit dem Namen Peter Dienel als seinem engagiertesten Protagonisten verbunden (vgl. Dienel 1992/1996, Forschungsstelle Bürgerbeteiligung und Planungsverfahren 2001 und Freitag 1997). Die Grundidee dieses Verfahrens setzt bei dem Befund an, dass in herkömmlichen politischen Entscheidungsmechanismen die in Verbänden, Vereinen

[7] Das bei der Europäischen Union als parlamentarische Beratungseinheit fungierende *Scientific and Technological Options Assessment Programme* (STOA) hat übrigens maßgeblichen Anteil daran gehabt, dass die mit dem Lauschsystem *Echelon* verbundenen Probleme (vgl. Punkt 3 dieser Arbeit) durch eine Resolution des Europäischen Parlaments zumindest ansatzweise den Weg auf die politische Agenda der EU und ihrer Mitgliedsstaaten gefunden haben (vgl. Winkel/Kösemen 2002).

[8] Natürlich stehen diese Verfahren nicht für einen jeweils kompletten PTA-Prozess, sondern für prinzipiell sinnvolle Elemente eines solchen Prozesses. Wie bereits angesprochen handelt es sich bei TA und PTA um komplexe Arrangements verschiedener Verfahren, von denen einige partizipativ angelegt sein können.

und Parteien organisierten Interessen überproportional stark vertreten sind. Dieser Asymmetrie und ihren oft als ungerecht empfundenen Ergebnissen soll entgegengewirkt werden. Dabei sehen die Verfechter des Planungszellenverfahrens durchaus, dass es schon aus technisch-organisatorischen Gründen nicht möglich ist, alle relevanten Gruppen konsequent in politische Entscheidungsprozesse einzubeziehen. Sie reagieren auf dieses Problem dadurch, dass sie erst gar nicht den Anspruch erheben, alle von einer politischen Maßnahme Betroffenen identifizieren zu wollen. Stattdessen werden Laien zufällig ausgewählt, die – für eine begrenzte Zeit, unterstützt durch zwei Prozessbegleiter und unter Vergütung der Teilnahme – eine spezielle Fragestellung bearbeiten sollen (vgl. Dienel 1992: 86 ff/263f., Freitag 1997: 20 f. und Lübke 1997:10 ff).” Durch die Zufallsauswahl soll eine annähernde Repräsentativität der Planungszelle erzielt und sollen gerade “spezifisch Nichtinteressierte” (so Dienel 1992: 263) und Angehörige benachteiligter sozialer Schichten erreicht werden.

Das Ziel von Planungszellenverfahren besteht darin, so genannte Bürgergutachten zu erstellen. Pro Planungsprojekt, mit dem durchaus mehrere Planungszellen parallel befasst sein können, soll ein Bürgergutachten erarbeitet werden, das der politischen Ebene zur Fundierung ihrer Entscheidung dienen kann bzw. dessen Ergebnisse sich durch den Beschluss eines Repräsentativorgans (etwa eines Stadtrates) in die politisch-administrative Problembearbeitung einspeisen lassen. In diesem Gutachten soll die Problemstellung analysiert und bewertet und ein Lösungsweg angeboten werden (vgl. Dienel 1992: 280, Freitag 1997: 7 und Saretzki 1997a: 301).

Die Durchführung von Planungszellen wird in der Praxis von einem öffentlichen Auftraggeber beschlossen, der einen unabhängigen Durchführungsträger mit der Abwicklung betraut. Der Letztgenannte übernimmt die Vorbereitung des Verfahrens, wählt die Prozessbegleiter aus, sorgt für die Teilnehmerauswahl und zieht gegebenenfalls geeignete Experten hinzu (vgl. Dienel 1992: 99 ff). Der eigentliche Planungszellenprozess – eingebürgert hat sich inzwischen eine Dauer von vier Tagen mit jeweils acht Arbeitsstunden – ist gekennzeichnet durch Arbeiten in fünfköpfigen Kleingruppen und ständige Gruppenwechsel. Jede Gruppenarbeitsphase endet mit der Erstellung eines Kurzberichtes. Weitere Elemente sind Fachvorträge, Ortsbegehungen, Bewertungssitzungen, Hearings und Sitzungen der gesamten Planungszelle (Plenumssitzungen). Die Anfertigung und Veröffentlichung des Bürgergutachtens bildet den Abschluss des Prozesses (vgl. Dienel 1992: 127 f./258 f., Dienel 1996: 431, Freitag 1997: 33 und Lackner 1999: 27 ff).

Heben Befürworter der Planungszelle die Verhinderung der einseitigen Durchsetzung von Partikularinteressen und die höhere Legitimität getroffener Entscheidungen als Vorteil hervor (vgl. Dienel 1992: 131 ff/265), so entzündet sich an eben diesem Anspruch auch die meiste Kritik (siehe etwa Ohlemacher 1991): Eine demokratische Legitimation sei schon wegen der fehlenden Einbindung des Verfahrens in den politisch-parlamentarischen Prozess nicht gegeben, und zudem könnten Planungszellen auch wegen der geringen Teilnehmerzahlen keinen Repräsentativitätsanspruch erhe-

ben. Weiterhin wenden Kritiker ein, dass Dienel das Ziel der Verhinderung einer asymmetrischen Interessendurchsetzung zu stark mit der Frage nach der soziodemographischen Zusammensetzung einer Gruppe verknüpfe, und dass hohe Absagequoten ein Indiz dafür seien, dass trotz der Zufallsauswahl gerade beteiligungsferne Gruppen durch das Planungszellenverfahren kaum erreicht werden könnten (vgl. Dienel 1992: 132, Freitag 1997: 33 ff/71 f. und Lackner 1999: 34 f.) Ungeklärt bleibe in dem Konzept auch, inwieweit Durchführungsträger, Prozessbegleiter und Experten auf das Ergebnis der Planungszellenarbeit Einfluss nehmen können bzw. inwieweit die Autonomie der Teilnehmer angesichts der Vorstrukturierung und des engen zeitlichen Rahmens gewährleistet ist (vgl. Baron 1995: 200 ff, Freitag 1997: 21 ff/71 f. und Lackner 1999: 33 f.).

Mit dem Planungszellenverfahren effektiv bearbeitbar sind nach Dienel unter anderem Probleme der Stadtentwicklung, des Bildungssektors, des Umweltschutzes, des Verkehrswesens, des Gesundheitswesens und der neuen Informationstechnologien (vgl. Dienel 1992: 137 f. und Lackner 1999: 30 f.). Zum letztgenannten Bereich wurden Mitte der 80er und Anfang der 90er-Jahre zwei Bürgergutachten unter der Leitung der Wuppertaler Forschungsstelle ausgearbeitet. Das Bundesministerium für Forschung und Technologie hatte 1986 ein Bürgergutachten über die Regelung der sozialen Folgen der neuen IT in Auftrag gegeben (vgl. Dienel 1987: 3/22 f.), das Bundespostministerium eines zum damals neuen ISDN, das zwischen 1989 und 1991 erstellt wurde (vgl. Dienel 1991: 29 ff). An beiden Bürgergutachten arbeiteten mehrere Planungszellen in verschiedenen Städten parallel, weil man einen Querschnitt bundesdeutscher Städte und Gemeinden erhalten wollte (vgl. Dienel 1987: 119 ff und Dienel 1991: 29 ff/47).[9] Die Planungszellen zur Erstellung des erstgenannten Gutachtens beschäftigten sich unter anderem mit Fragen der Teleheimarbeit, mit dem Einsatz von Robotern in der Produktion, mit den Chancen und Risken neuer IT im Gesundheitswesen, mit Fragen von IT-gestützter Bildungsvermittlung und mit den Anwendungsmöglichkeiten von Bildschirmtext (BTX) im Lebensmitteleinzelhandel. Die Mitwirkenden zeigten sich im Bürgergutachten prinzipiell offen für die neuen Technologien, äußerten aber gleichzeitig Befürchtungen. Angesprochen wurden etwa mögliche negative Auswirkungen für den familiären Bereich und die Gefahren von Arbeitsplatzverlusten, von Isolierung, Überforderung und geistiger Verarmung. Die Einschätzungen der Teilnehmer wurden in 43 so genannte Situationsanzeigen umgesetzt und mündeten in 78 konkrete Regelungsvorschläge ein (vgl. Dienel 1987:

[9] Für das Bürgergutachten Regelung sozialer Folgen neuer Informationstechnologien waren 14 parallel arbeitende Planungszellen mit insgesamt 302 Mitwirkenden in Hannover, Wetzlar und Morsbach an der Sieg tätig (vgl. Dienel 1987: 119 ff). Beim Bürgergutachten ISDN arbeiteten insgesamt 22 Planungszellen in Düsseldorf, Hamburg, Berlin, Frankfurt am Main, München, Saarbrücken, Rottweil und Freiburg. Hier wirkten insgesamt 519 Teilnehmer mit (vgl. Dienel 1991: 29 ff/47).

5/18ff/36). Das Bürgergutachten ISDN wiederum befasste sich einige Jahre später mit Telefonie, Fax, BTX und Temex, einem inzwischen weitgehend in Vergessenheit geratenen Dienst, mit dem Gerätefernsteuerung (Fernwirken) auf breiter Basis betrieben werden sollte. Allgemeine Auffassung zum ISDN (als technischer Basis einer verbesserten Bereitstellung der aufgeführten Dienste) war nach dem Gutachten, dass die Digitalisierung des Teilnehmeranschlusses und die daraus resultierenden erweiterten Kommunikationsmöglichkeiten zunächst vor allem für Geschäftsleute interessant seien, während die Privatnutzung (insbesondere wegen hoher Nutzungsentgelte) erst mit Verzögerung einsetzen werde. Die neuen Optionen in den Bereichen Telefon, Fax und BTX wurden positiv gesehen, nicht jedoch die Bildtelefonie (vgl. Dienel 1991: 7 ff/34 f.). In den weitergehenden Bewertungen hoben die beteiligten Bürger die Bedeutung des Datenschutzes hervor, sodass hier bereits ein zentraler Aspekt von IT-Sicherheit zu einem frühen Zeitpunkt thematisiert wurde. Insbesondere sprachen sie sich gegen die zentrale Speicherung der Verbindungsdaten aus. Konkret schlug sich dies unter anderem in der später faktisch bedeutsam gewordenen Forderung nieder, nur verkürzte Rufnummern für Verbindungsnachweise im Rahmen der Rechnungsstellung der Telekom auszuweisen (vgl. Dienel 1991: 161ff).

4.4.2 Konsensuskonferenzen und Bürgerforen als diskursive Politikberatung

Das Konzept der Konsensuskonferenz hat Ähnlichkeit mit dem der Planungszelle. Der zentrale Unterschied besteht darin, dass die Auswahl der Teilnehmerinnen und Teilnehmer bei der Konsensuskonferenz nicht auf dem Zufallsprinzip beruht. Unter dem Namen Bürgerforum verwendet auch die Akademie für Technikfolgenabschätzung in Baden-Württemberg ein leicht modifiziertes Konzept der Konsensuskonferenz (vgl. Müller/Schnell 1996: 61 ff und Wienhöfer 1996: 57).

Das Konzept der Konsensuskonferenz wurde 1977 erstmals in den USA unter dem Namen *Consensus Development Conference* als Expertendiskurs im medizinischen Sektor praktisch erprobt. In den 80er-Jahren übernahm Dänemark als erster skandinavischer Staat die Methode unter konsequenter Einbeziehung von Laien als allgemeines Mittel zur Technikfolgenabschätzung. Seit 1987 setzt das *Danish Board of Technology* dieses Verfahren ein. Auch Konsensuskonferenzen dienen der politischen Entscheidungsvorbereitung. Ihre Ergebnisse richten sich in Dänemark ausdrücklich an den parlamentarischen Bereich (vgl. Andersen/Jaeger 1999: 331 ff, Gloede/Hennen/Köberle 1997: 18, Guston 1998: 3 ff, Ott/Skopurinski 2000: 56 und Saretzki 1997a: 299 f.).

Konsensuskonferenzen setzen sich aus fünf Komponenten zusammen: einem vor allem mit organisatorischen Aufgaben beschäftigten Projektmanager, dem *Lay Panel*

oder Bürgerpanel, dem Expertenpanel, einem unabhängigen Moderator und dem vom Organisator eingesetzten, bis zu fünf Personen starken Beratungs- bzw. Planungspanel, das auch *Steering Commitee* genannt wird und für die Begleitung und Überwachung der gesamten Veranstaltung zuständig ist. Das Herzstück ist das Laienpanel, eine Gruppe interessierter, aber nicht einschlägig organisierter Bürgerinnen und Bürger. Im dänischen Beispiel ist es 14 bis 16 Mitglieder stark. Mit dieser Gruppe – die Laien sollen grundsätzliches Interesse an ethischen und sozialen Aspekten von Wissenschaft haben, aber kein spezifisches Interesse oder Fachwissen zu dem speziellen Thema – soll die Perspektive der Fachleute ergänzt und eine öffentliche Debatte simuliert werden. Das Panel ist die Bezugsgruppe für die teilnehmenden Fachleute. Die Laien formulieren Fragen an die Experten und wirken auch an deren Auswahl mit. Zudem verfassen sie den 15 bis 30seitigen Abschlussbericht. Dabei geht es weniger um die Generierung neuen Wissens als um die Beurteilung und Gewichtung von Argumenten (vgl. Andersen/Jaeger 1999: 331 f., Guston 1998: 5, Ott/Skopurinski 2000: 57 f., Saretzki 1997a: 300 und Sclove 1996).

Wie oben angesprochen, verzichtet das Konzept der Konsensuskonferenz bei der Teilnehmerzusammensetzung auf eine konsequente Zufallsauswahl. Zwar werden auch im dänischen Beispiel partiell aus Zufallsstichproben der landesweiten Einwohnermelderegister Bürgerinnen und Bürger angeschrieben und zur Teilnahme eingeladen. Die Praxis besteht aber ebenso darin, Anzeigen in lokalen Tageszeitungen zu schalten und zur Mitarbeit aufzurufen. Interessierte werden in beiden Fällen gebeten, einen Brief mit Angaben zur Person und zum Zugang am Thema zurückzusenden. Mit dem Verzicht auf eine reine Zufallsauswahl wird die Hoffnung verbunden, dass die Laien informierter und motivierter in der Konferenz mitwirken (vgl. Andersen/Jaeger 1999: 335, Baron 1995: 207 f., Ott/Skopurinski 2000: 58 f. und Sclove 1996).

Der eigentlichen Konsensuskonferenz, die drei bis vier Tage dauert, gehen zwei Vorbereitungswochenenden mit den Laien voraus, in denen diese in das Thema eingeführt werden, Schlüsselfragen an die Experten formulieren und auch an der Auswahl der Fachleute mitwirken (vgl. Andersen/Jaeger 1999: 331, Ott/Skopurinski 2000: 58 f. und Sclove 1996). Die Konferenz wird dann öffentlich abgehalten. Im ersten Teil der Veranstaltung stehen die Experten Rede und Antwort, auch das Publikum kann Fragen stellen. Die Diskussion offener Fragen – wieder unter Einschluss des Publikums – bestimmt den zentralen zweiten Teil, an dessen Ende das Laienpanel zusammentritt und das Abschlussgutachten formuliert. Die Präsentation des Abschlussgutachtens steht im dritten Teil der Veranstaltung im Mittelpunkt (vgl. Andersen/Jaeger 1999: 331 f., Ott/Skopurinski 2000: 58 f. und Sclove 1996).

Einerseits flexibler und andererseits zielgenauer als Konsensuskonferenzen sind Bürgerforen ausgerichtet, wie man sie in der Vergangenheit an der Akademie für Technikfolgenabschätzung in Baden-Württemberg durchgeführt hat. Zunächst wird auf die Vorbereitungswochenenden für die Laien verzichtet, außerdem obliegt es

dem Durchführungsträger allein, die Fachleute auszuwählen und die Leitfragen der Veranstaltung zu formulieren. Auch kann der zeitliche Ablauf des Bürgerforums entweder als Blockveranstaltung über drei bis vier Tage oder über mehrere Wochenenden hinweg gestaltet werden. Letzteres hat den Vorteil, dass die teilnehmenden Laien ihre gewonnenen Erkenntnisse zwischenzeitlich in ihrem sozialen Umfeld rückkoppeln können (vgl. Müller/Schnell 1996: 61 ff, Ott/Skopurinski 2000: 74 ff und Wienhöfer 1996: 56 ff).

Beide Methoden verfolgen das Ziel, einen herrschaftsfreien Diskurs im Habermas'schen Sinne zu initiieren. Durch die Prozeduralisierung der Kommunikation sollen rationale, über die individuelle lebensweltliche Perspektive hinausgehende und an den gesellschaftlichen Folgen orientierte Entscheidungen getroffen werden (vgl. Andersen/Jaeger 1999: 335 und Wienhöfer 1996: 55 ff). Allerdings wird auch die Legitimität und Repräsentativität dieser Art der Partizipation von Kritikern in Zweifel gezogen. Diese wenden insbesondere ein, dass gerade das Ziel entsprechender Aktivitäten, die Herstellung von Konsens, in vielen Fällen nicht erreichbar sei. Und in der Tat zeugt gerade das dänische Beispiel davon, dass Mehrheits- und Minderheitenvoten immer wieder vorkommen, worauf es dann zumeist dem Durchführungsträger obliegt, den Umgang mit diesen Voten zu bestimmen (vgl. Guston 1998: 5, Müller/Schnell 1996: 65 ff und Wienhöfer 1996: 57f.). Auf der anderen Seite mehren sich aber die Anzeichen dafür, dass Konsensuskonferenzen die Möglichkeit bieten können, der politischen Diskussion neue Impulse zu verschaffen, wenn sie zeitnah an anstehende politische Entscheidungen platziert werden und eine entsprechende Öffentlichkeitsarbeit stattfindet. Dafür spricht auch das dänische Beispiel. Dort werden die Konferenzen im Parlamentsgebäude abgehalten, sodass die Parlamentarier leichten Zugang zur Konferenz haben. Zudem werden die Konferenzen in lokalen Diskussionsveranstaltungen fortgesetzt, sodass deren Ergebnisse auf breiter Basis in den politischen Diskurs einfließen können (vgl. Sclove 1996).

Die Erfahrung zeigt, dass eine offensive Öffentlichkeitsarbeit und die Anbindung der Aktivitäten an eine etablierte Institution, wie sie das *Danish Board of Technology* darstellt, für den Erfolg einer Konsensuskonferenz von zentraler Bedeutung sind. An mangelnder Öffentlichkeitsarbeit machten die Initiatoren des *Citizens Panel on Telecommunications and the Future of Democracy*, das 1997 in den USA als erste Konsensuskonferenz nach dänischem Vorbild durchgeführt wurde, den geringen Widerhall der Konferenzergebnisse in der politischen Diskussion fest. Organisiert worden war die Konferenz, die vom 2. bis 4. April im Rahmen einer größeren Veranstaltung an der Tufts-Universität in Medford bei Boston stattfand, von diversen nichtstaatlichen Einrichtungen, die überwiegend aus dem wissenschaftlichen Bereich stammten (vgl. Guston 1998: 3 ff/32). Diese Konferenz entsprach in ihrer Durchführung weitgehend dem dänischen Vorbild. Die Mitglieder des 15-köpfigen Laienpanels waren einerseits auf der Grundlage einer Zufallsstichprobe der Bevölkerung rund um Boston bestimmt worden, anderseits auf der Basis einer öffentlichen Ausschreibung und

Einladung. Man hatte an öffentlichen Plätzen entsprechende Plakate ausgehängt und Verbände und Multiplikatoren in der Region gezielt angesprochen. Der Konferenz vorgeschaltet wurden zwei Vorbereitungswochenenden, in denen das Laienpanel die Unterthemen der Konferenz festlegte. Nach dessen Vorgabe wurden Fragen eines allgemeinen Zugangs zum Internet, eines IT-unterstützten lebenslangen Lernens sowie der politischen und rechtlichen Beeinflussung von Netzkommunikation auf die Tagesordnung gesetzt. Auf die Auswahl der Experten hatten die Laien indessen keinen Einfluss. Die eigentliche Konferenz war weitgehend öffentlich und bestand aus einer Mischung aus Expertenvorträgen, Nachfragen von Panel und Publikum, allgemeinen Diskussionen sowie Sitzungen des Laienpanels. Eine abschließende Diskussion zwischen Panel und Experten – in Dänemark obligatorisch – fand nicht statt. Dies war auch gar nicht möglich, weil viele Experten am zweiten Tag bereits abgereist waren. Der Abschlussbericht fiel mit vier Seiten recht kurz aus. Die darin enthaltenen Feststellungen, Bewertungen und Empfehlungen hatten einen sehr allgemeinen Charakter, was auch daran lag, dass die Themensetzung zu wenig fokussiert und nicht auf die damals aktuelle politische Agenda abgestimmt gewesen war. Das *Consensus-Statement* forderte, dass der Staat bei der Regulierung der Telekommunikation die Interessen der Bürgerinnen und Bürger stärker beachten solle und nicht einseitig den Marktinteressen den Vorrang geben dürfe. Inhalte und Standards müssten durch die öffentliche Hand, die Wirtschaft und die informierte Öffentlichkeit gemeinsam gestaltet werden (vgl. insb. Citizens Panel on Telecommunication and the Future of Democracy 1997, siehe aber auch Guston 1998: 7 ff/31 ff und Sclove 1997).

4.4.3 Der Runde Tisch und das Mediationsverfahren als Mittel authentischer Entscheidungsbeteiligung

Die Verfechter von Planungszelle und Konsensuskonferenz gehen davon aus, dass eine am Gemeinwohl orientierte Lösung dadurch erzielt werden kann, dass Bürger in Entscheidungsverfahren einbezogen werden, die von deren Ergebnissen nicht unmittelbar betroffen sind. An einem zur raschen Bearbeitung eines neu aufgetretenen Problems eingerichteten Runden Tisch und in den komplexer angelegten Mediationsverfahren wird diese Prämisse in ihr Gegenteil verkehrt. Hier sollen die von einer Entscheidung Betroffenen selbst an der Entscheidungsfindung mitwirken können (vgl. Lackner 1999: 36). Ein weiterer Unterschied liegt darin, dass Runde Tische und Mediationsverfahren regelmäßig konkrete Fragen diskutieren, während die vorgenannten Partizipationsformen schwerpunktmäßig auf einer eher allgemeinen Ebene im Bereich der politischen Willensbildung angesiedelt sind (vgl. Baron 1995: 216 f.). Was den Runden Tisch und das Mediationsverfahren, das hier im Vordergrund ste-

hen soll, voneinander unterscheidet, ist nicht zuletzt, dass das Mediationsverfahren tendenziell einen höheren Aufwand erfordert als die Veranstaltung eines Runden Tisches. Vor diesem Hintergrund ist es durchaus statthaft, das "Mediationsverfahren als das zur Zeit ambitionierteste Instrument einer partizipativen Technikfolgenabschätzung" zu klassifizieren (so Baron 1995: 218).

Mediationsverfahren wurden ab Mitte der 70er-Jahre erstmals in den USA eingesetzt, und zwar zunächst im privat- und arbeitsrechtlichen Rahmen, später auch bei politischen Konflikten (vgl. Fietkau/Pfingsten 1995: 55). In den 80er-Jahren wurden Mediationen erstmals gesetzlich institutionalisiert. Anwendung finden sie insbesondere bei Umweltkonflikten, aber auch im Planungs- und im Familienbereich. In Deutschland wird mit diesem Verfahren seit über 20 Jahren experimentiert (vgl. Fietkau/Pfingsten 1995: 55 ff, Lackner 1999: 9 f. und Saretzki 1997b: 31 ff).

Mediation wird in Konfliktfällen angewandt, in denen Konfliktparteien existieren und in denen die Chance besteht, zwischen den widerstreitenden Standpunkten eine Annäherung herbeizuführen. Mit dem Mediator wird ein neutraler Dritter eingeschaltet, der versuchen soll, einen Konsens oder Kompromiss auszuhandeln, dem alle Parteien zustimmen können. Aufgabe des Mediators ist es, die Verhandlungen zu organisieren, die Diskussion zu leiten und für einen Verhandlungsablauf zu sorgen, in dem alle Mitwirkenden die Chance zur Einbringung ihrer Position haben (vgl. Bechmann 1997: 153, Gloede/Hennen/Koeberle 1997: 15 f. und Roth 1997: 434).

Mittels Mediation nicht verhandelbar sind wertbeladene Großkonflikte wie etwa Fragen der friedlichen Nutzung der Kernenergie und Fragen, auf die Konfliktparteien nur mit Ja-Nein-Optionen reagieren können. Mediationen finden in der Regel unter Ausschluss der Öffentlichkeit statt, um eine vertrauliche Verhandlungsatmosphäre zu gewährleisten und die Beteiligten nicht dem Druck auszusetzen, sich für ihr Agieren im Verfahren gegenüber ihren Anhängern oder der Öffentlichkeit rechtfertigen zu müssen (vgl. Lackner 1999: 11 ff). Mediationen sind stärker als andere Verfahren an geographisch begrenzte Räume gebunden, denn zu ihrer Einleitung bedarf es einer überschaubaren Akteurskonstellation und eines identifizierbaren (konkreten) Interessenkonfliktes. Für einen überregionalen oder übernationalen Einsatz erscheinen sie weniger geeignet. Wichtig ist hier auch, dass die zu behandelnden Probleme nicht allzu komplex sind, sodass sie von den Beteiligten noch reflektiert werden können.

Problematisch an Mediationsverfahren ist die trotz aller Vorkehrungen nicht immer beherrschbare Tendenz der Bevorzugung von Interessen mit einem hohen Organisationsgrad. Diese besteht schon deshalb, weil zur Mitwirkung neben zeitlichen Ressourcen auch ein hohes Maß an Artikulations-, Kommunikations- und Konfliktfähigkeit gefordert ist, über das andere Beteiligte oft nicht in dem erforderlichen Ausmaß verfügen (vgl. Baron 216 f., Fietkau/Pfingsten 1995: 57 ff, Gloede/Hennen/Koeberle

1997: 15, Lackner 1999: 21 f. und Tils 1997: 46 ff). Bis heute finden sich keine Beispiele für Mediationsverfahren im IT-Bereich.[10]

4.4.4 Die Zukunftskonferenz als Triebkraft kreativer Erneuerung

Bis in die 60er-Jahre zurück reicht die Geschichte der Zukunftskonferenz, die in den USA als *Future Search Conference* zunächst im Bereich der Organisationsentwicklung angewendet wurde. Von diesem Instrument erwarten seine Befürworter kreative Energieschübe, die einen entscheidenden Beitrag zum Wandel in Organisationen und Institutionen leisten sollen (vgl. Burow 2000: 167 ff und Weisbord/Janoff 1995).
Das Konzept der Zukunftskonferenz ähnelt dem der auch in Deutschland eingesetzten Zukunftswerkstatt. Die Zukunftskonferenz unterscheidet sich von der Zukunftswerkstatt aber dadurch, dass der Teilnehmerkreis über "Gleichgesinnte" hinaus erweitert wird, und dadurch, dass die einzelnen Arbeitsphasen, die bei der Zukunftswerkstatt aus Kritikphase, Kreativitätsphase und Realisierungsphase bestehen, ausgeweitet und ergänzt werden (vgl. Burow 2000: 171 f./183 f.). An einer Zukunftskonferenz nehmen bis zu 64 Personen teil, die in Achtergruppen verteilt im Hinblick auf verschiedene Aspekte Zukunftsvisionen zu entwerfen suchen. Diese Personen sind in Zusammenarbeit mit zwei Moderatoren und einer aus Teilnehmern bestehenden Steuerungsgruppe "so ausgewählt worden, dass sie möglichst weitgehend das ganze System repräsentieren" (so Burow 2000: 172).
Die Dauer einer solchen Konferenz beträgt fast immer 15 bis 20 Arbeitsstunden, die in vier bis fünf Halbtagseinheiten abgeleistet werden. Der Teilnehmerkreis soll möglichst aus allen Gruppen zusammengesetzt sein, die für die behandelte Problemstellung relevant sind, und die Teilnehmer sollen den Konferenzprozess so weit wie möglich selbst gestalten. Abgesehen davon, dass sie die Aufgabenstellung formulieren, leisten weder die Moderatoren noch die Angehörigen der Steuerungsgruppe in-

[10] In Deutschland hatten die meisten Mediationen relativ konkrete Umwelt- und Planungskonflikte zum Thema. Zum Beispiel wurde 1997 beim Konflikt um die Überdeckelung der vierten Elbtunnelröhre eine so genannte *Data-Mediation* durchgeführt. Ausgangslage des Konfliktes war, dass eine Bürgerinitiative sich für die Überdeckelung einsetzte, um die Lärmbelästigung für die Anwohner zu reduzieren, die zuständige Verwaltung dies aber wegen zu hoher Kosten ablehnte. Hatte die Bürgerinitiative Kosten von 110 Millionen Mark errechnet, so war die Verwaltung in ihren Berechnungen auf 395,5 Millionen Mark gekommen. Nachdem Gespräche zwischen Verwaltung und Bürgerinitiative keine Ergebnisse erbracht hatten, stimmte die Verwaltung einer Mediation zur Kostenermittlung zu, die erfolgreich abgeschlossen werden konnte. Man einigte sich auf eine Bezifferung der Kosten in einer Spanne zwischen 189 und 207 Millionen Mark. Auf diese Weise konnte die Datenlage verbessert und die Diskussion versachlicht werden (vgl. Holznagel/Ramsauer 1997: 65 ff).

haltliche Vorarbeit (vgl. Bonsen 1998, Burow 2000: 172 ff und Weisbord/Janoff 1995). Die eigentliche Konferenz durchläuft fünf Phasen bis zum Ergebnis. Zunächst werden die Entwicklungen im behandelten Themenbereich auf einer Zeitachse aufgezeichnet, daran anschließend werden allgemeine Trends erörtert. Der dritte Schritt besteht darin, die Teilnehmenden die Situation in ihren positiven und negativen Aspekten aus der individuellen Perspektive bewerten zu lassen, bevor dann persönliche Visionen entwickelt werden. Aus den Ergebnissen der ersten vier Phasen werden im letzten Schritt dann die Gemeinsamkeiten herausgearbeitet und in einen konkreten Aktionsplan transformiert (vgl. Burow 2000: 173 ff und Weisbord/Janoff 1995).
Zukunftskonferenzen sind schon seit geraumer Zeit nicht mehr auf Wirtschaftsunternehmen und das Feld der Organisationsentwicklung beschränkt. Sie haben auch im TA-Bereich bereits vermehrt Anwendung gefunden und dort einen Beitrag dazu geleistet, Interessenkonflikte zum Ausgleich zu bringen. Dabei scheint es mit Hilfe von Zukunftskonferenzen möglich zu sein, Themenstellungen von hoher Komplexität zu bearbeiten.[11]

4.4.5 Der Szenarioworkshop als Ansatz, um Wissen durch Vernetzung produktiv zu machen

Die Methode des Szenarioworkshops bedient sich eines Prognoseinstrumentes, das aus der Unternehmensentwicklungsplanung und der Raumplanung stammt. Mit der so genannten Szenariotechnik, die für die Einbindung partizipativer Komponenten offen ist, soll vernetztes Denken gefördert werden, um Probleme, die aus immer dynamischer werdenden soziotechnischen Entwicklungen erwachsen, einer möglichst umfassenden Bearbeitung zuzuführen (dies und das Folgende nach Fink/Gausemeier/Schlake 1997, insb. 203 ff). Man kann fünf verschiedene Schritte

[11] So wurde im März 1998 unter der Ägide des *Danish Board of Technology* eine Zukunftskonferenz in Kopenhagen durchgeführt, die sich mit der Verkehrssituation der Stadt befasste. Der Hintergrund: Innerhalb eines Jahrzehntes hatte der Verkehr in der dänischen Hauptstadt stark zugenommen, und die Verkehrsinfrastruktur war an vielen unterschiedlichen Stellen immer weiter ausgebaut worden. Parallel dazu hatten sich die Umweltprobleme Kopenhagens drastisch vermehrt. Die Diskussion dieses Themas durch die verschiedenen Interessengruppen steckte in einer Sackgasse. Die Zukunftskonferenz hatte die Aufgabe, diese Gruppen an einen Tisch zu bringen, die Probleme einer kontroversen Diskussion zuzuführen und die Herausarbeitung eines gemeinsamen Nenners zu ermöglichen. Ein Ergebnis bestand in der Feststellung, dass es Kopenhagen an einer Koordinierungsinstanz für die entsprechenden Aktivitäten mangelt. Auf diesen Impuls hat die dänische Regierung inzwischen reagiert und das *Development Council of Copenhagen* ins Leben gerufen, das unter anderem die Verkehrsplanung der Stadt koordinieren soll (vgl. EUROPTA 2000: 52).

des Szenariomanagements unterscheiden: Szenariovorbereitung, Szenariofeldanalyse, Szenarioprognostik, Szenariobildung und Szenariotransfer. Bei den ersten beiden Schritten geht es im Wesentlichen um die Identifizierung des zu bearbeitenden Problemfeldes und der wichtigsten Einflussfaktoren, die für Gestaltungseinflüsse zugänglich sind. Die Phase der Prognostik führt dann zur Ermittlung möglicher Zukunftsprojektionen, aus denen diejenigen, welche begründbar relevant erscheinen, zur weiteren Bearbeitung ausgewählt werden. Die Szenariobildung stellt eine Phase der Kommentierung und Bewertung der vorgelegten Projektionen dar, aus denen dann unter Berücksichtigung der wichtigsten Schlüsselfaktoren plausibel erscheinende Szenarien abgeleitet werden. Im abschließenden Szenariotransfer werden die erarbeiteten Möglichkeiten in konkrete Strategien, Handlungsempfehlungen und Maßnahmen übersetzt.

Die Konzeption von Szenarioworkshops unterscheidet sich in einem wesentlichen Punkt von den in den vorausgegangenen Kapiteln dargestellten Verfahren. Stellten diese zumeist die Bürgerbeteiligung in den Vordergrund, so bilden die Bürgerinnen und Bürger im Szenarioworkshop lediglich eine von vier Gruppen, die gleichberechtigt am Prozess teilhaben können. Daneben wirken politische Entscheidungsträger, Vertreter der Wirtschaft und Experten mit. Nicht die Herauskristallisierung des Willens einer informierten Öffentlichkeit ist das Ziel des Szenarioworkshops, sondern die Synthese verschiedener Gruppenmeinungen. (vgl. Andersen/Jaeger 1999: 332 ff).

Szenarioworkshops sind vielseitig einsetzbar. Wie das Mediationsverfahren sind sie zur Bearbeitung konkreter Problemstellungen und Konfliktlagen geeignet. Die Verankerung von Partizipationselementen in den Workshops ist in unterschiedlicher Intensität möglich (vgl. Andersen/Jaeger 1999: 332 ff). Dass ein Szenarioworkshop zur Bearbeitung technischer, regulatorischer und organisationeller Fragen genutzt werden kann, beweist unter anderem der Einsatz dieses Instruments im Rahmen der Studie *Women and the Net* des STOA. Im Juli 1997 fand dieser Workshop in Innsbruck statt. Durchgeführt wurde die Studie vom Bonner Forum Informatiker und Informatikerinnen für Frieden und gesellschaftliche Verantwortung (FIFF) mit (methodischer) Unterstützung der englischen Organisation *European Awareness Scenario Workshops*, die im Innovationsprogramm der Europäischen Kommission verankert ist. Im Innsbrucker Workshop ging es darum, wie der bis dato noch geringe Anteil von Internetnutzerinnen gesteigert werden könnte, wie sich das Internet auf soziale Beziehungen auswirkt, und welche Folgen das Internet für die Arbeitssituation von Frauen hat (vgl. EASW 1998).

4.4.6 Elektronische Kommunikation in Partizipationsprozessen als Königsweg?

Partizipation in TA-Prozessen wurde in der Vergangenheit immer wieder durch Organisations-, Informations- und Kommunikationsprobleme erschwert (dies und das Folgende nach Riehm 2000). Seit Mitte der neunziger Jahre besteht die Möglichkeit, PTA-Prozesse durchzuführen, die sich der Potenziale des Internet bedienen. Das Wissenschaftszentrum Berlin hat schon 1994 mit dem Netzforum[12] ein solches Experiment gestartet. Die Akademie für Technikfolgenabschätzung in Baden-Württemberg begann einige Jahre später, nämlich im Oktober 1997, das Projekt Elektronische Zahlungsmittel (PEZ), in dem mit einem auf elektronische Kommunikation gestützten Partizipationsmodell experimentiert wurde. Die Verantwortlichen selbst ordnen dieses Modell ein als in der "Nähe partizipativer und diskursiver TA-Elemente" liegend (so Böhle/Riem 1999: 1, siehe auch Riehm 2000: 61).
Das Projekt PEZ, welches hier exemplarisch näher betrachtet werden soll, hatte zum Ziel, problemorientierte Sachstandsanalysen zu zwei Bereichen zu erarbeiten. Erkundet werden sollte erstens der Handel mit digitalen Produkten, Dienstleistungen und Anrechten und zweitens das Problemfeld der elektronischen Zahlungssysteme (dies und das Folgende nach Böhle/Riehm 1998/1999). Das Ziel des Projektes bestand in der ersten Phase nur darin, eine geeignete Informationsbasis zu schaffen und nicht darin, Partizipationsmöglichkeiten zu eröffnen und bestehende Konflikte zu lösen. Es wurden Expertengespräche geführt und ausführliche Internetrecherchen unternommen, um das Forschungsfeld auszuleuchten. Im zweiten Teil des Verfahrens kamen dann die partizipationsspezifischen Möglichkeiten des Internet zum Einsatz. Im *World Wide Web* wurde eine Homepage[13] eingerichtet, die den aktuellen Stand des Projektes widerspiegelte. Projektbegleitend kam es zur Einrichtung der E-Mail-Liste EZI-L. Mit EZI-L sollte versucht werden, Interessierte stärker am TA-Prozess zu beteiligen, ungeklärte Sachverhalte aufzuarbeiten, Konflikte aufzudecken, die im Projekt gewonnenen Erkenntnisse kontinuierlich und nicht erst mit dem Abschlussbericht zu verbreiten sowie eine breite öffentliche Diskussion über die Ergebnisse herbeizuführen. Zentrales Element der Liste war ein *Newsletter* namens EZI-N, der zwischen Oktober 1997 und September 1998 in 20 Ausgaben an die Teilnehmer versendet wurde. Er enthielt Neuigkeiten aus dem Projekt und Informationen rund um neuartige Zahlungssysteme im Internet. Mit diesem Mittel sollte eine Art "elektronische Öffentlichkeit" (so Riehm 2000: 65) geschaffen und zwischen Laien und Experten vermittelt werden (vgl. Böhle/Riehm 1999: 4 f. und Riehm 2000: 62 ff). Die Teilnahme an der Liste stand grundsätzlich jedem offen. Spezielle Mitwirkungs-

[12] Dieses Forum existiert immer noch unter folgender URL: http://duplox.wz-berlin.de/netzforum.

[13] Die URL: http://www.itas.fzk.de/deu/projekt/pez.htm.

einladungen erfolgten über Benachrichtigungen in vier E-Mail-Listen mit verwandten Schwerpunkten sowie durch einen Verteiler von etwa 60 Adressen von Experten. Auch die erste Ausgabe des *Newsletters* vom 17. Oktober 1997 wurde über diesen Verteiler verbreitet. Während der Zeit, in der der *Newsletter* versandt wurde, hatten sich insgesamt 1219 Teilnehmer mit E-Mail-Adressen angemeldet. Allerdings war die Fluktuationsrate recht hoch (vgl. Böhle/Riehm 1999: 5 ff/22 sowie Riehm 2000: 62 f.).

Gerade im Hinblick auf die Auseinandersetzung mit Fragen der neuen IT eignet sich Internetkommunikation dazu, eine Fachöffentlichkeit zu erreichen und zur Teilnahme zu motivieren. Hier scheint es in zunehmendem Maße zu gelingen, Interessierte miteinander zu vernetzen und zu intensiven Diskussionsprozessen zu animieren. Auch gewinnen TA-Projekte auf diesem Wege an Flexibilität, weil etwa durch eine E-Mail-Liste während des Projektes Zwischenergebnisse schnell vermittelt und in die Diskussion eingespeist werden können. Als in einer E-Mail-Liste diskutabel erscheinen nach den an der Akademie für Technikfolgenabschätzung in Baden Württemberg gesammelten Erfahrungen hauptsächlich sachorientierte Themen von mittlerer oder geringerer Komplexität (vgl. Böhle/Riem 1999: 22 ff und Riehm 2000: 64 f.). Was die mittels Internetkommunikation behandelten Sachgebiete betrifft, stießen unter anderem Fragen der Anonymität von Kommunikationsakten, der Authentifizierung gesendeter und empfangener Daten sowie der Ausgestaltung und Anwendung elektronischer Zahlungssysteme und damit auch zentrale Fragen aus dem Bereich der IT-Sicherheit auf große Resonanz (vgl. Böhle/Riem 1999: 11 ff).

Nur auf den ersten Blick beachtlich erscheinen die hohen Teilnehmerzahlen von EZI-L. Die Anmeldung in der Liste bedeutete nämlich noch nicht, dass auch eine intensive Teilnahme an der Diskussion erfolgte. Denn eine nachträgliche Analyse der E-Mail-Diskussion ergab, dass nur 19 Prozent der Teilnehmer sich aktiv an der Diskussion beteiligt hatten. Allein ein Viertel aller Beiträge war von nur vier Personen verfasst worden (vgl. Böhle/Riehm 1999: 5 ff/22, Riehm 2000: 62 f.).

5 Komponenten von PTA und Probleme der IT-Sicherheit – eine erste Zusammensicht

Wie in den Kapiteln zur IT-Sicherheit ausgeführt, ist deren erfolgreiche Förderung im Sinne mehrseitiger Sicherheit vor allem an drei Voraussetzungen gebunden:

- (1) Gewährleistung eines möglichst hohen Maßes an Verfügbarkeit, Integrität, Verbindlichkeit und Vertraulichkeit von Informationen und Kommunikationsbeziehungen (unter Berücksichtigung des Umstands, das IT-Sicherheit ein knappes Gut und ein dynamisches Phänomen darstellt, und insbesondere der Tatsache, dass IT-Sicherheit für unterschiedliche Seiten Unterschiedliches be-

deuten kann) durch die Ermöglichung geeigneter Sicherheitsprozesse auf der Basis von Sicherheitsmanagement und Sicherheitskultur

- (2) Verankerung der faktisch hohen Zuverlässigkeit der technischen Systeme in den vier aufgeführten Dimensionen im Bewusstsein der Gesellschaftsmitglieder im Sinne der Erzeugung von Vertrauen, das unter anderem durch die gesellschaftliche bzw. die institutionelle Einbindung der Technik gestärkt werden kann
- (3) Herstellung von Akzeptanz für Entscheidungen, die regelmäßig auf Kompromissen und Kompensationen basieren und daher aus der individuellen Perspektive als suboptimal empfunden werden müssen, wobei unterstellt werden kann, dass Beteiligung ein Mittel darstellt, um eine solche Haltung zu fördern.

Weil alle aufgeführten Partizipationsverfahren prinzipiell geeignet erscheinen, die Sicherheitsvorstellungen unterschiedlicher Seiten zum Abgleich zu bringen, die Herausbildung von Vertrauen in die Verfügbarkeit, Integrität, Verbindlichkeit und Vertraulichkeit von Informationen und Kommunikationsbeziehungen (insbesondere im Falle ihrer institutionellen Verankerung) zu fördern, und den von Entscheidungen über IT-Sicherheit Betroffenen das Gefühl zu vermitteln, dass ihre Interessen in die Entscheidungsprozesse eingeflossen sind, ist ihre Einführung zur Umsetzung des Leitbilds der mehrseitigen Sicherheit in ihrer gesamten Breite denkbar.

Damit ist aber natürlich noch nichts darüber gesagt, welche Partizipationsverfahren sich zur Bearbeitung welcher IT-Sicherheitsprobleme anbieten, und wie groß deren Beitrag zur Schaffung der auf diesem Feld erforderlichen Konfliktbearbeitungsstrukturen und –kulturen tatsächlich sein kann. Die Auseinandersetzung mit diesen zentralen Fragen stellt eine Herausforderung dar, der sich die Sozialwissenschaften nach Jahren einer kaum nachvollziehbaren Zurückhaltung endlich in vollem Umfang stellen sollten.

Die in den folgenden Kapiteln zu diesem Thema angestellten Überlegungen zielen darauf ab, dem erforderlichen fachwissenschaftlichen Diskurs und der Durchführung geeigneter Pilotprojekte Vorschub zu leisten. Um Missverständnissen vorzubeugen, sei an dieser Stelle noch einmal unterstrichen, dass die entsprechenden Thesen nicht mit dem Anspruch verbunden werden, Antworten zu geben, sondern lediglich mit der Absicht, Denkanstöße zu vermitteln und einen Beitrag zur Entwicklung adäquater Fragestellungen zu leisten. Im besten Falle könnten sie sich darüber hinaus geeignet erweisen, einige Anhaltspunkte für sinnvolle weiterführende Aktivitäten zu markieren.

5.1 Die Erstellung von Bürgergutachten in Planungszellen und das Leitbild der mehrseitigen Sicherheit

Schon weil es sich dabei um ein außerordentlich teures Verfahren handelt, ist die Erstellung von Bürgergutachten in Planungszellen zur Förderung des Leitbilds der mehrseitigen IT-Sicherheit nur in einem sehr begrenzten Ausmaß möglich. Sie bietet sich dort an, wo Fragen von grundlegender Bedeutung zur Entscheidung anstehen, also etwa die Frage, wie sich eine IT-sicherheitsspezifische Grundausstattung für alle Teilnehmer der Netzkommunikation darstellen sollte. Hoffnungsvoll stimmt hier der Umstand, dass das Planungszellenverfahren im Bereich der IT-Gestaltung in der Vergangenheit mit durchaus akzeptablen Ergebnissen erprobt worden ist, und dies auch unter Einbeziehung von Teilaspekten der IT-Sicherheit. Die dabei aufgetretenen Schwierigkeiten und insbesondere die Umsetzungsdefizite, die natürlich nicht übersehen werden dürfen, resultierten weniger aus den Eigenarten des Verfahrens als aus der fehlenden Einbindung der Projekte in die Strukturen des politisch-administrativen Systems und aus der bewusst gewählten Konkurrenz zur dominierenden korporatistischen Entscheidungsfindung. Was das Planungszellenverfahren unter dem Gesichtspunkt der Förderung mehrseitiger IT-Sicherheit darüber hinaus attraktiv macht, ist der Umstand, dass es – wenn man der Einschätzung von Lars Holtkamp folgen will – als "einziges von allen punktuellen dialogorientierten Verfahren relativ repräsentativ" arbeitet (so Holtkamp 2000: 98), oder – um es bescheidener zu formulieren – dass es den Anspruch einer ausgewogenen Interessenartikulation zumindest mit einem gewissen Maß an Plausibilität erheben kann. Alles in allem erscheint es sinnvoll, die Möglichkeiten, welche das Planungszellenverfahren zur Klärung von grundlegenden Fragen im Bereich der mehrseitigen IT-Sicherheit bietet, durch weiterführende Forschungen und die Sammlung praktischer Erfahrungen genauer auszuloten.

5.2 Die Konsensuskonferenz und das Leitbild der mehrseitigen Sicherheit

Den Anspruch, repräsentative Ergebnisse zu produzieren, kann man für die Konsensuskonferenz, die wegen ihrer spezifischen Anlage und Ausrichtung ebenfalls geeignet erscheint, bei Grundsatzkonflikten im Bereich der IT-Sicherheit sinnvolle Beiträge zu leisten, nicht erheben. Daher dürfen die Gefahren, die aus sozialen Asymmetrien erwachsen können, auch hier nicht vernachlässigt werden. Auf der anderen Seite weist die Konsensuskonferenz gegenüber dem Planungszellenverfahren aber den zentralen Vorteil auf, dass sie leichter in die gegebenen repräsentativen und korporatistischen Strukturen eingepasst werden kann und zudem darauf angelegt ist, die Öf-

fentlichkeit für neu auftretende Probleme zu sensibilisieren. Weil viele Fragen der IT-Sicherheit mit dem Übergang der modernen Gesellschaft in das Stadium der digitalen Informationsgesellschaft für breite Schichten der Bevölkerung zentrale Bedeutung gewinnen werden, ist auch der letztgenannte Aspekt hier von großer Bedeutung. Positiv hervorzuheben ist zudem die Tatsache, dass man (insbesondere in Dänemark) durchaus gute Erfahrungen mit diesem Instrument der Technikfolgenabschätzung und Technikbewertung gesammelt hat. Der Umstand, dass sich bei der Konsensuskonferenz durch den Verzicht auf eine durchgängige Zufallsauswahl eine qualifiziertere und engagiertere Mitwirkung der Laien erreichen lässt, kann im Bereich der IT-Sicherheit besonders zu Buche schlagen, weil es hier bereits heute breite und dynamische zivilgesellschaftliche Aktivitäten gibt, die sich vielleicht in diese Richtung kanalisieren lassen. Was für die Erstellung von Bürgergutachten in Planungszellenverfahren gilt, gilt daher auch für die Konsensuskonferenz: Dieses Verfahren sollte im Hinblick auf seine Potenziale zur Umsetzung des Leitbilds der mehrseitigen IT-Sicherheit näher erforscht und erprobt werden.

5.3 Der Runde Tisch, das Mediationsverfahren und das Leitbild der mehrseitigen Sicherheit

Weil er ohne größeren Vorlauf und ohne besonderen Aufwand mit unmittelbarem Problembezug eingerichtet werden kann, erscheint der Runde Tisch dort als Konfliktlösungsinstrument geeignet, wo es darum geht, kurzfristig auftretende Fragen aus dem Bereich der IT-Sicherheit ohne zeitlichen Verzug zu behandeln. Voraussetzung einer erfolgreichen Problembearbeitung ist dabei allerdings, dass die relevanten Interessen jeweils durch eine handlungsfähige Vertretung abgedeckt sind, was den Anwendungsradius dieses Instruments nicht unerheblich einschränkt. Die Einrichtung eines Runden Tisches könnte aber dort vorteilhaft sein, wo die IT-Systeme einer in ihren internen Machtverhältnissen relativ symmetrisch strukturierten Organisation (beispielsweise in einer Behörde oder in einem größeren Unternehmen) weiterentwickelt werden sollen, um eine als bedrohlich empfundene Sicherheitslücke in einer für alle Seiten akzeptablen Weise zu schließen.

In Fällen, in denen sich die am Runden Tisch behandelten Probleme als besonders hartnäckig oder weitreichend entpuppen, kann sich die Frage stellen, ob ein weniger komplexes Rundtischverfahren in ein komplexeres Mediationsverfahren mit größerer Problembearbeitungskapazität überführt werden sollte. Allerdings legt schon der Befund, dass sich bis heute kein Beispiel für Mediationsverfahren im IT-Bereich findet, den Schluss nahe, dass die Möglichkeiten dieses Instruments zur Bearbeitung von Problemen der IT-Sicherheit eher eng begrenzt sind. Wie die Einrichtung eines Runden Tisches könnte sein Einsatz in diesem Bereich schon deshalb mit Schwierig-

keiten verbunden sein, weil zumindest in Einzelfällen die Gefahr besteht, dass eher unbedarfte Nutzer auf professionelle und damit weit überlegene Verhandlungspartner aus IT-Abteilungen oder der IT-Wirtschaft treffen, ohne dass dies durch eine Fremdorganisation von Interessen ausgeglichen wird. Als bedenklich muss hier zudem der Umstand angesehen werden, dass Mediationen erst dann stattfinden, wenn Konflikte bereits ausgebrochen sind. Im Bereich der IT-Sicherheit sollte man sich nämlich möglichst frühzeitig um den Ausgleich divergierender Interessen bemühen, weil sich Konflikte hier oft an den Ergebnissen von Entscheidungen über die Ausgestaltung von Software entzünden, welche nur schwer rückholbar sind. Und schließlich kommt hier noch ein weiterer Aspekt erschwerend hinzu: Nicht nur der Umstand, dass Mediationsverfahren die Gefahr bergen, dass Kompromisse zum Nachteil von nicht am Verfahren beteiligten Dritten geschlossen werden, sondern auch die Tatsache, dass Mediationsverfahren mit der Anforderung einer transparenten Entscheidungsfindung häufig nicht vereinbar sind, kann sich bei der Bearbeitung von Problemen der IT-Sicherheit negativ auswirken. Denn neben einer symmetrischen Interessenartikulation ist auch ein Mindestmaß an Transparenz für die Umsetzung des Leitbilds der mehrseitigen Sicherheit eine zentrale Voraussetzungen.
Vor diesem Hintergrund spricht vieles dafür, dass hier lediglich der Runde Tisch in seiner einfachen Variante, nicht aber das komplexere Mediationsverfahren zum Gegenstand weiterführender Analysen und Projekte erhoben werden sollte.

5.4 Die Zukunftskonferenz, der Szenarioworkshop und das Leitbild der mehrseitigen Sicherheit

Zukunftskonferenzen richten sich auf noch zu entwickelnde Sachbereiche und können daher natürlich auch für eine antizipative Auseinandersetzung mit Fragen der IT-Sicherheit produktiv gemacht werden. Nichts anderes gilt im Hinblick auf Szenarioworkshops. Eine antizipative Auseinandersetzung mit Fragen der IT-Sicherheit ist schon deshalb sinnvoll, weil in diesem Bereich oft in sehr dynamischen Wandlungsprozessen Fakten geschaffen werden, die sich später kaum noch korrigieren lassen. Ein möglicher Gegenstand einer Zukunftskonferenz oder eines Szenarioworkshops wäre die Ermittlung der Anforderungen, die an multifunktionale *Smartcards* zu stellen sind, welche für die unterschiedlichsten Bereiche vom Gesundheitswesen über die Abwicklung von Behördenkontakten bis hin zum Bankwesen Funktionen der Informationsspeicherung, des Vertraulichkeitsschutzes und der authentischen Kommunikation in integrierter Form bereitstellen können.
Was den Szenarioworkshop in diesem Zusammenhang besonders interessant erscheinen lässt, ist neben seinen vielfältigen Einsatzmöglichkeiten der Umstand, dass man hier im Unterschied zu den meisten anderen Partizipationsverfahren darauf ver-

zichtet, die Bürgerbeteiligung exklusiv in den Vordergrund zu rücken, und stattdessen eine gleichwertige und systematische Einbeziehung von weiteren Akteuren aus Politik, Wirtschaft und Wissenschaft vorsieht. Dies korrespondiert mit den Anforderungen an die Herstellung von IT-Sicherheit gleich in zweifacher Hinsicht: Erstens hat sich in der Vergangenheit gezeigt, dass zur Herausarbeitung mehrseitig akzeptabler IT-Sicherheitslösungen häufig Interessenausgleichsprozesse zwischen Anwendern und Akteuren aus der Wirtschaft (wie Herstellern von Hard- und Software, Netzbetreibern, *Serviceprovidern* und *Contentprovidern*) erforderlich sind, die wiederum oft erst nach Intervention der Politik und mit Unterstützung der Wissenschaft möglich werden. Zweitens zeichnen sich realistische Ansätze zur Bewältigung oder Eindämmung der neuen Sicherheitsgefahren regelmäßig dadurch aus, dass sie nicht auf das Agieren einzelner Institutionen oder Akteure setzen, sondern auf eine konzertierte Problembearbeitung im Dreieck von Macht, Markt und Gesellschaft.
In der Gesamtsicht erscheint es naheliegend, auch die Zukunftskonferenz und den Szenarioworkshop als Mittel zur Förderung von mehrseitiger IT-Sicherheit in den Blick zu nehmen. Angesichts seiner spezifischen Anlage, die den Belangen der IT-Sicherheit in besonderem Maße entgegenkommt, führt wohl kaum ein Weg an der Schlussfolgerung vorbei, dass dem Szenarioworkshop dabei nicht nur größere Aufmerksamkeit als der Zukunftskonferenz, sondern auch als dem Planungszellenverfahren, der Konsensuskonferenz und dem Rundtischverfahren gewidmet werden sollte.

5.5 Elektronische Kommunikation in Partizipationsprozessen und das Leitbild der mehrseitigen Sicherheit

Digitaltechnisch gestützte Formen der Kommunikation und Kooperation werden zur Behandlung von Fragen der IT-Sicherheit bereits seit geraumer Zeit praktiziert, und vieles spricht dafür, dass derartige Aktivitäten noch deutlich zunehmen werden. Auf den ersten Blick erscheint dieser Befund geeignet, hinsichtlich der Umsetzung des Leitbilds der mehrseitigen IT-Sicherheit geradezu Euphorie auszulösen. Bei näherer Betrachtung der entsprechenden Diskurse stellt sich aber eine gewisse Ernüchterung ein. Dies ist nicht nur darin begründet, dass in den einzelnen Foren oft bestimmte Teilnehmer dominieren und andere nur eine marginale Rolle spielen, sondern auch darauf zurückzuführen, dass die entsprechenden Gruppen weitgehend exklusiv zusammengesetzt sind, und darauf, dass innerhalb der Gruppen autopoetische Tendenzen anzutreffen sind. Einerseits ist nämlich davon auszugehen, dass der weitaus überwiegende Teil derjenigen, für die Fragen der Verfügbarkeit, Integrität, Authenzität und Vertraulichkeit von Informationen und Kommunikationsbeziehungen zunehmend an Bedeutung gewinnt, überhaupt keinen Zugang zu den entsprechenden Diskursen finden. Dies gilt nicht nur im Hinblick auf breite Schichten der Anwender in

den Haushalten (vgl. Kubicek 1999: 332 ff, Leggewie 1998: 40 und Zwingenberger 1998: 227 ff), sondern auch auf Millionen von kleinen und mittleren Unternehmen, die „sukzessive und für sie selbst oft nicht einmal unmittelbar erkennbar" in den Sog einer Digitalisierung geraten, der für sie „durchaus ernstzunehmende Sicherheitsprobleme" aufwerfen kann (so Winkel/Andersen/Hecht/Tackenberg 2002: 26, siehe auch Fuchs 2000). Und andererseits ist davon auszugehen, dass diejenigen, die in entsprechenden Kontexten im Netz präsent sind, sich oft weniger an den Diskussionen beteiligen, um die Meinungen anderer kennen zu lernen als mit dem Bedürfnis, Gleichgesinnte zu finden und bereits gefasste Urteile bestätigen zu lassen (vgl. Holtz-Bacha 1997: 13 ff/1998: 219 ff und Leggewie 1998: 19). Nicht selten hat man es hier mit Gruppen zu tun, die in wesentlichen Prämissen übereinstimmen und sich deren Gültigkeit wechselseitig versichern. So gibt es Foren, in denen Erfordernisse des Datenschutzes und des Fernmeldegeheimnisses den Diskurs dominieren, und Foren, in denen Anforderungen des Schutzes kritischer Infrastrukturen in den Vordergrund gerückt werden. An Foren, welche die Möglichkeit bieten, die in vielerlei Hinsicht widerstreitenden Ziele dieser beiden für sich selbst jeweils legitimen Bestrebungen einem rationalen Abgleich zuzuführen, und auf die es im Sinne der Förderung von Prozessen zur Realisierung des Leitbilds der mehrseitigen Sicherheit eigentlich ankäme, herrscht aber nach wie vor Mangel.
Trotz der geschilderten Einschränkungen steht in Anbetracht der Leistungsmerkmale und der Kostenvorteile der Netzkommunikation aber wohl außer Zweifel, dass die IT-Potenziale zur Förderung des Leitbilds der mehrseitigen IT-Sicherheit immens sind, wenn es gelingt, Einrichtungen bzw. Mechanismen zu etablieren, die thematisch und sozial adäquate Beteiligungsstrukturen und Abläufe gewährleisten können. Vieles spricht daher dafür, neben dem Szenarioworkshop als besonders interessantem Typus einer Präsenzveranstaltung die IT-gestützte Partizipation in den Mittelpunkt der theoretischen Reflexion zu stellen und auch bei der Entwicklung von Pilotprojekten eine entsprechende Prioritätensetzung vorzunehmen.

6 Schlussbetrachtungen und weiterführende Überlegungen

Es bleibt abzuwarten, ob und inwieweit sich die TA-Community und Fachleute aus anderen einschlägigen Bereichen der Herausforderung, Aspekte von IT-Sicherheit und PTA zum Zwecke der Entwicklung neuer Wegen zur Realisierung des Leitbilds der mehrseitigen IT-Sicherheit gezielt miteinander zu verbinden, stellen werden. Denjenigen, die einwenden, dass partizipative Entscheidungsverfahren eine andere und vielleicht auch eine geringere demokratische Legitimität aufweisen als repräsentative Verfahren, muss aus der Sicht derer, die sich dieser Herausforderung stellen

wollen, nicht unbedingt widersprochen werden. Denn im Bereich der IT-Sicherheit geht es in der Regel nicht darum, zwischen repräsentativ und diskursiv ausgerichteter demokratischer Problembearbeitung und Konfliktbewältigung frei auszuwählen. Hier geht es vielmehr zuerst einmal darum, eine Antwort auf die grundsätzliche Frage zu geben, ob man den Anspruch der demokratischen Beeinflussung des soziotechnischen Wandels – welche in den meisten Fällen aus sachlogischen Gründen eben nicht repräsentativ, sondern allein diskursiv erfolgen kann – aufrechterhalten oder aufgeben will.

Eine Frage, die über das in den vorausgegangenen Kapiteln bearbeitete Themenspektrum hinausgeht, welche aber hier dennoch nicht gänzlich ausgeblendet bleiben darf, ist die, wie man mit den neuen Sicherheitsproblemen der Informationsgesellschaft auf der politischen Ebene umgehen soll, und wie sich diese Probleme in der Praxis so effektiv wie möglich bearbeiten lassen.

Weil Fragen der IT-Sicherheit einerseits wegen der grenzüberschreitenden Anlage der Netzwerke eine globale Qualität aufweisen, andererseits aber auch oft nur in lokalspezifischen oder sachgebietsbezogenen Kontexten beurteilt werden können, erscheint eine flächendeckende Implementation des Leitbilds der mehrseitigen Sicherheit letztlich nur auf der Basis einer entsprechenden *Global Governance*-Infrastruktur denkbar. Hier sollte also die globale, die europäische, die nationale, die regionale und die lokale Ebene ebenso in den Blick genommen werden wie eine breite Palette von Akteuren aus Staat, Wirtschaft und Zivilgesellschaft. Bekanntlich stellt die Entwicklung solcher Strukturen aber ein äußerst anspruchsvolles Projekt dar, das – wenn überhaupt – nur im Rahmen von langfristig angelegten Gestaltungsprozessen erfolgreich sein kann. Heute ist nicht absehbar, ob überhaupt die Chance besteht, eine *Global Governance*-Infrastruktur zur Bearbeitung von IT-Sicherheitsproblemen irgendwann einmal Wirklichkeit werden zu lassen.

Ein großer Schritt, um hierzulande zur Etablierung von Strukturen und Kulturen beizutragen, die sowohl in einzelnen gesellschaftlichen Teileinheiten wie Unternehmen und Behörden als auch auf der gesamtgesellschaftlichen Ebene als Basis von am Leitbild der mehrseitigen Sicherheit orientierten Sicherheitsprozessen dienen können, könnte durch die Schaffung der Institution eines Datensicherheitsbeauftragten getan werden. Was die Einbindung einer solchen Institution in das System der Bundesrepublik betrifft, wäre die auf unterschiedlichen Ebenen (Bund und Land) und in unterschiedlichen Bereichen (Politik und Arbeitswelt) verankerte Institution des Datenschutzbeauftragten durchaus geeignet, als Vorbild herangezogen zu werden. Was die inhaltliche bzw. die politische Seite betrifft, stellt sich die Lage aber anders dar. Ein Datensicherheitsbeauftragter hätte nämlich eine völlig andere Rolle auszufüllen als ein Datenschutzbeauftragter. Während Datenschutzbeauftragte die Aufgabe haben, das Recht der informationellen Selbstbestimmung (und daneben das Fernmeldegeheimnis) unter den veränderten soziotechnischen Vorzeichen des elektronischen Zeitalters zu verteidigen (und damit als Konfliktpartei zu agieren), müssten sich Da-

tensicherheitsbeauftragte interessenneutral verhalten. Ihre Aufgabe bestünde vor allem darin, Sicherheitsprozesse insbesondere durch den Aufbau geeigneter Netzwerke zu ermöglichen und dabei dafür Sorge zu tragen, dass unterschiedliche Sicherheitsbilder und Sicherheitsinteressen abgeglichen und Sicherheitskonflikte in möglichst symmetrischen Konstellationen verhandelt werden können.[14]

Allerdings ist der Bundesrepublik Deutschland das IT-Sicherheitsbewusstsein noch bei weitem nicht so stark ausgeprägt, als dass man in absehbarer Zeit mit der Schaffung einer solchen Institution rechnen dürfte. In den kommenden Jahren wird man daher auch hierzulande in hohem Maße darauf angewiesen sein, dass Fragen der IT-Sicherheit einerseits durch fachspezifische Einrichtungen wie den Forschungsverbund Datensicherheit in Nordrhein-Westfalen oder das Horst Görtz-Institut für IT-Sicherheit an der Ruhr-Universität Bochum und andererseits durch im Bereich von TA und PTA tätige Einrichtungen wie die dem TAB oder der Akademie für Technikfolgenabschätzung in Baden-Württemberg mit einem Mindestmaß an Professionalität und Zuverlässigkeit bearbeitet werden.

Die Funktionen, die in diesem Zusammenhang zu erfüllen sind, lassen sich folgendermaßen zusammenfassen:

- Werbung für das Leitbild der mehrseitigen IT-Sicherheit in der Öffentlichkeit
- Beobachtung der technischen, sozialen, kulturellen und ökonomischen Entwicklungen im Bereich der IT-Sicherheit und Identifizierung von zukunftsweisenden Lösungen zur Realisierung von mehrseitiger IT-Sicherheit
- Durchführung bzw. Unterstützung und Begleitung von anwendungsorientierten Forschungen und Pilotprojekten, wobei – wenn sich die entsprechenden Thesen (vgl. Punkt 5.4. und Punkt 5.5. dieser Arbeit) als stichhaltig erweisen sollten – die Szenariotechnik und der netzgestützte Diskurs eine wichtige Rolle spielen könnten
- Aufklärung und Information in konkreten Fragen der IT-Sicherheit unter besonderer Berücksichtigung des Umstands, dass die Förderung von mehrseitiger IT-Sicherheit weniger ein technisches Problem darstellt als ein Problem der sozialen Organisation und der Kultur
- Mitwirkung am Aufbau und Ausbau von Arenen und Netzwerken, in denen divergierende IT-Sicherheitsbilder ermittelt und zum Abgleich gebracht und insbesondere auch konkrete IT-Sicherheitskonflikte auf der Basis von Kompromissen und Kompensationen beigelegt werden können

[14] Damit weicht das hier vertretene Verständnis von einem IT-Sicherheitsbeauftragten von dem entsprechenden Verständnis ab, das in der Wirtschaft herrscht. IT-Sicherheitsbeauftragte, wie sie in erster Linie in Großunternehmen anzutreffen sind, haben vor allem die Aufgabe, die Informationen und Kommunikationsbeziehungen eines Unternehmens gegenüber Angriffen von innen und außen zu schützen (vgl. Cole/Matzer 1999: 187 ff und Plate 1997: 373).

- Artikulation von IT-Sicherheitsinteressen marginalisierter Gruppen im Sinne der Wahrnehmung einer Anwaltsfunktion
- Politikberatung in Fragen der IT-Sicherheit, die von Parteien und Verbänden unabhängig ist.

Die mit der Wahrnehmung dieser Funktionen verbundenen Anforderungen sind sehr hoch. Um die damit betrauten Einrichtungen zu stärken, wäre es sinnvoll, deren Ausstattungen zu verbessern und sie besser als bisher in die formellen Strukturen des politisch-administrativen Handelns einzubinden. Gleichzeitig ergibt sich hier die Notwendigkeit, die Formen der korporatistischen und der diskursiven Problembearbeitung besser als bisher miteinander zu verzahnen.

7 Literaturverzeichnis

Akademie für Technikfolgenabschätzung in Baden-Württemberg (2000): Die TA-Akademie im Überblick, Stuttgart.

Andersen, Jan A. (1997): Technology Assessment Network Building. The International Association for Technology Assessment and Forecasting Institutions. New York.

Andersen, Ida-Elisabeth und Birgit Jaeger (1999): Scenario workshops and consensus conferences: towards more democratic decision-making. In: Science and Public Policy 5. S. 331-340

Baron, Waldemar M. (1995): Technikfolgenabschätzung. Ansätze zur Institutionalisierung und Chancen der Partizipation. Opladen.

Bechman, Gotthard (1997): Diskursivität und Technikgestaltung. In: Gloede, Fritz; Leonhard Hennen und Sabine Koeberle (Hrsg.): Diskursive Verständigung? Mediation und Partizipation in Technikkontroversen. Baden-Baden. S. 151-163.

Böhle, Knud und Ulrich Riehm (1998): Blütenträume. Über Zahlungssysteminnovationen und Internet-Handel in Deutschland. Karlsruhe.

Böhle, Knud und Ulrich Riehm (1999): Elektronische Kommunikation im Projekt Elektronische Zahlungssysteme (PEZ). Auswertung zum Diskussionsforum EZI-L und Dokumentation des Newsletters EZI-N. Karlsruhe.

Böhret, Carl und Peter Franz (1986): Die Technologiefolgenabschätzung als Instrument der politischen Steuerung des technischen Wandels. In: Bruder, Wolfgang (Hrsg.): Forschungs- und Technologiepolitik in der Bundesrepublik Deutschland. Opladen. S. 349-390.

Bonsen, Matthias zur (1998): Die Methode Zukunftskonferenz. In: Impulse – Zeitschrift des GABAL Netzwerk Lernen 2. S. 12-20.

Barthel, Jochen, Hans-Joachim Braczyk und Gerhard Fuchs (1999): Vertrauen in soziotechnische Systeme. In: Kubicek, Herbert u.a. (Hrsg.): Multimedia und Verwaltung. Jahrbuch Telekommunikation und Gesellschaft 1999. Heidelberg. S. 111-123.

Braczyk, Hans-Joachim, Jochen Barthel, Gerhard Fuchs und Kornelia Konrad (1999): Vertrauensbildung aus soziologischer Sicht – das Beispiel Sicherheit in der Kommunikationstechnik. In: Müller, Günter und Kurt-Hermann Stapf (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Band 2: Erwartung, Akzeptanz, Nutzung. Bonn und New York. S. 119-147.

Burow, Olaf A. (2000): Die Zukunftskonferenz: In: Burow, Olaf A. (Hrsg.): Ich bin gut – wir sind besser. Erfolgsmodelle kreativer Gruppen. Stuttgart. S. 167-185.

Citizens Panel on Telecommunications and the Future of Democracy (1997): Consensus Statement. Amherst.

Coenen, Reinhard (1998): Fünf Jahre IATAFI. In: TA-Datenbank-Nachrichten 3/4. S. 44-45.

Cole, Tim und Michael Matzer 1999: Managementaufgabe Sicherheit. München und Wien.

Der Bundesbeauftragte für den Datenschutz (1999): Der Bürger und seine Daten. Bonn.

Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen (1999): Neue Instrumente im Datenschutz. Düsseldorf.

Deckstein, Dina/Dworschak, Manfred/Kerbusk, Klaus-Peter/Mascolo, Georg/Müller Mathias/Ulrich Andreas (2000): Attentäter im Netz. In: Der Spiegel 20. S 60-71.

Dienel, Peter C. (1987): Bürgergutachten Regelung sozialer Folgen neuer Informationstechnologien. Wuppertal.

Dienel, Peter C. (1991): Bürgergutachten ISDN. Wuppertal.

Dienel, Peter C. (1992): Die Planungszelle. Eine Alternative zur Establishment-Demokratie. Opladen.

Dienel, Peter C. (1996): Das Modell Bürgergutachten als Organ politischen Lernens. In: Claußen, Bernhard und Rainer Geißler (Hrsg.): Die Politisierung des Menschen. Opladen. S. 425-442.

EASW (1998): Women in the Net. An EASW Workshop for and with women on their expectations and fears, on advantages and dangers on electronic communication networks in the information society. New York.

EUROPTA (2000): European Participatory Technology Assessment. Participatory Methods in Technology Assessment and Decision-Making. Copenhagen.

Fietkau, Hans-Joachim und Karin Pfingsten (1995): Umweltmediation. Verfahrenseffekte und Urteilsperspektiven. In: Archiv für Kommunalwissenschaften 1. S. 55-70.

Fink, Alexander; Jürgen Gausemeier und Oliver Schlake (1997): Szenario-Technik. In: Westphalen, Raban Graf von (Hrsg.): Technikfolgenabschätzung als politische Aufgabe. München und Wien. S. 203-221.

Forschungsstelle Bürgerbeteiligung und Planungsverfahren (2001): Aufgaben und Ziele der Forschungsstelle. Wuppertal.

Freitag, Günter (1997): Über das Konzept der Planungszelle als Instrument der Bürgerbeteiligung. Gelsenkirchen und Duisburg.

Fuchs, Gerhard (2000): Unternehmen im Netz. Umfrage zum Einsatz von Informations- und Kommunikationstechniken in kleinen und mittleren Unternehmen in der Region Stuttgart. Stuttgart.

Geiger, Gebhard (2000): Information Warfare. In: Datenschutz und Datensicherheit 3. S. 129-136.

Gloede, Fritz; Leonhard Hennen und Sabine Koeberle (1997): Einleitung. In: Gloede, Fritz; Leonhard Hennen und Sabine Koeberle (Hrsg.): Diskursive Verständigung? Mediation und Partizipation in Technikkontroversen. Baden-Baden. S. 11-24.

Guston, David H. (1998): Evaluating the Impact of the First U.S. Citizens' Panel on Telecommunications and the Future of Democracy. Prepared for delivery at the 1998 Annual Meeting of the American Political Science Association. Boston.

Hennen, Leonhard (1997): Technikdiskurse. In: Gloede, Fritz; Leonhard Hennen und Sabine Koeberle (Hrsg.): Diskursive Verständigung? Mediation und Partizipation in Technikkontroversen. Baden-Baden. S. 189-199.

Holtkamp, Lars (2000): Bürgerbeteiligung in Städten und Gemeinden. Berlin.

Holznagel, Bernd und Ulrich Ramsauer (1997): Konsensuale Sachverhaltsermittlung als Mediationsziel. Data-Mediation am Beispiel der Verhandlungen über den Hamburger Autobahndeckel. In: Forschungsjournal Neue Soziale Bewegungen 4. S. 65-72.

Holtz-Bacha, Christina (1997: Das fragmentierte Medienpublikum - Folgen für das politische System. In: Aus Politik und Zeitgeschichte B 42, S. 13-21.

Holtz-Bacha, Christina (1998): Fragmentierung der Gesellschaft durch das Internet. In: Gellner, Winand und Korff, Fritz von (Hrsg.): Demokratie und Internet. Baden-Baden. S. 219-226.

Hutter, Reinhard (2000): Angriffe auf Informationstechnik und Infrastrukturen – Realität oder Science Fiction? In: Aus Politik und Zeitgeschichte B 41-42. S. 31-38.

König, Dieter (1997): Technikfolgenabschätzung bei den Vereinten Nationen. In: Westphalen, Raban Graf von (Hrsg.): Technikfolgenabschätzung als politische Aufgabe. München und Wien. S. 281-286.

Kubicek, Herbert (1999): Was versteht man unter allgemeinem Zugang und worauf kommt es an? In: Kubicek, Herbert u.a. (Hrsg.): Multimedia und Verwaltung. Jahrbuch Telekommunikation und Gesellschaft. Heidelberg. S. 332-338.

Lackner, Stefanie (1999): Neue Verfahren der Bürgerteilhabe. In: Polis 28. S. 8-42.

Leggewie, Claus (1998): Demokratie auf der Datenautobahn. In: Leggewie, Claus und Maar, Christa (Hrsg.): Internet und Politik. Köln. S. 15-51.

Lübke, Dirk (1997): Laien machen Experten frisch. In: Solinger Tageblatt vom 15. März. S. 10.

Luhmann, Niklas (1992): Soziologie des Risikos. Berlin und New York 1991.

Mascolo, Georg/Schreiber Sylvia/Thielke, Thilo (2000): Bedroht von den Freuden. In: Der Spiegel 15. S. 216-218.

Meyer, Rolf (1997): Das Büro für Technikfolgenabschätzung beim Deutschen Bundestag. In: Westphalen, Raban Graf von (Hrsg.): Technikfolgenabschätzung als politische Aufgabe. München und Wien. S. 340-365.

Mohr, Hans (1997): Die Akademie für Technikfolgenabschätzung in Baden-Württemberg. In: Westphalen, Raban Graf von (Hrsg.): Technikfolgenabschätzung als politische Aufgabe. München und Wien. S. 410-424.

Müller, Albrecht und Thomas von Schnell (1996): Bürger als Gutachter der Technikgestaltung: Das Beispiel der Bürgerforen Biotechnologie und Gentechnik – eine Chance für die Zukunft? In: Wienhöfer, Elmar (Hrsg.): Bürgerforen als Verfahren der Technikfolgenbewertung. (Arbeitsbericht der Akademie für Technikfolgenabschätzung in Baden-Württemberg.) Stuttgart. S. 61-72.

Müller, Günter und Andreas Pfitzmann (1997): Mehrseitige Kommunikation – Vertrauen in Technik durch Technik. In: Müller, Günter und Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Band 1: Verfahren, Komponenten, Integration. Bonn und New York. S. 11-18.

Ohlemachter, Thomas (1991): Planungszellen und Stadtteilvertretungen. Über das Schicksal zweier Versuche, politische Beteiligung zu steigern. In: Stiftung Mitarbeit (Hrsg.): Modelle und Wege der lokalen Bürgerbeteiligung. Bonn. S. 52-72.

Ott, Klaus und Barbara Skopurinski (2000): Technikfolgenabschätzung und Ethik. Eine Verhältnisbestimmung in Theorie und Praxis. Zürich.

Plate, Angelika (1997): IT-Sicherheitsmanagement in der internationalen Standardisierung. In: Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): Mit Sicherheit in die Informationsgesellschaft. Ingelheim. S. 369-380.

Petermann, Thomas (2000): Zehn Jahre Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag. In: TA-Datenbank-Nachrichten 4. S. 96-97.

Rader, Michael (1998): TA-Aktivitäten auf Ebene der Europäischen Union. In: TA-Datenbank-Nachrichten 3/4. S.13-16.

Renn, Ortwin (2002): Im Supermarkt der Gutachten. Ortwin Renn im Gespräch mit Hans Schuh. In: Die Zeit Nr. 39 vom 19. September. S. 32.

Renn, Ortwin (1996): Vorwort. In: Wienhöfer, Elmar (Hrsg.): Bürgerforen als Verfahren der Technikfolgenbewertung. Stuttgart. S. 3-6.

Riehm, Ulrich (2000): Unterstützung partizipativer Elemente im TA-Prozess durch elektronische Kommunikation. In: TA-Datenbank-Nachrichten 3. S. 61-66.

Roth, Roland (1997): Die Kommune als Ort der Bürgerbeteiligung. In: Klein, Ansgar und Rainer Schmalz-Bruns (Hrsg.): Politische Beteiligung und Bürgerengagement in Deutschland. Bonn. S. 405-447.

Saretzki, Thomas (1997a): Demokratisierung von Expertise? Zur politischen Dynamik der Wissensgesellschaft. In: Klein, Ansgar und Rainer Schmalz-Bruns (Hrsg.): Politische Beteiligung und Bürgerengagement in Deutschland. Bonn. S. 277-313.

Saretzki, Thomas (1997b): Mediation, soziale Bewegung und Demokratie. In: Forschungsjournal Neue Soziale Bewegungen 4. S. 27-42.

Schuchardt, Wilgart und Rainer Wolf (1990): Technikfolgenabschätzung und Technikbewertung. Möglichkeiten und Schwierigkeiten der Technikkontrolle und Technikregulierung. In: Ropohl, Günter (Hrsg.): Schlüsseltexte zur Technikbewertung. Dortmund. S. 9-38.

Sclove, Richard E. (1996): Town Meetings on Technology. In: Technology Review 6. S. 100-105.

Sclove, Richard E. (1997): Telecommunications and the future of democracy. Preliminary Report on the First U.S. Citizens Panel. In: Lokal Alert 3. S. 105-110.

Simonis, Georg (1989): Bleiben die neuen Technologien sozial beherrschbar? In: Alemann, Ulrich von; Heribert Schatz und Georg Simonis (Hrsg.): Gesellschaft, Technik, Politik. Perspektiven der Technikgesellschaft. Opladen. S. 187-201.

Tils, Ralf (1997): Vorsicht: Mediation! Chancen und Risiken der Umweltmediation aus der Sicht von Umweltverbänden. In: Forschungsjournal Neue Soziale Bewegungen 4. S. 43-52.

Weisbord, Marvin und Sandra Janoff (1995): What Is a Future Search? New York.

Uhl, Dagmar/Thiele, Felix (2000): Fünf Jahre Europäische Akademie. In: TA-Datenbank-Nachrichten 4. S. 98-100.

Westphalen, Raban Graf von (1997): Einführung in die Technikfolgenabschätzung. In: Westphalen, Raban Graf von (Hrsg.): Technikfolgenabschätzung als politische Aufgabe. München und Wien. S. 9-14.

Wienhöfer, Elmar (1996): Bürgerforen als Methode einer partizipativen Technikfolgenbewertung. In: Wienhöfer, Elmar (Hrsg.): Bürgerforen als Verfahren der Technikfolgenbewertung. (Arbeitsbericht der Akademie für Technikfolgenabschätzung in Baden-Württemberg.) Stuttgart. S. 53-60.

Winkel, Olaf (1997a): Netzsicherheit als gesellschaftliches und politisches Problem. In: Online 1. S. 62-64.

Winkel, Olaf (1997b): Private Verschlüsselung als öffentliches Problem. In: Leviathan 4. S. 567-586.

Winkel, Olaf (1998): Electronic Commerce. In: Blätter für deutsche und internationale Politik 3. S. 288-291.

Winkel, Olaf (1999): Die Förderung von Vertrauen, Glaubwürdigkeit und Verlässlichkeit in der digitalisierten Informationsgesellschaft - Welchen Beitrag kann die elektronische Verschlüsselung dazu leisten? In: Rössler, Patrick und Werner Wirth (Hrsg.): Glaubwürdigkeit im Internet. München. S. 193-208.

Winkel, Olaf (2000a): Ist die elektronische Kryptographie demokratieverträglich? Einige grundlegende Anmerkungen zum schwierigen Verhältnis von Bürger und Staat im elektronischen Zeitalter unter Rückgriff auf Hobbes, Locke und Rousseau. In: Zeitschrift für Politik 1. S. 73-91.

Winkel, Olaf (2000b): Netzwerksicherheit – (k)ein Thema für Sozialwissenschaftler? In: RUBIN – Wissenschaftsmagazin 2. S. 6-12.

Winkel, Olaf (2000c): Sicherheit in der digitalen Informationsgesellschaft. IT-Sicherheit als politisches, ökonomisches und gesellschaftliches Problem. In: Aus Politik und Zeitgeschichte B 41-42. S. 19-30.

Winkel, Olaf (2000d): Telekommunikationssicherheit im Spannungsfeld von Kommerzialisierungsinteressen und den Zukunftsanforderungen der demokratischen Gesellschaft. In: Martinsen, Renate und Georg Simonis (Hrsg.): Demokratie und Technik. Opladen. S. 71-100.

Winkel, Olaf (2001): Multilateral Security – A Question of Social Organization and Culture. A Plea for a More Widely and Encompassing Inquiry. In: Heinrich Böll-Stiftung (Hrsg.): Arms Control in Cyberspace. Dokumentation einer internationalen Konferenz der Heinrich Böll-Stiftung am 29. und 30. Juni 2001 in Berlin. Berlin. S. 54-56.

Winkel, Olaf und Orkan Kösemen (2002): Die NSA und Echelon – ein Geheimdienst entdeckt die Wirtschaft. In: In: Blätter für deutsche und internationale Politik 10. S. 1227-1235.

Winkel, Olaf, Uwe Andersen, Volker Hecht und Hellen Tackenberg (2002): Der Schutz von sensiblen Informationen und kritischen Infrastrukturen in der mittelständischen Wirtschaft als politische Herausforderung. Neue Bedrohungen und Präventionsstrategien in der Informationsgesellschaft. Teil I. In: Die Kriminalprävention 1. S. 19-27.

Woolsey, James (2000): Ja, liebe Freunde, wir haben Euch ausgehorcht. Nachdruck aus dem Wall Street Journal Europe. In: Die Zeit Nr. 14 vom 15. April. S. 10

Wunrich, Christine (1997): STOA – die TA-Einrichtung des Europäischen Parlamentes. In: Westphalen, Raban Graf von (Hrsg.): Technikfolgenabschätzung als politische Aufgabe. München und Wien. S. 287-304.

Zwingenberger, Meike (1998): Gemeinschaftsformen in der globalen Informationsgesellschaft. In: Gellner, Wienand und Korff, Fritz von (Hrsg.): Demokratie und Internet. Baden-Baden. S. 227-239.