institut für RECHTS- & KRIMINALsoziologie

IRKS WORKING PAPER NO 1

Paradoxien der Sicherheitspolitik

Reinhard Kreissl

MÄRZ 2007
www.irks.at
ISSN 1994-490X

IRKS WORKING PAPER NO 1

Paradoxien der Sicherheitspolitik

Reinhard Kreissl

MÄRZ 2007
www.irks.at
ISSN 1994-490X

Paradoxien der Sicherheitspolitik

Reinhard Kreissl

Es handelt sich hier um einen Vortrag, der bei der 13. Jahresversammlung des Verbands für Sicherheitstechnik e.V. in der Handelskammer Hamburg im November 2006 gehalten wurde. Die Vortragsform wurde beibehalten und auf Anmerkungen und Literaturverweise verzichtet.

Wenn wir von Sicherheit reden, haben wir es mit einem höchst diffusen Feld zu tun. Ein bisschen Ordnung können wir schaffen, wenn wir mit Unterscheidungen arbeiten. Sie alle kennen den Unterschied von Security, Safety und Certainty, also körperliche Unversehrtheit, Sicherheit vor existenziellen Risiken und Gewissheit, dass die Dinge in der Zukunft so bleiben werden, wie wir sie kennen. Andere Unterscheidungen wären im Hinblick auf die Sicherheitspolitik die Differenz zwischen privatem und öffentlichen Sektor, zwischen Prävention und Repression, zwischen individueller und kollektiver, technischer und sozialer Sicherheit.

Ich möchte hier zunächst einen anderen Einstieg wählen und im Bereich Sicherheit probehalber zwischen Hardware, Software und Wetware unterscheiden. Ich unterscheide damit also zwischen materiellen Gegebenheiten – vom Stacheldrahtzaun über die Chipkarte mit Zugangscode bis zur Videokamera. Das wären Beispiele für Hardware. Software wären die dazu gehörigen Prozeduren und Verfahren – von Vorschriften für das Anlegen papierbasierter Akten über Datenbanken bis hin zu Programmen für Pattern Recognition, die automatisch visuelle Daten nach bestimmten Mustern absuchen und auswerten können. Wetware schließlich, dass sind wir, die feuchten analog gebauten Wesen, einerseits unheimlich komplex in der Architektur, andererseits bisher weitgehend unverstanden, einerseits in der Rolle des Prothesengottes, wie Sigmund Freud es einmal formulierte, andererseits schutzlos und angreifbar.

Nun ist es ein technisches Problem Soft- und Hardware im Bereich Sicherheit anzupassen und auszubauen. Speicherplatz kostet praktisch nichts mehr, das beschert uns die Datenflut. Die Kosten der Rechnerkapazität halbieren sich in den bekannten Schritten – auch hier besteht keinerlei Knappheit und Computer sind überall. Sie sind, wie es heißt »pervasive«, man findet sie immer und überall, auch an den ungewöhnlichsten Orten. Die rechtlichen Regelungen, die man früher als Datenschutz bezeichnete, gehören de facto der Vergangenheit an: also auch der Produktion und dem Austausch von Daten, sowie dem Sammeln von Information sind immer weniger Grenzen gesetzt – fragt man allerdings die Sicherheitsdienste, dann sind es immer noch zu viele. Was hingegen zunächst mehr oder weniger konstant bleibt und bisher nur in den trägen Zyklen der biologischen und kulturellen Evolution sich entwickelt, das sind wir.

Das hat eine Reihe von Konsequenzen: Was immer wir an Daten, etwa aus der Rasterfahndung oder dem Data-Mining oder durch sonstige Verfahren gewinnen können, es muss letztlich durch den Flaschenhals des menschlichen Gehirns und seiner beschränkten Verarbeitungskapazität. Wir stoßen hier auf Probleme an der Schnittstelle von Mensch und Maschine bzw. Programm, die theoretisch betrachtet aus der Kombination von Top-down und Bottom-up-Strategien bei der menschlichen Informationsverarbeitung erwachsen. Ich will Ihnen das an einem Beispiel verdeutlichen. Die berühmte Spur, die zu dem Appartement führte, in dem der Arbeitgeberpräsident Hans-Martin Schleyer seinerzeit von seinen Entführern aus der RAF in Deutschland gefangen gehalten wurde, war in den Fahndungsunterlagen der Ermittlungsbehörden vorhanden. Die Rasterfahndung funktionierte also – technisch gesehen. Hard- und Software taten das, was man erwartete. Aber die Beamten gingen dieser einen Spur nicht wirklich ernsthaft nach. Im Nachhinein, Schleyer war inzwischen ermordet worden und die Katastrophe hatte ihren Lauf genommen, war man schlauer. Ich verweise auf diese Geschichte gerne immer dann, wenn die Forderung nach noch mehr und noch umfassender Datensammlung auftaucht.

Es gibt eine ganze Reihe von Beispielen, nicht alle so spektakulär, an denen man zeigen kann, wie letztlich der berühmte Faktor Mensch immer wieder alle Bemühungen und Vorkehrungen nutzlos macht. Charles Perrow hat in seinem Buch mit dem Titel »Normale Katastrophen« gezeigt, wie eng gekoppelte komplexe Systeme unbeherrschbar werden können und wie mehr Sicherheitslücken durch neue Sicherheitsvorkehrungen entstehen. Das hat im übrigen bereits zu einem Umdenken im Bereich der Technologieentwicklung geführt. Moderne Atomkraftwerke haben heute weniger Sicherheitssysteme als früher. Man versucht statt dessen durch Vereinfachung Sicherheit in das Design des Systems einzubauen. Die dahinter stehende Überlegung ist so paradox wie simpel: je mehr Sicherheitssysteme ich verwende, desto größer sowohl die Gefahr eines Fehlalarms als auch eines Systemversagens.

Aber wir finden auch Prozesse, die in der anderen Richtung wirken: Prozesse der Anpassung der Wetware an die Erfordernisse von Soft- und Hardware. Im ersten Fall, der nicht berücksichtigen Spur aus der Rasterfahndung nach den Entführern ging es um die Wetware auf der Seite der professionellen sicherheitspolitischen Akteure. In anderen Fällen geht es eher um jene, die als Abnehmer von Sicherheitsdienstleistungen bezeichnet werden, die breite Öffentlichkeit, den Mann und die Frau auf der Straße. Wir sind in dieser Rolle als Bürger manchmal in der Situation des armen Mannes, der sich zum ersten Mal in seinem Leben einen Maßanzug schneidern lässt. Er geht zur endgültigen Anprobe und steht vor dem Spiegel. Der Anzug wirft Falten, der Schneider fordert ihn auf, eine völlig krumme Körperhaltung einzunehmen und sich solange zu verbiegen, bis der Anzug perfekt passt. Am Schluss humpelt er aus dem Atelier des Schneiders

stolz mit seinem neuen, jetzt dank seiner gekrümmten Körperhaltung faltenfrei sitzenden Anzug. Zwei Passanten auf der gegenüberliegenden Straßenseite sehen den Mann, wie er mit krummen Rücken und angehobener Hüfte dahin humpelt. Der eine sagt: Schau dort, der arme Krüppel. Darauf der andere: Ja, aber einen guten Schneider hat er....

Ein bisschen sind wir in einer vergleichbaren Situation und jedes Mal, wenn man einen Flughafen betritt, fühlt man sich ein wenig wie der Mann mit dem neuen Anzug. Man muss sich Erfordernissen anpassen und erniedrigende Prozeduren über sich ergehen lassen, die dem eigenen normalen Verhalten nicht entsprechen. Auch andere öffentliche Räume gleichen sich immer mehr diesem Paradigma an. Als ich vor kurzem für ein paar Tage in New York war, durchlief ich mehrmals am Tag irgendwelche Sicherheitsprozeduren und der Satz, den ich in diesen Tagen am häufigsten hörte war: »It's for your own security Sir!« Ich hatte New York das letzte Mal vor dem 11. September 2001 besucht und mir kam die Stadt, ja das ganze Land vor, als sei es in eine kollektive Hysterie oder Paranoia verfallen. Die Einreiseformalitäten riefen Erinnerungen an den Übertritt von West- nach Ostberlin zur Zeit des Kalten Krieges wach.

Nun könnte man die Probleme des ersten Typs als technische Probleme abtun. Bessere Methoden der Datenerhebung und –auswertung sollten die Lösung sein. Das wird nicht gehen, solange wir den Flaschenhals des menschlichen Gehirns nicht erweitern können.

Probleme des zweiten Typs – der vom Schneider zum Krüppel gemachte Anzugträger – werden vermutlich an Schärfe zunehmen, ob damit Sicherheitsgewinne erzielt werden können, möchte ich im folgenden untersuchen.

Es gibt aus dem Dilemma der Sicherheitspolitik keinen einfachen Ausweg, keine Lösung. Aber man kann versuchen zumindest besser zu verstehen, was hier passiert und warum man auf solche Probleme stößt.

Ich führe wieder eine Unterscheidung ein und unterscheide zwischen Risiko und Gefahr. Der Unterschied zwischen diesen beiden liegt aus sozialwissenschaftlicher Sicht in der Art der Zurechnung. Gefahren sind etwas, das von außen hereinbricht. Ein Blitz, der beim Gewitter in das Haus einschlagen kann, das ist eine Gefahr. Mit einem Risiko hingegen haben wir es dann zu tun, wenn die eintretenden Schäden nicht extern – also etwa der Natur oder dem Zufall – zurechenbar sind, sondern die Folgen meiner eigenen Entscheidungen in der Vergangenheit sind. Lungenkrebs ist so gesehen ein Risiko, weil er die Folge meiner eigenen Entscheidung (oder ich sollte besser sagen – der Unfähigkeit der Entscheidung) ist, das Rauchen aufzugeben.

Nun merkt man sehr schnell, dass die Unterscheidung von Gefahr und Risiko nicht besonders trennscharf ist: Warum kann man den Blitz nicht als Risiko begreifen, gegen das ich mich durch die Installation eines Blitzableiters schützen kann und ist Lungenkrebs nicht auch eine Gefahr, die durch Passivrauchen oder genetische Mutationen hervorgerufen werden kann – also etwas, das sozusagen von außen über mich hereinbricht? Kann man also nicht durch entsprechende Hard- und Softwaremaßnahmen die Sicherheit erhöhen und die Wetware sichern?

Leider ist das nicht so einfach. An der Differenz von Risiko und Gefahr, also an Katastrophen, die hereinbrechen und solchen, die sich als Folge eigener Entscheidungen begreifen lassen, zeigt sich, dass wir in einer selbstgemachten und symbolisch strukturierten Umwelt agieren und heillos verstrickt sind in selbstgemachte Probleme, die wir nicht in den Griff bekommen. Ob wir etwas als Risiko oder Gefahr begreifen hängt auch davon ab, *wie* wir die Dinge betrachten. In einer Gesellschaft, die das Schicksal und die Götter als kausale Kräfte kennt, sind alle Schadensereignisse letztlich Gefahren – sie brechen schicksalshaft herein oder sind als Strafe von den Götter gesendet. In einer Gesellschaft, die anfängt, die Welt zu entzaubern, das heißt, nach Mechanismen, Zusammenhängen und Kausalitäten zu suchen, werden aus Gefahren Risiken. Risiken sind, ich wiederhole es noch mal: zukünftige Schadensereignisse, die aufgrund meines oder unseres oder irgendjemands gegenwärtigen Handelns eintreten – oder auch nicht.

Ein gutes Beispiel ist das Wetters: Die als Klimakatastrophe apostrophierte Entwicklung der globalen klimatischen Verhältnisse lässt sich nicht in den Griff bekommen, da die Analyse selbst Teil des Problems ist. Die Phänomene sind zwar natürlicher Art, aber sie sind – so die derzeit herrschende und gut abgesicherte Interpretation – von Menschen beeinflusst. Jedes neue Modell, das die verschiedenen Szenarien durchrechnet, wird – vorausgesetzt es wird kommuniziert – die Verhaltensweisen der Akteure verändern und damit die Werte der in dem Modell angenommenen Parameter beeinflussen.

Man kann die Folgen dieses Sachverhalts für die meteorologische Sicherheitspolitik vor der eigenen Haustüre beobachten. Vor einigen Jahren tauchten Überschwemmungen und Stürme zusehends häufiger auch in unseren Breitengraden auf. Man forderte damals vom Deutschen Wetterdienst, dass er frühzeitig vor solchen Ereignissen warnen sollte. Damit entstand die neue Kategorie der Unwetterwarnung im Wetterbericht nach den Abendnachrichten. Man hatte die Meteorologen kritisiert, dass sie nicht rechtzeitig auf die drohenden Unwetter hingewiesen hätten. Und so war es aus der Sicht der sicherheitspolitischen Akteure, hier also des Deutschen Wetterdiensts, sinnvoller, in Zukunft eher einmal zu früh, als einmal zu spät zu solchen Warnungen zu greifen. Die Folge davon ist eine Inflationierung der Warnhinweise mit der Konsequenz, dass sie tendenziell nicht mehr ernst genommen werden und ihre Wirkung verlieren. Die meteoro-

logische Sicherheitsbehörde aber ist aus dem Schneider: Denn sollte es wirklich zu einem Unwetter kommen, dann kann sie sagen, sie habe rechtzeitig gewarnt. Wenn einem jetzt dazu ähnliche Beispiele aus dem Bereich der Terrorismusbekämpfung einfallen, dann ist das kein Zufall. Der Mechanismus ist der gleiche.

Dieser Mechanismus ist relativ einfach: Je stärker die reale Vernetzung der Welt voranschreitet – Stichwort Globalisierung – und je mehr man weiß über die Vernetzung von Ereignissen, je länger die Kausalketten werden, die in der Handlungsplanung und bei Entscheidungen in Rechnung gestellt werden, desto mehr öffnet sich der Horizont der Akteure für mögliche Varianten von Zukunft und desto mehr werden »natürliche« Phänomene als Ereignisse erscheinen, die von den eigenen Handlungen abhängen, desto mehr wird die Zukunft einerseits unberechenbarer, andererseits von einem selbst und den eigenen Entscheidungen abhängig und desto eher wird man auf ein möglicherweise eintretendes Schadensereignis hinweisen, wenn man als sicherheitspolitischer Akteur handelt. Im Extremfall ist dann meine Konsumentscheidung bestimmend für die Überlebenschancen von Menschen am anderen Ende der Welt. Der Unterschied zwischen Risiko von Gefahr hängt dabei ab von gesellschaftlich-kulturellen Definitionen und von realen Entwicklungen, aber reale Entwicklungen können durch die Art, wie man sie definiert, erheblich beeinflusst werden.

Nochmals: es sind zwei Dimensionen, die hier zusammen gedacht werden müssen. Auf der einen Seite die real zunehmende Komplexität der Welt, mehr Vernetzung, mehr Mobilität, mehr transnationale Kontakte, mehr Kommunikation, mehr Zerstörungspotential und mehr Verletzlichkeit. Auf der anderen Seite: ein gestiegenes Kontingenz- und Folgenbewusstein durch mehr Wissen, mehr Theorie, mehr Information und mehr globalen Input vor Ort. Die Dinge entwickeln sich nach einer Dynamik, die wir alle zwar befeuern, aber nicht steuern können.

Die ökonomische Theorie ist voll von solchen Paradoxien, man weiß, dass es sie gibt und ist ihnen trotzdem mehr oder weniger hilflos ausgeliefert. Die kollektiv irrationalen Folgen individuell rationalen Handelns entstehen oft dann, wenn sich individuelle Verhaltensweisen aufgrund der gegenseitigen Erwartungen von Alter und Ego verstärken. Diese Erwartungen können durchaus auch in technische Systeme eingebaut sein, wie etwa der letzte große Börsencrash an der New Yorker Börse in den Neunziger Jahren zeigte. Eine Reihe von automatischen, über Stop-Loss-Regeln ausgelöste Verkaufsorders im Computerhandel schaukelte sich hoch mit der Folge, dass alle anderen Programme ebenfalls verkauften, was zunächst den Kurs einzelner Papiere und dann den Index drückte, was dann wiederum mehr Verkäufe auslöste. Die Algorithmen, auf denen der computergestützte Handel basierte, waren vollkommen rational, aber in ihrer Vernetzung oder Interaktion erzeugten sie unvorhergesehene Effekte.

Man kann das ganze auf eine einfache Formel bringen: Je mehr ich weiß, je mehr Faktoren ich in Rechnung stelle, desto problematischer erscheint mir die Welt. Wissenschaft und Forschung, also die staatlich oder gesellschaftlich organisierte Produktion von Wissen führen insgesamt zu mehr Unsicherheit – oder wenn man es lieber religiös möchte: Selig sind die Armen im Geiste, denn sie haben diese Probleme nicht.

Lassen Sie mich noch kurz ein anderes Beispiel betrachten, an dem die Differenz von Risiko und Gefahr und die damit einhergehenden Probleme einer Paralyse durch Präventionsbemühungen in einem ganz alltäglichen Zusammenhang deutlich werden. Im Bereich der Drogenprävention tummeln sich viele Experten, die viel herausfinden und den Eltern ihr Wissen über einschlägige Organisationen andienen, die Tipps und Ratschläge für den richtigen Umgang mit ihren Kindern geben und Hinweise, wie man als Elternteil den möglichen Drogenkonsum der eigenen Sprösslinge frühzeitig feststellen kann. Dort ist dann zu lesen: Ist ihr Kind sehr zurückgezogen, dann kann das ein Ausdruck für Probleme sein, die zu Drogenkonsum führen. Wirkt ihr Kind aufgekratzt und hyperaktiv, so kann auch das ein Ausdruck von Drogenproblemen sein. Ihre Aufgabe als Eltern ist es, ihrem Kind die angemessene Umgebung zu schaffen. Sprechen Sie mit ihren Kind, aber drängen Sie es nicht zu sehr, das könnte Abwehrreaktionen hervorrufen, die kontraproduktiv sind und ihr Kind in eine Drogenkarriere treiben. Wenn man solche Broschüren liest, dann ist man am Ende verwirrter als vorher. Man kann dann noch in die Buchhandlung gehen und Ratgeber kaufen: wie erziehe ich mein Kind richtig und zu einem Leben ohne Drogen und am Ende steht man da, völlig paralysiert und tut – wenn man noch in der Lage ist, einen klaren Gedanken zu fassen – hoffentlich das, was einem, in der konkreten Situation als vernünftig erscheint.

Wenn man sich den Bereich der Ratgeberliteratur insgesamt ansieht, dann stellt man fest, dass er den gesamten Lebenszyklus umfasst: vom Flirtratgeber, über die Kindererziehung, den Scheidungsratgeber bis hin zu Büchern übers Sterben. Was hat das mit unserem Thema zu tun? Es lässt sich als Beleg für eine Verunsicherung und den Zerfall traditioneller Orientierungen lesen. Ganz im Sinne der Risikologik wird dem Publikum vermittelt, was es heute tun muss, um morgen nicht den Schaden zu haben.

Gerade der Bereich Familie und Erziehung ist ein klassisches Beispiel, an dem sich viel verdeutlichen lässt, was auch für die Sicherheitspolitik von Bedeutung ist. An der wachsenden Anzahl von Patchworkfamilien lassen sich Probleme demonstrieren, vor denen auch die Sicherheitspolitik steht. Solche Patchworks entstehen durch die serielle Monogamie: man heiratet, kriegt Kinder trennt sich, heiratet möglicherweise wieder, kriegt noch mal Kinder mit dem neuen Partner und kann – so scheint es – eine ziemliche Freiheit in der Gestaltung der eigenen

Lebensperspektive genießen. Gleichzeitig aber wächst mit der Entkoppelung des traditionellen Familiensystems auch die Abhängigkeit, und geht die Freiheit zurück. Versuchen Sie mal als alleinerziehender Vater mit einer neuen Lebensgefährtin, die ebenfalls Kinder hat, einen gemeinsamen Urlaub zu planen. Sie müssen dann die Urlaubspläne der Ex-Partner und ihrer neuen Lebensgefährten koordinieren, die ihrerseits wiederum Zeitpläne für den Urlaub haben, die dann wiederum abhängen von den Planungen ihrer Ex-Lebensgefährten. So entsteht ein dichtes Netz von Abhängigkeiten von Menschen, mit denen man persönlich gar nichts zu tun haben muss. Als Betroffener haben Sie zwar ein Handy und können alle Stake- und Shareholder des familiären Chaos zeitnah erreichen, aber das macht es nur noch schwieriger, denn die können auch Sie anrufen und mitteilen, dass die geplante Lösung doch nicht funktioniert.

Man kann sich an solchen relativ alltäglichen Beispielen verdeutlichen, wie sich sozusagen die Morphologie des Sozialen verändert, wie Dinge einerseits elastischer werden, wenn sich fest gefügte Traditionen auflösen, wie damit die individuellen Freiheitsgrade, aber auch der Entscheidungsdruck auf der einen Seite steigen, wie jedoch auf der anderen Seite die Unübersichtlichkeit zunimmt und die vermeintlich gewonnene Freiheit über notwendige Koordinationsmaßnahmen, die eine Folge weitreichender Vernetzung sind, wieder eingeschränkt wird. Jede Entscheidung ist riskant, sie kann Fernwirkungen haben, die im Augenblick des Entscheidens nicht zu überblicken sind und Dinge, die an ganz anderen Orten geschehen, können die Verhältnisse vor Ort beeinflussen.

Kleine Zwischenbilanz: Sicherheit ist ein diffuses Feld. Maßnahmen zur Erhöhung der Sicherheit erfordern mehr Wissen. Mehr Wissen führt dazu, dass ein größerer Bereich der Welt auf den Bildschirmen der Handlungsplanung erscheint und das heißt: die eigenen Entscheidungen werden im Hinblick auf zukünftige Ereignisse als riskant erfahren. Risikodenken aber kennt keine Stopregeln, sondern dehnt sich aus bis zur Erschöpfung der Ressourcen. Mit zunehmender Differenzierung steigt die Unsicherheit und es werden Maßnahmen getroffen, die sicherstellen sollen, dass die Dinge so sind wie sie sind und nicht anders. Diese Maßnahmen können sich ihrerseits wiederum selbst ad Absurdum führen.

Wie sich das damit verbundene Problem der Authentifizierung verschärft, lässt sich an einem einfachen Beispiel aus dem Alltag demonstrieren. Als die italienischen Winzer aus dem Chiantigebiet feststellten, dass unter dem Namen »Chianti« Wein angeboten wurde, der nicht aus der Region stammte, führten sie ein eigenes geschütztes Logo, den Gallo Nero, den schwarzen Hahn ein, der nur auf Flaschen angebracht werden durfte, die aus der Ursprungsregion kamen. Als auch dieser offensichtlich von anderen kopiert wurde, ergänzte man den »Gallo« um eine am Flaschenhals angebrachte Banderole, die belegen sollte, dass der regionale Ursprung des Weins kontrolliert wurde. Das DOC (Denominazione

Originale Controlata) auf dieser Banderole war der Ausweis dafür. Inzwischen wurde das DOC um ein »G« erweitert, das die Kontrolle »G«-arantieren soll.

Was bei solchen Prozessen zusehends entwertet wird, ist das individuelle Sensorium für Risiken und Gefahren. Die kulturell gewachsenen Fähigkeiten der Wetware verlieren in diesem Prozess an Bedeutung oder wie es die Sozialwissenschaft formuliert: wir begeben uns zusehends in die Hände abstrakter Systeme. Mit etwas geschick und einem Werkzeugkasten konnte man bei einem VW-Käfer noch alle technischen Probleme selbst beheben – wenn das nicht mehr ging, war der Wagen reif für den Schrotthändler. Fährt man heute mit seinem Auto in die Werkstatt, dann stöpselt der Mechaniker als erstes den Laptop an das Fahrzeug, um eine computergestützte Diagnose zu machen. Im Motorraum sind nur kleine schwarze Kästen, denen man nicht ansieht, ob sie funktionieren oder nicht, die man nicht reparieren, sondern nur austauschen kann.

Um Missverständnisse an dieser Stelle zu vermeiden: Die Prozesse, um die es hier geht, spielen sich sowohl in der äußeren Welt, als auch in den Köpfen der Menschen und in der Interaktion zwischen ihnen ab. Es steigt die subjektiv wahrgenommene Unsicherheit oder das Bewusstsein, dass alles auch ganz anders sein und sich jederzeit ändern kann. Es nimmt aber auch die reale Vernetzung und Unübersichtlichkeit der richtigen Welt zu. Das Problem ist, dass wir uns im Bereich der Sicherheitspolitik nicht auf die eine oder andere Seite schlagen können. Wir sehen was wir sehen und sehen nicht, was wir nicht sehen und vor allen Dingen wir wissen, dass wir das, was wir nicht sehen, nicht sehen. Und wir wissen oder vermuten oder befürchten, dass dort im Unsichtbaren die Gefahr lauern könnte! Das Risiko ist, dass wir vielleicht nicht hinschauen!

Nun kann man Sicherheitspolitik in zwei Richtungen verstehen, die ich als instrumentelle und als symbolische bezeichnen möchte. Symbolische Sicherheitspolitik wird auf der parlamentarisch-medialen Vorderbühne gemacht. Als Maggie Thatcher in England Anfang der Achtziger Jahre schlechte Umfragewerte hatte, begann sie den Falklandkrieg. Die vermeintliche Bedrohung von Schafherden auf britischem Territorium irgendwo im Atlantik auf die sie reagierte, ließ ihre Popularität steigen. Sie gewann die nächsten Wahlen. Auch der Film Wag the Dog, den einige von Ihnen vielleicht kennen, zeigt, wie dieser politisch-psychologische Mechanismus funktioniert. In der Sozialpsychologie gibt es die bekannte Regel: der projizierbare Außenfeind stärkt die Binnensolidarität. Politiker neigen dazu, Bedrohungen zu stilisieren und nach drastischen Maßnahmen zu rufen und der Bereich der Politik der Inneren Sicherheit ist eines der wenigen verbliebenen Politikfelder, auf denen die Politik noch den Eindruck erwecken kann, dass sie etwas bewirkt. Ein Großteil der Kompetenz ist in die EU abgewandert und die Macht global agierender ökonomischer Akteure gestaltet heute die ge-

sellschaftlichen Verhältnisse nachhaltiger als jede parlamentarische Politik und lässt den Nationalstaat alt aussehen.

Bei praktischer oder instrumenteller Sicherheitspolitik hingegen geht es vor allen Dingen darum, wem, was, in welchem Ausmaß zuzurechnen ist. Wer haftet? Wer zahlt? Wer ist im Schadensfall schuld? Da Schicksal und Zufall weitgehend ausgedient haben und die Sicherheitsbehörden bürokratisch organisiert sind, muss die Verantwortung für den Schadensfall entlang des Dienstwegs weitergereicht werden. Letztendlich sollte es immer möglich sein, einen Schuldigen zu finden: der Beamte, der etwas übersehen hat, der Abteilungsleiter, der eine Information nicht weitergeleitet hat, der politisch Verantwortliche, der die Mittel nicht zur Verfügung gestellt hat. Hier wird immer noch versucht, individuell zuzurechnen. Aber wenn man sich die Verhältnisse genauer betrachtet, dann zeigt sich, dass wir es, wie Ulrich Beck es einmal formulierte, mit »organisierter Unverantwortlichkeit« zu tun haben. Zurechnung wird ab einem bestimmten Grad der Komplexität und Reflexivität zur Fiktion und letztlich läuft alles vermutlich irgendwann darauf hinaus, dass ein jeder angehalten ist, sich alles selbst zuzurechnen und dann heißt es: willkommen in der Risikogesellschaft zweiter Ordnung!

Wenn alles unsicher, vielschichtig und vorläufig wird, wenn die Welt, in der wir leben nicht mehr »lesbar« ist, sondern hinter jeder Ecke das Risiko lauert, dann gewinnt Sicherheitspolitik eine neue Aufgabe. Sie greift zusehends zu Maßnahmen, die darauf zielen, den Zerfall der natürlichen Signifikanz oder wenn man so will, der traditionellen Ordnung der Welt zu kompensieren. Das beginnt bei der Regelanfrage für Bewerber im öffentlichen Dienst und endet bei der Einführung biometrischer Merkmale im Rahmen der Personenidentifikation. Die Logik dieser Politik ist die: man schafft eine Datenstruktur, die sicherheitsrelevante Informationen enthält, um etwa ein neueres Beispiel zu nehmen, über Mitgliedschaften in terrorverdächtigen Vereinigungen oder über Vorstrafen im Bereich Sexualdelikte und wendet diese Daten an, um Personen in Kategorien zu ordnen und Berechtigungen zu überprüfen. Trifft man auf eine Person, so kann man sie durch Rückgriff auf die Datenstruktur identifizieren, bzw. überprüfen. Solche Datenstrukturen sind für sich genommen nicht neu. Aber sie gewinnen zusehends an Bedeutung. Das tun sie deshalb, weil man mit den Bordmitteln der erfahrung und des gesunden Menschenverstands nicht mehr in der Lage ist, Menschen nach sicherheitsrelevanten Kriterien zu identifizieren. Wenn ich zu meiner Bankfiliale um die Ecke gehe, bei der ich seit Jahrzehnten Kunde bin, um einen Scheck einzulösen, dann brauche ich mich nicht auszuweisen. Tue ich das aber an einem anderen Ort, dann verlangt man eine Identifikation und diese wiederum muss möglichst so beschaffen sein, dass sie eine sichere und eindeutige Beziehung zwischen mir als physisch präsentem Wesen und meiner sozial dokumentierten Existenz als Person herstellt. Das ist das System der Kontrollen

durch Personaldokumente Chipkarten, Pin-Codes, Fingerabdrücke und neue Biometrie. Sie hat die zwei Seiten – Datenstruktur und Identifikationssystem und dient dazu Berechtigungen zu erteilen. Diese Politik operiert mehr oder weniger lautlos, ohne von der Öffentlichkeit groß wahrgenommen zu werden. Mit zunehmender Mobilität und Unübersichtlichkeit steigt die Nachfrage nach dieser Art von identifikatorischer Sicherheitspolitik. Üblicherweise sind die Nachfrager nach entsprechenden Dienstleistungen Organisationen, aber auch im Alltag wird sich vermutlich eine Art mundaner identifikatorischer Sicherheitspolitik verbreiten.

Der gesellschaftliche Nebeneffekt dieser Entwicklung ist, wie mein Kollege Aldo Legnaro gezeigt hat, eine Umkehr der Beweislast. Das heißt, ein jeder ist zunächst erst einmal verdächtig. Beispiele wären hier etwa die Massen-DNA-Tests im Rahmen der Fahndung nach Straftätern oder auch nur an die ganz gewöhnlichen Flughafenkontrollen. Es ist meine Aufgabe als Bürger nachzuweisen, wer ich bin und gegenüber den Zugangskontrolleuren oder Sicherheitsbehörden zu belegen, dass ich nichts Böses im Schilde führe.

Ihre Begründung zieht diese Art der Sicherheitspolitik aus der Anfälligkeit moderner Gesellschaften; der Unordnung ihrer sozialen Strukturen und der daraus gefolgerten Anfälligkeit für Störungen und Katastrophen. Sicherheit ist nicht mehr ein Zustand, der sich quasi naturwüchsig durch das traditionelle Handeln der Akteure ergibt, sondern Sicherheit muss aktiv hergestellt werden. In den Fokus gerät damit nicht die Abweichung, sondern die Normalität, oder wie Michel Foucault und Gilles Deleuze es formuliert haben: wir befinden uns im Übergang von der Disziplinargesellschaft zur Sicherheits- und Kontrollgesellschaft.

Der aktuelle traumatische Prototyp für solche Störungen der Normalität ist natürlich der 11. September. Aber schon der Philosoph Anders oder der Gesellschaftskritiker Traube haben in den fünfziger und sechziger Jahren des vergangenen Jahrhunderts warnend auf die Nebenfolgen der durch ihre technologische Entwicklung und soziale Differenzierung verletzlich werdenden Gesellschaften hingewiesen. Es setzt nach dieser Logik eine Entwicklung ein, die problematisch ist: Immer nachdem etwas passiert ist, wird die Sicherheitspolitik neu kalibriert, und zwar so, dass das, was passiert ist, in der Form möglichst nicht mehr geschehen kann. Man hofft, dass die Zukunft sich als eine Wiederholung der Vergangenheit darstellt, auf die man dann vorbereitet ist und deren katastrophische Folgen man durch rechtzeitiges Eingreifen verhindern kann. Unglücklicherweise ist das aber selten der Fall.

Ein sehr gutes Beispiel aus der jüngsten Vergangenheit, an dem man die Probleme dieser Politik zeigen kann ist die Kategorie des sogenannten Schläfers. Als Schläfer bezeichnete man jene terrorverdächtigen Figuren, die noch nichts unternommen hatten, die aber wie ein schlafendes Virus jederzeit zu tödlichen Ge-

fahren mutieren können. Im Bild des Schläfers kommt die ganze Problematik dieser Sicherheitspolitik zum Ausdruck: Man sucht etwas, dessen wesentliches Merkmal darin besteht, dass man es nicht sieht und nicht erkennt. Damit haben die professionell tätigen Akteure der Sicherheitspolitik ihre liebe Not. Es werden Dateien abgeglichen und Daten auf der Basis eines vorgegebenen Rasters verglichen, um solche Personen zu ermitteln, die möglicherweise in die Kategorie des Schläfers passen könnten.

Hier nun taucht wieder ein Problem auf, das uns bereits mehrmals begegnet ist: Wir sehen etwas, was wir gleichzeitig nicht sehen oder wie es im Englischen so treffend heißt, »seen but unnoticed.« Möglicherweise befindet sich eine Spur im Netz der Fahnder, aber sie nehmen sie nicht wahr und erkennen sie erst dann, wenn der Schläfer sozusagen aufwacht.

Auf der kulturell alltäglichen Ebene hat diese Konstellation ebenfalls Auswirkungen: Der Nachbar, den wir wahrnehmen als freundlich und zuvorkommend, kann ein Schläfer sein. Allgemein gesprochen wird unter diesen Bedingungen das natürliche Empfinden für Gefahr und Ordnung außer Kraft gesetzt. Der Mensch ist von Haus aus, sozusagen biologisch, mit der Fähigkeit ausgestattet, jene mit denen er alltäglichen Umgang pflegt, einzuschätzen. Psychologische Untersuchungen zeigen, dass mit dieser Intuition eine ganz gute Trefferquote erzielt. Wenn diese Fähigkeit infrage gestellt wird, weil beispielsweise neue Raster von Gefahr und Bedrohung vorgegeben werden, dann kann das im Extremfall zu einer pathologischen Blickverschiebung führen. Man verlässt sich dann nicht mehr auf Gefühl und Alltagswissen, das gemeinhin bei weitem ausreicht, um problematische Situationen zu meistern und Gefahren aus dem Weg zu gehen.

Die Umpolung der neuen Sicherheitspolitik von Gefahr auf Risiko – also auf einen reflexiven Blick nach dem Motto: ist das, was ich im trivialen Alltag heute tue und vor allen Dingen auch, was ich unterlasse, morgen vielleicht gefährlich – erodiert eine Tiefenschicht des kulturellen Bewusstseins, die man als ontologische Sicherheit bezeichnet hat. Das, was sich normalerweise ungefragt und ohne bewusstes Zutun abspielt, wird plötzlich infrage gestellt: Ist das Fleisch wirklich genießbar? Sind die Strahlungen des Handys krebserregend? Ist der türkischer Gemüsehändler ein Islamist? Wird in der Moschee um die Ecke ein neuer Terroranschlag vorbereitet? Kann ich man noch guten Gewissens U-Bahn fahren, nach Ägypten fliegen, in ein volles Fußballstadion gehen? All diese Fragen stellen sich erst dann, wenn die fraglos geltenden Routinen außer Kraft gesetzt sind. Und die Akteure des Alltags werden durch die umfassende Wahrnehmung der Sicherheitsmaßnahmen – Videokameras, Zugangskontrollen, Bodyscans, Taschenüberprüfungen, Ausweiskontrollen – fortlaufend daran erinnert, dass sie sich auf unsicherem Terrain bewegen und sie müssen dabei, wie ich vorhin bereits sagte, permanent ihre Unschuld beweisen.

Glücklicherweise halten entsprechende Schübe von kollektiver Paranoia meist nur eine kurze Zeit vor. Die Mediengesellschaft braucht immer wieder neue Ereignisse, die sie in die Schlagzeilen hievt. Aber es würde mich nicht verwundern, wenn die langfristigen Folgen zu einer strukturellen Verunsicherung oder zu »ontologischer Unsicherheit« führen.

Nun kann man im Angesicht des hier in grober Stilisierung entwickelten Szenarios versuchen, eine Bilanz zu ziehen. Was sind die Kosten und was ist der mögliche Nutzen einer sich immer weiter ausdehnenden Sicherheitspolitik, einer Strategie die aufgrund der Risikologik jeden erst mal bis zum technisch-bürokratischen Beweis des Gegenteils für verdächtig hält.

Für die Anbieter von Sicherheitsdienstleistungen, von Soft-, Hard- und Wetware ist diese Situation geradezu ideal: das Sicherheitsdenken dehnt sich aus und die Nachfrage steigt, je mehr angeboten wird. Die Nachfrage nach zertifizierenden und authentifizierenden Technologien wird im Angesicht der zunehmenden Unlesbarkeit der Welt steigen. ISO und DIN werden wachsen. An dieser Front stehen also rosige Zeiten bevor.

Auf der anderen Seite kann man fragen, ob durch die praktizierten Sicherheitsmaßnahmen in nennenswertem Umfang Schäden verhindert worden sind? Diese Frage ist aus den oben erwähnten Gründen schwer zu beantworten. Ein verhinderter Terroranschlag ist ein eigenartiges Unereignis, eine nicht explodierte Bombe ist – zynisch formuliert – medial von minderer Bedeutung. Der psychosoziale Modus der Bedrohung jedoch ist etwas, das wie Feuchtigkeit an den Wänden des Alltagslebens hochzieht. Der Alltag wird undurchsichtig, verliert an Kontur, Verunsicherung – die dann durch mehr und dichtere Kontrollen wieder beseitigt werden soll – macht sich breit.

Man sollte diesen politisch-psychologischen Flurschaden mit in Rechnung stellen, wenn man über Sicherheitspolitik nachdenkt. Letztlich sind in der Logik derjenigen, die mit ihren aktuell massiven punktuellen Angriffen zur Hochkonjunktur der Sicherheitspolitik beigetragen haben, die realen Schäden gleichsam nur die Trägersubstanz, mit deren Hilfe sie Angst und Schrecken verbreiten wollen. Und daher sollte man sich, wenn es um eine rationale Sicherheitspolitik geht, immer auch fragen, ob die ergriffenen Maßnahmen nicht eher das Gegenteil von dem bewirken, was sie versprechen. Sicherheit als realer Zustand ist nur dann zu haben, wenn er auch als symbolisches Gut existiert, oder anders formuliert: objektive und subjektive Sicherheit bedingen einander und es besteht immer die Gefahr, dass wir durch ein mehr an Investitionen in vermeintlich objektive Sicherheit zugleich auch subjektive Unsicherheit produzieren.