EUROPÄISCHE AKADEMIE
zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen
Bad Neuenahr-Ahrweiler GmbH
Direktor: Professor Dr. Dr. h. c. Carl Friedrich Gethmann

GRAUE REIHE · NR. 49 · JUNI 2009

Globale Fernerkundungssysteme und Sicherheit

Beiträge durch neue Sicherheitsdienstleistungen?

Stephan Lingner, Wolfgang Rathgeber (Hrsg.)

EUROPÄISCHE AKADEMIE
zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen
Bad Neuenahr-Ahrweiler GmbH
Direktor: Professor Dr. Dr. h. c. Carl Friedrich Gethmann

GRAUE REIHE · NR. 49 · JUNI 2009

Globale Fernerkundungssysteme und Sicherheit

Beiträge durch neue Sicherheitsdienstleistungen?

Stephan Lingner, Wolfgang Rathgeber (Hrsg.)

Herausgeber

EUROPÄISCHE AKADEMIE
zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen
Bad Neuenahr-Ahrweiler GmbH
Direktor: Professor Dr. Dr. h. c. Carl Friedrich Gethmann

Die Schriften der „Graue Reihe" umfassen aktuelle Materialien und Dokumentationen, die von den Wissenschaftlern der Europäischen Akademie zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen Bad Neuenahr-Ahrweiler GmbH laufend erarbeitet werden. Die Publikationen der „Graue Reihe" werden als Manuskripte gedruckt und erscheinen in loser Folge im Selbstverlag der Europäischen Akademie. Sie können über die Europäische Akademie auf schriftliche Anfrage bezogen und auf der Homepage der Europäischen Akademie (www.ea-aw.de) heruntergeladen werden.

Europäische Akademie
zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen
Bad Neuenahr-Ahrweiler GmbH

Wilhelmstraße 56, 53474 Bad Neuenahr-Ahrweiler
Tel. +49 (0) 26 41 973-300, Fax +49 (0) 26 41 973-320
E-mail: europaeische.akademie@ea-aw.de
Homepage: www.ea-aw.de

Direktor
Professor Dr. Dr. h.c. Carl Friedrich Gethmann (V.i.S.d.P.)

ISSN
1435-487 X

Redaktion
Katharina Mader, M.A.

Layout und Druck
Lambertz Druck, Köln · Bornheim, www.lambertzdruck.de

Vorwort

Weltweit haben sich in den vergangenen Jahren Sicherheitslage und Sicherheitsempfinden signifikant verändert. Zahlreiche Institutionen setzen sich nun mit den Problemen ziviler Sicherheit auseinander, da deren Aufrechterhaltung als Grundvoraussetzung für ein geordnetes gesellschaftliches Leben bei Ermöglichung weitgehender Freiheit des Einzelnen angesehen wird. Das bundesdeutsche Sicherheitsforschungsprogramm formuliert hierzu:

> Die Versorgungsnetze als Lebensnerven der Gesellschaft können trotz robuster Technik schon durch kleine Störungen ausfallen. Kleine terroristisch oder kriminell motivierte Gruppen können sich große Wirkung verschaffen und erhebliche Schäden bewirken. Die globale Mobilität erleichtert die Verbreitung von Gefahren. Naturkatastrophen und technische Unfälle können in einer dicht vernetzten Welt große Folgeschäden auslösen.[1]

Der vorliegende Band greift das Thema unter dem Blickwinkel der Möglichkeiten und Grenzen neuer und geplanter Systeme zur Erdfernerkundung aus dem Weltall auf, die diese für die zivile Sicherheit bieten. Dabei gilt es, die Vor- und Nachteile der Gewinnung weltraumgestützter Informationen auszuloten, die einerseits durch flächenhafte Abdeckung und frühzeitige Erkennung und andererseits durch Auflösungslimitierungen und Validierungs- sowie Akzeptanzfragen gekennzeichnet sind. Die folgenden Beiträge sind Ergebnisse einer wissenschaftlichen Konferenz mit dem Titel „Globale Fernerkundungssysteme und Sicherheit" der Europäischen Akademie GmbH und des European Space Policy Institute (ESPI) am 9./10. Oktober 2008 in Wien. Die Konferenz wurde vom Deutschen Zentrum für Luft- und Raumfahrt e.V. (DLR) unterstützt.[2]

Bad Neuenahr-Ahrweiler/Wien, Juni 2009

Stephan Lingner
Europäische Akademie GmbH, Bad Neuenahr-Ahrweiler

Wolfgang Rathgeber
European Space Policy Institute, Wien

---

[1] Vgl. http://www.bmbf.de/de/6293.php (2.2.2009).

[2] Neben den Autoren beteiligten sich Dr. Lothar Beckel (GEOSPACE International GmbH, Salzburg), Staatsrat Dr. Heiner Heseler (Bremen), Rüdiger Koppe (EADS-Astrium GmbH, Taufkirchen) sowie Dr. Nicola Rohner-Willsch (DLR, Köln-Porz) an der Konferenz.

Inhalt

Einführung

Stephan Lingner und Wolfgang Rathgeber

Die Ära der weltraumgestützten Erdfernerkundung begann nur wenige Jahre nach dem Start der ersten Raumsonde Sputnik 1. Seither stellten die Raumfahrtnationen eine Vielzahl von Satelliten für Zwecke der Erkundung, Navigation und Kommunikation in den Dienst, die unseren Alltag und unser Bild der Erde nachhaltig verändert haben. Mittlerweile ermöglichen globale Erdbeobachtungssysteme eine permanente Ortung von Fahrzeugen, Personen, Landschafts- und Infrastrukturen. Die europäische Galileo-Initiative soll in wenigen Jahren einen weiteren Leistungszuwachs von Navigationsdiensten für die gewerbliche und private Nutzung ermöglichen. Darüber hinaus verspricht das europäische GMES-System[1] potentiellen Nutzern eine hochauflösende, flächendeckende Erdbeobachtung u.a. für Zwecke des Zivilschutzes, der Krisenprävention und der Stadtplanung. Zusätzlich wird es die Möglichkeiten der Navigationsdienste durch Einbindung geographischer Flächeninformation wesentlich erweitern.

Angesichts „realer" und empfundener Bedrohungen durch umweltbedingte und humanitäre Krisen sowie durch Gefährdungen der inneren und äußeren Sicherheit mehren sich seitens der Gesellschaft Erwartungen an leistungsfähige Überwachungsdienstleistungen. Diese Erwartungen an entsprechende Informationsangebote sind allerdings vor dem Hintergrund offener Fragen zu reflektieren. Hierzu gehört die realistische Beurteilung der zeitlich-räumlichen Verfügbarkeit, der Qualität und Authentizität sowie der Validität entsprechender Daten. Ihre Verbreitung wirft darüber hinaus Fragen des Schutzes der persönlichen Privatsphäre (z.B. bei Erfassung von Bewegungsdaten), des Schutzes sensibler Orte oder Einrichtungen, der rechtlichen Belastbarkeit fernerkundlicher Zuschreibungen (z.B. für Zwecke der Verifikation) sowie der Haftung für Ausfälle und Fehler entsprechender Informationsdienstleistungen auf. Angesichts der Risikolagen und verbleibender Unsicherheiten spielen Probleme des angemessenen Handelns unter Ungewissheit eine bedeutende Rolle.

Schließlich ist zu skizzieren, unter welchen Bedingungen sich auf Behörden, Unternehmen oder Einzelpersonen zugeschnittene Beratungsdienste an den Schnittstel-

[1] GMES = Global Monitoring for Environment and Security.

len zwischen Dienstleistern und -nutzern sicherheitsrelevanter Fernerkundungsdaten etablieren können. Für die Abschätzung des Zugewinns an praktisch verwertbarer Geoinformation ist zu erörtern, welche spezifischen Erwartungen und Anforderungen sich für die Nutzer einer modernen Sicherheitsberatung ergeben.

Dr. rer. nat. Stephan Lingner, Dipl.-Geol.
Europäische Akademie GmbH, Bad Neuenahr-Ahrweiler
Stellvertreter des Direktors
Arbeitsschwerpunkte: Technikfolgenbeurteilung, Umwelt- und Raumfahrtfragen

Dr.-Ing. Wolfgang Rathgeber
European Space Policy Institute (ESPI), Wien
Wissenschaftlicher Mitarbeiter
Arbeitsschwerpunkte: Raumfahrt und Sicherheit

NEUE FERNERKUNDUNGSPOTENTIALE FÜR DIE ZIVILE SICHERHEIT

Das europäische GMES-Programm und seine Relevanz für Sicherheitsaspekte in Europa

Josef Aschbacher und Thomas Beer

1 GMES bei der ESA-Ministerratskonferenz

Am 25./26. November 2008 entschieden die Ressortminister von 18 Mitgliedsstaaten der Europäischen Weltraumagentur ESA und Kanada über das 2. Segment von GMES. Sie genehmigten 831 Millionen Euro für die Entwicklung des Programms „Global Monitoring for Environment and Security". Dieser Beitrag folgt einer bereits sehr erfolgreichen Zeichnung von Segment 1 des Programms in Höhe von 758 Millionen Euro. Zusätzlich leistete die Europäische Kommission einen Beitrag von 620 Millionen Euro. Damit hat das Weltraumsegment von GMES einen finanziellen Rahmen von etwa 2.3 Milliarden Euro, was den Aufbau der vollen operationellen Fähigkeiten (FOC) der Weltraumkomponente von GMES bis ca. 2017 sichert.

GMES umfasst Dienste im Zusammenhang mit Umweltfragen, Klimawandel, Ressourcenmanagement, Sicherheit und anderen globalen Anliegen. Die Dienste bauen hauptsächlich auf satellitengestützten und vor Ort gemessenen Erdbeobachtungs-, aber auch sozioökonomischen Daten auf. Diese werden so verarbeitet, dass sie allen Bürgern in Europa nachhaltig als gebrauchsfertige Informationen zur Verfügung stehen.

2 GMES-Forum in Lille

Im Rahmen der französischen EU-Ratspräsidentschaft fand am 16./17. September 2008 in der nordfranzösischen Stadt Lille das „Forum GMES 2008" statt. Auch das Lille-Forum war ein weiterer Meilenstein auf dem Weg zu einem operationellen GMES-System: Es diente als Plattform zur Demonstrierung erster vorooperationeller GMES-Dienste zum Nutzen der maritimen Umwelt und der Atmosphäre, der Landnutzung und der humanitären Hilfe. Das Forum zeigte aber auch ein deutliches Interesse von Besuchern aus dem Bereich „Sicherheit". Ihre Fragen waren vor allem darauf gerichtet, ob, wie und wann GMES auch für ihre Belange zur Verfügung stehen werde.

3 Ziele von GMES

GMES ist neben GALILEO das zweite große „Flaggschiff“ der europäischen Raumfahrtpolitik. Während sich GALILEO auf die satellitengestützte Navigation und Ortsbestimmung konzentriert, dient GMES der Erfüllung von zwei politischen Hauptanforderungen für Europa in Bezug auf weltraumgestützte Informationsdienste: Erstens wird GMES politischen Entscheidungsträgern einen unabhängigen Informationszugang gewähren, um die Umwelt- und Sicherheitspolitik auf europäischer und nationaler Ebene voranzutreiben. Zweitens bündelt GMES die europäischen Beiträge zum internationalen System der Erdbeobachtungssysteme (GEOSS), welches auf der Grundlage des auf dem 3. Erdbeobachtungsgipfel im Februar 2005 in Brüssel angenommenen Zehn-Jahres-Umsetzungsplans eingeleitet wurde. Nach derzeitigem Planungsstand soll GMES mit dem erfolgreichen Start und In-Orbit-Test des ersten speziellen GMES-Satelliten („Sentinel 1“) im Jahr 2012 operationellen Status erlangen.

Die Europäische Kommission, handelnd für die EU, und die ESA entwickeln GMES gemeinsam, wobei die ESA für das Management und die Koordination der GMES-Weltraumkomponente verantwortlich ist. Diese wird als ein fakultatives ESA-Programm implementiert und, wie im ESA-/EG-Rahmenabkommen von 2004 vorgesehen, gemeinsam mit der EU-Kommission finanziert. GMES ist damit ein weiterer Beleg für die enge Zusammenarbeit zwischen ESA und EU, welche mit der Unterzeichnung des Rahmenabkommens formalisiert worden ist.

Auf Seiten der EU-Kommission wurde am 12. November 2008 die offizielle Mitteilung „Global Monitoring for Environment and Security: we care for a safer planet“ herausgegeben. In diesem Dokument wird u.a. der Fahrplan zu einem operationellen GMES-Programm aufgezeigt, welches im Wesentlichen von der EU-Kommission finanziert werden wird.

Die Gesamtarchitektur von GMES umfasst drei Hauptbestandteile: die Dienste, die weltraumgestützten und die in-situ Beobachtungen. GMES ist nutzerorientiert und die verschiedenen Dienste von GMES erzeugen den wirtschaftlichen und gesellschaftlichen Nutzen ausschließlich aus dem Blickwinkel derjenigen, welche die Dienste tatsächlich in Gebrauch nehmen. Zwei Arten von Diensten sind zu unterscheiden: Die sogenannten GMES-Kerndienste richten sich per Definition an institutionelle Akteure auf der EU-Ebene. Sie unterstützen die Entscheidungsträ-

ger gezielt bei der Erarbeitung, Umsetzung oder Überwachung gemeinsamer europäischer Politiken und Beiträgen Europas zu internationalen Verpflichtungen. Die Kerndienste werden z. Zt. von der EU, mit Unterstützung der ESA, aufgebaut und sollen von der EU auch langfristig finanziert werden. Aus der Vielzahl der möglichen Anwendungen werden aktuell die folgenden Kerndienste entwickelt: Beobachtung des Landes (Land Monitoring Core Service), Beobachtung der Meere und Küsten (Ocean Monitoring Core Service) und Einsatz für schnelle Kartierung in Notfällen (Emergency Response Core Service). In Ergänzung dazu wurden noch zwei weitere Kern-Dienste, nämlich „Atmosphäre" sowie „Sicherheit", aufgenommen. Seit 2002 hat die ESA im Rahmen ihres GMES-Service-Element-Programms eine Reihe von vor-operationellen Diensten entwickelt, welche nun in die von der EU-Kommission verantworteten Kerndienste eingespeist werden. Anlässlich des eingangs erwähnten GMES-Forums in Lille wurden die ersten dieser vor-operationellen Kerndienste der Öffentlichkeit präsentiert.

Neben diesen Kerndiensten werden die sogenannten „Downstream"-Dienste entwickelt, die entweder aus den Kerndiensten oder direkt aus den Daten der GMES-Beobachtungssysteme abgeleitet werden. So können z.B. aus dem „Land Monitoring Core Service" nutzerspezifische Informationen entwickelt werden, die für Firmen im Nahrungsmittel- und Rohstoffbereich wichtig sein könnten. Solche „Downstream"-Dienste sollen somit bewusst einen regionalen, lokalen und auch kommerziellen Markt ansprechen.

4 Die GMES-Weltraumkomponente

Die unter der Verantwortung der ESA stehende Weltraumkomponente umfasst das Weltraumsegment und das dazugehörige Bodensegment, einschließlich der Koordination des Zugangs zu nationalen, zu EUMETSAT- (der in Darmstadt ansässigen europäischen Organisation für Wettersatelliten) und zu anderen von Dritten finanzierten Erdbeobachtungsmissionen.

Damit das GMES-Programm seine Aufgaben erfüllen kann, müssen die Daten aus dem Orbit kontinuierlich fließen. Das ist mit den z. Zt. im All befindlichen Satelliten nicht gewährleistet, es ist kein unmittelbarer Ersatz bei Ausfall oder Erreichen der Lebensdauer vorgesehen. Deshalb werden bei GMES stets mehrere spezielle GMES-Satelliten gleichzeitig im All sein, die ausschließlich der Erdbeobachtung dienen.

Die folgenden Missionskonzepte wurden für die derzeit fünf geplanten Sentinel- („Wächter-“) Satelliten der GMES-Weltraumkomponente festgelegt:

- Sentinel 1: eine interferometrische Radarmission im C-Band; für wetter-unabhängige Tag-/Nacht-Anwendungen; geplanter Start des ersten von zwei Sentinel-1: 2012;
- Sentinel 2: eine Mission mit multispektralen, optischen Abbildungsgeräten; geplanter Start des ersten von zwei Sentinel-2: 2013;
- Sentinel 3: eine Mission mit einem Altimeter sowie Radiometern im optischen und Infrarotbereich zur Beobachtung der Meeres- und Landoberflächen; geplanter Start des ersten von zwei Sentinel-3: 2013;
- Sentinel 4: Mission zur Beobachtung der Erdatmosphäre aus der geostationären Umlaufbahn; geplant für 2017;
- Sentinel 5: Mission zur Beobachtung der Erdatmosphäre aus der polaren Umlaufbahn; geplant für 2019.

Im Gegensatz zu den Sentinels 1, 2 und 3 sind die „Wächter“ 4 und 5 keine eigenständigen Satelliten, sondern Instrumentenpakete, die auf zwei Wettersatelliten von EUMETSAT mitfliegen werden. Jedes dieser Missionskonzepte ist auf einen spezifischen Erdbeobachtungsdatenstrom ausgerichtet, der zur Deckung des Nutzerbedarfs an entsprechenden Diensten und Informationen erforderlich ist.

Die Sentinels sind aber, wie bereits erwähnt, nicht die einzigen im Weltraum stationierten „Zuträger“ für die GMES-Dienste. Für GMES ist entscheidend, die bereits in vielen europäischen Ländern bestehenden und geplanten Datenerfassungssysteme vielfältigster Art miteinander zu verknüpfen und die Aktivitäten zu bündeln. Demzufolge wird sich GMES auf eine Phalanx von nationalen, EUMETSAT- und Drittmissionen stützen können, welche als sogenannte „Contributing Missions“ einen Teil ihrer Kapazitäten für GMES zur Verfügung stellen werden. Als Kandidaten für diese Art von Mission gelten auch die deutschen Satellitensysteme Terrasar-X, RapidEye und EnMap. Rein militärische Satelliten wie z. B. der deutsche SarLupe gehören nicht zu dem Portfolio dieser Missionen, wohl aber dual-use-Systeme wie das französische Pleiades oder die italienischen Cosmo-Skymed Satelliten. Im Rahmen ihrer Gesamtzuständigkeit für die Weltraumkomponente, einschließlich der „Contributing Missions“, ist die ESA für die Verhandlung der Datenüberlassungsverträge mit den entsprechenden Satelliten-Betreibern zuständig.

5 GMES im sicherheitspolischen Umfeld

Um die potentielle Bedeutung von GMES für die Bereiche Sicherheit und Verteidigung zu ermessen, bedarf es eines Blickes auf die aktuelle sicherheitspolitische Situation Europas. Diese hat sich im Laufe der vergangenen Jahre erheblich fortentwickelt. Europe sieht sich heute neuen Bedrohungen gegenüber, welche in unterschiedlichen Erscheinungsformen auftreten und schwer vorherzusagen sind. Gleichzeitig beginnt die Trennlinie zwischen ziviler und militärischer Verantwortlichkeit zu verschwimmen und der Begriff „Sicherheit" in unterschiedlichen Bereichen Anwendung zu finden. Dies spiegelt sich auch in den vier relevanten Strategiedokumenten mit Einfluss auf die Europäische Sicherheit und Verteidigung unter Einbezug des Weltraums wider:

Die Verknüpfung von Raumfahrt- und Sicherheitspolitik entspricht den grundlegenden Forderungen der „Europäischen Sicherheitsstrategie" (ESS) vom Dezember 2003. Die Schlussfolgerungen der vom EU-Rat verabschiedeten ESS beruhen auf der Annahme, dass Sicherheit und Verteidigung der EU und ihrer Mitgliedsländer künftig nur in dem Maße zu gewährleisten sind, in dem es gelingt, die technisch-industriellen Kapazitäten Europas zur Lösung sicherheitspolitischer Aufgaben zu mobilisieren. Art und Umfang dieser Aufgaben hängen mit dem erweiterten Sicherheitsbegriff zusammen, auf den sich die Europäische Sicherheits-und Verteidigungspolitik (ESVP) stützt und der im Wesentlichen auf die Petersberg-Erklärung des WEU-Ministerrats aus dem Jahre 1992 zurückgeht. Er umfasst den Schutz der Bürger und der politisch-gesellschaftlichen Infrastrukturen Europas vor jenen Bedrohungen, gegen die sich die ESS in ihren Grundzügen richtet: Terrorismus, die Verbreitung von Massenvernichtungswaffen, internationale Kriminalität und der Verfall der staatlichen Autorität in Bürgerkriegsregionen. Damit stellen sich der ESS zahlreiche und höchst unterschiedliche Aufgaben der zivilen und militärischen, der inneren und der internationalen Sicherheit sowie der Katastrophenhilfe.

Das nachfolgende EU „Military Headline Goal 2010" vom Juni 2004 beginnt die Forderungen der ESS umzusetzen und fordert die EU-Mitgliedsstaaten auf, „… (to) be able by 2010 to respond with rapid and decisive action applying a fully coherent approach to the whole spectrum of crisis management operations covered by the Treaty of the European Union". Synergien von zivilen und militärischen Fähigkeiten werden in diesem Dokument bereits ausdrücklich gefordert. Der Einbezug des Weltraums in diese Bemühungen um die Implementierung der ESS

ließ nicht lange auf sich warten: Im November 2004 verabschiedete der EU-Rat die „European Space Policy: ESDP and Space“ als Richtlinie für die Koordination aller Aktivitäten der EU-Mitgliedsstaaten hinsichtlich der Nutzung des Weltraums für die zivilen und militärischen Zwecke der ESVP. GMES wird hier bereits als Beispiel für ein System erwähnt, welches sicherheitsrelevante Ziele in ein ziviles Raumfahrtprogramm integriert. Die in diesem Dokument enthaltene Forderung an die EU-Mitgliedsstaaten, eine umfassende (nicht nur der ESVP gewidmete) Europäische Weltraumpolitik zu beschließen, welche zivile als auch militärische Komponenten in Betracht zieht, wurde im Mai 2007 erfüllt: Im Rahmen der 4. Sitzung des gemeinsam von der EU-Kommission und der ESA ins Leben gerufenen „Weltraum-Rates“ wurde die „Europäische Weltraum-Politik“ (EWP) beschlossen. Diese bezieht ausdrücklich Anwendungen aus dem Verteidigungs- und Sicherheitsbereich mit ein, um die Synergien zwischen militärischen und zivilen Weltraumprogrammen zu verstärken.

Damit die Investitionen effizienter werden, geht es dabei insbesondere um die Interoperabilität dieser Systeme, z. B. durch Vermeidung von doppelten Entwicklungskosten im militärischen und zivilen Bereich. Die EWP enthält aber nicht nur konkrete Hinweise auf die Gemeinsamkeiten von zivilen und militärischen Anwendungen, sie unterstreicht im Kapitel „Sicherheit und Verteidigung“ auch die potentielle Bedeutung von GMES für militärische Zwecke: „Many civilian programmes have a multiple-use capacity and planned systems such as GALILEO and GMES may have military users“.

6 Die Rolle der ESA auf dem Gebiet der Sicherheit innerhalb von GMES

Die Mitarbeit der ESA in Programmen mit „dual-use“-Charakter wie GMES war nicht immer unstrittig. Das Gründungsübereinkommen der ESA verpflichtet diese in Art. II auf den Zweck, „die Zusammenarbeit europäischer Staaten *für ausschließlich friedliche Zwecke* auf dem Gebiet der Weltraumforschung [...] sicherzustellen“. Etwaige Zweifel an der rechtlichen Befugnis der ESA, an „dual-use“-Programmen teilzunehmen, wurden in 2003 mit der Akzeptanz der international deutlich vorherrschenden völkerrechtlichen Interpretation von „friedlicher Zweck“ durch die ESA-Mitgliedsstaaten ausgeräumt (verboten sind „aggressive“ Tätigkeiten, nicht aber „militärische“).

Diese rechtliche Bewertung der ESA-Statuten beinhaltet, dass die Konvention keineswegs der ESA verbietet, an Weltraumprogrammen mit ausdrücklicher Ausrichtung auf Sicherheit und Verteidigung mitzuwirken. In derselben Entscheidung wurde auch das wichtige Potential der ESA im Hinblick auf eine potentielle Unterstützung von „security"-Aktivitäten unterstrichen, beruhend auf der jahrzehntelangen Erfahrung der ESA in der Konzipierung und Umsetzung komplexer Satellitenprogramme und Forschungsmissionen. Damit war die Grundlage für eine engere Einbeziehung der ESA in „dual use"-Aktivitäten gelegt.

In der Zwischenzeit hat die ESA auch den notwendigen regulatorischen Rahmen geschaffen, der ihr die Mitarbeit an Projekten mit Sicherheitsbezügen erlaubt. Dazu zählt ein Sicherheitsabkommen mit dem Rat der EU, welches den Austausch von eingestuften Dokumenten erlaubt. Schließlich befindet sich die ESA nun auch in einem Dialog mit allen wichtigen Akteuren innerhalb der Europäischen Sicherheitsdebatte, wie z.B den verschiedenen EU-Organen und -Agenturen (Rat, Kommission, Europäisches Satellitenzentrum, Europäische Verteidigungs-Agentur), aber auch mit NATO und WEU. Damit erfüllt die ESA gleichzeitig eine Forderung der EWP, welche zu einem „strukturierten Dialog" aller relevanten Teilnehmer im Bereich „security and defence" aufruft.

7 Die potentielle Rolle von GMES im Bereich Sicherheit

Im März 2007 fanden erste, vom Rat der EU initiierte Diskussionen über mögliche Beiträge von GMES-Diensten zum Nutzen der zivilen und militärischen Komponente der ESVP statt. Diese und nachfolgende Konsultationen zwischen den relevanten EU-Akteuren im Bereich Sicherheit und Verteidigung führten zu drei wesentlichen Schlussfolgerungen:

a) Militärische Nutzer von GMES sollen die gleichen Rechte wie die zivilen Nutzer der GMES-Dienste haben, unabhängig davon, dass GMES weiterhin als ein ziviles System unter ziviler Kontrolle gilt;
b) Um diese Rechte wirkungsvoll geltend zu machen, benötigt die militärische Nutzerfamilie eine der Sensitivität ihrer Daten angepasste GMES-Datenpolitik;
c) Militärische Nutzer haben spezielle, von den zivilen Nutzern unterschiedliche Anforderungen, welche die Schaffung von speziellen GMES-Diensten rechtfertigen können.

Darauf aufbauend wurden die folgenden drei, für die EU-Politik relevanten Bereiche identifiziert, die von GMES-Diensten profitieren können:

7.1 Grenzüberwachung

GMES-Dienste können durch die Lieferung satellitengestützten Kartenmaterials und durch satellitengestützte Beobachtung zu einer Verbesserung der weiträumigen Überwachung von Landesgrenzen beitragen. Die Verhinderung unerlaubter Grenzübertritte und grenzüberschreitender Kriminalität sind die beiden wesentlichen Ziele dieser Überwachung. Unter diesem Blickwinkel hat die EU-Kommission entschieden, ihr 2008 ins Leben gerufene Projekt EUROSUR (European Border Surveillance System) um die GMES-Komponente zu erweitern. GMES soll diese Art der Überwachung noch effektiver gestalten.

Auch die ESA ist an diesen Arbeiten beteiligt: Das dem GMES-Service-Element-Programm zugeordnete Projekt MARISS ist speziell der Meeresüberwachung gewidmet und soll grenzüberschreitenden Waffen-, Menschen- und Drogenschmuggel verhindern. Dieses Projekt wird in Zusammenarbeit mit der Europäischen Grenzschutzagentur FRONTEX, der European Maritime Safety Agency EMSA, nationalen Marinekommandos und NATO-Institutionen implementiert. Ein weiteres aktuelles ESA Projekt betrifft das „Dual use European Security IR Element“ (DESIRE), welches die Entwicklung eines hochauflösenden Sensors im Infrarot-Bereich zum Gegenstand hat und speziell für die Grenzüberwachung eingesetzt werden könnte. Schließlich wird auch das von der ESA finanzierte GMES-Service-Element, das Projekt RESPOND, zur schnellen Verfügbarmachung von Kartenmaterial in diesem Bereich einen wichtigen Beitrag leisten.

7.2 See-Überwachung

Mit der Verabschiedung einer „Integrated Maritime Policy for the European Union“ („Blaues Buch“) hat die EU-Kommission im Jahre 2007 die Notwendigkeit einer kohärenten Überwachung der Küstengewässer, der offenen See und der Ozeane begründet. Ziel dieser Überwachung ist die allgemeine Sicherheit in den für die EU relevanten Seegebieten, aber auch Umweltschutz und Sicherheit der Navigation. GMES kann einen wesentlichen Beitrag zur Umsetzung dieser Politik leisten, welche sowohl zivilen als auch militärischen Zwecken dienen soll.

See-Überwachung aus der Sicht von Verteidigung und Sicherheit ist Gegenstand eines aktuellen Arbeitsprojekts der Europäischen Verteidigungs-Agentur (EDA), MARSUR (Maritime Surveillance). In diesem Rahmen hat die EDA im Frühjahr 2008 ein „Food-for-Thought" Papier mit konkreten Anforderungen für eine Nutzung von GMES durch MARSUR vorgelegt. Neben MARSUR wird auch ESAs MARISS Projekt an der Umsetzung der im „Blauen Buch" enthaltenen Empfehlungen mitwirken.

7.3 Unterstützung der Außenbeziehungen der EU

Wie zuletzt in einer Entschließung des EU-Rats vom 29. September 2008 zur Weiterentwicklung der europäischen Raumfahrtpolitik betont, kann die Raumfahrt einen bedeutenden Beitrag zur GASP/ESVP, einschließlich der Petersberg-Aufgaben, und folglich zur Sicherheit der europäischen Bürger leisten. Europa müsse in der Lage sein, die Nichteinhaltung internationaler Verträge und Verpflichtungen aufzudecken, welche ein zentrales Instrument zur Sicherung und Förderung der europäischen Werte sind. Die Entschließung unterstreicht, dass GMES sich auf einige Beobachtungs-Kapazitäten mit doppeltem Verwendungszweck (dual use) stützt, welche für sicherheitsrelevante Anwendungen von Bedeutung sind:

- GMES bietet das gesamte Arsenal der technischen Bildaufzeichnung, das auch von der klassischen militärischen Aufklärung genutzt werden kann;
- Der Dauerbetrieb des GMES-Weltraumsegments eignet sich insbesondere zu militärischen und sicherheitspolitischen Überwachungsaufgaben, etwa zur Verifikation von Rüstungskontrollverträgen;
- GMES deckt die gesamte Erdoberfläche ab;
- Der Betrieb des Raumsegments ist keinerlei politischen und geographischen Grenzen oder Hindernissen unterworfen, weil er außerhalb nationaler Jurisdiktion erfolgt.

GMES-Daten eignen sich somit vorzüglich zur Planung, Vorbereitung und Durchführung von Krisen- und Konfliktseinsätzen im Rahmen der GASP/ESVP.

In ihrem 7. Rahmenprogramm hat die EU-Kommission bereits entsprechende Aktivitäten lanciert. Ihre Projekte SAFER und G-MOSAIC beinhalten eine weltraumgestützte Unterstützung von Krisenoperationen im Rahmen von ESVP, einschließlich „post crisis" und „damage assessment". Auch ESAs RESPOND Projekt hat entsprechende Kapazitäten für diesen Bereich bereits unter Beweis gestellt.

8 Schlussbemerkungen

Die Europäische Weltraumpolitik hat der Nutzung des Weltraums für die Zwecke von Sicherheit und Verteidigung einen hohen Stellenwert eingeräumt und gleichzeitig bestätigt, dass weltraumgestützte Technik einen wesentlichen Beitrag zur Bekämpfung der neuen Bedrohungsszenarien leisten kann. GMES wird als ein Programm erwähnt, welches auch militärische Nutzer haben kann (dieser Aspekt wurde auch vom Vize-Präsidenten der EU-Kommission Verheugen immer wieder erwähnt). Alle relevanten europäischen Akteure im Bereich Sicherheit, Verteidigung und Weltraum befinden sich in einem strukturierten Dialog, mit dem Ziel von Synergien zwischen zivilen und militärischen Weltraum-Anwendungen. Diese Tatsachen stellen ein Umfeld dar, das dem Element „S" in GMES in Sachen Sicherheit und Verteidigung eine der zivilen Sicherheit ähnliche Rolle zukommen lassen wird.

Bereits heute bietet GMES eine Reihe von vor-operationellen Diensten an, welche Relevanz für Sicherheit und Verteidigung haben. Dies gilt insbesondere für den Bereich der schnellen Kartenerstellung und der Identifizierung von Schiffsverkehr. Militärische Nutzer können auf diese Dienste zugreifen, genauso wie die zivilen Nutzer. Weitere für die militärische ESVP-Komponente relevante Dienste werden auf mittlere und längere Sicht verfügbar werden und dem militärischen Nutzer ebenfalls offenstehen.

Die Akzeptanz dieser Dienste durch die Akteure im Bereich Sicherheit und Verteidigung hängt nicht nur von den technischen Kapazitäten der Dienste, sondern insbesondere auch von der mit den Diensten verbundenen Datenpolitik ab. Der militärische Nutzer (aber auch der zivile) hat ein Interesse an der Sicherheit und Integrität der Daten. Er möchte sicher sein, dass weder seine spezifischen Aufträge an das System, noch die an ihn übermittelten Daten unbefugten Dritten zugänglich sein können. Dieser Aspekt der GMES-Datenpolitik ist heute zwar erkannt, aber noch nicht umgesetzt. Das wird zunächst zu einer gewissen Zurückhaltung der Akteure aus dem Bereich Sicherheit und Verteidigung hinsichtlich einer Nutzung der bereits bestehenden Dienste führen.

Die Anforderungen aller potentieller Nutzer an GMES aus dem Bereich „Sicherheit und Verteidigung" sind zwar noch nicht abschließend definiert, aber ein Blick auf die Kapazitäten der Sentinels und der geplanten „Contributing Missions" lässt

vermuten, dass insbesondere im Bereich der „sehr hohen Auflösung“ noch Bedarf an Nachbesserung besteht. Ob dies eines Tages zur Entwicklung einer speziellen „Sentinel-S“-Mission mit Instrumenten zur gezielten Unterstützung der militärischen Komponente der ESVP führen wird, ist noch nicht abzuschätzen.

Um die Anforderungen der militärischen Nutzer zu definieren, und damit möglicherweise neue spezielle GMES-Dienste zu entwickeln, sind weitere Anstrengungen auf dem Gebiet des „strukturierten Dialogs“ nötig. Dies wird eine noch engere Zusammenarbeit zwischen Kommission und Rat der EU erforderlich machen. Die ESA wird sich aktiv an diesem Prozess beteiligen. Folgende Themen werden Gegenstand dieses Dialogs sein müssen:

a) umfassende Definition der militärischen Nutzer-Bedürfnisse;
b) Datensicherheit;
c) zeitliche Verfügbarkeit und Zuverlässigkeit von Produkten für den militärischen Nutzer;
d) die Rolle der bereits bestehenden europäischen Einrichtungen im Bereich Sicherheit und Verteidigung (wie z.B. das Europäische Satellitenzentrum, die Europäische Verteidigungs-Agentur, FRONTEX, etc.);
e) das GMES-Management („governance“) in Hinblick auf die Sicherheits-Dimension.

Dieser Prozess hat gerade in den letzten zwölf Monaten erhebliche politische Unterstützung sowohl von Seiten der EU als auch der ESA bekommen und es kann erwartet werden, dass die sicherheitspolitische Seite von GMES im Jahre 2009 noch höher auf der Agenda der kompetenten Gremien platziert werden wird.

Dr. Mag. rer. nat. Josef Aschbacher
Europan Space Agency (ESA), Frascati
Leiter des GMES-Weltraum-Büros bei der ESA, Frascati, Italien

Dr. jur. Thomas Beer
Europan Space Agency (ESA), Frascati
Koordinator für GMES-Politik im GMES-Weltraum-Büro bei der ESA, Frascati, Italien

Von Fernerkundungsdaten zur Kriseninformation

Monika Gähler und Harald Mehl

1 Hintergrund

Weltweit treten verschiedene Arten von Naturkatastrophen und vom Menschen verursachte Krisen auf. In Krisen liegen die Herausforderungen insbesondere in der schnellen Bereitstellung der relevanten Information und im Zusammenwirken aller Beteiligten. Somit steigt mit der weltweiten Zunahme von Naturkatastrophen, humanitären Notsituationen und zivilen Gefahrenlagen auch der Bedarf an zeitnaher, präziser und flächendeckender Lageinformation.

Diese aktuellen und umfassenden Informationen können inzwischen zu einem großen Teil durch Analyse von satellitengestützten Fernerkundungsdaten bereitgestellt werden. Diese Daten können wertvolle Informationen im Bereich der Naturkatastrophen-Vorsorge, -Frühwarnung und -Ausbreitung sowie auch zur Schadensabschätzung nach Katastrophen, zur schnellen Übersicht akuter Ereignisse und zum Beobachten von Wiederaufbaumaßnahmen liefern.

Voraussetzung hierfür ist besonders die Sensor- und Systementwicklung. Innerhalb der letzten zehn Jahre haben Satellitenbilder eine Qualität im Bezug auf Verfügbarkeit und Genauigkeit erreicht, die es ermöglicht, sie routinemäßig für die Gewinnung von zeitnaher Kriseninformation einzusetzen. Darüber hinaus sind Strukturen und Kapazitäten notwendig, die eine schnelle Aufnahme und Aufbereitung der Satellitendaten ermöglichen. Vor diesem Hintergrund hat das Deutsche Zentrum für Luft- und Raumfahrt e.V. (DLR) das Zentrum für satellitengestützte Kriseninformation (ZKI) als Service des Deutschen Fernerkundungsdatenzentrums (DFD) eingerichtet (vgl. Kapitel 3). Die Entwicklung des ZKI auf deutscher Seite ging mit dem Auf- bzw. Ausbau der GMES (Global Monitoring for Environment and Security)-Aktivitäten auf europäischer Ebene einher.

2 Europäische GMES-Initiative

Neben dem europäischen Satelliten-Navigationssystem Galileo ist das Programm zum „Global Monitoring for Envionment and Security“ eine der Säulen der europäischen Raumfahrtstrategie und wird getragen von der Europäischen Kommis-

sion und der europäischen Raumfahrtagentur ESA. Primäres Ziel der GMES-Initiative ist es, durch den Aufbau einer gemeinsamen, eigenständigen europäischen Infrastruktur, bestehend aus Beobachtungssystemen (ESA-GMES-Sentinel-Satelliten; vgl. Beitrag von Aschbacher in dieser Publikation) und maßgeschneiderten Diensten, das enorme Potential der Erdbeobachtung auch zur Unterstützung politischer Entscheidungsträger und Behörden auf europäischer, nationaler, regionaler und lokaler Ebene optimal nutzen zu können. Die Gesamtverantwortung liegt bei der Europäischen Kommission und hier derzeit beim Kommissariat für Unternehmen und Industrie.

Innerhalb des 6. Forschungsrahmenprogramms implementierte die Kommission erste Forschungs- und Entwicklungsprojekte, die sich mit den GMES-Anwendungsthemen auseinandersetzten. Die zeitgleich durch ESA implementierten und finanzierten GMES-Service Elements (GSE) analysierten den Bedarf der Anwender, die Verfügbarkeit der Informationen und die Lieferfähigkeit der Anbieter von Geoinformationsdiensten im GMES. Nach dem Aufbau der GMES-Kapazitäten

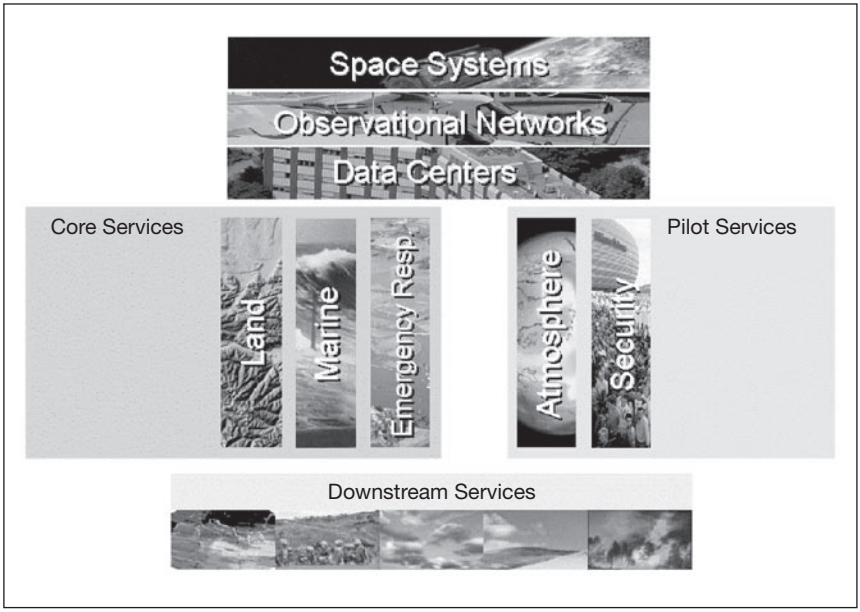

Abbildung 1: Prä-operationelle GMES-Services

bis 2009 sollen die GMES-Dienste in den operationellen Betrieb sowie eine evolutionäre Weiterentwicklung übergeführt werden. Dies wird zunächst durch GMES-Kerndienste für „Land“ (Land Monitoring Core Service), „Ozean“ (Ocean Monitoring Core Service) und „Notfallkartierung“ (Emergency Response Core Service) geschehen. In Ergänzung dazu wurden noch zwei weitere Pilot-Dienste zu den Themen „Atmosphäre“ (Atmosphere Pilot Service) sowie „Zivile Sicherheit“ (Security Pilot Service) aufgenommen. Ferner sollen zu diesen Themen aus den Basisinformationen dieser Dienste weitere „Downstream-Services“ abgeleitet werden (vgl. auch Abbildung 1 sowie Schreier und Dech 2007).

Sowohl auf Seiten der ESA als auch auf Seiten der Europäischen Kommission gibt es dementsprechend eine Reihe spezifischer Aktivitäten u. a. zum Themenkomplex „zivile Sicherheit und Kriseninformation aus Fernerkundungsdaten“. Das DLR und verschiedene Verbundpartner sind in eine Reihe von Projekten zum Thema satellitengestützte Kriseninformation involviert (RESPOND, Risk-EOS, LIMES, BOSS-4GMES, GMOSS, SAFER, G-MOSAIC). Entwickelt, aufgebaut und optimiert werden Methoden und Dienste wie z.B. für Schnellkartierungskapazitäten zur Unterstützung des Katastrophenmanagements oder auch für den Informationsbedarf der Einsatzkräfte bei Großveranstaltungen. Verschiedene Nutzer aus diesen Themenbereichen wie z.B. auf deutscher Seite das Technische Hilfswerk (THW), das Deutsche Rote Kreuz (DRK) und das Bundeskriminalamt (BKA), sind hierbei ebenfalls bereits eingebunden.

3 Aufgaben und Funktionen des ZKI

Satellitengestützte Kriseninformationen werden im Deutschen Zentrum für Luft- und Raumfahrt e.V. (DLR) durch das Zentrum für satellitengestützte Kriseninformation erstellt und als Service verschiedenen Nutzern zur Verfügung gestellt. Aufgabe des ZKI ist dabei die schnelle Beschaffung, Aufbereitung und Analyse von Satellitendaten bei Natur- und Umweltkatastrophen, für humanitäre Hilfsaktivitäten und zur Wahrung der zivilen Sicherheit (vgl. Voigt et al. 2005, 2007).

Im Falle einer Notfallkartierung direkt nach einer Katastrophe werden in einem 24 Stunden/sieben Tage die Woche bestehenden Service vor allem Überblicks- und Schadenskarten erstellt. Die Auswertungen werden nach den spezifischen Bedürfnissen für nationale und internationale politische Bedarfsträger sowie Hilfsorga-

nisationen durchgeführt. Durch die mehrjährige kontinuierliche Arbeit des ZKI ist das DLR inzwischen etablierter Ansprechpartner in Deutschland und Europa sowie in internationalen Institutionen zum satellitengestützten Katastrophenmonitoring und -management geworden.

Hauptziele des ZKI sind:

- die Entwicklung eines Krisenmanagementservices,
- Schulungen der Nutzer und
- Forschung und Weiterentwicklung.

Bei der Entwicklung eines Krisenmanagementservices werden im DLR bestehende technische Expertise z.B. zum Datenempfang, zur -archivierung oder dem Datenmanagement und vorhandene wissenschaftliche Expertise im Bereich der Umwelt- und Geo- sowie der Kriseninformation effektiv zusammengeführt. Aus dieser Kombination können ZKI-Produkte im Krisenbereich der Vorbereitung und Prävention, z.B. das Tsunami-Frühwarnsystem, im Krisenbereich der Katastrophenhilfe, beispielsweise Lagekarten, und im Krisenbereich der Wiederaufbaumaßnahmen, z.B. Detailkarten einzelner Gebäude, erzeugt werden. Diese können letztlich Endnutzern wie politischen Entscheidungsträgern, Lagezentren, Hilfsorganisationen und der Öffentlichkeit zur Verfügung gestellt werden.

Neben der Erzeugung von satellitengestützten Kriseninformationen und der Entwicklung eines Krisenmanagementservices werden Nutzer in Workshops und Übungen in Grundlagen der Karteninterpretation und Möglichkeiten und Grenzen von Luft- und Satellitenbildern geschult, damit sie ein grundlegendes Verständnis von der Arbeit und den Produkten des ZKI entwickeln. Zugleich dienen Nutzertreffen und u.a. auch Schulungen dazu, die Nutzerinteressen und -bedürfnisse besser zu verstehen und den Service darauf abzustimmen.

Letztlich bilden Forschung und Weiterentwicklung des Kriseninformationsservices einen wichtigen Bestandteil der ZKI-Tätigkeiten. Im Kontext der Notfallkartierung wird dabei versucht, neue Fernerkundungsmethoden zu entwickeln und diese in bestehende Prozessketten zu integrieren. Schwerpunktthemen sind Hochwasserdetektion, Erdbebenschadenserkennung und Kartierungen von Flüchtlingscamps.

Die im Krisenfall durchgeführte Notfallkartierung kann anhand der in Abbildung 2 dargestellten Prozesskette beschrieben werden. Tritt eine Krise wie z.B.

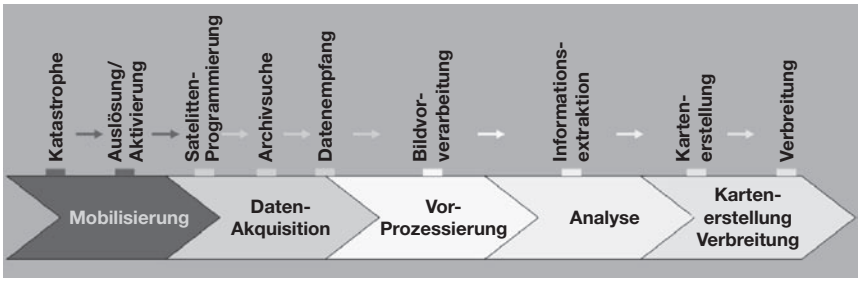

Abbildung 2: Von Fernerkundungsdaten zur Kriseninformation – Prozesskette einer Notfallkartierung (Rapid Mapping)

eine Naturkatastrophe, bspw. ein „Erdbeben", auf, werden in der Mobilisierungsphase zunächst Leitstellen und zuständige Institutionen benachrichtigt, die entweder direkt das ZKI alarmieren oder Nutzer wie z.B. Hilfsorganisationen verständigen, die die Alarmierung des ZKI auslösen. Im ZKI beginnt die Koordinierung der Notfallkartierung mit der internen Information über die Krisensituation und daraufhin mit der Beschaffung von adäquaten und schnell zugänglichen Satellitendaten. Dies sind zum Einem zumeist Archivszenen (vor der Krise) und zum Anderen Neuakquisitionen von Satellitenbildern. Werden Satellitendaten an das ZKI ausgeliefert, beginnt die Vorprozessierungsphase, in der beispielsweise Lagekorrekturen oder Bildfusionen durchgeführt werden. Ist die Vorprozessierung abgeschlossen, folgt die Analyse und Auswertung der Daten mit Blick auf krisenrelevante Informationen. Es können je nach Art der Katastrophe und nach Fragestellung z.B. Veränderungsanalysen, Schadensbewertungen oder thematische Auswertungen wie Hochwasserdetektion oder Brandflächenerkennung durchgeführt werden. Nach der Extraktion der Informationen werden diese in Kartenprodukte integriert. Zur Kartenerzeugung werden außerdem z.B. Informationstexte, Legenden und Übersichtkarten erzeugt. Sind die Krisenprodukte (z.B. Karten oder Vektordaten) erstellt, werden diese letztlich an die Nutzer ausgeliefert. ZKI-Produkte werden hauptsächlich über die ZKI-Internetseite (www.zki.dlr.de), per ftp-Server oder via email und gelegentlich auch als ausgedruckte Kartenprodukte verbreitet.

Seit dem Jahr 2002 hat das ZKI in mehr als fünfzig Fällen die Partner mit satellitengestützter Lageinformation unterstützt, darunter Einsätze wie die Tsuna-

mi-Katastrophe im Indischen Ozean (2004), das schwere Erdbeben in Pakistan (2005), aber ebenfalls die Waldbrände der letzten Jahre im Mittelmeerraum, die Überflutungen der Elbe (2002, 2006) sowie in Großbritannien 2007. Bei der Analyse stützt sich das ZKI auf Daten, die im Rahmen von verschiedenen Initiativen wie z.B. der „International Charter on Space and Major Disasters“ zur Verfügung gestellt werden (vgl. Kapitel 4). Die Kartierungsarbeiten werden meistens im Rahmen von GMES-Projekten erstellt und finanziert.

Ein Beispiel für ein satellitengestütztes Kriseninformationsprodukt ist die Karte in Abbildung 3 im Raum Wittenberg (Sachsen-Anhalt), die das Elbehochwasser vom 4. April 2006 darstellt. Für das Elbehochwasser wurden verschiedene Satellitendaten (Optik und Radar) vor und nach der Katastrophe zunächst radiometrisch und geometrisch korrigiert, analysiert und dann mit anderen Geodaten kombiniert (topographische Karten). In der dargestellten Karte wurden die Hochwasserflächen aus ERS-Daten abgeleitet.

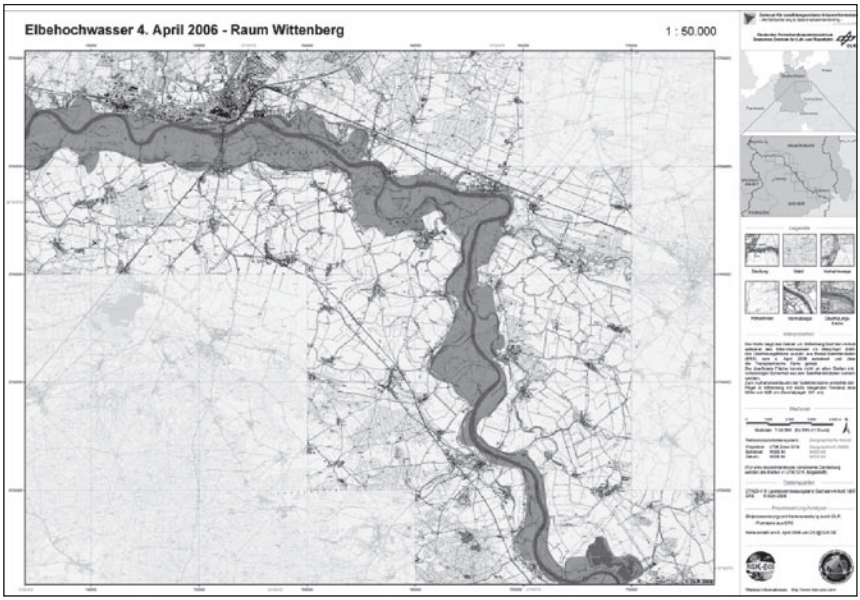

Abbildung 3: ZKI-Beispielkarte: Elbehochwasser 2006 – Detektion von Überflutungsflächen im Raum Wittenberg abgeleitet aus ERS und visualisiert auf einer topographischen Karte

4 International Charter „Space & Major Disasters“

Da eine Notfallkartierung gerade bei großen Katastrophenfällen nicht von einem Satellitenbetreiber oder einer Weltraumagentur bewältigt werden kann, und diese Dienste außerdem finanziell recht aufwändig sind, haben sich mehrere Weltraumorganisationen und Satellitenbetreiber im Jahr 2000 zusammengeschlossen und die International Charter „Space & Major Disasters“ gegründet. Ziel der International Charter ist es, ein einheitliches System zur Bestellung und Auslieferung von Satellitenbilddaten im Falle großer Naturkatastrophen und technischer Unfälle aufzubauen, um satellitengestützte Kriseninformationen kostenlos für autorisierte Nutzer wie Zivilschutz- und Rettungsorganisationen sowie Verteidigungs- und Sicherheitsinstitutionen zur Verfügung zu stellen.

Seit 2000 wurde die International Charter bereits über 170 Mal aktiviert, wobei die häufigsten Katastrophen Überflutungen, gefolgt von Erdbeben und Stürmen sind (Abbildung 4).

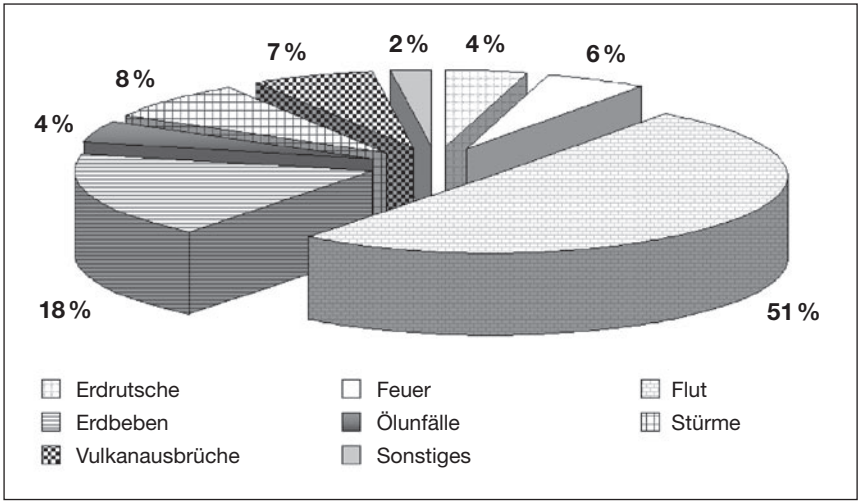

Abbildung 4: Häufigkeiten der Katastrophen bei Aktivierungen der International Charter „Space & Major Disasters“ (2002–2006)

5 Netzwerke und Partnerschaften

Neben der Zusammenarbeit innerhalb der International Charter „Space & Major Disasters“ und innerhalb der GMES-Projekte ist die erfolgreiche Durchführung von ZKI-Notfallkartierungen geprägt von Netzwerken und Partnerschaften sowohl mit Weltraumorganisationen und Industrie als auch der Europäischen Weltraumbehörde ESA, der französischen Weltraumorganisation CNES (Centre National d'Etudes Spatiales) oder dem Satellitenbetreiber EUSI (European Space Imaging). Für die Forschung und Weiterentwicklung ist zudem die Kooperation mit anderen Forschungsinstituten, z.B. dem Geoforschungszentrum im Potsdam (GFZ) oder dem europäischen Joint Research Center (JRC), essentiell. Eine der wichtigsten Komponenten stellt natürlich der Kontakt zu den Nutzern der ZKI-Produkte wie beispielsweise zum Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem dort beheimateten Gemeinsamen Melde- und Lagezentrum sowie zum Deutschen Roten Kreuz oder zum Technischen Hilfswerk dar.

6 Fazit

Erdbeobachtung kann zunehmend einen wertvollen Beitrag zur Katastrophenvorsorge und zum -management leisten, der sowohl Entscheidungsträgern aber auch vor allem den Einsatzkräften vor Ort zu Gute kommt. Fernerkundungsdaten bieten eine optimale Basis für die flächendeckende, zeitnahe und präzise Lageinformation in Krisensituationen. Sowohl die räumliche als auch zeitliche Auflösung insbesondere der neuen Sensoren können zukünftig den Nutzeranforderungen besser gerecht werden. Entscheidend ist dabei, dass die gesamte Datenkette von der Aufnahme bis zum Informationsprodukt zur Verfügung steht und optimiert ist, um eine quasi-Echtzeitfähigkeit zu gewährleisten. Hierfür sind jedoch auch Strukturen (z.B. Finanzierungs- und Einsatzstrategien) dauerhaft zu institutionalisieren, die einen derartigen Service gewährleisten können, so dass durch satellitengestützte Kriseninformation die Erdbeobachtung zivile und humanitäre Anwendungen unterstützen kann.

Durch die Initiative GMES kann die Analyse von Satellitendaten zu vielfältigen direkten Anwendungen führen und können operationelle Dienste entwickelt, bereitgestellt und optimiert werden. Die Geoinformationsdienste von GMES wer-

den nicht ausschließlich auf Satellitendaten basieren. Allerdings werden Satellitendaten die unabdingbare Grundlage dieser Informationsdienste sein.

So transparent und einfach die Informationen für den Entscheidungsträger aufbereitet werden müssen, so komplex ist der Entwurf, Aufbau und Betrieb von Satellitensystemen. In seinem Standort in Oberpfaffenhofen bei München konzentriert das Deutsche Zentrum für Luft- und Raumfahrt (DLR) alle diese Fähigkeiten. So werden vom German Space Operations and Control Center (GSOC) nationale, europäische und internationale Weltraummissionen geleitet. Das Deutsche Fernerkundungsdatenzentrum (DFD) in Oberpfaffenhofen ist verantwortlich für den Empfang der Daten von Fernerkundungssatelliten und das zentrale Archiv vieler Daten, der nationalen Fernerkundungsbibliothek.

Das Zentrum für satellitenbasierte Kriseninformation (ZKI) liefert öffentlichen, nationalen und internationalen Organisationen aufbereitete Satellitenkarten, welche im Falle von humanitären Krisen und Naturkatastrophen den Hilfs- und Einsatzkräften vor Ort wertvolle Hinweise auf das Ausmaß der Katastrophe geben, weltweit in einem 24h/sieben Tage-Service. Die Auswertungen werden nach den spezifischen Bedürfnissen für nationale und internationale politische Entscheidungsträger, Lagezentren sowie Hilfsorganisationen durchgeführt und daneben auch der Öffentlichkeit frei zugänglich gemacht. Das ZKI operiert dabei im nationalen, europäischen und internationalen Kontext und ist eng vernetzt mit verschiedenen behördlichen Partnern, Nicht-Regierungsorganisationen (humanitäre Hilfsorganisationen) sowie Satellitenbetreibern und Weltraumorganisationen.

Dr. rer. nat. Monika Gähler
Deutsches Zentrum für Luft- und Raumfahrt (DLR), Oberpfaffenhofen
Leitung des Schnittstellenprojekts zu GMES „DeSecure“ im Deutschen Fernerkundungsdatenzentrum des DLR

Dr. rer. nat. Harald Mehl
Deutsches Zentrum für Luft- und Raumfahrt (DLR), Oberpfaffenhofen
Abteilungsleiter „Umwelt und Sicherheit“ und stellvertretender Institutsleiter des Deutschen Fernerkundungsdatenzentrums des DLR

Literaturverzeichnis

Schreier G, Dech S, „GMES: Globale Beobachtung der Umwelt und der Sicherheit – ein europäisches Programm zur Stärkung der satellitenbasierten Erdbeobachtung“, in: Mitteilungen des DVW-Bayern e.V., 3/2007, 291–300

Voigt S, Kemper T, Riedlinger T, Kiefl R, Scholte K, Mehl H, „Satellite image analysis for disaster and crisis-management support“, in: IEEE Transactions on Geoscience and Remote Sensing, 45 (6), 2007, 1520–1528

Voigt S, Riedlinger T, Reinartz P, Künzer C, Kiefl R, Kemper T, Mehl H, „Experience and Perspective of Providing Satellite Based Crisis Information, Emergency Mapping & Disaster Monitoring Information to Decision Makers and Relief Workers“, in: Geoinformation for Disastermanagement, Springer, Heidelberg 2005, 519–531

FERNERKUNDUNG, SICHERHEIT UND GESELLSCHAFT

Sicherheit in den Städten

Welchen Beitrag können globale Fernerkundungssysteme leisten?

Holger Floeting

Einführung

Sicherheit in den Städten ist ein immer wieder aktuelles Thema der öffentlichen Diskussion. Dabei werden – meist abhängig von aktuellen mehr oder weniger schlagzeilenträchtigen Ereignissen – unterschiedliche Aspekte des Themas betont:

- Sicherheit vor terroristischen Anschlägen nach den Ereignissen des 11. Septembers 2001 in New York, den Zuganschlägen in Madrid im Jahr 2004, der Festnahme der „Kofferbomber" in Nordrhein-Westfalen im Jahr 2006;
- Sicherheit vor Naturkatastrophen nach dem Oder- und Elbe-Hochwasser in den Jahren 1997 bzw. 2002 und anderen Großschadensereignissen wie Fluten und Stürmen;
- Sicherheit im öffentlichen Personenverkehr nach dem brutalen Angriff auf einen Rentner in der Münchener U-Bahn im Dezember 2007 und anderen Fällen von (jungendlicher) Gewaltkriminalität im öffentlichen Raum;
- Alkoholmissbrauch nach mehreren Fällen von Rauschtrinken („Komasaufen") Jugendlicher in unterschiedlichen deutschen Großstädten und dem Tod eines Jugendlichen als Folge schweren Alkoholmissbrauchs in Berlin im Februar 2007;
- Migranten als Täter im Zuge der Diskussion um den Umgang mit jugendlichen Intensivtätern und einer allgemeinen Integrationsdebatte;
- Vandalismus nach gemeldeten Zerstörungen von Telefonzellen, Bussen, Bahnen usw.;
- alltägliche Störungen der öffentlichen Ordnung: vom „Hundehaufen" bis zum Lärm auf der Straße.

Im ersten Teil geht der Beitrag auf bestehende Ängste der Bevölkerung als Grundlage der Wahrnehmung von Bedrohungen und Risiken ein. Im zweiten Teil erläutert er, was unter „Sicherheit" in den Städten verstanden wird und welche vielfältigen Sicherheitsaufgaben damit verbunden sind. Im dritten Teil werden Bereiche identifiziert, die sich als Einsatzfelder globaler Fernerkundungssysteme eignen und eine Einordnung globaler Fernerkundungssysteme in das umfassende Ange-

bot technischer Sicherheitslösungen vorgenommen. Im vierten Teil werden mögliche Auswirkungen einer sicherheitstechnischen „Aufrüstung“ auf die Stadtentwicklung dargestellt.

Ängste, Bedrohungen und Risikowahrnehmung

Die Risikoforschung hat in den letzten Jahren eine Reihe grundsätzlicher Erkenntnisse geliefert:

- Die größten Ängste der Menschen sind nicht zwangsläufig verbunden mit den größten Risiken, denen sie ausgesetzt sind oder dem Grad des möglichen Schadens, den sie erleiden können.
- Die Risikoeinschätzung von Laien und Experten unterscheidet sich demzufolge erheblich. Laien schätzen kontrollierbare Risiken und freiwillig eingegangene Risiken i.d.R. als weniger riskant ein. Große Schadensereignisse und wissenschaftlich unsichere Risikoeinschätzungen werden von Laien dagegen als riskanter wahrgenommen. Dabei wird die Einschätzung stark geprägt von der persönlichen Betroffenheit vom Risiko bzw. der persönlichen Vertrautheit mit ihm und dem persönlichen Nutzen aus riskantem Verhalten. Eintrittswahrscheinlichkeiten von Risiken werden von Laien häufig auf Basis von Heuristiken (z.B. Ereignisse sind leicht vorstellbar oder man erinnert ähnliche Ereignisse häufiger) eingeschätzt.
- Zwischen den Experten werden Risiken aber auch sehr unterschiedlich eingeschätzt. Vorannahmen und Entscheidungen der Experten beeinflussen die Risikoeinschätzung erheblich. Eine einheitliche Bewertung von Risiken lässt sich, nicht zuletzt aufgrund der Komplexität der Fragestellungen, häufig auch gar nicht finden (vgl. Schütz und Peters 2002).
- Medien vermitteln ein stark selektives Abbild von Risiken, indem sie beispielsweise häufiger und ausführlicher über ungewöhnliche als alltägliche Risiken berichten.

Eine auf Risikoabschätzungen beruhende städtische Sicherheitspolitik muss diese Unterschiede berücksichtigen. Sie muss ihre Präventionsaktivitäten, Gefahrenabwehrkonzepte und -maßnahmen und Interventionen an den Risiken orientieren. Sie kann subjektive Unsicherheiten der Menschen nicht als „Zerrbild der Wirklichkeit“ abtun, sondern muss die Ängste der Bürger ernst nehmen, denn das alltägli-

che Leben der Bürger wird stärker von ihren subjektiven Einschätzungen bestimmt als von scheinbar objektiven Risikoeinschätzungen. Damit ist eine Stadt oder ein Stadtraum, der als unsicher wahrgenommen wird, ein Raum der ungern, nicht oder mit besonderer Vorsicht genutzt wird. Die subjektive Sicherheitseinschätzung beeinflusst damit die räumlichen Nutzungsmuster von Städten und Stadträumen in erheblichem Maß.

Im Auftrag eines Versicherungsunternehmens wird in Deutschland seit einigen Jahren eine Umfrage zu den Ängsten der Deutschen durchgeführt, die es erlaubt, einen Eindruck von der Entwicklung der Ängste in der Bevölkerung über einen längeren Zeitraum zu gewinnen (vgl. Abbildung 1).[1] Danach ist beispielsweise die Angst vor Straftaten in der Bevölkerung in den letzten Jahren zurückgegangen, während die Angst vor Terrorismus nach dem 11. September 2001 schlagartig

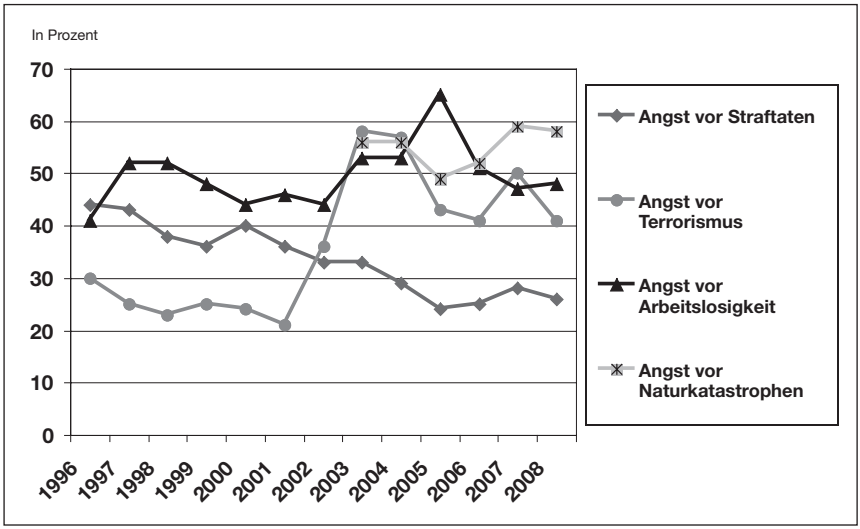

Abbildung 1: Angst (Quelle: R+V Versicherung, Die Ängste der Deutschen 1996–2008)

[1] Befragt wurde im Jahr 2008 eine repräsentative Stichprobe von 2.460 Personen im Alter ab 14 Jahren, davon 1.684 Befragte in Westdeutschland und 776 in Ostdeutschland. Die Untersuchung basiert auf strukturierten persönlichen Interviews mit geschlossenen Fragen. Durch Aktualisierungen der Fragestellungen sind die Ergebnisse über die Jahre nur bedingt vergleichbar (Angaben des Infocenters der R+V Versicherung, Wiesbaden).

gestiegen ist, seitdem aber (mit Ausnahme des Jahres 2007) kontinuierlich zurückgegangen ist. An der Entwicklung der Zahlen im Bezug auf die Angst vor Terrorismus lässt sich sehr gut verdeutlichen, dass die Einschätzungen sehr stark von aktuellen Ereignissen und deren medialer Vermittlung abhängen. Neu hinzugetreten ist in der Umfrage die Angst vor Naturkatastrophen, die in den letzten Jahren annähernd ebenso häufig oder häufiger genannt wird wie die Angst vor Terrorismus. Zum Vergleich: Bestimmte grundsätzliche Lebensrisiken, z.B. Arbeitslosigkeit, spielen bei den Ängsten eine wesentlich wichtigere Rolle als etwa die Angst vor Straftaten. Damit bestätigen sich die eingangs vorgestellten grundlegenden Erkenntnisse der Risikoforschung im Bezug auf die Einschätzung von Risiken durch Laien deutlich.

Stellt man diesen Ängsten die tatsächliche Entwicklung von Risiken gegenüber, wird die zum Teil erhebliche Diskrepanz zwischen subjektiver Wahrnehmung und tatsächlicher Bedrohung deutlich. Zumindest wird jedoch klar, dass eine differenzierte Betrachtung der Risiken notwendig ist. Beispielhaft werden im Folgenden drei Bedrohungsbereiche näher betrachtet, die bei den Ängsten der Deutschen, wenn auch über die Jahre in unterschiedlicher Ausprägung, häufig benannt werden: Kriminalität, Naturkatastrophen und Terrorismus.

Kriminalität entsteht innerhalb eines mehrstufig verlaufenden Prozesses der Wahrnehmung und Bewertung von Handlungen und Sachverhalten. Sie ist ein von Struktur und Intensität strafrechtlicher Kontrolle abhängiger Sachverhalt und das Ergebnis vorheriger gesellschaftlicher Festlegungen. Kriminalität – wie sie sich in der Statistik widerspiegelt – ist kein repräsentativer Ausschnitt, viel mehr wird damit die Tätigkeit von Polizei, Staatsanwaltschaft und Gerichten abgebildet (Häfele 2008). Wie sicher sind also die deutschen Städte und Gemeinden vor Kriminalität? Die polizeiliche Kriminalstatistik in Deutschland zeigt seit Jahren einen Rückgang der Straßenkriminalität. Es gibt aber eine Zunahme der Gewaltkriminalität und eine besonders starke Zunahme bei den Delikten gefährliche und schwere Körperverletzung. Obwohl die mediale Erörterung anderes erwarten lassen könnte, nimmt die Zahl der nicht-deutschen Tatverdächtigen kontinuierlich ab. Andererseits besteht aber ein hoher Anteil nicht-deutscher Tatverdächtiger gerade bei Straftaten, die einen hohen Organisationsgrad erfordern wie beispielsweise die Fälschung von Zahlungskarten, gewerbsmäßige Bandenhehlerei, Glücksspiel, Geld- und Wertzeichenfälschung oder Menschenhandel. Eine längerfristi-

ge Betrachtung zeigt eine ungefähr gleich bleibende Aufklärungsquote bei vielen Delikten. Hohe Aufklärungsquoten existieren z.B. bei Rauschgiftdelikten, Mord, Totschlag (deutlich über 90 Prozent der Straftaten), gefährliche und schwere Körperverletzung, Vergewaltigung, sexuelle Nötigung (um oder über 80 Prozent). Vergleichsweise geringe Aufklärungsquoten bestehen dagegen bei Sachbeschädigung (nur zwischen einem Fünftel und einem Viertel der Straftaten) und maximal ein Fünftel der Wohnungseinbruchdiebstähle wurde in den letzten Jahren aufgeklärt.

Bei der Risikoeinschätzung müssen Verzerrungen durch statistische Artefakte berücksichtigt werden. So sind beispielsweise Verschiebungen zwischen Hell- und Dunkelfeld der Kriminalität aufgrund veränderten Anzeigeverhaltens oder veränderter Verfolgungsintensität möglich. Bedeutsame deliktübergreifende Erscheinungsformen der Kriminalität werden nicht abgebildet, da anhand gesetzlicher Tatbestände erfasst wird. Straftaten mit langer Ermittlungsdauer mindern die Aktualität der Daten, da eine Erfassung erst bei Abgabe an die Staatsanwaltschaft erfolgt. Die polizeiliche Kriminalstatistik und die Verurteiltenstatistik der Justiz lassen sich nicht miteinander vergleichen. Es fand bisher keine Differenzierung nach Migrationshintergrund, sondern nur nach Staatsangehörigkeit statt, sodass erklärungsrelevante Variablen bei der Kriminalitätsrisikoeinschätzung möglicherweise nicht herangezogen werden können. Die Bevölkerungsstruktur und die Tätermobilität ebenso wie das Anzeigeverhalten und die Deliktstrukturen können sich zwischen den Städten erheblich unterscheiden, sodass Vergleiche verzerrt sein können (vgl. Polizeiliche Kriminalstatistik 2007). Individuelle Risikoeinschätzungen lassen sich aus der Statistik aber wegen der Hellfeld-Dunkelfeld-Problematik kaum ableiten. Aussagekräftiger sind die wenigen vorhandenen Dunkelfeldstudien, die nahe legen, dass Menschen häufiger Opfer von Straftaten werden, je jünger sie sind und wenn sie männlich sind (vgl. Häfele 2008).

Auch andere Risiken müssen differenziert betrachtet werden. So nehmen beispielsweise Häufigkeit und Schäden von Naturkatastrophen in Deutschland seit den 1970er Jahren tatsächlich zu. In den 35 Jahren von 1970 bis 2005 gab es insgesamt 640 Schadensereignisse, die man als Naturkatastrophen klassifizieren kann. Stürme sind dabei die häufigsten Ereignisse. Sie forderten die meisten Todesopfer und produzierten die höchsten volkswirtschaftlichen und versicherten Schäden (Rauch 2008). Meteorologische Beobachtungen von Sturmereignissen gibt es seit Jahrhunderten. Auch instrumentelle Messwerte von Windfeldern werden seit etwa

100 Jahren erhoben. Dennoch sind Bewertungen von Risiken in diesem Bereich sehr komplex, weil sich vorhandene Messwerte nur schwer miteinander vergleichen lassen, topographische Einflüsse zu erheblichen kleinräumlichen Abweichungen der Ausprägung von Sturmereignissen führen können und Schäden zum Teil erst nach häufigen Windangriffen beispielsweise durch Materialermüdung auftreten (Münchener Rück 2008). Auch im Bereich von Georisiken, die sich einfacher einschätzen lassen, kommt es auf eine differenzierte Betrachtung an. Im Gedächtnis der Öffentlichkeit sind beispielsweise die „Jahrhundertfluten" an Oder und Elbe. Vernachlässigt werden bei dieser Betrachtung oft die wiederkehrenden Schäden kleinerer Hochwasser. Bei der zielgerichteten Planung von Vorsorgemaßnahmen (Entsiegelung, Renaturierung von Gewässern, technische Schutzbauten usw.) sind diese Risiken aber mit zu berücksichtigen (Kron 2008).

Auch die Bedrohung durch terroristische Anschläge hat in den letzten Jahren zugenommen. Im Jahr 2007 wurden in neun EU-Staaten[2] 583 fehlgeschlagene, vereitelte oder ausgeführte Anschläge registriert. Für Deutschland werden 20 genannt. Die weit überwiegende Zahl von Angriffen in den neun Staaten waren Brandanschläge. Zwei Todesopfer waren zu beklagen (Europol 2008). Ängste erzeugt die Bedrohung durch terroristische Anschläge vor allem durch das für die Bevölkerung noch stärker als im Bezug auf Bedrohungen durch die allgemeine Kriminalität oder durch Naturkatastrophen nahezu uneinschätzbare Risiko.

Sicherheit in den Städten

Nahezu so vielgestaltig wie die tatsächlichen oder vermeintlichen Bedrohungen und Risiken, ist auch der Sicherheitsbegriff: nationale Sicherheit, kollektive Sicherheit, individuelle Sicherheit, öffentliche Sicherheit und Ordnung, technische Sicherheit und soziale Sicherheit. Kommunen beschäftigen sich als Akteure nur mit einem „Ausschnitt" des Themas „Sicherheit", auch wenn grundsätzlich die Sicherheit in Städten und Gemeinden eine weit über diesen Ausschnitt hinaus gehende Aufgabe ist.

Das Politikfeld „innere Sicherheit", das auch die Sicherheit in den Städten und Gemeinden betrifft, hat sich in Deutschland in den letzten Jahren erheblich ver-

[2] Dänemark, Deutschland, Frankreich, Griechenland, Italien, Österreich, Portugal, Spanien, Vereinigtes Königreich.

ändert. Die Neuorientierung in diesem Bereich ist mit einer Veränderung der Gesamtkonzeption zur Gefahrenabwehr, der Erarbeitung von Risikoanalysen und Erstellung von Risikokatastern und der Durchführung von Krisenabwehrplanungen verbunden. Die internationale Zusammenarbeit hat auch im Bereich der inneren Sicherheit an Bedeutung gewonnen. Hat man es doch in zunehmendem Maß mit Risiken und Bedrohungen zu tun, die nicht vor Ländergrenzen halt machen. Die ohnehin komplexe Struktur von Akteuren, die mit Aufgaben des Bevölkerungsschutzes, der Gefahrenabwehr und der Sicherheit und Ordnung betraut sind, wird durch die Einbeziehung privater Akteure und die in der innenpolitischen Diskussion immer wieder geforderte stärkere zivil-militärische Zusammenarbeit auch im Bereich der inneren Sicherheit zunehmende komplexer. Der Entwicklung von Kooperationsmodellen zwischen Bund, Ländern, Kommunen, Hilfs- und Freiwilligenorganisationen usw. kommt damit eine besonders wichtige Rolle bei der Umsetzung integrierter Sicherheitskonzepte zu.

Die kommunalen Aktivitäten in Bezug auf die Sicherheit in der Stadt konzentrieren sich im Wesentlichen auf die Aufgaben der Gefahrenabwehr (Erteilung und Entziehung von Gewerbeerlaubnissen für Gaststätten, Spielhallen usw., Festlegung von Sperrbezirken, Überwachung von Ausländervereinen usw., Unterbringung von Obdachlosen, Regelung der Polizeistunde, Umgang mit Jugendschutz und Versammlungsrecht usw.), Maßnahmen der Städtebaupolitik (Festlegung von Nutzungsstrukturen, Vermeidung von städtebaulichen Angsträumen usw.) und die Gestaltung von Rahmenbedingungen zur Kriminalprävention (Sozial-, Jugend-, Familien-, Wohnungs-, Bildungs-, Kultur-, Beschäftigungspolitik usw.) sowie seit den 1990er Jahren die aktive Beteiligung an kriminalpräventiven Gremien und deren Aktionen.[3]

Betrachtet man die Sicherheitsaufgaben in den Städten im Einzelnen wird die Vielgestaltigkeit des Aufgabenfeldes deutlich (vgl. Abbildung 2).

Zur Sicherheit in Städten und Gemeinden gehört der Umgang mit Naturgefahren (Wetterrisiken und andere Naturgefahren) und technischen Gefahren (Kraftwerksunfall, Großbrand, Havarien, Ausfall von Versorgungseinrichtungen, Gefahr-

---

[3] 1990 wurde der erste „Rat für Kriminalitätsverhütung“ in Schleswig-Holstein gegründet. Auf kommunaler und subkommunaler Ebene haben sich in den 1990er Jahren ressortübergreifende Zusammenschlüsse etabliert. Von den lokalen Gremien sind etwa zwei Drittel durch kommunalparlamentarischen Beschluss genehmigt. Der Hauptwirkungsbereich ist die Kommune als Ganzes, daneben bestehen Stadtteil- und Kreisgremien. Typisch ist ein mehrgliedriger Aufbau mit Lenkungsausschuss und Arbeitgruppen (vgl. Schreiber 2007).

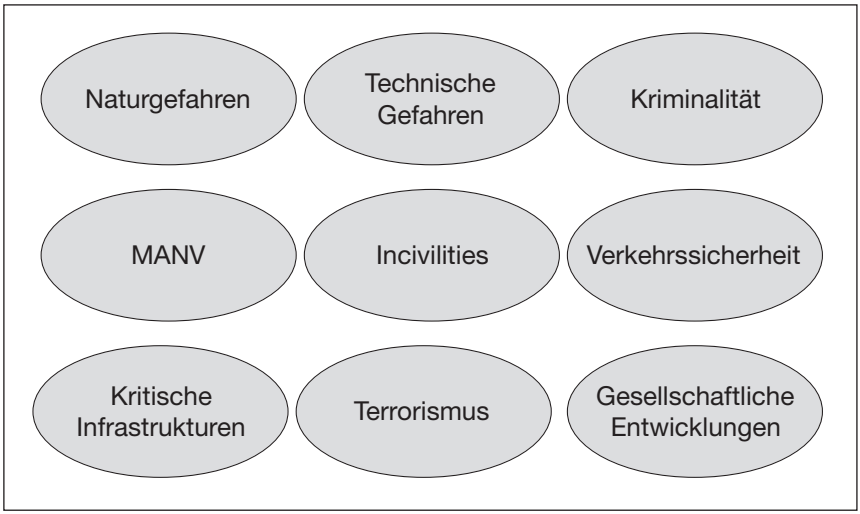

Abbildung 2: Sicherheitsaufgaben in den Städten

gutschadensereignisse usw.) ebenso wie mit Bedrohungen durch Terrorismus, der Schutz kritischer Infrastrukturen (Wasser-, Energieversorgung, Transport-, Telekommunikationssystem, Gesundheitsversorgung, Notfalldienste, Behördendienste, Bankdienste) ebenso wie der Umgang mit Massenanfällen von Verletzten und Erkrankten. Zur Sicherheit in den Städten und Gemeinden gehören grundsätzliche Sicherheitsaufgaben wie die Verkehrssicherheit ebenso wie der Umgang mit alltäglichen Störungen der Sicherheit und Ordnung, die von der Kriminalität (Beschaffungs-, Jugend-, Gewalt-, Umwelt-, Wirtschafts-, organisierter Kriminalität usw.) bis hin zum Umgang mit „Incivilities“ (Störungen der öffentlichen Ordnung vom Hundekot auf der Straße über ungepflegte öffentliche Anlagen bis zu Graffiti und Zerstörungen im öffentlichen Raum) reichen. Die genannten Bereiche beeinflussen die Sicherheit in den Städten und Gemeinden, auch wenn die Befassung mit ihnen nicht immer eine kommunale Aufgabe ist, sondern andere Akteure dafür zuständig sind. Eine integrierte städtische Sicherheitspolitik muss dennoch alle Aufgabenfelder im Blick haben.

Gerade der Bereich der „Incivilities“ stand in den letzten Jahren im Mittelpunkt der Diskussion um die Eingriffsmöglichkeiten zur Verbesserung der Sicherheit in Städten und Gemeinden (vgl. Häfele 2006).

Die „Broken-Windows"-These (Wilson/Kelling 1982) bildete zusammen mit der „Defensible-Space"-These (Newman 1996) die theoretische Grundlage für die Formulierung neuer Grundsätze des Zusammenwirkens von Prävention und Repression in städtischen Umgebungen. Die „Broken-Windows"-These besagt dabei, dass Unordnung und Verwahrlosung in einem Wohnquartier als Zeichen des Zusammenbruchs sozialer Kontrolle wahrgenommen würden, abweichendes Verhalten an der Untergrenze der Strafwürdigkeit größere Vergehen nach sich ziehen würde und die Eindämmung von schwerwiegenden Straftaten es erfordere, bereits abweichendes Verhalten im Vorfeld der Strafwürdigkeit zu ahnden; nach der „Defensible-Space"-These wird das Wohnumfeld in unterschiedliche Zonen einteilt, wonach die Festlegung der Nutzungen unterschiedliche Verantwortungsstufen für den jeweiligen Raumausschnitt erzeuge. Städte und Gemeinden müssen daher in geeigneter Weise mit gesellschaftlichen Entwicklungen (Migration, Arbeitslosigkeit, soziale Polarisierung, politische Radikalisierung usw.) umgehen, die die Sicherheit beeinflussen.

Einsatzfelder globaler Fernerkundungssysteme

Der technologische Fortschritt im Bereich der globalen Fernerkundung im Bezug auf die zeitliche und räumliche Verfügbarkeit von Daten, die Datenqualität sowie der verbesserte Zugang zu globalen Fernerkundungsdaten hat deren breitere Anwendung und Integration (z.B. in GIS-Systeme) begünstigt. Die in den letzten Jahren kontinuierlich gesunkenen Kosten für die Datenübertragung und -speicherung haben diese Entwicklung unterstützt. Auch die mit der Technologie verbundenen Automatisierungspotenziale (z.B. bei der Interpretation von Fernerkundungsdaten) haben zu einer weiteren Verbreitung beigetragen, wenngleich die Zunahme der Datenmengen hierbei eine stetig wachsende Herausforderung darstellt. Die hohen Bereitstellungskosten von Fernerkundungsdaten sind aber nach wie vor eine erhebliche Hürde für deren weiter verbreitete Nutzung, auch wenn sich die Kostensituation mittlerweile durchaus differenziert darstellt. Während für einige Fragestellungen (beispielsweise Klimadaten) umfangreiche Datenbestände vergleichsweise kostengünstig (z. T. kostenlos) zur Verfügung stehen, können spezifische Datenanforderungen mit hochauflösenden Datensätzen (wie sie z.B. bei Sicherheitsfragestellungen entstehen) weiterhin mit hohen Kosten pro Szene verbunden sein. Die Anwendungsfelder von Daten globaler Fernerkundungsszenen

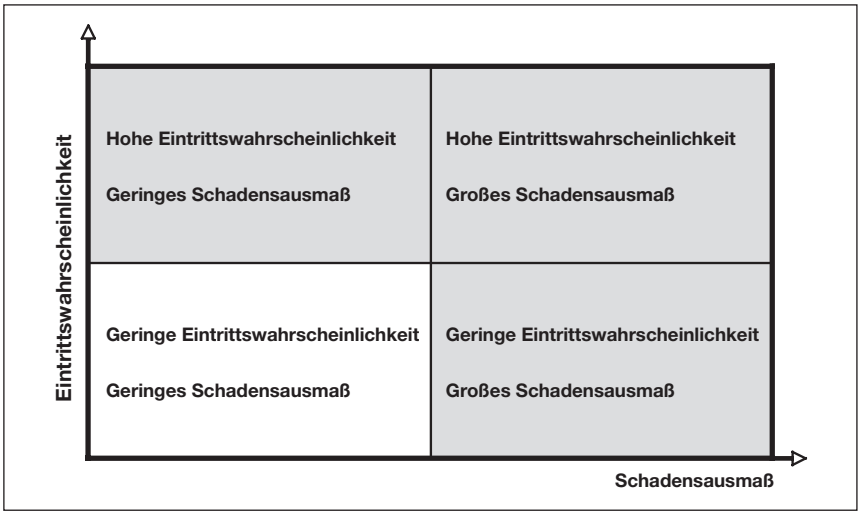

Abbildung 3: Anwendungsfelder von Fernerkundungssystemen

im Bereich „Sicherheit" konzentrieren sich daher auf Risiken und Bedrohungen mit hoher Eintrittswahrscheinlichkeit sowie auf Risiken und Bedrohungen mit geringer Eintrittswahrscheinlichkeit, aber großem Schadensausmaß (vgl. Abbildung 3).

Ob sich globale Fernerkundungssysteme zum Einsatz in den Anwendungsfeldern städtischer Sicherheit eignen, hängt von einer Reihe von Faktoren ab. Dazu zählen

- die zeitliche Verfügbarkeit der Daten;
- die Periodizität von Daten;
- die Kosten der Datengewinnung;
- die Aussagekraft der Daten;
- die Automatisierungspotenziale;
- das Vorhandensein alternativer Datengewinnungsmethoden;
- die Verknüpfbarkeit von Daten mit anderen Datenbeständen;
- die Integrationsmöglichkeit in bestehende Auswertungssysteme (z.B. GIS-Systeme);
- die Qualifikation der Entscheidungsträger und Mitarbeiter.

Als Vorteile des Einsatzes von Sicherheitstechnik werden immer wieder genannt (vgl. u.a. DStGB 2003):

- die Programmier- und Parametrierbarkeit von Sicherheitstechnik und damit die Zuverlässigkeit des Funktionierens;
- die Effizienz von Sicherheitstechnik aufgrund der hohen Verfügbarkeit, Dauerhaftigkeit, technischen Wirksamkeit und Genauigkeit;
- die Innovationsorientierung von Sicherheitstechnik;
- die Kosten-Nutzen-Effizienz, die insbesondere unter Berücksichtigung von potenziellen verhinderten Schäden, verminderten Versicherungskosten usw. bewertet werden muss.

Die Rolle globaler Fernerkundungssysteme im Bezug auf die Sicherheit in Städten und Gemeinden muss im Kontext der Anwendung von Sicherheitstechnologien insgesamt diskutiert werden. Die Sicherheitsdiskussion in Europa hat eine Vielzahl neuer Anwendungsfelder für technische Sicherheitslösungen entstehen lassen, die aber nur teilweise die städtische Sicherheit betreffen und die sich auch nur teilweise zur Nutzung globaler Fernerkundungssysteme eignen (vgl. Abbildung 4).

– Personenzugangskontrollen **– Personenscanning** **– Gepäckscanning**	**– Fahrzeugzugangskontrollen** **– Warenkontrollen** **– Fahrzeugscanning** **– Transportbehälterscanning** **– Warenscanning**	**– Fernüberwachung von** – öffentlichen Räumen – Straßen – Energieversorgung
Grenzüberwachung an Land	**Grenzüberwachung auf See**	**Luftraumüberwachung**
Aufklärung	**Hafen- und Schiffssicherheit**	**Wasserqualitätsüberwachung**
Grundstücksschutz	**– CBR Sicherheit** **– EMP Sicherheit**	**Daten- und Datennetzsicherheit**

Abbildung 4: Neue Anwendungsfelder für technische Sicherheitslösungen in Europa

Neben Fernerkundungssystemen zur Datengewinnung gibt es eine Vielzahl weiterer sicherheitstechnischer Systeme in den Städten und Gemeinden:

- Informationssysteme (für Akteure und Bürger);
- Warnmittel und Warnsysteme (für die Bürgerbenachrichtigung);
- Expertensysteme (zur Entscheidungsunterstützung);
- Vorgangsbearbeitungssysteme (zur Kooperation bei extrem heterogener Akteursstruktur);
- Auskunftssysteme (für Akteure und Bürger);
- Messnetze (zur Informationsgewinnung und Alarmierung);
- Geodaten-basierte Anwendungen (zur räumlichen Analyse und Prognose potenzieller und tatsächlicher Schadensereignisse);
- Data Mining (zur Erstellung umfassender Profile);
- Augmented Reality (zur Unterstützung von Helfern und Entscheidern);
- Ubiquitous Computing (zur umfassenden Vernetzung).

Weitgehend unstrittig ist die Anwendung globaler Fernerkundungssysteme für die Beobachtung der Landoberfläche, den Schutz der Atmosphäre, das Krisenmanagement und den Katastrophenschutz, die Überwachung von Großereignissen und die Überwachung sicherheitskritischer Infrastrukturen. Strittig sind dagegen Fragen, die den Zusammenhang von globalen Fernerkundungssystemen und den Schutz der Privatsphäre betreffen. Besonders stark diskutiert werden dabei z. Z. öffentlich zugängliche globale Fernerkundungsdaten (z.B. Google Maps) und deren Verknüpfung mit anderen Datenbeständen (z.B. Fotos von Gebäuden im Rahmen von Google Streetview). Dieses Beispiel macht deutlich, wie wichtig eine integrierte Betrachtung der eingesetzten Sicherheitstechnologien ist. In den Städten und Gemeinden ist eine Vielzahl von Anwendungsmöglichkeiten von Sicherheitstechnik denkbar. Vor allem die Kombination unterschiedlicher Sicherheitstechniken wie die globale Fernerkundung, die Videoüberwachung (vgl. Hempel 2003, Wehrheim 2004), die Nutzung biometrischer Merkmale für die Identifikation (vgl. Horvath 2005) und die kontaktlose Datenübermittlung beispielsweise bei RFID-Systemen (vgl. DStGB 2003, Glitza 2004) ermöglicht die Entwicklung komplexer Identifikations-, Zugangs- und Überwachungssysteme, die zur Regelung der Zugänglichkeit bestimmter Stadtbereiche (Innenstädte, ÖPNV, Botschaften, Ministerien, Behörden usw.) eingesetzt werden können und die Überwachung größerer Stadtbereiche und deren individuelle Nutzung ermöglichen. Schon heute werden derartige konvergente Technologien genutzt,

wobei globale Fernerkundungsdaten dabei bisher eine untergeordnete Rolle spielen. Einerseits besteht das Bedürfnis, die technischen Möglichkeiten zur Gefahrenabwehr umfassend zu nutzen, andererseits entstehen mit zunehmender Erfassung von personenbezogenen oder personenbeziehbaren Daten in ihrer stadträumlichen Differenzierung und den Möglichkeiten der Verknüpfung von Einzeldaten völlig neue Potenziale der Überwachung. Die Verknüpfung von globalen Fernerkundungsdaten und Katasterdaten sind eine derartige sensible Schnittstelle. Neben der technischen Konvergenz spielt in diesem Zusammenhang aber auch die organisatorische Konvergenz eine besondere Rolle. Mit der zunehmenden Vermischung von Aufgaben der Gefahrenabwehr der inneren und äußeren Sicherheit und dem Wunsch einer möglichst umfassenden informationsbasierten Lagebeurteilung kann die Verknüpfung von Einzelinformationen verbunden sein, die sich zu einem umfassenden individuellen Datenprofil verdichten lassen. Die immer wichtigere Rolle von privatwirtschaftlichen Akteuren als Besitzer, Verwalter und Bereitsteller von Geodaten bringt eine neue Facette in die Datenschutzdiskussion. Ohne gleich das monströse Bild des „gläsernen Menschen" zu zeichnen, entsteht doch durch die technischen und organisatorischen Konvergenzprozesse eine bisher nie vorhandene Möglichkeit, umfassende Informationen über den Einzelnen zu gewinnen. Auch die Gefahr, dass Daten *ex post* für Zwecke genutzt werden, die ursprünglich autorisiert waren, wächst mit der zunehmenden technischen und organisatorischen Vernetzung (vgl. Floeting 2006).

Auswirkungen einer sicherheitstechnischen „Aufrüstung" auf die Stadtentwicklung

Mit einer veränderten Gefahrensituation, der Zunahme des Einsatzes von Sicherheitstechnik in bestimmten Räumen der Städte und dem Bedeutungsgewinn von Sicherheitsfragen für das Leben in den Städten sind eine Reihe möglicher Entwicklungen verbunden. Zu erwarten sind sowohl grundsätzliche Veränderungen von Einstellungen gegenüber Städten, langfristige Veränderungen der baulich-räumlichen Strukturen als auch Veränderungen in der Nutzung von Stadträumen. Beispielhaft seien einige Bereiche angesprochen, die zu diskutieren wären:

– Städte könnten zunehmend als unsichere Orte wahrgenommen werden, weil sie als unübersichtlicher Raum mit unübersichtlichen Risiken und Bedrohungen wahrgenommen werden.

- Die zunehmende oder lang anhaltende Bedrohung könnte mit einer verstärkten „Aufrüstung“ durch Sicherheitsmaßnahmen, -technologien und -architekturen verbunden sein.
- Vermeintliche „Archipele der Sicherheit“ wie Shopping Malls, Bahnhöfe, innerstädtische Plätze, Business Improvement Districts und Gated Communities könnten entstehen.
- Stadträume könnten nach ihrem Sicherheitsstatus unterschiedlich bewertet werden. Globale Fernerkundungsdaten könnten in Kombination mit anderen geobasierten Daten die Folie bilden, auf der die Sicherheitsbewertungen abgebildet werden. Die Folge wäre eine Polarisierung in sichere und unsichere Räume, wobei gerade die in Zukunft z.B. aufgrund der demographischen Entwicklung und des fortschreitenden technologisch-ökonomischen Strukturwandels zunehmenden Zwischennutzungen auf „ungeordneten Flächen“ als unsichere Flächen wahrgenommen werden könnten.
- Zwischen unerwünschten Nachbarschaften könnten „Kontrollzonen“ oder „Sicherheitszonen“ entstehen. Je nach gewünschtem Sicherheitsstatus könnten – temporär begrenzbare – Zugangsbeschränkungen für bestimmte Stadtbereiche ausgesprochen und technisch überwacht werden.
- Öffentliche Räume würden ihren Charakter durch zunehmende technische Überwachung verändern, bis hin zum Verlust von öffentlichen Räumen und zur Vermischung von öffentlichen und privaten Räumen.
- Neue Sicherheitsregimes könnten Auswirkungen auf die Infrastrukturplanung haben, z.B. könnte es für notwendig angesehen werden, die Gestaltung von Zugangsbereichen der Verkehrsinfrastruktur zu verändern (wie im Bereich der Flughäfen mittlerweile schon z. T. umgesetzt) und Einschränkungen bei der Verknüpfung von Verkehrsträgern vorzunehmen.
- Die städtebauliche Gestaltung könnte erheblich von den Sicherheitsüberlegungen – zumindest an exponierten Standorten – geprägt werden, mit erheblichen Auswirkungen auf die Stadtgestalt in Zentren, in denen sich derartige Standorte konzentrieren (z.B. Berlin oder Frankfurt a. M.).
- Umfassende stadträumliche Sicherheitskonzepte könnten implementiert werden (wie das Londoner Beispiel zeigt).
- Veränderte Sicherheitsbedingungen haben auch Auswirkungen auf die Umsetzbarkeit von Großereignissen, die zu einem gern eingesetzten Instrument neuerer Stadtentwicklungspolitik im Rahmen der Inszenierung von Räumen geworden sind.

– In letzter Konsequenz könnte das subjektive Unsicherheitsgefühl mit einer Verlagerung von Aktivitäten in den virtuellen Raum verbunden sein.
– Schließlich stellt sich die Frage, wie Städte aussehen, die bei sinkenden finanziellen Mitteln zunehmende Anteile für Sicherheitsinfrastruktur investieren müssen oder wollen (vgl. Floeting 2006).

Städte werden sich in Zukunft in stärkerem Maß mit Sicherheitsfragen auseinandersetzen müssen. Dabei darf es nicht nur um die unmittelbar handlungsleitenden Fragen des Umgangs mit Gefahren-, Bedrohungssituationen und Schadensereignissen gehen. Darüber hinaus geht es um eine Auseinandersetzung mit den langfristigen Folgen der Eingriffe von Maßnahmen der Inneren Sicherheit für das Leben in den Städten.

Fazit

Eine auf Risikoabschätzungen basierende integrierte städtische Sicherheitspolitik muss die Unterschiede zwischen subjektiver Risikowahrnehmung und professioneller Risikoeinschätzung berücksichtigen, ohne die subjektiven Unsicherheiten der Bürger „wegzudiskutieren". Sicherheitstechnologien können zur Begrenzung von Risiken und zum besseren Umgang mit ihnen beitragen. Der Einsatz von Sicherheitstechnologien im städtischen Kontext wird aber bisher polarisiert diskutiert. Chancen und Risiken ihres Einsatzes werden bisher kaum in ihrem spezifischen Anwendungskontext betrachtet. Das Zusammenwirken unterschiedlicher Sicherheitstechnologien wird dabei kaum berücksichtigt. Globale Fernerkundungssysteme sind nur in ausgewählten Bereichen der urbanen Sicherheit einsetzbar. Sie sind eine wichtige Grundlage geodaten-basierter Anwendungen. Negative gesellschaftliche Wirkungen der sicherheitstechnischen „Aufrüstung" resultieren unmittelbar eher aus anderen Sicherheitstechnologien. Technische und organisatorische Konvergenzprozesse verändern jedoch auch die Rolle globaler Fernerkundungssysteme im Kontext neuer urbaner Sicherheitsregimes, die häufiger als Antwort auf *ad hoc* formulierte Sicherheitsanforderungen entstehen und weniger als Ansätze einer integrierten städtischen Sicherheitspolitik planmäßig entwickelt werden.

Dipl.-Geogr. Holger Floeting
Deutsches Institut für Urbanistik (Difu), Berlin
Arbeitsbereich Wirtschaft und Finanzen

Literaturverzeichnis

Bundeskriminalamt, Polizeiliche Kriminalstatistik 2006 Bundesrepublik Deutschland, Wiesbaden 2007

Deutscher Städte- und Gemeindebund (DStGB), Kommune schafft Sicherheit. Trends und Konzepte kommunaler Sicherheitsvorsorge, Verlagsbeilage „Stadt und Gemeinde interaktiv", Ausgabe 12/2003

European Police Office, EU Terrorism Situation and Trend Report, The Hague 2008

Floeting H, „Sicherheitstechnologien und neue urbane Sicherheitsregimes", in: ITA manu:script, Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften, Wien 2006

Glitza KH, Mundwasser gegen einen Hauch von Toll Collect. CD Sicherheitsmanagement 4/2004, 125–129

Häfele J, „(Un-)Sicherheit in städtischen Räumen", Vortrag beim Seminar „Sichere Städte – Herausforderungen und Handlungsmöglichkeiten kommunaler Sicherheitspolitik" des Difu (Deutsches Instiut für Urbanistik), 21.4.2008 in Berlin (unveröffentlicht)

Häfele J, „Incivilities, Kriminalität und Kriminalpolitik", in: Neue Kriminalpolitik 18/2006, 104–109

Hempel L, „Verdrängen statt Vorbeugen", Telepolis, 15.1.2003, http://www.heise.de/tp/r4/artikel/13/13928/1.html (19.3.2009)

Horvath J, Prepare to be scanned. Biometrics and the surveillance society, Telepolis, 2.8.2005, http://www.telepolis.de/r4/artikel/20/20635/1.html (19.3.2009)

Kron W, „Land unter beim Hochwasserschutz", in: Süddeutsche Zeitung, 20.4.2006

Münchener Rück, Stürme – weltweit bedeutendste Elementargefahr, 2008, http://www.munichre.com/de/ts/geo_risks/natural_catastrophes_and_risks/windstorm/default.aspx (19.3.2009)

Newman O, Creating Defensible Space, U.S. Department of Housing and Urban Development, Office of Policy Development and Research, Washington D.C. 1996

Rauch E, Windstorm – the most significant hazard worldwide, http://www.munichre.com/en/ts/geo_risks/natural_catastrophes_and_risks/windstorm/default.aspx (19.3.2009)

R+V Versicherung AG, Die Ängste der Deutschen, 2008, http://www.ruv.de/de/presse/r_v_infocenter/studien/aengste_deutsche_2008.jsp (19.3.2009)

Schreiber V, Lokale Präventionsgremien in Deutschland, Frankfurt am Main 2007

Schütz H, Peters HP, „Risiken aus der Perspektive von Wissenschaft, Medien und Öffentlichkeit", in: Aus Politik und Zeitgeschichte, B10–11, 2002, 40–46

Wehrheim J, „Städte im Blickpunkt Innerer Sicherheit", in: Aus Politik und Zeitgeschichte, B44, 2004, 21–27

Wilson GL, Wilson JQ, „Broken Windows". in: The Atlantic, March 1982

Über ubiquitäre IuK-Technik, Fernerkundung, Sicherheitsfragen und Erkenntnisinteressen

Andreas Metzner-Szigeth

1 Einleitung

Wenn man es mit neuartigen Phänomenen zu tun hat, oder mit Prozessen, die mitten im Fluss des Geschehens liegen, ist es womöglich eine gute Herangehensweise, von der Gewohnheit Abstand zu nehmen, sie abschließend behandeln zu wollen. Sich damit zu begnügen, sie erschließend zu bearbeiten, mag zwar unbefriedigend sein, ist aber in diesem Fall weiterführend. Solche Entwicklungen zu beurteilen, um zu ihrer Gestaltung beizutragen, verlangt schon von der Sache her nach Sensibilität und Offenheit, vor allem aber nach einer gehörigen Portion Respekt ihnen gegenüber. Warum? Nun, solange diese Entwicklungsprozesse in „statu nascendi" sind, sich also in einem frühen Stadium befinden, bleiben sie – bei aller Fähigkeit zur Einsicht, die wir uns selbst gern attestieren – zumindest teilweise undurchschaubar, nicht zuletzt mit Blick auf ihre Konsequenzen. Und gemeint sind damit weniger ihre Folgen für das schlicht Bestehende als vielmehr die Kräfte, die sie im dynamischen Fortgang der Ereignisse freisetzen – besonders jene, die dazu geeignet sind, die Zielsetzungen und Wertvorstellungen, an denen uns liegt, unweigerlich in ihren Wirkungskreis hinein zu ziehen. Wenn man das engere Thema (einer Reflexion über die Rolle der Satellitentechnik für all jene Sicherheitsfragen, die uns wichtig genug sind, um sie an die erste Stelle unserer Tagesordnung zu setzen) hinreichend gut erschließen will, um ihre Pros und Kontras angemessen zu diskutieren, muss man es also notwendigerweise aus einem weiteren Rahmen heraus entwickeln. Nach dem ersten Punkt, der „Einleitung", in der wir uns gerade noch befinden, fährt mein Beitrag daher zweitens mit der Skizzierung dieses Rahmens fort, und zwar unter dem Titel „Konvergenz und Transformation". Darauf folgt drittens eine Erörterung zum Thema „UC, RFID und der Beitrag der Satelliten". Der vierte und schließliche Punkt ist kein Resümee, sondern ein „Ausblick", der sich der Frage nach der Sicherheit und ihrer Gestaltung widmet.

2 Konvergenz und Transformation

2.1 Leitfragen

Einem kritischen Erkenntnisinteresse folgend, kann es nicht nur um einen beschreibenden Anspruch gehen. Vielmehr sind emanzipatorische Interessen und gestaltungsorientierte Momente geltend zu machen. Um das Feld der gesellschaftlichen Transformationsprozesse in ihrer Verbindung mit den Einflüssen technisch-medialer und infrastruktureller Entwicklungen gedanklich zu erschließen, dienen daher zwei Leitfragen: 1.) Was ist die „Natur" der sozio-kulturellen, politisch-ökonomischen und psycho-sozialen Veränderungen, welche dabei sind – in den Zusammenhängen der rapiden Entwicklung von Informations- und Kommunikationstechnologien (ICT) im Allgemeinen und der computervermittelten Kommunikation (CMC) im Besonderen – unsere Lebens- und Arbeitswelten umzugestalten? Und 2.) Wie können wir Einfluss darauf nehmen, dass die Potentiale von Internet, computervermittelter Kommunikation und digitalen Medien sinnvoll und konstruktiv eingesetzt und fortentwickelt werden? Da leicht einzusehen ist, dass beide Fragen nicht beantwortet werden können, ohne die Zusammenhänge und Wechselwirkungen zwischen den Dimensionen des Sozialen und des Technischen aufzuschließen, soll genau diese Aufgabe in das Zentrum der weiteren Erörterung gestellt werden.

2.2 Konvergenz

In Forschung und Lehre ist es wichtig, sich mit je einzelnen Themen intensiv zu befassen – etwa mit „Virtual Reality"-Systemen, der „netz-basierten" Wissens-Kommunikation oder „Location-based Technologies". Meiner Meinung nach kann das aber nur dann wirklich gut gelingen, wenn man das je einzelne Thema erstens mit Blick auf die beiden (gerade erwähnten) *Leitfragen* erschließt, und zweitens die Charakteristika des einzelnen Komplexes, Problems oder Mediums, das hierbei im Mittelpunkt steht, in den Zusammenhängen der *Konvergenz* von ICT, CMC und digitalen Medien herausarbeitet.

Systematisch zu berücksichtigen sind so die Folgewirkungen und Gestaltungspotentiale, die sich wesentlich innerhalb und durch den Prozess der Konvergenz[1] entfalten. Einerseits ist das die Konvergenz von Technologien, nämlich vor allem die der Datenverarbeitung (Computer), der Signalübertragung (Telefon, Funk), sowie der Präsentationserzeugung, inklusive Aufzeichnung und Wiedergabe derselben (von der Fotografie über den Film bis hin zur Virtuellen Realität im engeren Sinne). Wesentlich angetrieben wird sie inzwischen durch das ihnen gemeinsame Moment

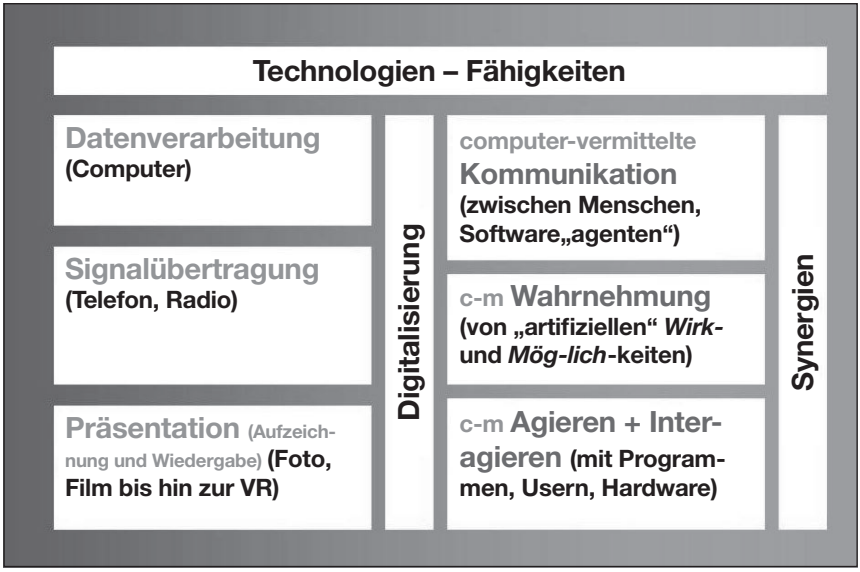

Abbildung 1: Konvergenz

[1] Auf die Vielschichtigkeit der weiteren Konvergenzprozesse, also zwischen Technologien, Infrastrukturen und den Ebenen, auf denen Inhalte, Anwendungen und Dienstleistungen gestaltet und vermarktet werden (vgl. OECD 1998:15f.), kann hier ebenso wenig näher eingegangen werden, wie auf die Diskussion von gegenläufigen Bewegungen, Hindernissen und Fragen der Beurteilung der damit verbundenen Gestaltungsmöglichkeiten. Vgl. im engeren Sinne der hier artikulierten These auch die Kompilationen verschiedener Trends im Rahmen einer BDI-/FhG-Studie (vgl. Wahlster/Weyrich 2002, besonders S. 20 „Plattform für die Konvergenz aller Medien“) sowie die Ausführungen in Keil-Slavik (2003) über „Mediatronic“, die darüber hinaus hinsichtlich der Verbindungen von Vernetzung und Vergesellschaftung interessant sind.

der *Digitalisierung*. Zum anderen geht es um Konvergenz im Sinne der Kombination menschlicher Fähigkeiten, die mit ihrer Hilfe ausgebaut werden, also vor allem die Funktionen der computer-vermittelten Kommunikation, der computer-vermittelten Wahrnehmung und des computer-vermittelten Agierens und Interagierens. Triebkraft dieser Konvergenz sind im Wesentlichen die *Synergien*, die sich durch ihren kombinierten und simultanen Einsatz erreichen lassen.

Anzumerken bleibt, dass hier keine systematische Unterscheidung von „Technik" und „Technologie" vorgenommen wurde, erstens, weil sie im außerdeutschen Sprachraum keine Rolle spielt, vor allem keine wissenschaftlich signifikante, und zweitens, weil sowieso komplexere Unterscheidungen erforderlich sind, nämlich mindestens die zwischen den Bedeutungsebenen der artefaktischen Technik, des technischen Handelns, des technischen Wissens und der Technikkultur.[2]

Hinzuweisen ist ferner darauf, dass es bei der gerade angesprochenen Erweiterung „menschlicher Fähigkeiten" darum geht, etwas tun zu können, das man in dem Ausmaß, der Qualität, der Reichweite und dieser Folgewirksamkeit bisher so nicht tun konnte, was nicht nur Lernprozesse voraussetzt, sondern auch die Inanspruchnahme technischer Assistenz, und in diesem Sinne über das hinausgeht, was der Begriff der „Kompetenzen" aussagt.[3]

Das Internet hat inzwischen schon einige Entwicklungsphasen durchlaufen. Damit verbunden ist klar, dass es sich auch anders hätte entwickeln können, als es geschehen ist, und dass seine vitale Entwicklungsdynamik zwar nicht ungebrochen, wohl aber zukunftsoffen ist. Wenn also gegenwärtig, in einer – für die Moderne eher uncharakteristischen – Art von „status quo"-Fixierung, so getan wird, als ob die Geschichte – zumindest im Prinzip – damit zu Ende erzählt wäre, geschieht dies aller historischen Evidenz und aller (r)evolutionären Perspektiven

---

[2] Wobei die Bedeutungsebene der „artefaktischen Technik" mehr oder minder dem deutschen „Technik"-Begriff entspricht, jedenfalls in seiner zu kurz gegriffenen Unterscheidung gegenüber der „Technologie", die wiederum mit der (keineswegs kongruenten) Bedeutungsebene des „technischen Wissens" korrespondiert.

[3] Der Begriff der „Kompetenzen" reicht hier nicht hin, insofern er entweder im Sinne von Befugnissen etwas zu tun (oder zu lassen) verstanden wird oder im Sinne erlernter Fähigkeiten etwas erkennen, machen oder in einer bestimmten Weise handeln, Aufgaben bewältigen oder Probleme lösen zu können. „Fähigkeiten" geht insofern darüber hinaus, als nicht nur einzelne Personen gemeint sein müssen, sondern darüber hinaus die Ausstattungen derselben, die sie „befähigen", d. h. in den Stand versetzen, etwas Besonderes tun zu können, was sie ohne die („kompetente") Nutzung technischer Mittel nicht tun könnten (wie am Beispiel einer Taucherausrüstung zu illustrieren ist, die einen Taucher – entsprechende „Kompetenzen" vorausgesetzt – in die Lage versetzt, unter Wasser zu arbeiten oder seinem Hobby nachgehen zu können).

zum Trotz (vgl. u. a. Münker/Roesler 1997; Maresch/Rötzer 2001; Metzner-Szigeth 2007). Diese m. E. ideologisch bedingte, etwas kurzschlüssige Haltung wird von manchen Autoren ganz ungeachtet der Tatsache eingenommen, dass man wahrlich kein Prophet oder Visionär sein muss, um etwa für die nahe Zukunft zu bemerken, dass es

1.) in einem Prozess der Verflechtung von Internet und Mobiltelefon zu einer *Entörtlichung* gesellschaftlicher Informations- und Kommunikationspraktiken kommt, d. h. zu einer beträchtlich ortwechselflexibilisierten Netzkommunikation;

2.) zu einer sukzessiven *Durchdringung* aller möglichen arbeits- und lebensweltlichen Interaktionszusammenhänge oder Handlungsfelder durch Technologien des „pervasive" oder „ubiquituous computing" (vgl. Hilty et al. 2003; Siemoneit 2003) kommt, und

3.), was die Formen der netzbasierten Kommunikation angeht, zur Ablösung (d. h., exakter formuliert, zur Verdrängung auf den zweiten Platz) der textbasierten Kommunikation durch eine weiter um sich greifende *Multi-Medialisierung* der Menge an Einzeldiensten, wie E-Mail, IRC etc. (zur Trendübersicht vgl. Wahlster/Weyrich 2002).[4]

2.3 Grundsatzthese

Ausgehend von der (digitalen und synergetischen) Konvergenz stellt sich natürlich die Frage „wie" diese mit den psycho-sozialen, politisch-ökonomischen und soziokulturellen Veränderungen korrespondiert. Meine Grundsatz-These hierzu ist, dass die fraglichen Transformationen nicht einfach eine Folge erweiterter Kapazitäten von Symbolverarbeitung, Signalübertragung und Präsentationserzeugung oder auch der erweiterten Möglichkeiten ihrer Nutzung und breiten Anwendung sind, sondern sich Internet, CMC und digitale Medien wesentlich dadurch auszeichnen, dass sie die Verhältnisse von Raum und Zeit sowie von Virtualität und Realität in einem bisher unbekannten Ausmaß verfügbar und gestaltbar machen, sie auf komplexe Weise „umstricken" (vgl. hierzu u. a. Giddens 1990, Läpple 1991, Großklaus 1995 sowie Gunkel und Gunkel 1997).

---

[4] Zwar nicht unbedingt in ferner Zukunft, aber erheblich weiter weg liegt die *Virtualisierung* im engeren Sinne, d. h. die artifizielle Erzeugung dreidimensionaler, mit Bezug auf den „User" interaktionsfähiger, begehbarer Handlungs- bzw. Kommunikations-Umgebungen und vor allem die (was ihre Praktikabilität angeht) wohl ziemlich voraussetzungsvolle Verknüpfung der Virtual Reality (VR)-Technologie mit dem Netz (der Internet-Technologie), die völlig offen steht, nicht zuletzt hinsichtlich der damit verfolgten Ziele.

So richtig es ist, dass jeder „User“ ohne nennenswerte Verzögerung zwischen Senden und Empfangen Nachrichten zu jeder Zeit an jeden beliebigen Ort schicken (oder von dort erhalten) kann, so falsch ist es, daraus zu folgern, Raum und Zeit würden als wesentliche Dimensionen unserer Wirklichkeit an Bedeutung verlieren. Das Gegenteil ist der Fall, denn wo der „Aufenthalt“ in Ort und Zeit früher fraglos vorausgesetzt oder kontextuell wahrscheinlich war, muss dies im heute recht häufigen Bedarfsfall innerhalb der (Netz- und/oder Mobil-)Kommunikation nachgefragt und mit Mitteln der Kommunikation selbst geklärt werden, wo die Kommunikationspartner sich befinden, wie viel Uhr es dort ist, ob die Sonne scheint oder es schneit, und andere kontextuelle Relevanzen mehr. Castells’ „Raum der Ströme“ (vgl. Castells 2001a:431ff.) ist freilich ein besonderer Fall, der sich in der Tat durch seine Ortlosigkeit und seine Eigenzeit auszeichnet, insofern hier in einer Sphäre der globalen elektronischen Zirkulation mit Wertpapieren (oder eben gerade nicht mehr „Papieren“) gehandelt wird, auf einem Markt, der die Charakteristika des Markt„platzes“ abgestreift hat.

Statt der Vertretung eindimensionaler Thesen, die etwa die „Aufhebung“ (oder gar „Vernichtung“) von Raum und Zeit im Sinne ihrer gesellschaftlichen Kulturbedeutsamkeit durch elektronische Kommunikation propagieren, und mit Virtualität nur etwas assoziieren, was im positiven oder (meist) negativen Sinne auf eine „Enthebung“ aus der Realität hinausläuft, muss – so die forschungspragmatische Konsequenz dieser Grundsatzthese – die sehr viel weitergehende und tiefer reichende Frage untersucht werden, „welche“ Gestaltungspotentiale den neuen Medien innewohnen, um neue Verhältnisse zu schaffen. Gemeint sind damit:

1.) neue Verhältnisse des räumlich-zeitlichen Aufeinander-Bezug-Nehmens von Kommunikations- und Interaktions-Sequenzen und

2.) neue Verhältnisse des Aufeinander-Verweisens distinkter Wirklichkeits-Ebenen: „wirklicher“, „imaginierter“, „repräsentierter“, „modellierter“, „simulierter“ und „virtualisierter“.

Beispiele dafür sind etwa (ad 1.) Online-Tauschbörsen, die Anbieter und Nachfrager über zeitliche und räumliche Distanzen hinweg zueinander führen, und zwar bis hin zu globalen Skalen, also bis hin zur Überbrückung von Tages- bzw. Arbeitszeiten und Nacht- bzw. Ruhezeiten sowie von Feiertagen und Wochenenden, und (ad 2.) Navigationssysteme, die unsere Sinneswahrnehmungen während des Autofahrens nicht nur auf die umgebende Wirklichkeit gerichtet sein lassen,

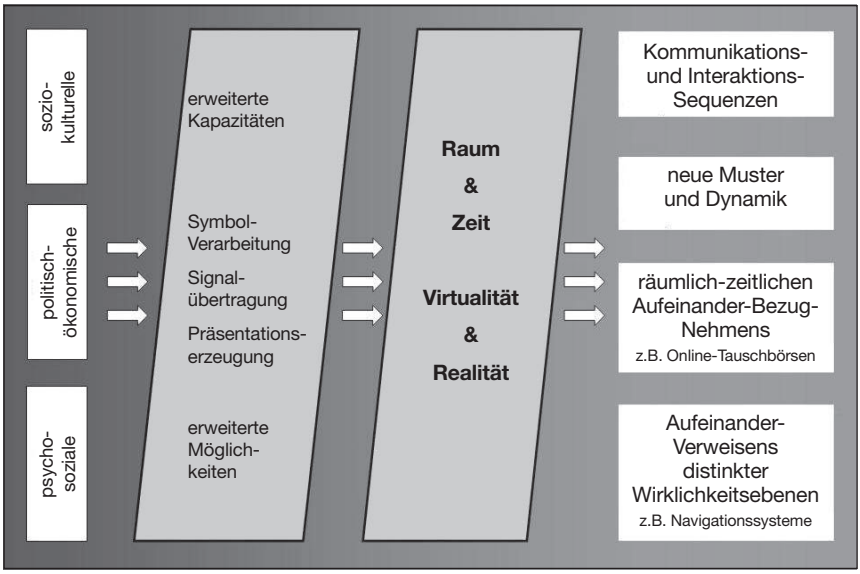

Abbildung 2: Grundsatzthese

sondern zusätzlich auf eine artifiziell erzeugte „Roadmap" richtet, sowie auf weitere textuelle und auditive Inputs.

Dinge sind eins oder liegen nebeneinander und Ereignisse sind eins oder folgen aufeinander – ohne die Kategorien von Raum und Zeit gäbe es weder ein Nebeneinander noch ein Nacheinander im Sinne ihrer Ordnung, und damit (wären) auch keine Ursache-/Wirkungs-Beziehungen zwischen ihnen (denkbar). Wenn es aber ohne (Bezugnahme auf) Raum und Zeit weder Identität noch Differenz gibt, gilt dies auch für das, was das menschliche Individuum ausmacht. Das Individuum kann sich nicht an zwei Orten gleichzeitig aufhalten (man kennt das vom Krimi), und es kann das, was seine „Personalität" ausmacht, nur in der Zeit entwickeln. Ohne einen in Raum und Zeit lebendigen, existierenden Körper also keine Person, keine menschliche Identität. Nichtsdestoweniger kann sich ein Avatar, dessen Rolle wir in elektronischen Kontexten annehmen, an einem anderen Ort aufhalten, und persönliche Softwareagenten können zu Zeiten, in denen wir anderes zu tun haben, unsere zeitliche Präsenz stellvertretend wahrnehmen.

Im Medium der Sprache lassen sich „Gegenstände“ oder „Ereignisse“ vorstellen, und mit diesen Vorstellungen lässt sich operieren, ohne konkret handeln zu müssen, ohne also die Gegenstände zu bewegen oder zu verändern, ohne die Ereignisse zu bewirken oder zu verhindern. Ohne Sprache gäbe es keine Möglichkeit die Wirklichkeit zu „verlassen“, Imaginationen zu haben, diese mitzuteilen und auszudrücken; das gesprochene Wort und das gemalte Bild – gemeinsam ist ihnen der symbolische Gehalt, die Fähigkeit für etwas Anderes stehen zu können.

Einzusehen ist daher, dass die Wechselspiele von Wirklichkeit und Imagination so alt sind wie die Menschheit selbst. Man kann sich die eigene Person oder eine fremde Person in Situationen vorstellen, sich vorstellen, wie sie handeln wird oder was sie sagen wird – kann mit diesen Vorstellungen im Medium der Sprache operieren, sie mitteilen, in Wort oder Bild – kann sie vertexten oder verbildlichen und im Schauspiel, Tanz oder in der Malerei ausdrücken. So gesehen ist die menschliche Identität ohne das Moment des Imaginativen ebenso wenig möglich wie ein „menschliches“ Leben, und zwar ganz unabhängig davon, dass das Neue, welches in dieses Verhältnis zusammen mit dem Netz-Medium eintritt, mit Castells trennscharf zu differenzieren ist, als einen Zusammenhang „realer Virtualität“ gestaltend (vgl. Castells 2001a:452, sowie in Verbindung zu Fragen von Individualisierung und Vergemeinschaftung Metzner-Szigeth 2008a).

Imagination (bzw. auf gut deutsch „Vorstellungskraft“) hat es immer gegeben. Auch die menschliche „Gesellschaft“ (selbst) *ist* imaginierte Wirklichkeit oder *arbeitet* zumindest mit Mitteln imaginierter Wirklichkeiten, wie z. B. des „Bestehens“ von Institutionen (etwa der Ehe, Korporationen aller Art, oder auch des Staates), die keineswegs in dem Sinne „dastehen“ können, wie etwa ein Gebäude. Handlungsorientierend „wirk“sam sind sie, weil wir daran glauben, dass sie es sind. Sie werden also im Resultat unseres ihr-Bestehen-für-wahr/wirklich/notwendig-Haltens als etwas – in unserem Verhalten bzw. Handeln – „Wirk“-liches hervorgebracht (vgl. Castoriadis 1984; vgl. auch Habermas 1985:380ff.). Davon zu unterscheiden ist das, was Castells „reale Virtualität“ nennt. Diese ist in der Tat neuartig, wenn auch Ergebnis von (jetzt in ihrer Digitalisierung verschmelzenden aber vormals getrennt verlaufenden) Entwicklungen, die historisch tief reichen (Signalübertragung, Datenverarbeitung, Aufzeichnung und Wiedergabe von Bild und Ton).

Ihre enorme Plastizität gewinnt die netzbasierte Kommunikation (CMC) vor dem Hintergrund der Universalität und Medialität des Computers, d. h. einer Maschi-

ne, die theoretisch dazu in der Lage ist, jede denkbare andere Maschine zu emulieren, und daher nicht nur als „Rechner" fungieren kann, sondern genauso gut als „Symbolverarbeiter" oder „Virtualitätsgenerator" und daher nicht nur ein Werkzeug oder eine Maschine darstellt, sondern selbst die Qualitäten eines Mediums annimmt (vgl. u.a. Krämer 1988; Schelhove 1997; vgl. orientierungsweise Bühl 2000:103ff.), welche auch in Eigenschaften ihrer Vernetzung überführt werden.

Die konventionelle (und leider immer noch gängige) Entgegensetzung von netzbasierter Kommunikation bzw. CMC (virtuell, körperlos, jenseits von Zeit und Raum) und „Face-to-Face"(F2F)-Kommunikation (real, körperlich, in Zeit und Raum) ist gerade in Anbetracht dieser Plastizität viel zu grobschnittig, verkürzt, zu verwoben, durchmengt mit anderen Themen, um analytischen Zwecken zu genügen.

- *Raum und Zeit* wurden schon früher mit Hilfe von Kommunikationsmedien (etwa auch schon solchen wie den – von Bruce Chatwin (1988) populär gemachten – „Songlines") überbrückt, und die gesellschaftlichen Beziehungen in diesem Kontinuum verändert, strukturiert und Umgestaltungen unterworfen.
- Auch ein Verhältnis von *Virtualität und Realität* gab es vorher, durch Techniken und Technologien der in (In-)Bildsetzung, angefangen von den neolitischen Höhlenmalereien in Altamira, über die Entdeckung der Perspektivik, die Ausstellungen im Louvre, das Kino, das TV, bis hin zu den derzeit verfügbaren VR-Technologien, die kaum mehr sind, als eine erste Realisierungsform ihrer Grundidee (vgl. Lem 1986).

Vorläufig abschließen will ich diesen Punkt hier mit einem kurzen Hinweis darauf, dass etwas zu beobachten ist, was man mit dem Begriff „lebensweltliche Hybridisierung" bezeichnen könnte. Ein dafür exemplarischer Fall liegt dann vor, wenn eine Person mit einem Handy durch die Stadt läuft, von keiner anderen Person begleitet, und andauernde Gespräche führt. Für einen Beobachter, der einer solchen Person begegnet, ohne sofort zu bemerken, das ein mobiles Telekommunikationsgerät im Spiel ist, ergibt sich fast zwangsläufig eine Irritation, denn irgendwie sind wir alle darauf disponiert, in solchen Situationen unwillkürlich hinzuhören, vielleicht, weil man möglicherweise selber angesprochen sein könnte. Wird dann bemerkt, dass man nicht gemeint ist, etwa weil kein Blickkontakt aufgenommen wurde, hat das schnell zur Folge, die beobachte Person während eines irritierenden Augenblicks für „nicht ganz normal" zu halten, weil sie in Selbstgesprächen versunken zu sein

scheint. Das Interessante dabei ist, wenn wir uns so verhalten, also gleichzeitig telefonieren und durch die Straßen der Stadt gehen, dass wir uns irgendwie in zwei Welten gleichzeitig bewegen, nämlich einer „normalen" physischen Umwelt und einem artifiziell erzeugten „elektronischen" Raum. Hinzu tritt, dass andere Personen, und damit Kommunikations- und Interaktionspartner, dies auch tun, was zu einer Auffächerung möglicher Konstellationen führt. Solche „Hybridisierungen" spielen jedenfalls eine immer größere Rolle. Sie haben Vorteile, etwa in Logistik und Handlungskoordination, führen aber auch zu Problemen, wie etwa im Zuge des reziproken Aufbaus der generellen Erwartung der permanenten Erreichbarkeit und Lokalisierbarkeit von Akteuren, oder bezüglich der Bewältigung einer unaufhörlich wachsenden Dichte an („push") Nachrichten und („pull") Informationen, sowie (last not least) dem Risiko von Zusammenstößen mit anderen Passanten oder Drehtüren, vor die man läuft, weil man statt auf die Gegend zu achten mit dem Telefon beschäftigt war.[5]

2.4 Forschungsfelder

Was die Gesellschaft angeht, verändern sich verbunden mit der Transformation ihrer kulturellen Grundlagen durch die breite Nutzung neuer Medien sowohl die Wirkungsbedingungen gesellschaftlicher Teilsysteme als auch die Arbeitsweise von Organisationen und die Interaktionsmöglichkeiten von Individuen. Entscheidend ist aber nicht einfach die Summe der Veränderungen aller Interaktionsfelder und Lebensbereiche, sondern vielmehr das sich wandelnde Verhältnis der Durchdringung und Abgrenzung „lebensweltlicher" und „systemischer" Kommunikations- und Handlungszusammenhänge. Von dieser theoretisch hergeleiteten These

[5] Und an dieser Stelle lohnt sich ein kleiner Exkurs, denn der tragische Einzelfall eines wegen der Verwendung von Navigationsequipment abgestürzten Reisebusses (vgl. eine Meldung des Tagesspiegels vom 26.7.2007 mit dem Titel „Fahrer folgte Navigationssystem – Bus stürzte ab"; http://www.tagesspiegel.de/weltspiegel/Busunglueck;art1117,2346658), deutet auf ein systematisches Problem hin. Dafür sprechen auch die Ergebnisse einer Umfrage zur Sicherheit von Navigationsgeräten, die das britische Versicherungsunternehmen „Direct Line" im Auftrag der Zeitung „Mirror" (vgl. http://www.mirror.co.uk/news/top-stories/2008/07/21/satnav-danger-revealed-navigation-device-blamed-for-causing-300-000-crashes-89520-20656554/) durchgeführt hat: Jeder zehnte Teilnehmer gab an, schon einmal unerlaubt auf Befehl seines Navigationsgeräts gewendet zu haben. Ein Viertel der Befragten wurde mindestens einmal von seinem elektronischen Begleiter falsch herum in eine Einbahnstraße gelenkt und ein Drittel wird durch sein Gerät manchmal verwirrt. Immerhin noch jeder fünfzigste britische Autofahrer gab an, wegen seines „Navis" schon einmal einen Unfall verursacht oder fast verursacht zu haben. Das entspricht einer Anzahl von 300.000 Autofahrern.

aus ist die programmatische Konsequenz abzuleiten, dass es geboten ist, diese Neuordnungsprozesse, die Herde gesellschaftlicher Auseinandersetzungsprozesse und Interessenskonflikte darstellen, zu Zwecken ihrer empirischen Untersuchung systematisch zu erschließen. Ihre Bedeutung lässt sich etwa anhand der folgenden vier Forschungsfelder zeigen (vgl. ursprünglich Banse und Metzner-Szigeth 2003), die nun anhand von Abbildung 3 erläutert werden.

1. *„Identität und Gemeinschaft":* Hierbei geht es um die sich verändernden Muster der Identitätsbildung und der Vergemeinschaftung, um die Assoziationsformen zusammen lebender, gemeinsam handelnder und miteinander kommunizierender Personen. Auf diese wird einerseits durch die mittels ICTs ermöglichte Entbindung und Neuverschränkung von raum-zeitlichen Zusammenhängen zwischen ihnen eingewirkt. Andererseits wird auf sie eingewirkt über die veränderte Wahrnehmung von sich selbst und von anderen, infolge des durch die ICTs veränderten Verhältnisses von Wirklichkeit und Virtualität (z. B. Ano- und Pseudonymisierung). Beispiele für das Forschungsfeld von Identität und Gemeinschaft sind das Phänomen des „Gender-Switching" in elektronischen Foren oder das Hineinschlüpfen in Avatar-Identitäten im Kontext entsprechend ausgestatteter Chat-Umgebungen oder Spielwelten. Dort werden auch die mit diesen Identitäten korrespondierenden Zugehörigkeiten zu lebensweltlichen Gruppierungen oder Fantasy-Clans angenommen und demonstriert. Beispiele, die die Breite des Spektrums solcher Arrangements illustrieren, sind etwa „The WELL" („Whole Earth 'Lectronic Link"),[6] eine elektronische Gemeinschaft, die sich dem Gedankenaustausch und der Kreativität verschrieben hat, und schon in der „Gründerzeit" des Internet etabliert wurde (seit 1985 online), oder heutzutage „Second Life"[7] oder „World of Warcraft"[8], wo der Aufbau von bzw. das Handeln in „Fantasy"-Welten im Vordergrund steht, welche animationstechnisch hoch aufgerüstet sind und teils mit einem nicht unerheblichem Suchtpotential verbunden daherkommen.
2. *„Wissen und Wirtschaften":* Hierbei geht es einerseits um die sich – nicht zuletzt infolge des Einsatzes von ICTs – verändernde Relation der Produktionsfaktoren Arbeit, Kapital, Natur und Wissen, zum anderen aber um ein sich – in einem

[6] Vgl. http://www.well.com/.

[7] Vgl. http://de.secondlife.com/.

[8] Vgl. http://www.worldofwarcraft.com/.

Abbildung 3: Forschungsfelder

inneren Zusammenhang damit – wandelndes Verhältnis, nämlich das zwischen privaten und öffentlichen Gütern, in dem sich alles um Vorleistungen und Verwertungsrechte dreht, die bestimmen, wie vorhandenes Wissen zur Herstellung neuen Wissens genutzt werden kann, und in dem die Aneignung der Ware oder des Gemeinguts „Wissen" anders verläuft und neu verteilt wird. Beispiele dafür verbinden sich mit den Stichworten „digital rights" versus „open source" oder auch Fragen des „tacit" oder „impliziten" Wissens oder des „autochthonen" Wissens, das hier von technisch und organisatorisch hoch entwickelten Unternehmen erschlossen, angeeignet (möglicherweise auch ohne Gegenleistung) und im Zuge der Herstellung von vermarktbaren (Wissens-)Produkten verwertet wird.

3. *„Privatheit und Öffentlichkeit":* Hierbei geht es um den (fortschreitenden) Strukturwandel der Öffentlichkeit, der zusammen mit den multidirektionalen Kommunikationsmöglichkeiten der ICTs in eine weitere Phase eintritt, in der das (ursprüngliche) Verhältnis ihrer Verbindungen zur Sphäre des Privaten (einmal mehr) verschoben und rekonfiguriert wird, was seinerseits nicht ohne

Folgen für die politische Verfasstheit der Gesellschaft bleibt. Beispiele hierfür sind etwa die Verknüpfung der mobilen Telekommunikation mit Computer-Anwendungen, welche die Kombination von stationärer Telekommunikation („Haus- bzw. Büroanschluss") und Personal-Computern ergänzen oder ersetzen, und zukünftig – v. a. in Verbindung mit dem UMTS-Netzwerk – eine beträchtliche Ortsflexibilisierung von gesellschaftlichen Interaktions- und Kommunikationspraxen erwarten lassen, welche Privates und Öffentliches frisch durchmischt und neu sortiert. Ein anderes Beispiel ist die Veränderung der *massenmedial* geprägten „politischen Öffentlichkeit", die wir heute vor allem als eine über das Fernsehen gestaltete Größe kennen. Sie war schon früher unter dem Einfluss der Presse für die Herausbildung moderner Nationalstaaten das Leitmedium und spielt bis heute eine bedeutende Rolle in der Konsolidierung repräsentativer demokratischer Systeme. Sie wurde von Radio und Fernsehen kolonisiert, könnte nun aber zusehends zu einer auch *netzmedial* beeinflussten Öffentlichkeit werden, was dazu führt, dass in die „politische Öffentlichkeit" andere, bidirektionale und interaktive Muster zumindest eingewoben werden (etwa im Zusammenhang mit neuen Artikulationsformen und Mobilisierungsforen für Protestbewegungen), auch wenn die Dominanz der Massenmedien damit nicht überwunden, wohl aber in Ansätzen durchbrochen wird (vgl. u. a. Grunwald et al. 2006).

4. *„(Un-)Sicherheit und Vertrauen":* Hierbei geht es um die veränderte Balance zwischen einer wesentlichen Umgebungsbedingung – (Un-)Sicherheit – und einer wesentlichen Akteursressource – Vertrauen – jeglichen gesellschaftlichen Handelns, die sich insofern beide durch ICTs verändern, als dass durch sie gleichzeitig neue Transparenzen und Intransparenzen entstehen, bislang unbekannte Authentizitätsprobleme und Manipulationsoptionen. Man kann leicht erkennen, dass in Kontexten elektronischer Kommunikation, abhängig von der Bandbreite der Übertragung für Interaktions- und Kommunikationsprozesse ganz andere Umgebungsbedingungen eingestellt werden. Themen dabei sind etwa die Zuverlässigkeit der technischen Infrastruktur, die Transparenz der Vorgänge, die für Nicht-Experten oft nicht gegeben ist, und die Authentizität oder Wahrheit dessen, was wir dort auf unseren Bildschirmen (oder anderen Medien) zu sehen (oder wahrzunehmen) bekommen. Einzelprobleme, die hier beispielhaft genannt werden können, sind etwa die Löschung oder/und die Manipulation oder/und der Diebstahl der eigenen sozialen Identität, verfilmt

mit Sandra Bullock in „Das Netz“ („The Net“, USA 1995, Regie: Irwin Winkler), aber vielen „Usern“ auch aus eigener Praxis zumindest als Bedrohung bekannt, und die zahllosen Versuche hier durch (software-)technische und (sozial-)organisatorische Maßnahmen vorzubeugen oder Abhilfe zu schaffen. Vor allem spielt (Un-)Sicherheit und Vertrauen natürlich überall dort eine prominente Rolle, wo es um geschäftliche Transaktionen geht, die mit empfindlichen Verlusten verbunden sein könnten.

3 Ubiquitous Computing, Radio Frequency Identification und der Beitrag der Satelliten

3.1 Dimensionen des Ubiquitous Computing

Der Begriff „Ubiquitous Computing“ stammt von Mark Weiser: Schon 1991 publizierte er im Journal „Scientific American (265(3):66–75)“ einen Aufsatz über „The Computer for the 21st Century“ und zeigte darin eine Vision auf,

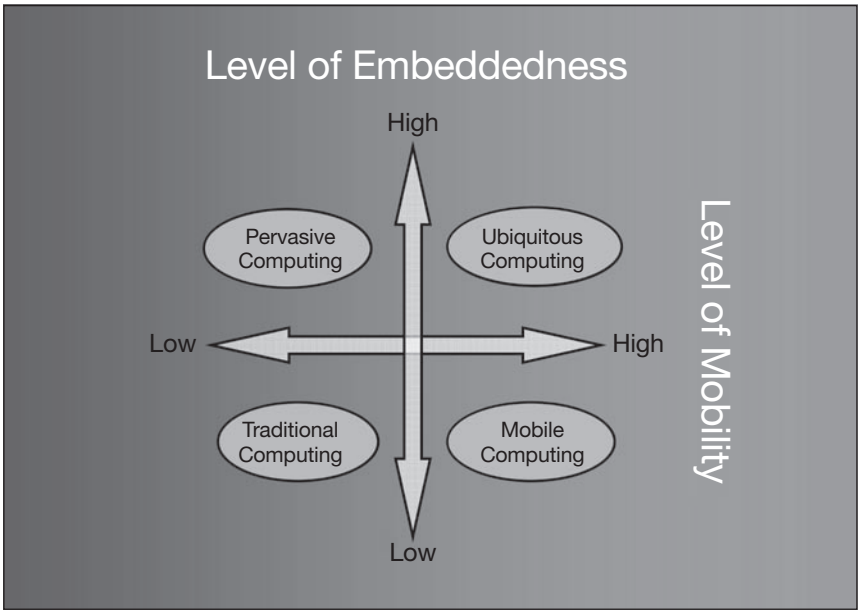

Abbildung 4: Dimensionen des Ubiquitous Computing
(Quelle: TAUCIS 2006:11, daselbst nach Lyytinen/Yoo 2002)

in der der (Personal-)Computer als Gerät verschwindet und durch „intelligente Gegenstände“ ersetzt wird, die die Menschen bei ihren Tätigkeiten unauffällig unterstützen und perspektivisch zu einem global ausgedehnten „Internet der Dinge“ verschmelzen.

„Ubiquitous Computing“ (oder „allgegenwärtige Datenverarbeitung“) bezeichnet die Omnipräsenz von – in der Regel sehr kleinen – Sensoren, Prozessoren und Aktuatoren, die in alle möglichen ganz alltäglichen Gegenstände und Umgebungskörper eingebaut werden, und nicht nur miteinander kommunizieren, sondern vor allem auch Aktionen auslösen und diese steuern können, ja sogar dazu in der Lage sind, diese nach den von ihnen selbst wahrgenommenen Parametern und Variablen zu adaptieren und zu regulieren. Neben „Ubiquitous Computing“ stehen auf diesem Feld auch Begriffe wie „Mobile Computing“ (also „mobile Datenverarbeitung“), „Pervasive Computing“ (oder „durchdringende Datenverarbeitung“) sowie „Ambient Intelligence“ (oder „Intelligenz der Umgebung“) in der Diskussion.

Die „Dimensionen des Ubiquitous Computung“ lassen sich anhand von Abbildung 4 wie folgt erläutern:

– Ausgehend von der „traditionellen Datenverarbeitung“ [Quadrant unten links] mit Servern, PCs, Terminals und konventionellen Ein- und Ausgabegeräten als Interface führt eine Erhöhung der Mobilität zum „Mobile Computing“ [Quadrant unten rechts].
– Eine verstärkte Einbettung miniaturisierter Computer in andere Gegenstände des Gebrauchs oder der Umgebung führt hingegen zum „Pervasive Computing“ [Quadrant oben links].
– Und miteinander kombiniert führen Mobilität und Einbettung zur allgegenwärtigen Datenverarbeitung, dem „Ubiquitous Computing“ [Quadrant oben rechts].

Einzelne aber zentrale UC-Technologien sind: RFID Systeme, Sensoren-Netze, Ad hoc-Netze, und Location-based Services.

3.2 Erkennung und Etikettierung (durch AI und RFID)

Bei der „Radio Frequency Identification"-Technologie[9] geht es um ein Verfahren, das mit Hilfe von elektromagnetischen Wellen eine automatische und berührungslose Identifizierung und Lokalisierung von Gegenständen und Lebewesen erlaubt, sozusagen „en passant", also während sich diese an einem Lesegerät vorbei bewegen, wobei gleichzeitig auch weitere Daten aus- oder eingelesen werden können. Funktional betrachtet lässt sich RFID auch als eine Alternative zur regulären Erkennung von Personen oder Gegenständen mittels „künstlicher Intelligenz" (kurz AI) verstehen, die etwa im (zuletzt auf der Internationalen Funkausstellung vorgestellten) „Lächel-Erkennungs-Chip" von Digitalkameras Anwendung gefunden hat. Dies gilt um so mehr, als der Entwicklungsstand von AI deutlich hinter früheren Erwartungen zurückgeblieben ist, insofern es mit ihrer Hilfe noch nicht so gut gelingt, bestimmte Aufgaben zu erfüllen, wie etwa die Erkennung eines Objekts anhand von Farbe, Größe, Gewicht usw. bis hin zur Erkennung von Personen mittels der Nutzung biometrischer Daten (z.B. Fingerabdruck, Gesichtsgeometrie, Iris, Stimme, Unterschrift), vor allem, wenn dabei wechselnde Umgebungen und Bewegungen im Spiel sind. Alternativ zur AI-gebundenen Erkennung schafft es die RFID-gebundene Identifizierung, alle Arten von Objekten (und sogar alle individuellen Exemplare einer Objektklasse) zu erfassen und voneinander zu unterscheiden. Voraussetzung dafür ist lediglich, dass sie sich mit einem RFID-Tag etikettieren lassen, der eine einzigartige, singuläre und spezifische Kennung zur Auslesung bereit hält, für Gegenstände aller Art, seien es Konsumgüter, Verpackungen, Transportbehälter, Fahrzeuge, Tiere, Menschen, Pässe oder Geldscheine (vgl. BSI 2004 zu den Risiken und Chancen des Einsatzes von RFID-Systemen im Allgemeinen sowie Langheinrich 2005 zu den Aspekten der Privatsphäre im Besonderen).

Ein Punkt von entscheidender Bedeutung ist, dass UC-Systeme zwar die Eigenschaften und Anforderungen ihrer Komponenten und der diesen zugrunde liegenden Basistechnologien „erben", diese „Erbmasse" aber sozusagen kräftig durchkneten und damit eine neuartige Konfiguration erreichen. Allemal ist dies für Daten-Schutz und -Sicherheit von Bedeutung, denn die Kombination der Eigen-

[9] Ein RFID-System besteht aus einem Transponder, der sich am oder in Gegenständen bzw. Lebewesen befindet und diese kennzeichnet sowie einem Lesegerät zum Auslesen der Transponder-Kennung. Das Lesegerät enthält eine Software (ein Mikroprogramm), das den eigentlichen Leseprozess steuert und eine RFID-Middleware mit Schnittstellen zu weiteren EDV-Systemen und Datenbanken (vgl. orientierungsweise http://de.wikipedia.org/wiki/RFID).

schaften und Anforderungen der Einzelkomponenten geht über die „Summe“ derselben hinaus und eröffnet neue Qualitäten hinsichtlich der Auslegung von ICT und der Vernetzung vielfältiger (darauf aufbauender) Anwendungen und Dienstleistungen jeglicher Art.

3.3 Datenfluss im Ubiquitous Computing

Um die Vernetzung, den Datenfluss und die Informationsspeicherung in ubiquitären Systemen zu erläutern, ist es sinnvoll, dies anhand eines kleinen Ausschnitts einer möglichen zukünftigen Netzlandschaft zu tun:

- Erstens sind hier „mobile Entitäten“ (also Menschen, Tiere, Fahrzeuge oder Maschinen) zu sehen, die [hier als drei dunkelblaue Kreise angedeutet] ein enges Body Area Network (BAN) mit sich führen, welches etwa auch medizinische Sensoren und Aktuatoren enthalten kann.
- Zweitens werden sie je von einem etwas weiter reichenden Personal Area Network (PAN) umgeben, welches etwa PDAs (also Persönliche Digitale Assistenten) oder Mobiltelephone enthält, die bspw. mittels Infrarot-Datenübertragung oder Bluetooth kommunizieren [hier in Form von drei etwas weiteren hellblauen Kreisen dargestellt].

  Die UC-Devices in den BANs und PANs sind idealiter jeweils mit einem (identifizierbaren und lokalisierbaren) User verbunden, dessen persönliche Daten und Profile sie in ihrer Datenbank [vgl. die halbhohen roten Zylinder] speichern und übertragen können, gesteuert über Sensoren und Aktuatoren, um kontrollierbare Reaktionen und Serviceangebote zu ermöglichen.
- Drittens können die UC-Devices aus mehreren verschiedenen BANs und PANs sich als Ad-hoc-Netzwerke [hier als dazwischen liegende schwarze Doppelpfeile eingetragen] miteinander verbinden, um einem aufeinander bezogenen Datenaustausch und ein aufeinander bezogenes Verhaltensrepertoire zu ermöglichen.
- Viertens werden in gleicher Weise auch Daten mit UC-Devices in der umgebenden lokalen Infrastruktur ausgetauscht [vgl. alle schwarzen Doppelpfeile in der darüber liegenden Ebene].
- Fünftens können die mobilen Einheiten auch mit Hilfe von Sensornetzen (z.B. optisch oder vor allem auch elektromagnetisch unter Nutzung passiver oder aktiver RFID-Systeme) erfasst, lokalisiert und identifiziert werden [weiße Pfeile].

– Sechstens können auch die mobilen Einheiten selbst – unter Nutzung von GPS oder anderer Lokalisierungssysteme – ihre aktuelle Position bestimmen, etwa um Wege zu finden, etwas zu bestellen oder etwas zu bewirken, sobald ein bestimmter Ort passiert wird oder erreicht worden ist.

Je nach der Infrastruktur in Reichweite greifen die mobilen Einheiten sukzessive (z.B. via Wireless LAN, GSM- bzw. UMTS-Mobilfunk oder WiMAX[10])

– über das lokale Netz (LAN);
– über das Metropolitan Area Network (MAN);
– auf das Internet bzw. Wide Area Network (WAN) zu (wobei natürlich irgendwann zu kabelgebundenen Übertragungswegen gewechselt wird).

Prinzipiell sind sie damit auch umgekehrt über alle Wege unter einer festen IPv6-Adresse[11] erreichbar, wobei natürlich immer Datenspuren hinterlassen, gespeichert und ausgewertet werden können.

– Es kann schließlich von jeder Lokalität aus über diese Wege auf entfernte Dienste (Remote Services) zugegriffen werden, wobei
– auch die entfernten Service Provider umgekehrt über die verschiedenen Verbindungswege auf die lokalen Geräte im jeweiligen LAN, BAN und PAN zugreifen und mit ihnen in Wechselwirkung treten können.

3.4 Satelliten

Hier kommen nun die Satellitentechnik und die avisierten Fortschritte derselben ins Spiel. Insofern ihr Leistungsspektrum alle möglichen technischen Einzelleistungen zu Zwecken der Beobachtung und Erkundung, Positionsbestimmung und

---

[10] WiMAX, Worldwide Interoperability for Microwave Access, bezeichnet Funksysteme nach einem bestimmten Übertragungs-Standard, der sich zum einen vorwiegend für ortsfeste Systeme eignet (z.B. Richtfunksysteme), aber auch für den Einsatz in tragbaren Geräten. WiMAX-Netze finden auch bei der Anbindung von GSM-/UMTS-Basisstationen (Backhauling-Bereich), als auch bei der Bereitstellung drahtloser Internet-Zugänge (Zugangs-Bereich) Verwendung (vgl. ferner http://de.wikipedia.org/wiki/WiMAX).

[11] Eine sehr zentrale technische Tendenz ist die Konvergenz der meisten Kommunikationstechniken zu IP-basierten Netzwerken. So hat man früher Modems („IP-über-Telefon") benutzt, um heutzutage VoIP („Telefonie-über-IP") zu favorisieren. Analog ist eine Entwicklung zu IP als Netzwerkschicht über sehr heterogene Zugangstechnologien im Gange. Speziell IPv6 bietet sehr flexible neue Mechanismen für die drahtlose, mobile Kommunikation und mit dem gewaltigen Adressraum auch die Möglichkeit, alle Geräte der ubiquitären Umgebungen aus der Ferne zu adressieren.

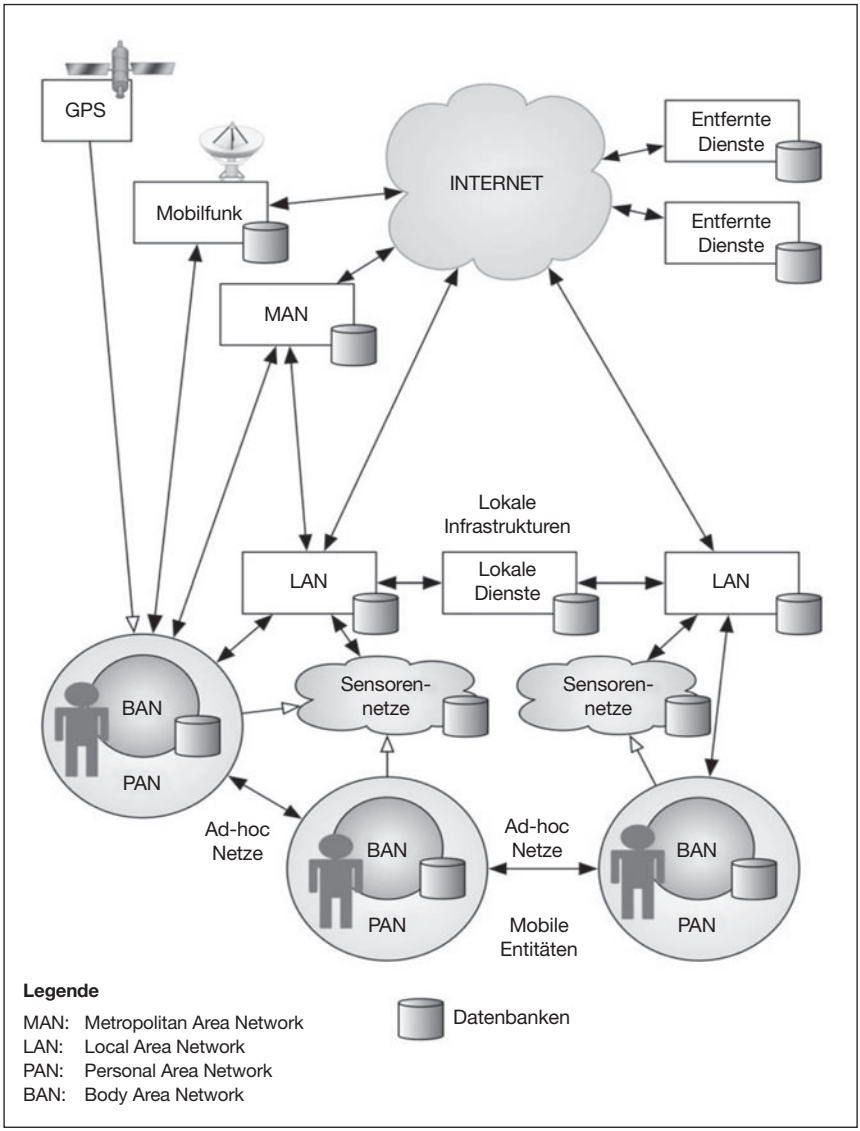

Abbildung 5: Datenfluss im Ubiquitous Computing (Quelle: TAUCIS 2006:40)

Navigation sowie Information und Kommunikation umfasst (vgl. auch Backhaus et al. 2008), ist sie dazu prädestiniert, sich sozusagen „von oben herab" mit der gerade beschriebenen digitalen Netzlandschaft zu verbinden.

Satelliten vermögen schon als einzelne High-Tech-Produkte sehr viel (die permanente und flächendeckende Ortung von Fahrzeugen oder Personen, hochauflösende Überwachung von Infrastrukturen oder Landschaften). Sie vermögen aber weit mehr, wenn sie zu den besonderen Knoten eines rapide sich erweiternden und immer dichter werdenden Netzwerks mutieren. Dieses kann schlicht und ergreifend alles in sich aufnehmen und zwecks weiterer Verarbeitung prozessieren, was einzelne Knoten an besonderen Leistungen, distinkten Services oder individuellen Profilen in digitalisierter Form zur Verfügung stellen können.

Von ausschlaggebender Bedeutung ist hierbei, dass es immer besser gelingt, die von Satelliten ermittelten Daten quasi in Echtzeit ihren Anwendern zur Verfügung zu stellen, statt sie wie früher nur periodisch auszulesen und dann erst zeitaufwendig aufzubereiten, um sie danach an andere Institutionen mit Anwenderinteressen weiterzuleiten.

In Verbindung mit der Satellitentechnik ergeben sich so Kombinations- und Konfigurations-Möglichkeiten, deren Fülle und Dynamik derzeit (zumindest m. E. nach) nur grob vorhergesehen werden können,[12] ganz zu schweigen von den weiteren sozio-kulturellen, politisch-ökonomischen und psycho-sozialen Implikationen, die mit ihnen verbunden sind.

Dies gilt umso mehr, als wir schon in der nahen Zukunft damit rechnen müssen, dass die europäische Galileo-Initiative (im Verhältnis zum GPS-System) eine bemerkenswerte Steigerung der Leistungsfähigkeit in punkto der Verwendung von Navigationsdiensten für private, gewerbliche und administrative Zwecke ermöglichen wird. Durch die Einbindung Geographischer Informations-Systeme[13] (GIS)

---

[12] Einige eher unschöne Beispiele dafür sind etwa die Verbreitung illegaler pornographischer Bilder über die Nebenfunktionen von Navigationsdiensten; das heimliche „Tracking" der Mobiltelefone von (Ehe-)Partnern und Angehörigen; Softwaremanipulationen an Mobiltelefonen, um Verbindungen erfassen und abhören zu können; die schon mit Google Earth (zugegebenermaßen noch sehr unterentwickelt) gegebenen Möglichkeiten festzustellen, ob und wann sich vielleicht ein „falsches" Auto in der eigenen Hauseinfahrt befunden haben mag; oder schließlich die Chance bei den systematisch eingescannten (hochauflösend photographierten) Straßenansichten von Google Maps vielfältige (wenn auch zufällig entstandene) Einblicke in die Privatsphäre seiner Nachbarn und anderer Mitmenschen zu erhalten.

[13] Vgl. orientierungsweise http://en.wikipedia.org/wiki/Geographic_information_system.

werden sich die damit gegebenen Möglichkeiten darüber hinaus noch zusätzlich erweitern lassen. Hinzu tritt das europäische GMES-System (vgl. De Bernardinis 2007), das potentiellen Nutzern eine hochauflösende, flächendeckende Erdbeobachtung u.a. für Zwecke des Zivilschutzes, der Krisenprävention und der Stadtplanung verspricht.

Deutlich wird hier, dass auch der Komplex „UC, RFID und der Beitrag der Satelliten" in die Mechanismen eingebunden ist, die ich eben durch zwei Thesen umrissen habe – auch seine Gestaltungspotentiale tragen dazu bei, neue Verhältnisse zu schaffen: neue Verhältnisse des räumlich-zeitlichen Aufeinander-Bezug-Nehmens von Kommunikations- und Interaktions-Sequenzen; und neue Verhältnisse des Aufeinander-Verweisens distinkter Wirklichkeits-Ebenen: „wirklicher", „imaginierter", „repräsentierter", „modellierter", „simulierter" oder „virtualisierter".

Die Bedeutung der beiden einzelnen Faktoren, die im gleich folgenden Katalog aufgeführt werden, kann daher (nicht einfach vor dem Hintergrund des Status Quo, sondern) nur vor dem Hintergrund der dynamischen Veränderung dieser Verhältnisse weiter untersucht und besser verstanden werden. Gemeint sind hier:

1.) das höhere Vermögen zur räumlich-zeitlichen Auflösung und Abdeckung in der Ortung (und dem „Tracking") von Gegenständen oder Personen, unabhängig davon, ob es sich dabei um stationäre oder mobile Größen handelt;
2.) die Verschneidung der von Satelliten zur Verfügung gestellten Daten mit geographisch passend zugeordneten Informationen aus anderen Quellen, vermittels eines simultanen Zugriffs auf entsprechende GIS-Datenbanken oder deren Aufbereitung in Anwender-Programmen, die sie etwa als „augmented reality" (für eine ganze Palette an möglichen Nutzungsformen durch ein weites Spektrum an möglichen Anwendern) zur Verfügung stellen.

Im Besonderen wird der Nutzen der GMES-Initiative unter Verweis auf die gestiegene Anfälligkeit des öffentlichen Raums sowie vernetzte und verletzliche Infrastrukturen begründet, gegenüber Einwirkungen durch organisierte Kriminalität, Terror-Netzwerke, technische Unfälle oder Naturkatastrophen.

Infolge der Erfüllung der Bedingungen der Möglichkeit zur Realisierung dieser Nutzen kommt es auf breiter Front zu einem Anschwellen der Datenströ-

me, nicht zuletzt solcher, die persönliche und personenbeziehbare Daten mit sich führen – und diese stehen sowieso schon in den Debatten um Ubiquitous Computing, RFID, Videoüberwachung und Vorratsdatenspeicherung in einer (durchaus kontroversen) Diskussion (vgl. u.a. Flöting 2006 sowie Lingner 2007).

Neben den intendierten Nutzen (sowie den Kosten dieser Vorhaben) sind daher auch unerwünschte und bedenkliche Auswirkungsmöglichkeiten ihrer Realisierung unbedingt im Auge zu behalten, also etwa:

- (mögliche) Verluste in punkto Privatheit und Autonomie (bzw. der informationellen und physischen Selbstbestimmung);
- (mögliche) sozial-geograpische Nebenwirkungen in Gestalt von verschärften Segregationen (Stichworte: Exklusion, Polarisierung, Marginalisierung – „software-sorted geographies“[14]);
- Beeinträchtigungen von Urbanität hinsichtlich ihrer Öffentlichkeitsfunktion;
- die unklaren und bestreitbaren Bedingungen der Aneignung bzw. des Zur-Verfügung-Stellens von hochgenauen, sensiblen und personalisierbaren Daten (zur weiteren Verwendung, Aufbereitung, Weitergabe usw.);
- die mögliche militärische Übernahme von Leistungen (Stichwort: „dual use“);
- das Proliferationsrisiko im Verhältnis zu Dritten;
- die mögliche (Um-)Nutzung der Technologien und Dienste zu obstruktiven Zwecken (Stichwort: technische „Aufrüstungs“-Spirale) etwa zur besseren Planung von kriminellen Manövern oder terroristischen Attacken.

4 Ausblick

4.1 Fortschritt „ist“ gestaltete (Un-)Sicherheit

Die europäische Modernisierung ist durch den Gedanken der „Aufklärung“, aber auch durch die Idee des „Fortschritts“ bestimmt. Wo jene darauf abstellt, die Vernunftbegabung des Menschen im Sinne seiner Unabhängigkeit und Mündigkeit auszubauen, zielt diese darauf, die Naturkräfte mit den Mitteln der Wissenschaften zu erforschen und in Gestalt von Technik zu entwickeln. Die Versprechen dieses zivilisatorischen Aufbruchs heißen „Freiheit“, „Wohlstand“ und „Sicherheit“.

[14] Vgl. dazu u.a. Graham 2005.

Im wohlverstandenen Sinne ist es daher richtig zu sagen: „Man darf dem Fortschritt nicht im Wege stehen!“ In der so geführten populären Rede kommt jedoch ein eindimensionales apologetisches Fortschrittsverständnis zum Ausdruck, welches zwar heftig mit dem ebenso eindimensionalen apokalyptischen Fortschrittsverständnis konfligiert, welches Fortschritt (unter geänderten Vorzeichen) als einen unaufhaltsamen, alles verschlingenden Moloch versteht; aber das deterministische, unilineare Fortschrittsmodell kontrastiert viel stärker mit einer Auffassung, die Fortschritt nicht essentialistisch, sondern prozessorientiert als Steigerung von Gestaltungs-Möglichkeiten und Entwicklungs-Optionen versteht.

Im letzteren Sinne ist Fortschritt ein (von Menschen) gestalteter Prozess, der Kontingenzen gerade nicht reduziert, also Entwicklungsrichtungen und -möglichkeiten zusehends festlegt, sondern Kontingenzen vervielfacht, also immer neue Optionen eröffnet. Fortschritt – eine Mixtur aus „Chancen“ und „Risiken“ – ist demzufolge ambivalent: er schafft Sicherheiten, indem er zur Lösung von Problemen beiträgt, also ordnungsstiftend und stabilisierend wirkt, und er fungiert als „Unsicherheitsgenerator“, indem er Optionen multipliziert, die als Entscheidungen unter Unsicherheit abzuarbeiten sind, wodurch das Bestehende permanent in Frage gestellt wird.

„Sicherheit“ ist daher im Zusammenhang mit der Gestaltung technischer Systeme von vorne herein ein zentrales Thema – und zwar keineswegs nur in einem verkürzten, auf die „artefaktische Technik“ und ihre unmittelbaren Risiken gerichteten Blickwinkel. Statt dessen geht es um alle Entscheidungen, die zu treffen sind, um die technische Dimension der Gestaltung gesellschaftlicher Wirklichkeit zu betreiben. Das ist Anlass genug, sich Gedanken über „offene Fragen“ zu machen, und das, was uns fehlt.

4.2 Über „offene Fragen“ und „das, was uns fehlt“

Im Programm, mit dem die interessierte Öffentlichkeit zur Tagung über „Globale Fernerkundungssysteme und Sicherheit“ (Wien, 9.–10. Oktober 2008) eingeladen wurde, war unter anderem folgendes zu lesen: „Angesichts ‚realer‘ und empfundener Bedrohungen durch umweltbedingte und humanitäre Krisen sowie durch Gefährdungen der inneren und äußeren Sicherheit mehren sich seitens der Gesellschaft Erwartungen an leistungsfähige Überwachungsdienstleistungen.“ Und:

„Diese Erwartungen an entsprechende Informationsangebote sind allerdings vor dem Hintergrund offener Fragen zu diskutieren."[15]

Die „Erwartungen an leistungsfähige Überwachungsdienstleistungen" sind allerdings durchaus nicht nur „vor dem Hintergrund offener Fragen zu diskutieren", seien es nun diese Punkte oder auch andere, sondern es muss gestattet sein, früher einzusetzen, und schon die so adressierten (Sicherheits-, Schutz- und Überwachungs-) Erwartungen selbst zu hinterfragen.

„Sicherheit" kann zwar als ein rein technisch herzustellendes Phänomen gedacht werden, oder auch als etwas vorgestellt werden, was sich allein durch militärische (Stichwort „Krieg dem Terror") oder polizeiliche Mittel erreichen ließe. Ohne in Abrede stellen zu wollen, dass technische, militärische und polizeiliche Maßnahmen notwendige Elemente einer umfassenden Sicherheitsstrategie sein mögen, bleibt festzustellen, dass sich Sicherheit realiter ebenso wenig rein technisch gewährleisten lässt, wie auch militärische und polizeiliche Mittel nicht hinreichend sein können. Eine Fixierung auf sie kann vielmehr „kontraproduktiv" sein, in dem Sinne als Fortschritte in Richtung mehr Sicherheit (durch falsche Weichenstellungen und deren Opportunitätskosten) gebremst und verringert werden (können). Sie kann sogar zu „perversen Effekten" (Boudon 1977) führen, also zu einer nicht-intendierten Verschlimmerung der Sicherheitslage infolge einer zu eng geführten und einseitigen „Sicherheitsphilosophie" – und diese ist „das, was uns fehlt".

4.3 Exkurs zur „Sicherheitsphilosophie"

Um zumindest einen Eindruck davon zu geben, wie eine solche „Sicherheitsphilosophie" angedacht werden könnte, möchte ich nun einige Punkte erläutern. Dies geschieht hier in Form eines Exkurses, zumal diese Ansätze eigentlich im Zusammenhang eines anderen Papiers über einen integrativen Ansatz der Technikfol-

---

[15] Im Programm (siehe unter: http://www.espi.or.at/images/stories/dokumente/press/programm_ht_fernerkundung_102008.pdf) folgen daraufhin eine ganze Reihe – zugegebenermaßen sehr wichtiger – einzelner Punkte, auf die ich hier nicht weiter eingehen kann: „Hierzu gehört die realistische Beurteilung der Verfügbarkeit, der Qualität und der Validität entsprechender Daten. Ihre Verbreitung kann darüber hinaus auch Fragen des Schutzes der persönlichen Privatsphäre (z.B. bei Erfassung von Bewegungsdaten), des Schutzes sensibler Orte oder Einrichtungen, der rechtlichen Belastbarkeit fernerkundlicher Zuschreibungen sowie der Haftung für Ausfälle und Fehler entsprechender Informationsdienstleistungen aufwerfen. Angesichts der Risikolagen und verbleibender Unsicherheiten spielen grundsätzlich auch Fragen des angemessenen Handelns unter Ungewissheit eine bedeutende Rolle."

genabschätzung in Verbindung zur „nachhaltigen Entwicklung“ entwickelt wurden (vgl. Metzner-Szigeth 2008b). Letztere ist meines Erachtens aber auch für die „Sicherheitsphilosophie“, die es zu etablieren gilt, von zentraler Bedeutung, insofern der Sicherheitsgedanke sich keineswegs nur im Kontext der technischen Risikoproblematik diskutieren lässt, sondern sich auch in allen vier Dimensionen nachhaltiger Entwicklung fruchtbar erörtern lässt (vgl. auch Metzner-Szigeth 2009).

„Verwundbarkeit“ hat eine externe und eine interne Komponente. Allgemein sind – auf der Mikro-Ebene – der einzelne Mensch, oder die einzelne Gemeinschaft, in der er lebt, und – auf der Meso-Ebene – die einzelne Stadt bzw. Region oder das einzelne ausdifferenzierte Funktionssystem, oder schließlich – auf der Makro-Ebene – komplette Gesellschaften existenziellen (!) Gefährdungen ausgesetzt („exposure“), und sind in unterschiedlichem Maße dazu in der Lage, diesem „Ausgesetzt-Sein“ (aus eigener Kraft oder mit Hilfe) zu begegnen („coping“). „Vulnerabilität“ ist ein „unscharfes Konzept“. Aufgrund seines Assoziationsreichtums

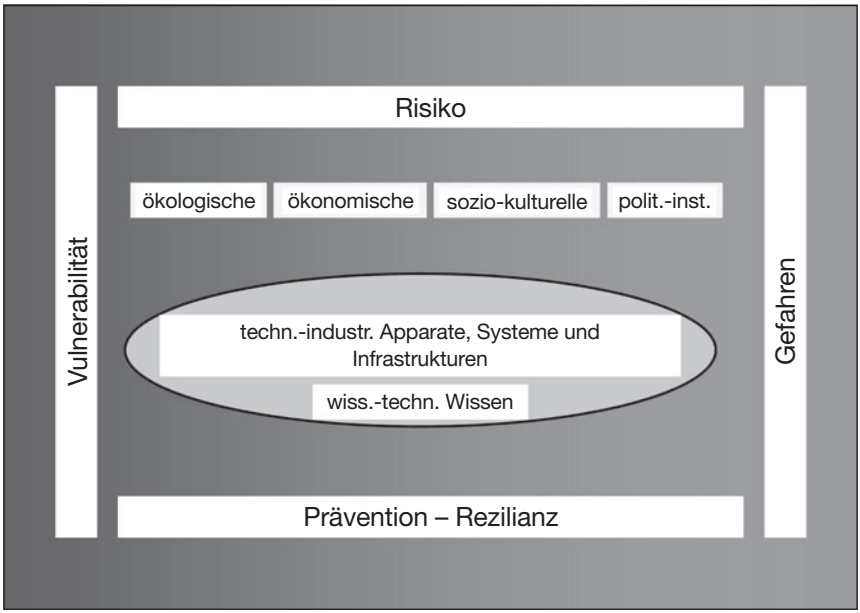

Abbildung 6: Vulnerabilität und Nachhaltigkeit

sowie seines Kerngedankens ist es jedoch außerordentlich instruktiv (vgl. auch Bijker 2006). Im Folgenden sollen seine Gehalte daher in Verbindung mit einigen weiteren wichtigen Größen entfaltet werden, die für jede „Sicherheitsphilosophie" von kardinaler Bedeutung sein müssen.

Abb. 6 präsentiert auf der rechten Seite einen Balken mit der Bezeichnung „Gefahren". Aufzuschlüsseln sind diese nach verschiedenen Klassen:

1.) Epidemien, also z.B. AIDS, BSE oder Vogelgrippe;
2.) „Natur"katastrophen, und zwar auch insoweit sie in einem ursächlichen Zusammenhang mit globalen Umwelt- u. Klimaveränderungen stehen, also nicht nur *natürlichen*, sondern auch *menschlichen* Ursprungs sind, also z.B. Stürme, Erdrutsche und Lawinen, Fluten, Dürren und Beben;
3.) technisch-industrielle Unfälle, also Ereignisse etwa vom Typus „Exxon Valdez", „Bophal" und „Tschernobyl", aber auch solche „kleineren" Maßstabs;
4.) kriegerische Auseinandersetzungen, in deren Folge etwa Ölfelder in Flammen stehen oder einst fruchtbare Landstriche verwüstet werden;
5.) terroristische Anschläge und Sabotageakte, vor allem insofern sie dazu geeignet sind, massive Verluste an Menschenleben oder/und den Zusammenbruch gesellschaftlicher Infrastrukturen und Funktionssysteme (wie z.B. Internet-Kommunikation oder weltweiter elektronischer Wertpapierhandel) zu evozieren. Beispiele dafür sind die Attacke auf das „World Trade Center" und – weniger spektakulär – die saisonalen „Computer-Viren" und „Software-Würmer".

Links sehen wir einen Balken mit der Bezeichnung „Vulnerabilität". Ihm können eine ganze Reihe von Faktoren zugeordnet werden, nämlich

1.) Faktoren *allgemeiner Natur*, wie z.B. die steigende Interaktionsdichte, der zunehmende Vernetzungsgrad, die wachsende Bevölkerung, und vor allem die mit der „Globalisierung" verbundene „Entgrenzung" raumübergreifender Ursache-Wirkungs-Ketten; und
2.) Faktoren *besonderer Natur*, also
   – z.B. – bezogen auf die ökologische Umwelt – etwa die Belastung oder Degradation von Süßwasser-Ökosystemen oder Gebirgslandschaften;
   – z.B. – bezogen auf die Wirtschaft – etwa die Angewiesenheit auf einzelne Schlüsselressourcen, der Deckungsgrad an Erwerbsquellen, oder die Verschuldungsquote;

– z.B. – bezogen auf die sozio-kulturelle Dimension – etwa das Wissen und Können der Menschen in Relation zur Teilhabe an Wissens-Reservoiren (Stichwort: „Digital Divide“); und schließlich
– z.B. – bezogen auf die politisch-institutionelle Dimension – etwa die Möglichkeiten nötige Informationen zu bekommen und Entscheidungsprozesse mitzubestimmen.

Hinzu treten Faktoren, die mit Blick auf „technisch-industrielle Apparate, Systeme und Infrastrukturen“ (abgebildet in der mittleren Ellipse) Sinn machen, also etwa

– die vom Risikoforscher Charles Perrow (1984) markierten Faktoren der „hohen Komplexität“ und „engen Kopplung“, die v.a. dann problematisch sind, wenn sie zusammen auftreten; sowie
– die vom Komplexitätsforscher John Casti hervorgehobene „Adaptabilität“ technischer Systeme variablen Umwelten und Ereignissen gegenüber;
– der Grad der „Fehlerfreundlichkeit“ oder „Zuverlässigkeit“ von Abläufen;
– die „Robustheit“ von Installationen;
– die „Singularität“ bautechnischer Strukturen, also etwa Brücken, Tunnel, Staudämme für Zwecke der raumübergreifenden Versorgung; oder
– die „Zentralität“ von Infrastruktur-Netzen (wenn etwa alle U-Bahn-Linien durch eine „main station“ laufen).

Im Regelfall dient „wissenschaftlich-technisches Wissen“ (ebenfalls inmitten der Abbildung angeordnet) „konstruktiven“ Zwecken. Dass dies nicht immer gelingt, wissen wir. Und dass partikulare Interessen versuchen, auf Wissenschaft und Technik Einfluss zu nehmen oder sich ihrer schlicht zu bedienen, wissen wir auch. Nichtsdestoweniger beschäftigen sich vermutlich alle in „Wissenschaft, Forschung und Entwicklung“ Tätigen mit der Frage, wie dies am besten zu erreichen ist (... konstruktiven Zwecken zu dienen) – *zumindest* im Rahmen ihrer arbeitsteilig an sie herangetragenen Aufgaben. Die allgemeine Befassung mit der Frage, wie man dies am besten erreichen kann, auch unter Beachtung der verschiedenen Zielsetzungen, die sich mit den vier Dimensionen nachhaltiger Entwicklung verbinden, ist jedoch das ureigenste Gebiet der Technikfolgenabschätzung.

Der obere Balken mit der Bezeichnung „Risiko“, steht nicht von ungefähr zwischen der Vulnerabilität auf der linken und den Gefahren auf der rechten Seite. Er soll zum Ausdruck bringen, dass das Maß des Gefahren-Ausgesetzt-Seins, hin-

sichtlich des Schadensausmaßes einerseits und der Eintrittwahrscheinlichkeit andererseits, in Korrelation mit den potentiellen Gefahren und der Vulnerabilität zu sehen ist.

Nicht minder gilt dies für den unteren Balken mit der Bezeichnung „Prävention und Rezilianz“:

– Bei der Prävention geht es darum, Schäden zu begrenzen und in ihrer Eintrittswahrscheinlichkeit herabzusetzen, *bevor* sich die fraglichen Risiken als Ereignisse manifestieren.
– Bei der Rezilianz geht es umgekehrt darum, Hilfen bereitzustellen und Kompensation leisten zu können, *nachdem* sich die fraglichen Risiken in Ereignissen niedergeschlagen haben.

Ob genug getan wurde, kann in beiden Fällen nur im Verhältnis zu den potentiellen Gefahren und der herrschenden Vulnerabilität beurteilt werden. Vor dem Hintergrund der gerade anhand von Abb. 6 ausgeführten Überlegungen lässt sich eine Generalthese aufstellen. Sie lautet: „Je weniger es gelingt, den wissenschaftlich-technischen Fortschritt *konstruktiv* zu gestalten, um so vulnerabler wird die Moderne!“ Erläutert werden kann sie so:

– Je höher die Nachhaltigkeit der vier Dimensionen ist, desto geringer ist ihre Vulnerabilität, und um so höher ist zugleich auch ihre Fähigkeit zu Prävention und Rezilianz, um eintretende Schäden in ihrem Ausmaß zu begrenzen, in ihrer Eintrittswahrscheinlichkeit zu verringern oder „wieder auf die Beine zu kommen“.
– Umgekehrt bedeutet das: Je größer ihre „nicht-Nachhaltigkeit“, desto vulnerabler, weniger präventionsfähig und reziliant ist eine Gesellschaft.
– Daraus folgt: Alles was wir tun – gerade auch mit den Mitteln der Technikfolgenabschätzung –, um wissenschaftlich-technisches Wissen „konstruktiv“ zu nutzen, um technisch-industrielle Systeme in ihren Folgen für die Nachhaltigkeit der vier Dimensionen günstig auszulegen, verringert die Vulnerabilität der Gesellschaft und erhöht gleichzeitig ihre Fähigkeit zu Prävention und Rezilianz.
– Umgekehrt gilt aber (leider), dass die Moderne um so vulnerabler wird, je weniger es gelingt, eben dies zu tun.

4.4 Schlussbemerkung

Damit komme ich zum eigentlichen Thema meines Beitrags zurück, den ich jetzt mit ein paar Gedanken zu „hellen" und „dunklen" Szenarien und einem kleinen Appell beschließe. Anhand des Bildes einer ubiquitären Vernetzung informations- und kommunikationstechnischer Systeme, der Omnipräsenz von UC- und RFID-„Devices" zuzüglich all der satelliten-gebundenen Möglichkeiten zur Kontrolle von Aufenthaltsorten, Bewegungsprofilen, Kommunikationsmustern, Transaktionsverläufen usw. liegt natürlich die Assoziation eines totalen (omnipotenten) Überwachungsstaates á la George Orwell nahe. Allerdings ist die Systemarchitektur (bisher jedenfalls) keineswegs auf ein hierarchisches Zentrum ausgelegt, sondern dezentral organisiert, so dass kollektive und individuelle Akteure mit sehr unterschiedlichen Einflussmöglichkeiten und -reichweiten daran partizipieren können. Hinzu tritt, dass ihr Einfluss nicht nur auf politischer Macht, sondern genauso gut auf ökonomischen Mitteln oder auch auf technischem oder kulturellen Wissen beruhen kann – und Macht, Geld und Wissen in modernen Gesellschaften in durchaus verteilter Form vorliegen. Umgekehrt wird Einfluss immer, selbst im Fall eines hierarchischen Zentrums, mit dem Problem der schieren Größe und Komplexität sowie der Interaktivität und Dynamik des Systems konfrontiert und dadurch limitiert. Ferner werden alle Versuche, eigenen Einfluss auszuweiten und echte Machtpositionen einzunehmen, normalerweise aufmerksam beobachtet, seitens von Wettbewerbern, NGOs usw., und das sollte dann – unter Bedingungen eines demokratischen Gemeinwesens – zur Auslösung von Gegenbewegungen führen.

Utopische Visionen können in jedem Fall – vermittels ihrer handlungsorientierenden Kräfte – positive oder/und negative *Folgen* nach sich ziehen. Wenn wir von Eu-topien oder Dys-topien reden, ist aber etwas anderes gemeint, nämlich mit welchen Vorzeichen ihre (gegenwärtige, prospektive) *Bewertung* von Zukünften erfolgt. Im ICT-Bereich verbreitete Eutopien (technizistischer, kommerzieller oder auch anarchistisch-kommunitärer Provenienz – so sehr sie sich auch in ihren *Wunschbildern* unterscheiden mögen – teilen meist recht naive Annahmen über Triebkräfte und resultierende Wirkungen (und zwar sowohl untereinander, als auch mit ebenso einfach gestrickten Dystopien). Wo die eutopischen Visionen suggerieren, dass alles zum Besten strebe, und man bloß alles laufen lassen müsse – oder es zumindest dann tun könne, wenn die (in ihrem Sinne) „richtige" Weichen-

stellung erfolgt sei, suggerieren die dystopischen Vision (v.a. das eben erwähnte Orwellsche Szenario), dass alles zum Schlechteren tendiere, in eine ausweglose Situation hineinführe, der nurmehr durch eine Kampfansage zu begegnen wäre, in diesem Fall gegenüber dem ganzen technischen Apparat, der ansonsten jenes *Angstbild* eines Systems realisieren müsste, welches das dystope Szenario befürchten lässt.

Um die konkreten Gestaltungsoptionen nutzen zu können, die es auf dem hier verhandelten Feld in Hülle und Fülle gibt, ist es unerlässlich über das hinauszugehen, was uns Visionen sagen können. Dazu dienen wissenschaftlich verfahrende „Foresight"-Methoden wie z.B. die „Szenario"-Technik.[16] Nachdem ich mich vergewissert habe, dass es beispielsweise im Hinblick auf die GMES-Initiative zwar eine von der renommierten Agentur PriceWaterhouseCoopers (2006) angefertigte Studie über die erwartbaren „sozio-ökonomischen" „Benefits" von GMES gibt, aber keine systematische Szenario-Analyse erarbeitet worden ist, die neben den „hellen Seiten" auch die „dunklen Seiten" dieser weitreichenden Unternehmung angeht[17], schlage ich vor, dieses dringend nachzuholen, um nicht die Chance zu verspielen, *mögliche* unerwünschte Folgen dieses Projekts schon frühzeitig sichtbar zu machen, um ihrer *tatsächlichen* Realisierung vorbeugen zu können.

Dr. phil. habil. Andreas Metzner-Szigeth
Universität Münster
Privatdozent für Soziologie am Fachbereich Erziehungswissenschaft und Sozialwissenschaften der Universität Münster; derzeit Gastprofessuren an der Universidad del País Vasco in San Sebastían, Spanien, sowie der Uniwersytet Śląski in Katowice, Polen.

[16] Vgl. hierzu u. a. Bradfield et al. 2005, van 't Klooster/van Asselt 2006.

[17] Vgl. exemplarisch Ducatel et al. 2001 sowie Wright et al. 2008 bzw. Wright 2008 für den Wert von „dark scenarios" im Zusammenhang von Zukunftsszenarien für die „ambient intelligence".

Literaturverzeichnis

Backhaus R, Rohner N, Schrogl KU, Satellites and Services for the Society: Visions and Perspectives, in: Proceedings of the International Week on Space Applications. Toulouse 2008, http://www.espi.or.at/images/stories/dokumente/presentations/2008/paper_rohner_backhaus_schrogl_spaceappli08_2col.pdf (22.3.2009)

Banse G, Metzner-Szigeth A, Veränderungen im Quadrat: Computervermittelte Kommunikation und moderne Gesellschaft – Überlegungen zum Design des europäischen Forschungs-Netzwerks „Kulturelle Diversität und neue Medien". Teorie Vědy. Časopis pro Teorii Vědy, Techniky a Komunikace/Theory of Science. Journal for Theory of Science, Technology & Communication, 11(H.1), 2003, 7–44

Bijker WE, The Vulnerability of Technological Culture, in: Nowotny H (Hrsg.), Cultures of Technology and the Quest for Innovation, New York, 2006, 52–69

Boudon R, Effets Pervers et Ordre Social, Paris 1977 (dt.: Widersprüche sozialen Handelns, Darmstadt/Neuwied 1979)

Bradfield R; Wright G; Burt G; Cairns G; Van Der Heijden K, The origins and evolution of scenario techniques in long range business planning, Futures 37, 2005, 795–812

Bundesamt für Sicherheit in der Informationstechnik (BSI), Risiken und Chancen des Einsatzes von RFID-Systemen – Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit, Bonn 2004, http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf (22.3.2009)

Bühl A, Die Virtuelle Gesellschaft des 21. Jahrhunderts – Sozialer Wandel im Digitalen Zeitalter, Opladen 2000

Castells M, Der Aufstieg der Netzwerkgesellschaft (Das Informationszeitalter – Wirtschaft, Gesellschaft, Kultur. Teil 1), Opladen 2001a

Casti JL, Complexification. New York 1994

Castoradis C, Gesellschaft als imaginäre Institution. Entwurf einer politischen Philosophie, Frankfurt am Main 1984

Chatwin B, The songlines, London 1988

De Bernardinis B, GMES Fast Track Emergency Response Core Service – Strategic Implementation Plan, Final Version, 24.4.2007, http://www.gmes.info/fileadmin/user_upload/Docs_Files/ERCS_Strategic_Implementation_Plan_Final.pdf (22.3.2009)

Ducatel K, Bogdanowicz M, Scapolo F, Leijten J, Burgelman JC, Scenarios for ambient intelligence in 2010, IPTS, Seville, February 2001, ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf (22.3.2009)

Floeting H, Sicherheitstechnologien und neue urbane Sicherheitsregimes, Wien 2006 (Österreichische Akademie der Wissenschaften, Institut für Technikfolgen-Abschätzung)

Giddens A, The consequences of modernity, Stanford/CA 1990

Graham SDN, Software-Sorted Geographies, in: Progress in Human Geography 29 (5), 2005, 1–19

Großklaus G, Medien-Zeit, Medien-Raum. Zum Wandel der raumzeitlichen Wahrnehmung in der Moderne, Frankfurt am Main 1995

Grunwald A, Banse G, Coenen C, Hennen L, Netzöffentlichkeit und digitale Demokratie. Tendenzen politischer Kommunikation im Internet, Berlin 2006

Gunkel DJ, Hetzel Gunkel A, Virtual Geographies: The New Worlds of Cyberspace, in: Critical Studies in Mass Communication, 14, 1997, 123–137

Habermas J, Der philosophische Diskurs der Moderne, Frankfurt am Main 1985

Hilty L, Behrendt S, Binswanger M, Bruinink A, Erdmann L, Fröhlich J, Köhler A, Kuster N, Som C, Würtenberger F, Das Vorsorgeprinzip in der Informationsgesellschaft – Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt, Bern, TA-SWISS, TA 46, 2003

Keil-Slawik R, Mediatronic: Convergent technologies and interdisciplinary research. In: Kameas A, Streitz N (eds.), Proceedings of the international conference „Tales of the Disappearing Computer" (Santorini, Greece, 1.–4. Juni 2003), Athen 2003, http://iug.upb.de/rks//Publikationen/.2003/2003-rks-tales.pdf (22.3.2009)

Krämer S (Hrsg.), Medien, Computer, Realität: Wirklichkeitsvorstellungen und Neue Medien, Frankfurt am Main 1998

Langheinrich M, Die Privatsphäre im Ubiquituous Computing – Datenschutzaspekte der RFID-Technologie, in: Fleisch E, Mattern F (Hgg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, Berlin, 2005, 329–362, http://www.vs.inf.ethz.ch/res/papers/langhein2004rfid.pdf (22.3.2009)

Läpple D, Essay über den Raum. Für ein gesellschaftswissenschaftliches Raumkonzept, in: Häußermann H, Ipsen D, Krämer-Badoni T, Läpple D, Rodenstein M, Siebel W, Stadt und Raum, Soziologische Analysen, Bd. 1, Pfaffenweiler 1991, 157–207

Lem S, Summa technologiae, Frankfurt am Main 1986 (3. Aufl., polnische Originalausgabe: Krakow 1964)

Lingner S, Gesellschaftliche Randbedingungen der Virtualisierung von Lebenswelten und ihre Folgen – Synopsis und Fazit, in: Lingner S, Allin S, Steinebach G, Gesellschaftliche Randbedingungen der Virtualisierung urbaner Lebenswelten, Bad Neuenahr-Ahrweiler (Europäische Akademie) 2007, 89–96

Lyytinen K, Yoo Y, Issues and Challenges in Ubiquitous Computing, CACM 45 (12), 2002, 62–65

Maresch R, Rötzer F, Cyberhypes. Möglichkeiten und Grenzen des Internet, Frankfurt am Main 2001

Metzner-Szigeth A, Internet & Gesellschaft: Ein Humanes Projekt?, in: Sic et Non – Zeitschrift für Philosophie und Kultur – im Netz, No. 8, 2007, http://www.sicetnon.org/content/pdf/internet&gesellschaft.pdf (22.3.2009)

Metzner-Szigeth A, Von Cyber-Identitäten, virtuellen Gemeinschaften und vernetzter Individualisierung – sozial-psychologische Überlegungen, in: Sic et Non – Zeitschrift für Philosophie und Kultur – im Netz, No. 9, 2008a, http://sicetnon.org/content/pdf/cyber-ident.pdf (22.3.2009)

Metzner-Szigeth A, Framing Technology Assessment: Risk, Vulnerability and Sustainable Development, in: Graubner CA, Schmidt H, Proske D (Hgg.), Proceedings of the 6th International Probabilistic Workshop (Darmstadt, 26.–27. November 2008), Darmstadt (Technische Universität Darmstadt) 2008b, 525–550

Metzner-Szigeth A, Contradictory Approaches? – On Realism and Constructivism in the Social Sciences Research on Risk, Technology and the Environment, in: Futures, 41 (2), 2009, 156-170, http://dx.doi.org/10.1016/j.futures.2008.09.017 (22.3.2009)

Münker S, Roesler A (Hgg.), Mythos Internet, Frankfurt am Main 1997
OECD, Towards a global information society – GII-GIS: Policy Requirements, Paris 1998
Perrow C, Normal Accidents – Living with High-Risk Technologies, New York 1984
PriceWaterhouseCoopers, Main Report, Socio-Economic Benefits Analysis of GMES, 2006, http://esamultimedia.esa.int/docs/GMES/261006_GMES_D10_final.pdf (22.3.2009)
Schelhove H, Das Medium aus der Maschine. Zur Metamorphose des Computers, Frankfurt am Main/New York 1997
Siemoneit O, Ubiquitous Computing – Neue Dimensionen Technischer Kultur, in: Trans, Internet-Zeitschrift für Kulturwissenschaften, 15, 11/2003, http://www.inst.at/trans/15Nr/10_4/siemoneit_oliver15.pdf (17.1.2006)
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin, Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS), Studie im Auftrag des BMBF, Kiel/Berlin 2006, https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf (22.3.2009)
van 't Klooster SA, van Asselt MBA, Practising the scenario-axes technique. Futures 38, 2006, 15–30
Wahlster W, Weyrich C (Hgg.), Forschen für die Internet-Gesellschaft: Trends, Technologien, Anwendungen. Ergebnisse einer gemeinsamen Initiative des Bundesverbands der Deutschen Industrie und der Fraunhofer-Gesellschaft, 2002, http://w4.siemens.de/ct/de/activities/inet_symp/downloads/ergebnisse.pdf (17.1.2006)
Weiser M, The Computer for the 21st Century, Sci Am 265, 3, 1991, 66–75
Wright D, Alternative futures: AmI scenarios and Minority Report. Futures 40, 2008, 473–488
Wright D, Gutwirth S, Friedewald M, Vildjiounaite E, Punie Y (Hgg.), Safeguards in a World of Ambient Intelligence. Dordrecht 2008

Sonstige Quellen

– Meldung des Tagesspiegel vom 26.7.2007 mit dem Titel „Fahrer folgte Navigationssystem – Bus stürzte ab": http://www.tagesspiegel.de/weltspiegel/Busunglueck;art1117,2346658 (22.3.2009)
– Ergebnisse einer Umfrage zur Sicherheit von Navigationsgeräten, die das britische Versicherungsunternehmen „Direct Line" im Auftrag der Zeitung „Mirror" durchführte: http://www.mirror.co.uk/news/top-stories/2008/07/21/satnav-danger-revealed-navigation-device-blamed-for-causing-300-000-crashes-89520-20656554/ (22.3.2009)
– The WELL: http://www.well.com/ (22.3.2009)
– Second Life: http://de.secondlife.com/ (22.3.2009)
– World of Warcraft: http://www.worldofwarcraft.com/ (22.3.2009)
– Wikipedia, Stichwort „RFID": http://de.wikipedia.org/wiki/RFID (22.3.2009)
– Wikipedia, Stichwort „WiMAX": http://de.wikipedia.org/wiki/WiMAX (22.3.2009)
– Wikipedia, Stichwort „geographic information system": http://en.wikipedia.org/wiki/Geographic_information_system (22.3.2009)
– Flyer zur Tagung „Globale Fernerkundungssysteme und Sicherheit" (Wien, 9.–10. Oktober 2008): http://www.espi.or.at/images/stories/dokumente/press/programm_ht_fernerkundung_102008.pdf (22.3.2009)
– Kinofilm mit dem Titel: Das Netz (The Net), USA 1995, Regie: Irwin Winkler

Rechtliche Fragen der Bereitstellung von Erdbeobachtungsdaten

Lesley Jane Smith

I Einleitung

Dieser Beitrag erläutert einige Schlüsselfragen bei der rechtlichen Regulierung von primären und sekundären Raumfahrtdaten. Der Umgang mit und Vertrieb von kommerziellen Fernerkundungsdaten ist bislang, von einigen Ausnahmen abgesehen, nationalrechtlich noch nicht systematisch erfasst. Die nationale und internationale Regelung der Fernerkundung und der Vertrieb ihrer Daten verdienen sowohl unter Zugangs- als auch unter sicherheitsrechtlichen Erwägungen erhöhte Aufmerksamkeit.

Dieser Beitrag gibt einen Überblick über die bestehenden nationalen, europäischen und internationalen Regelungen zur Fernbeobachtung. Er schließt mit einer Betrachtung darüber, wie in Zukunft Rechtssicherheit im privaten und öffentlichen Umgang mit Geo-Daten gewährleistet werden kann und – unter gleichwertiger Berücksichtigung der Gesichtspunkte – eine Regelung der Satellitenerkundung einerseits sowie öffentliche und private Interessen andererseits auf internationaler und nationaler Ebene in Einklang zu bringen sind.

1 Begriffsbestimmungen

Derzeit sind 69 Fernerkundungssatelliten im Einsatz (zwölf Radar- und 57 optische Satelliten).[1] Fernerkundungsdaten und -produkte werden für kommerzielle und nicht-kommerzielle Zwecke verwendet. Zu den kommerziellen Zwecken zählen u.a. Kartografie, Katastererfassung und das Erstellen von Wetterkarten; nichtkommerzielle Zwecke sind beispielsweise der Notfallschutz im Rahmen der Internationalen Charta für Weltraum und Naturkatastrophen oder die Beobachtung der Bodenbedeckung zur Entwicklung rechtspolitischer Vorgaben innerhalb der GMES-Initiative.[2]

---

[1] Vgl. World Commercial remote Sensing satellite data base, online: www.licensing.noaa.gov/Optical_remote_Sensing_Satellites_8-9-06withoutsensors.pdf und www.licensing.noaa.gov/Optical_remote_Sensing_Satellites_7-19-06.pdf (Januar 2009).

[2] www.gmes.info/index.php?id=home (Januar 2009).

Raumfahrtdaten reichen von Signalen bis hin zu unverarbeiteten Primärdaten, die nach der Verarbeitung als hochauflösende Bilder für Umweltinformationen, Bestandsbemessungen, Positionsbestimmungen und vieles mehr eingesetzt werden können. Satellitenbilder können u.U. sehr viel über eine Gesellschaft aussagen. Die auf Präzision ausgerichteten technologischen Möglichkeiten führen zwangsläufig zu erweiterten Anwendungen und zum Einsatz von Raumfahrt- oder GEO-Daten. Diese Daten werden z.B. für den Aufbau der sog. *Global Spatial Data Infrastructure (GSDI)* eingespeist und Informationsdienstanbieter gewinnen durch den Zugang zu öffentliche Informationen über Boden- und Flächennutzung, Infrastruktur und weitere Informationsprodukte einen enormen Qualitätsvorsprung. Die Anwendungsmöglichkeiten von GEO-Daten reichen von der Forschung bis hin zu interoperativen Informationssystemen und können so für ein breites Publikum verfügbar gemacht werden, das den Zugang zu diesen Daten wünscht oder sogar benötigt (Blamont 2008).

Fernerkundungsdaten sind eine wertvolle Datenquelle, weil sie vielseitig einsetzbar sind. Diese Anwendungsbreite bedeutet allerdings, dass eine Erörterung der jeweiligen Regulierungsregimes ein breites Spektrum umfassen muss, da jede einzelne Thematik eine Vielzahl von Aspekten beinhaltet.

2 Grundsatz der Erderkundungsfreiheit

Der Weltraum unterliegt den Regeln des allgemeinen und speziellen Raumfahrt-Völkerrechts. Die wenigen nationalstaatlichen Raumfahrtgesetze lehnen sich an die Vorgaben der fünf maßgeblichen völkerrechtlichen Raumfahrtverträge an.[3] Deren Umsetzung in nationales Recht ist Ausdruck der Kongruenz nationalrechtlicher Normen mit den höherrangigen völkerrechtlichen Prinzipien und sichert deren Einhaltung auf nationaler Ebene ohne Verlust der hoheitsrechtlichen Prärogative für den einzelnen Nationalstaat.[4]

---

[3] Weltraumvertrag v. 27. Januar 1967; Weltraumrettungs- und -rückführungsübereinkommen v. 22. April 1968; Weltraumhaftungsübereinkommen v. 29. März 1972; Weltraumregistrierungsübereinkommen v. 14. Januar 1975; Mondvertrag v. 18. Dezember 1979; alle völkerrechtlichen Raumfahrtverträge abrufbar über United Nations Office for Outer Space Affairs, www.unoosa.org.

[4] USA; Canada; Japan; Russland; Ukraine; Schweden; Vereinigte Königreich; Frankreich; Belgien; Niederlande.

Die Regelung von Fernerkundungsdaten basiert auf Grundsätzen aus verschiedenen Rechtsquellen: internationales Weltraumrecht, nationales Recht, mit Berücksichtigung von Sicherheitsaspekten und von Regimes für geistiges Eigentum und Lizenzbedingungen.

Auf internationaler Ebene wird die Nutzung des Weltraums in erster Linie durch die Bestimmungen des Weltraumvertrags *(Outer Space Treaty, OST)* von 1967 geregelt.[5] Dieser völkerrechtliche Vertrag, der der UN-Charta als *lex specialis* vorgeht, enthält die von der internationalen Gemeinschaft anerkannten Parameter für den Umgang mit dem Weltraum. Der Weltraumvertrag gilt als *magna charta* und Wegweiser des Weltraumrechts (Jakhu 2003). Als maßgebliches Ziel schreibt Art. I (2) des Weltraumvertrags, wie bereits in der Präambel hervorgehoben, die friedliche Nutzung des Weltraums vor. Alle Staaten können und dürfen den Weltraum erforschen und nutzen, sofern die Vorgabe einer friedlichen Nutzung eingehalten wird, die Weltraumaktivitäten dem Interesse der Sicherheit dienen und nicht diskriminierend sind (Art. III OST). Hieraus leitet sich der Grundsatz der Erkundungsfreiheit ab, die von Staaten und/oder kommerziellen Betreibern zu friedlichen Zwecken völkerrechtskonform ausgeübt werden darf. Die Fernerkundung ist also nicht explizit in den Bestimmungen des OST geregelt, aber gleichwohl integraler Bestandsteil zulässiger (friedlicher) Raumfahrtaktivitäten. Alle Fernerkundungsaktivitäten eigener nationaler Rechtssubjekte unterliegen gem. Art. VI OST der Verantwortlichkeit des Nationalstaats, unabhängig davon, ob sie von Regierungs- oder Nichtregierungsakteuren unternommen werden. Gerade weil der Weltraumvertrag gem. Art VI dem Nationalstaat die Verantwortung für nicht-staatliche Rechtssubjekte auferlegt, bleibt er sowohl für staatliche wie auch für kommerzielle Aktivitäten im Weltraum zuständig und verantwortlich. Diese internationale Zuständigkeit von Staaten führt weiter dazu, dass sie laut Art. VIII OST auch für die Raumfahrtaktivitäten eigener Raumfahrtgegenstände (Satelliten) im Ausland zuständig bleiben. Dieser Aspekt ist wegen der internationalen Haftungsregelungen in der Raumfahrtpraxis sowohl für die Fernerkundung als auch für sonstige Raumfahrtaktivitäten von großer Bedeutung. Er führt dazu, dass einzelne Raumfahrtstaaten die Genehmigungspflicht auch für Raumfahrtaktivitäten außerhalb ihres eigenen Staatsgebiets vorschreiben. So wird sichergestellt, dass sie auch über solche

[5] Weltraumvertrag, Fn. 3, supra.

privaten Aktivitäten ihrer Staatsbürger informiert sind, die sich außerhalb ihres Territoriums abspielen.[6]

3 UN-Fernerkundungsprinzipien

Neben dem Weltraumvertrag (OST) bilden die in der Praxis umstrittenen *UN Remote Sensing Principles* die einzige internationale Rechtsgrundlage für die Fernerkundung.[7] Diese im Jahre 1986 verabschiedeten *Principles* haben eine Vorreiterrolle inne; sie legen die grundsätzliche Zulässigkeit der Fernerkundung zu bestimmten Zwecken fest. Nur die Fernerkundung zu den in *Principle Ib, c,* und *d* festgelegten Zwecken ist von diesen Regelungen betroffen. Gemäß *Principle Ia* dient die Fernerkundung der Verbesserung des Ressourcenmanagements, der Bodennutzung und dem Umweltschutz. Diese Ziele werden durch die *Principles X* und *XI* – Schutz der Erde und Katastrophenmanagement – als Ausdruck der internationalen souveränen Gleichheit verdeutlicht.

Principle I unterscheidet drei verschiedene Kategorien: „primary data“[8], „processed data“ und „analysed information“. Die erste Kategorie bezieht sich auf Daten „acquired by remote sensors borne by a space object and that are transmitted or delivered to the ground from space by telemetry“. Die zweite Kategorie umfasst „the products resulting from the processing of the primary data, needed to make such data usable“, und in der dritten Kategorie wird festgelegt, dass „analysed information“ das Ergebnis der „interpretation of processed data, inputs of data and knowledge from other sources“ sind. Mit anderen Worten: Daten werden in den *Principles* als Informationsbausteine behandelt.

Die Verbindlichkeit der *Principles* ist umstritten, da sie nicht den Status eines völkerrechtlichen Vertrags oder Abkommens haben, sondern als UN-Beschluss im Sinne der klassischen Völkerrechtstheorie lediglich Ausdruck allgemeiner Grund-

---

[6] Ein typisches Beispiel hierfür liefern die USA mit ihrem Commercial Remote Sensing Policy, zuletzt 2003 revidiert und den begleitenden Lizenzierungsrichtlinien, zugänglich unter http://modisdb.usgs.gov/background.php (21. Januar 2009). Im Allgemeinen sind Staaten bestrebt, die Souveränität anderer Staaten nicht zu verletzen.

[7] UN Principles of Remotes Sensing U.N. Doc. A/Res/41/65 (1986).

[8] Mangels einer offiziellen deutschen Übersetzung werden zur Vermeidung sprachlicher Verwirrung die englischen Ausdrücke beibehalten.

sätze des Völkerrechts sind.[9] Im Rahmen der Diskussion über die Bindungswirkung der *Principles* ist anzumerken, dass sie die militärische Nutzung von Raumfahrtdaten nicht tangieren. Ihre Geltung beschränkt sich auf Staaten, umfasst keine Privat- und Rechtspersonen, so dass sie genau genommen gegen kommerzielle Unternehmen nicht angewendet werden können. Der fehlende Bezug auf den nicht-staatlichen Bereich unterstützt die Argumentation, dass sich die *Principles* ausschließlich auf Fernerkundung zu Zwecken des Gemeinwohls beziehen, nicht auf private Aktivitäten (Kries und Polley 2002). Ein weiterer Schwachpunkt der *Principles* in ihrer praktischen Anwendung ist ihre Wirkung auf die Rechte von erkundeten Staaten. Zwar garantiert *Principle XIII* die Beobachtungsfreiheit; die Beziehung zwischen erkundetem und erkundendem Staat bleibt jedoch ungeklärt.

In den Vorberatungen zu den *UN Remote Sensing Principles* hatte es einen Dissens mit den Entwicklungsländern gegeben, der das Erkundungsrecht fremder Staaten über ihrem Hoheitsgebiet betraf (Jakhu 2003[10]). Entgegen den Forderungen der Entwicklungsländer gesteht *Principle XII* dem erkundeten Staat ein Zugangsrecht zu Daten über das eigene Hoheitsgebiet lediglich gegen einen angemessenen Preis zu.[11] Im Ergebnis – und im Widerspruch zum Regelungsziel der *Principles* – wird das Recht des erkundeten Staats an seinen eigenen Daten der nationalen Sicherheitspolitik des Erkundungsstaats unterworfen. Hierin liegt ein offener Konflikt zwischen der nationalrechtlichen Sicherheitspolitik eines Erkundungsstaats und dem Recht des erkundeten Staats an seinen eigenen Daten, der bis heute nicht in zufriedenstellender Weise gelöst worden ist (Jakhu 2003).

Die überaus allgemeine Natur der *Principles* unterstreicht die dringende Notwendigkeit eines verbindlichen Systems zu ihrer Durchsetzung (Ospina 2007) oder (zumindest) eines Rahmengerüsts durchsetzbarer internationaler Gemeinwohlprinzipien[12], damit konzertiertes Handeln auf internationaler Ebene wirksame Ergebnisse bringen kann. Dies würde, z.B., ein effektiveres Katastrophenmana-

---

[9] Art 38(1) des Statuts des Internationale Gerichtshofs (IGH) enthält die Normenhierarchie des Völkerrechts, wonach das internationale Vertragsrecht nach Art 38(1)a den allgemeinen Prinzipien des Völkerrechts Art 31 (1)b vorgeht.

[10] Hierbei insbes. 85–89.

[11] Dem Wortlaut nach ist dies ein absolutes Recht und darf damit nicht zu diskriminierenden Zwecken genutzt werden.

[12] Siehe COPUOS TOP "International Cooperation in the Promotion of the Use of Geospatial data for Sustainable Development," COPUOS Report A/60/20E, online: http://www.unoosa.org/pdf/gadocs/A_61_20E.pdf (10.11.2007).

gement ermöglichen (gem. der Internationalen Charta für Weltraum und Naturkatastrophen oder der GMES-Initiative Globale Überwachung für Umwelt und Sicherheit).[13] Ein idealer Reformansatz wäre die Umwandlung der *Principles* in eine bindende Konvention.[14] Damit drängt sich die Frage auf, ob es neben den derzeit angewendeten Instrumenten alternative Möglichkeiten zur Regulierung der Verbreitung von EO-Daten gibt.

4 Fernerkundung und Fernerkundungsdaten – nationale Regelungen für kommerzielle Betreiber und die Rolle des Freedom of Information Act (FOI)

4.1 Nationale Regelungen

Regelungsprototypen für Fernerkundungsgesetze gab es zuerst in den USA, die das ausführlichste und umfassendste Lizenzsystem für Fernerkundung besitzen. Mit dem *US Land Remote Sensing Policy Act* (1992), später von der *Presidential Decision Directive* (2004) bestätigt, begann die Aufweichung des staatlichen Fernerkundungsauftrags in den USA zugunsten der Kommerzialisierung im Bereich der Raumfahrtdaten. Diese Gesetze wurden zwischenzeitlich ergänzt und liegen nun im *Commercial Remote Sensing Policy* vom 25. April 2003 vor. Grundsätzlich ist eine Genehmigung durch die National Oceanic and Atmospheric Administration (NOAA) erforderlich, die hinsichtlich Lizenzierung, Beobachtung und Regelbefolgung für private Erdfernerkundungssysteme genaue Bestimmungen enthält. Allerdings liegt die Erteilung dieser Genehmigung durchaus in der Ermessensfreiheit der jeweiligen Behörde.[15]

Eine nationale gesetzliche Kontrolle der kommerziellen Erdbeobachtung gibt es ferner in Kanada und Indien,[16] wobei das kanadische Regelungssystem im *Canada Remote Sensing Space Systems Act* von 2005 und in einer begleitenden Ver-

---

[13] Weitere Erörterungen bei A. Ito, Legal Aspects of the International Charter on Space and Major Disasters, Proceedings of the 47th Colloquium on the Law of Outer Space, International Institute of Space Law/ American Institute of Aeronautics and Astronautics, 2004, 233.

[14] Beispiel für einen Konventionsentwurf zur Fernerkundung in Feder, The Sky's the Limit? Evaluating the International Law of Remote Sensing, 23 N.Y.U.J. Int. L. & Pol. 599, 659 ff. Nach Auffassung des Autors ist dieses Beispiel, obwohl es bereits aus dem Jahr 1991 stammt, insofern bedeutsam, als es den Entwurf eines Rechtsdokuments darstellt, nicht lediglich einen allgemeinen Vorschlag zur Regulierung der Fernerkundung.

[15] National Oceanic and Atmospheric Administration, s. http://www.noaa.gov (Januar 2009).

[16] Dieser Beitrag befasst sich nicht mit Einzelheiten der indischen Gesetzgebung und Lizenzpolitik.

ordnung von 2007 ein höchst transparentes Lizenzsystem vorsieht. Es verlangt die Vorlage des sog. *Data Protection Plan* durch den kommerziellen Betreiber. Das kanadische Gesetz zählt zu den besten gesetzlichen Regelungen für den Umgang mit kommerziellen Raumfahrtdaten (Mann 2004).

In einigen Ländern ist der Bereich Fernerkundung und Weltraumdaten zwar gesetzlich geregelt, wobei aber die nationalen Vorschriften nicht immer kompatibel sind mit den Definitionen, die in internationalen Rechtsquellen, vor allem in den UN-Prinzipien, Verwendung finden. Das Problem der Begriffsbestimmung und Terminologie stellt praktisch einen eigenständigen Untersuchungsgegenstand dar. So wird z.B. im kanadischen Remote Sensing Space Systems Act „raw data" definiert als „sensor data from a remote sensing satellite, and any auxiliary data required to produce remote sensing products from the sensor data that have not been transformed into a remote sensing product."[17] „Remote sensing product" bezeichnet ein Bild oder Daten, die aus Rohdaten gewonnen werden, und zwar auf jegliche Art und Weise, die die Rohdaten verändert.[18] Das bedeutet, dass nach kanadischer Regelung ein „remote sensing product" sowohl die in *Principle I* festgelegten Kategorien „processed data" als auch „analysed information" einschließt.

Neben dem kanadischen Regelungsmodell hat die Bundesrepublik Deutschland im *Satellitendatensicherheitsgesetz* von 2007 eine gesetzliche Basis zur Kontrolle von raumgestützten Fernerkundungssystemen und Datenverbreitung eingeführt.[19] Demnach bedarf ein hochwertiges Erdfernerkundungssystem anhand von Kriterien über dessen Auflösungspräzision der Genehmigung nach § 3 SatDSig. Diese Zulassung ist sowohl für den Betrieb wie auch für den Vertrieb von Daten erforderlich. Darüber hinaus schreibt das Gesetz dem Betreiber Anzeige-, Dokumentations- und Auskunftspflichten vor, so dass er gemäß § 17 SatDSig 2007 in Eigenverantwortung zu prüfen hat, ob die entsprechenden Daten den Kriterien der Sensibilität unterliegen, was zu einem Verbot des Vertriebs führen kann.[20] Ob das nationale Raumfahrtgesetz eine spezifische Kontrolle für den raumfahrtgestütz-

---

[17] Remote Sensing Space Systems Act, S.C. 2005, c.45 Sec. 2., zugänglich unter http://www.canlii.org/ca/sta/r-5.4/part321316.html (Januar 2009).

[18] Ders.

[19] Das Satellitendatensicherheitsgesetz – SatDSig, BGBl 2007, I.S.2590, trat am 1. Dezember 2007 in Kraft.

[20] Für weitere Einzelheiten, s. Gerhard/Kroymann/Schmidt-Tedd, Ein Gesetz für die Raumfahrt: das neue Satellitendatensicherheitsgesetz, Zeitschrift für Luft und Weltraumrecht 57/1 (2008) 40–66.

ten Vertrieb von Daten vorsieht muss für das jeweilige Land im einzeln geprüft werden.[21]

4.2 Informationsfreiheit versus „Shutter Control"

Die Genehmigung der Fernerkundung kann insbesondere aus Gründen der nationalen Sicherheit verweigert werden, was im Zusammenhang mit Fernerkundungslizenzen allgemein als „Shutter Control" bezeichnet wird. Unter bestimmten Umständen ist der Betreiber verpflichtet, das Sammeln bzw. die Verbreitung von Daten einzuschränken, wenn außenpolitische Belange oder internationale Verpflichtungen dies erforderlich machen. „Shutter Control"-Bestimmungen gibt es nicht nur in den USA, sondern auch in Kanada und speziell in Israel, wo ein System gezielter staatlicher Kontrolle existiert (Rao/Murthi 2006).

Nationale Gesetzgebungen zu Informationsfreiheit und Zugang zu öffentlichen Daten (FOIAs) sind eine der wichtigsten Quellen zur Regulierung des Zugangs zu Fernerkundungs- und EO-Daten und -Informationen (vor allem EO-Umweltdaten) in den einzelnen Staaten. Sie definieren die Zugangsbestimmungen zu Daten und Informationen, die sich im Besitz der Regierung oder von Regierungsbehörden bzw. im Auftrag der Regierung in privaten Händen befinden. Ihre Bedeutung für die Zugangsbedingungen zu Fernerkundungs- und EO-Daten und -Informationen sollte nicht unterschätzt werden, da die Beschaffung von Fernerkundungs(roh)-daten nach wie vor überwiegend staatlich finanziert wird.

In diesen Statuten sind die Begriffe Eigentum und Nutzung von zentraler Bedeutung für die Festlegung der Zugangsbedingungen zu Daten und Information. In der Herangehensweise unterscheiden sich die einzelnen Rechtssprechungen allerdings teilweise erheblich.

5 Lizenzpraktiken in der Fernerkundung

Zahlreiche Regierungsorgane und internationale Organisationen sowie auch Privatunternehmen entwickeln ihre eigenen Datenrichtlinien und Lizenzbedingun-

[21] Z.B. gem. Sektion 1(c) des britischen Outer Space Act 1986 ch. 38, wird eine Zulassung für „any activity in outer space" benötigt; für das französische Raumfahrtgesetz s. Erläuterungen http://www.ump-senat.fr/Projet-de-loi-relatif-aux.html Loi 2008-518 v. 3. Juni 2008, Loi relative aux opérations spatiales (zuletzt Januar 2009). Das französische Gesetz schreibt eine Anzeigepflicht des Betreibers (Art. 23) neben strafrechtlichen Sanktionen bei Datenmissbrauch der Daten vor.

gen für die Beschaffung und Verbreitung von Fernerkundungs- und EO-Daten und -Informationen. Diese sind nicht notwendigerweise deckungsgleich mit den Regierungsrichtlinien für den Zugang zu öffentlichen Informationen, da letztere nur Daten betreffen, deren Beschaffung nicht staatlich finanziert ist. Die Methoden der Datenverbreitung lassen sich in zwei Grundtypen unterteilen: Auswahl und Einsetzung der Vertreiber für einen bestimmten Bereich (oder ein bestimmtes Produkt) sowie Lizenzierung der Daten und Informationen direkt an den Endverbraucher. Nachstehend werden einige Beispiele für beide Typen kurz erörtert.

Gemäß ihren Datenrichtlinien[22] behält die Europäische Raumfahrtagentur (ESA) im Namen ihrer Mitgliedstaaten das Eigentumsrecht an allen Primärdaten und hieraus hergeleiteten (Informations-)Produkten. Als Schutzmechanismen fungieren Datenbankenbestimmungen, Urheberrechtsgesetze und andere Formen geistigen Eigentumsrechts.

Die Verbreitungsmodalitäten (wie auch die Preise) sind abhängig von der Nutzungskategorie: Nutzung zum Zwecke von Forschung und Anwendungsentwicklung zur Beförderung der Missionsziele (Nutzungskategorie 1) und Nutzung zu allen anderen Zwecken (Nutzungskategorie 2). ESA ist allein verantwortlich für die Verbreitung von Daten der Nutzungskategorie 1, die ausschließlich für Projektzwecke und gegen Wiederbeschaffungskosten genehmigt wird. Die von der ESA eingesetzten „Verbreitungsinstanzen" haben die Aufgabe, Dienstleistungen für die Nutzung gemäß Kategorie 2 anzubieten, wobei ihnen in der Preisgestaltung freie Hand gelassen wird. Diese Verbreitungsinstanzen sind verpflichtet, wertschöpferisch tätigen Betreibern und Dienstleistungsanbietern den Zugang zu den Daten zu garantieren und sicherzustellen, dass die Nutzer das Recht zum Verkauf von Produkten und Dienstleistungen erhalten.[23] In diesem Zusammenhang sei daran erinnert, dass ESA-Unternehmungen und -Projekte zumindest teilweise durch die etatmäßigen Zuwendungen ihrer Mitgliedstaaten – und damit öffentlich – finanziert werden, was die implizite Zustimmung der jeweiligen Regierungsebenen zu ESAs eigener Zugangspolitik nahe legt.

---

[22] Weitere Einzelheiten über Zugangsrechte und zu den ESA-Satelliten können über http://eopi.esa.int/esa/esa?e=XDctYy0WaRLaJNhebsewi1ErZRG7wKE9gap7LbOboTo6u1ZOcpyMvGnZhVgTGK1sKPQogqSaiNyqkCeUdJR2IAVRcXPiXjm4nt abgerufen werden; z.B. Earth Explorer Data Policy, S. http://eopi.esa.int/doc/download/EE_data_policy.pdf; ferner Envisat Data Policy; http://eopi.esa.int/doc/download/envisat_data.pdf; (Januar 2009).

[23] Nr. 6.6 Envisat Data Policy Summary, id.

Die Europäische Meteorologische Satelliten Organisation (EUMETSAT) besitzt die alleinigen Eigentumsrechte sowie alle geistigen Eigentums- und Nutzungsrechte an ihren Satelliten und Daten.[24] Die nationalen meteorologischen Dienste haben die Alleinvertretungsrechte für die Vergabe von Lizenzen für EUMETSAT-Daten in ihrem jeweiligen Hoheitsgebiet und sind für die Verbreitung kommerzieller Daten verantwortlich.[25]

Auf den Internetseiten verschiedener internationaler Satellitenorganisationen, Raumfahrtagenturen und Betreiber lassen sich zahlreiche weitere Beispiele für die Regulierung von Satellitendaten finden und vergleichen.

6 Europäischer Ansatz: Geodaten

Zwei wesentliche Grundsätze werden zur Zeit in der europäischen Umweltinformations- und Raumfahrtpolitik verfolgt: zum einen die Öffnung bzw. der Zugang über interoperable Geo-Portale mit den von EU-mitgliedsstaatlichen Regelungen erfassten Geo-Daten; zum anderen die in der *UN Convention on Access to Information* von 1998 enthaltene Kostenerwägung, die eine Datenbeteiligung befürwortet, um so eine Reduktion der Fernerkundungskosten zu erreichen. Hierdurch soll der breitere Zugang der Behörden zu Umwelt- und Geoinformationen ermöglicht werden. Diese Tendenz hat in verschiedenen Richtlinien der EU bereits ihren Niederschlag gefunden.

Die *Re-use of Public Sector Information-Richtlinie* (RL 2003/98)[26] schreibt die Nutzung des Wertschöpfungspotenzials von Raumfahrtdaten aus dem öffentlichen Sektor vor. Dieser Ansatz gestattet einen vereinfachten Zugang zu Informationen der öffentlichen Hand, gegebenenfalls gegen angemessene Bezahlung, und erreicht damit eine erweiterte Wertschöpfung sowie den Zugang zu wichtigen Daten, ohne dass sie neu erhoben werden müssen.

---

[24] Präambel Resolution EUM/C/98/Res. IV, EUMETSAT Principles on Data Policy. 1.–3. Juli 1998 (im Folgenden: EUMETSAT Resolution). Die Zugangsbestimmungen hängen unter anderem davon ab, ob es sich um Pflicht- oder Wahlprogramme handelt, wobei die Resolutionen im Einzelnen revidiert werden, S. zuletzt EUMETSAT Council Resolution EUM/C/64/08 Res II v. Juli 2008; S. ferner Smith/Doldirina, „Remote Sensing: A case for moving space data towards the public good", Space Policy 24 (2008) 22–32.

[25] Para II EUMETSAT Resolution.

[26] Richtlinie 2003/4/EG vom 28. Januar 2003 über den Zugang der Öffentlichkeit zu Umweltinformationen, ABl EU Nr. L 41/26 v. 14. Februar 2003.

Die *Public Access to Environmental Information-Richtlinie* (RL 2003/2004)[27] ist die unmittelbare Umsetzung des UN Arhuus-Abkommens durch die EU und schreibt eine aktive Informationspflicht der Mitgliedsstaaten vor.

Schließlich ist die Richtlinie 2007/2 *INSPIRE*[28] zu erwähnen, die den Mitgliedsstaaten den Aufbau einer Geoportalstruktur für Mitgliedstaaten vorschreibt, welche wiederum in einer späteren Entwicklungsphase zu einem EU-weiten Geoportal führen wird.

Dies ist ein Versuch, „(to) secure storage, maintenance and making available of spatial data within the European Community at the most appropriate level".[29] In diesem frühen Stadium lassen sich hinsichtlich der Wirksamkeit dieser Richtlinie nur Vermutungen anstellen. Nach Ablauf der Einführungsphase (2010 für die erste Phase) wird sich hier ein klareres Bild ergeben.[30]

II Resümee: Juristische Kernfragen der Zukunft

Aufgrund der technologischen Entwicklung, die im letzten Jahrzehnt zu einer enormen Ausdehnung des kommerziellen Erdbeobachtungssektors geführt hat, werden die Internationalen Fernerkundungsprinzipien von 1986 höchstwahrscheinlich durch nationale Gesetzgebung und Fernerkundungspraxis verdrängt werden, wenn es nicht gelingt, sie in Form einer bindenden Konvention zu formulieren.

Auf nationaler Ebene hat insbesondere die verbreitete Nutzung des Internet im täglichen Privat- und Arbeitsleben im Vorfeld ein Quasi-Zugangsrecht zu nicht sicherheitsrelevanten Erdbeobachtungsinformationen geschaffen. Weitere Fragen stellen sich für die Zukunft, sofern die Nutzung von Erdbeobachtungsdaten z.B. zu einer erhöhten öffentlichen Transparenz einzelner Personen- und Gruppenprofile in unserer Zivilgesellschaft führt: die Frage des Personendatenschutzes und des Schutzes

---

[27] Richtlinie 2003/98 v. 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors, ABl EU Nr. L 345/90 vom 31. Dezember 2003 (kurz PSI genannt), umgesetzt als Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen v. 3. Dezember 2006 BGBl. I S. 2913, Inkrafttreten 9. Dezember 2006.

[28] Richtlinie 2007/2/EG v. 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE), ABl EU Nr. L 108/1 v. 25. April 2007.

[29] Präambel, INSPIRE Directive, id.

[30] Art. 21 INSPIRE Richtlinie, FN 28 oben. Zur Geschichte des Entwurfs und aktuellen Informationen siehe: http://inspire.jrc.it (10.11.2007). Für eine detaillierte Analyse der Bestimmungen der Direktive siehe Smith/Doldirina, „The EU INSPIRE Directive: a Suitable Mechanism to Make Spatial Data (More) Available?" Proceedings of the 50th International Space Law Colloquium 2007 (American Institute of Aeronautics and Astronautics, 2008), 109–118.

der Privatsphäre. Über GoogleMap, GoogleEarth und GoogleStreetView ist dieser Zugriff zum Teil bereits möglich. Unlängst haben die Datenschutzbeauftragten in ihrer Stellungnahme zum kommerziellen Einsatz satellitengestützter Daten vor möglichen Verknüpfungsmöglichkeiten zur Erstellung von Personenprofilen gewarnt.[31]

Die verbleibenden juristischen Fragen für die Zukunft werden sich u.a. auch auf die Authentizität und Integrität der Information nebst einer Haftung im Sinne der Verantwortlichkeit für die Vertreiber von Erdbeobachtungsinformationen konzentrieren. Da einige der Hauptregelungen hierfür aus dem EU-Recht abgeleitet werden, spricht vieles dafür, Lösungen innerhalb der EU zu suchen.

Die eigentliche Herausforderung der Zukunft liegt in der Schaffung einer klaren Regelung für den staatlichen Schutz privater Interessen vor dem Hintergrund, dass nationale Regelungskompetenzen nicht-ortsansässigen ausländischen Satellitenbetreibern keine rechtlichen Beschränkungen auferlegen können. Die Lösung liegt nicht allein in den Händen des nationalen Gesetzgebers, sondern bedarf der Mitwirkung der international zuständigen Regulierungsebenen, die aufgrund der Tatsache, dass diese Daten und Informationen allseits zugänglich sind, zumindest klare Strukturen für Kompetenzverteilung und Einhaltung der Regelungen vorschreiben können. Sofern im Bereich der Erdbeobachtung neue Regelungsansätze angestrebt werden, darf dies nur auf der zuständigen Regulierungsebene der UNCOPOUS, *United Nations Committee on the Peaceful Use of Outer Space,* der UNRCC (*UN Regional Cartography Conference)* und der GSDI *(Global Spatial Data Infrastructure)* geschehen. Im Bereich des internationalen Weltraumrechts darf nur auf internationaler Ebene agiert werden.

Professor Dr. iur. Lesley Jane Smith, LL.M.
Riga Graduate School of Law
Professorin an der Leuphana Universität Lüneburg und an der Riga Graduate School of Law mit den Arbeitsschwerpunkten Vergleichendes Zivilrecht und Entwicklungen in der Angleichung des europäischen Privatrechts nebst der Kommerzialiserung des Raumfahrtrechts

---

[31] S. Datenschutzrechtliche Rahmenbedingungen für die Bereitstellung von Geodaten für die Wirtschaft, unabhängiges Landeszentrum für Datenschutz Schleswig Holstein (ULD), Bericht v. 22.09. 2008, abrufbar unter https://www.datenschutzzentrum.de/geodaten/datenschutzrechtliche-rahmenbedingungen-bereitstellung-geodaten.pdf (zuletzt Januar 2009).

Literaturverzeichnis

Blamont J, „We the People; Consequences of the revolution in the management of space applications“, in: Space Policy 24, 2008, 13–21

Jakhu R, „International Law governing Acquisition and Dissemination of Satellite Imagery“, in: Journal of Space Law 29, 1&2, 2003, 65–91

von Kries W, Polley I, „Report of the ‚Project 2001‘ Working Group on Remote Sensing“, in: Böckstiegel KH (Hrsg.), Project 2001, 2002, 145–198

Mann B, „Drafting Legislation to regulate Remote sensing satellites: a How-To Guide from Canada“, in: Proceedings of the 47th IAF/American Institute of Aeronautics and Astronautics, 2004

Ospina S, „SOS – Is Anyone Getting This Message?“, in: Proceedings of the 49th Colloquium on the Law of Outer Space, International Institute of Space Law/American Institute of Aeronautics and Astronautics, 2007

Rao M, Sridhara Murthi KR, „Keeping up with remote sensing and GI advances – policy and legal perspectives“, in: Space Policy 22, 2006, 262–273

DIE NUTZBARMACHUNG VON SATELLITENGESTÜTZTEN SICHERHEITSDIENSTEN

Die Nutzung von Fernaufklärung für Sicherheit

Heinz Gärtner

1 Fragestellung

In diesem Essay soll die Wirksamkeit von sicherheitspolitischen Instrumenten wie Fernaufklärung zur Aufklärung und Verhinderung von Bedrohungen, Gefährdungen und Risiken sowie die Lösung von Problemen und Konflikten diskutiert werden. Dafür bieten sich zwei Analyseansätze an, der fähigkeits- und angebotsorientierte Ansatz und der nachfrage- und bedrohungsorientierte umfassende Sicherheitsansatz. Die These lautet, dass Fernaufklärung für bestimmte vordefinierte Bedrohungen, Gefährdungen und Risiken (wie Hurrikanverlauf und Fahrzeugbewegungen) im Rahmen des fähigkeits- und angebotsorientierten Ansatzes unentbehrlich ist. Wendet man aber den umfassenden nachfrage- und bedrohungsorientierten Ansatz an, kann Fernaufklärung nur mehr einen kleinen Teil der Nachfrage nach geeigneten Instrumenten abdecken.

a) Fähigkeitsorientierter Ansatz

Globale Fernerkundungssysteme sind in der Lage, vielfältige Sicherheitsleistungen anzubieten. Erdbeobachtungen sind unerlässlich für zivile Sicherheit, die Bereitstellung von Fernerkundungsdaten für Kriseninformation und die Erkennung von Gefahrenzonen. Fernerkundungssysteme sind fähigkeitsorientiert. Sie können mittels Aufklärung in einem bestimmten Spektrum dazu beitragen, dass Krisen verhindert und Menschen und Infrastruktur geschützt werden. In diesem fähigkeitsorienten Ansatz sind Fernerkundungssyteme die unabhängige, Sicherheitsprobleme die abhängige Variable. Der Vorteil dieses Ansatzes ist, dass eine hohe Kompatibilität zwischen Instrumenten für Problemlösung und den Problemen selbst besteht, weil die Anwendung von Fernerkundungssystemen das Anwendungsspektrum selbst definiert, die Aufklärung von Fahrzeug- und Truppenbewegungen, das Feststellen von Detonationen, Warnungen vor dem Herannahen von Hurrikanen und Hochwasservorwarnungen, u.v.a.

Der Nachteil des fähigkeitsorientierten Ansatzes ist, dass er Probleme außerhalb des vordefinierten Einsatzspektrums ausblendet. Bestimmte angebotene Instrumente sind für einige Probleme einsetzbar, für andere nicht. Die Gefahr besteht,

dass für den Besitzer eines Hammers alles wie ein Nagel aussieht. Um die Möglichkeiten und Grenzen von Fernerkundungssystemen feststellen zu können, muss das Sicherheitsspektrum daher ausgeweitet werden.

b) Umfassender bedrohungsorientierter Sicherheitsansatz

Zur Anwendung eines umfassenden Sicherheitsansatzes werden die umfassenden politischen, ökonomischen, ökologischen, gesellschaftlichen und militärischen Sicherheitsprobleme als unabhängige, die Instrumente als die abhängige Variable genommen, also die Variablen des fähigkeitsorientierten Ansatzes vertauscht. Für Aufklärung, Verhinderung von Bedrohungen, Gefährdungen und Risiken sowie Lösung von Problemen werden maßgeschneiderte Instrumente benötigt, von denen Fernaufklärung ein notwendiges aber nicht hinreichendes Instrumentarium darstellt. Dieses ist in dem umfassenden und bedrohungsorientierten Ansatz die abhängige Variable. Der Vorteil dieses Ansatzes ist, dass Bedrohungen, Risiken und Gefährdungen in all seinen Dimensionen analysiert werden. Er ist ein Anreiz, umfassende Antworten zu finden. Der Nachteil ist, dass die Schärfe der Analyse verloren geht, und viele aber wenig wirksame Antworten gegeben werden. Die Nachfrage nach sicherheitspolitischen Instrumenten deckt sich oft nicht mit dem vorhandenen Angebot.

2 Bedrohungsanalyse

Die Bedrohungen, Gefährdungen und Risiken sind seit Ende des Ost-West-Konflikts vielfältig geworden. Zu nennen sind zu allererst fragile und funktionsgestörte Staaten mit fragmentiertem politischen, wirtschaftlichen und gesellschaftlichen System. Diese sind oft, aber nicht ausschließlich, Nährboden für Terrorismus und organisierte Kriminalität. Sie sind Ursache von unkontrollierten Flüchtlingsströmen und mit ihnen gehen Wirtschaftsräume verloren. In der Europäischen Sicherheitsstrategie (ESS) und dem Vertrag von Lissabon werden weiters regionale Konflikte, die Proliferation von Massenvernichtungswaffen durch Weitergabe von Staaten an staatliche und nicht-staatlichen Akteure, Natur- und von Menschen gemachte Katastrophen und Epidemien genannt.

Es gibt nun zwei Möglichkeiten, Bedrohungen, Gefährdungen und Risiken zu begegnen. Man kann die Fähigkeiten erhöhen, um diese abzuwehren, man kann

aber auch selbst versuchen, sie zu verringern. Die Erhöhung massiver militärischer Fähigkeiten war die vorrangige Antwort auf die Bedrohung aus dem Osten während des Kalten Krieges. Die notwendigen Fähigkeiten, den oben genannten Herausforderungen zu begegnen, haben sich seither geändert. Die Europäische Union (EU) hat im Lissabonner Vertrag die sogenannten „Petersberger Aufgaben" weiter entwickelt. Sie beinhalten nun Konfliktverhütung, Abrüstung und Entwaffnungsoperationen, Beratungs- und Unterstützungsmaßnahmen, humanitäre und Rettungsoperationen, friedenserhaltende Missionen sowie Kampfeinsätze im Rahmen der Krisenbewältigung einschließlich Frieden schaffender Maßnahmen sowie Operationen zur Stabilisierung der Lage nach Konflikten. Mit all diesen Maßnahmen soll auch zur Bekämpfung des Terrorismus beigetragen werden.

Bedrohungen und Risiken können aber auch verringert werden. Die Verhinderung des Entstehens von fragilen und funktionsgestörten Staaten hat in diesem Rahmen erste Priorität. Funktionierende Staaten brauchen eine intakte Verwaltung, eine Regierung mit einem legitimen Monopol ausgebildete Sicherheitskräfte einzusetzen, und eine sich entwickelnde Zivilgesellschaft. Der Terrorismus darf nicht nur in seinen Auswirkungen, sondern muss auch an seinen Ursachen bekämpft werden. Radikalisierung, Armut, Jugendarbeitslosigkeit, Marginalisierung u.a. können zur Entstehung des Terrorismus beitragen und mit wirtschaftlichen, politischen und Integrationsmaßnahmen eingedämmt und verringert werden.

Das Raketenabwehrsystem, das gegen feindliche Staaten mit Nuklearwaffen gerichtet sein soll, ist eine militärische Fähigkeit mit sehr unsicherer Wirkung. Die Technologie ist nicht ausgreift und die Bedrohung nicht ausreichend analysiert. Russland befürchtet, dass die Raketen nicht nur gegen anfliegende Raketen eingesetzt werden können, sondern auch gegen weiche Ziele wie Moskau. Im globalen Rahmen können damit zweitschlagsfähige Raketen geschützt werden. Satelliten mit niedrigen Flugbahnen könnten Ziel der Abwehrraketen werden. Militärschläge gegen den Iran oder gegen Nordkorea sind schlechte Optionen, da die Zerstörung der Atomanlagen ungewiss ist und mit Vergeltungen in der Golfregion bzw. gegen Südkorea gerechnet werden muss.

Die Verringerung der Bedrohung durch Maßnahmen der Nicht-Verbreitung ist unerlässlich. Der Atomwaffensperrvertrag (NPT) bietet immer noch eine ausgezeichnete Grundlage. Er verbietet den Nuklearwaffenstaaten, Nuklearwaffen an Nichtnuklearwaffenstaaten weiter zu geben, und diesen solche anzunehmen. Die

Internationale Atomenergiebehörde (IAEO) soll die Einhaltung der Bestimmungen überwachen. Der Vertrag betont das Recht auf zivile Nutzung der Nuklearenergie und verpflichtet die Nuklearmächte, Schritte zur nuklearen Abrüstung einzuleiten. Zur besseren Implementierung des Vertrags sind weitere Instrumente vorgesehen. Ein zusätzliches Protokoll, das nicht von allen Mitgliedstaaten angenommen wurde, soll Inspektionen überall vor Ort erlauben. „Die Proliferation Security Initiative" (PSI) soll das Abfangen von verdächtigen Lieferungen ermöglichen. Die UN-Resolution 1540 verbietet die Weitergabe von Massenvernichtungswaffen und dazugehörigen Materialien an nichtstaatliche Akteure.

3 Die Rolle von Fernaufklärung

Fernaufklärung kann bei der Bekämpfung von vielen dieser Bedrohungen und Risiken und bei der Lösung von Problemen eine hilfreiche Rolle spielen, sind dabei aber in keiner Weise hinreichend. Aufklärung von oben kann unterstützend wirken, ist in den meisten Fällen ohne Maßnahmen am Boden mangelhaft, wirkungslos, ja kann sogar trügerisch sein. Offensichtlich können Wiederaufbaumaßnahmen wie Friedensoperationen nur von Menschen am Boden ausgeführt werden. Fernaufklärung kann Hinweise auf illegale Nuklearanlagen oder verdächtige Schiffe geben, kontrolliert müssen sie vor Ort werden. Die Inspektion von Millionen von Containern kann bestenfalls mit Sensoren am Boden erfolgen. Terrorismus ist primär mit nachrichtlichen und strafrechtlichen Maßnahmen zu bekämpfen, obwohl natürlich Ausbildungszentren, Trainingslager und Nachschublinien etwa von Al Qaida in Afghanistan und Pakistan aus der Luft festgestellt werden können.

Fernaufklärung alleine kann aber auch falsche Ergebnisse bringen oder gar missbraucht werden. Das wohl bekannteste Beispiel aus jüngerer Zeit ist die Demonstration des US-Außenministers Colin Powells im Februar 2003 vor dem Sicherheitsrat der Vereinten Nationen, die mit Satellitenbildern die Existenz von Massenvernichtungswaffen im Irak hätten beweisen sollen, die es bekanntlich nicht gab. In den achtziger Jahren wurden in der Nähe von Moskau Bunkeranlagen entdeckt, die aber nicht Silos für Nuklearanklagen waren, wie man aus den Luftbildern hätte schließen können, sondern Schutzbunker für die Kremlführung im Falles eines amerikanischen Nuklearangriffs. Eineinhalb Jahre nach dem Militär-

schlag Israels im September 2007 gegen eine vermutete nukleare Einrichtung in Syrien ist immer noch nicht klar, welcher Art diese Anlage war. Viele gefährliche Aktivitäten entziehen sich einfach der noch so gewissenhaftesten Fernaufklärung, wie der Aufbau eines nuklearen Netzwerks des pakistanischen Nuklearwissenschaftlers A.Q. Khan. Als 1999 in New York das West-Nil-Virus auftrat wusste man wochenlang nicht, ob es sich um einen Angriff mit Biowaffen oder um einen natürlichen Virus handelte.

Historisch das wohl berühmteste Beispiel erfolgreicher Luftaufklärung sind die Bilder sowjetischer Raketen auf Kuba von 1962, die Kennedy veranlassten, Druck auf die Sowjetunion auszuüben, die Raketen abzuziehen. Was Kennedy von den Bildern nicht wusste, war, dass ein Teil der Raketen bereits nuklear bestückt war, was ihn möglicherweise zu einer anderen Vorgehensweise veranlasst hätte. Ein erfolgreiches Beispiel des Zusammenwirkens verschiedener Fernaufklärungssysteme (Satelliten, Sensoren etc.) ist die ziemlich genaue Bestimmung der Größe und des Ausmaßes des Tests Nordkoreas einer Nuklearbombe 2006.

4 Ausblick

Die Welt steht vor einem Umbruch. Die Bipolarität des Ost-West Konflikts war zu Beginn der 1990er Jahre zu Ende. Das von dem Politologen Charles Krauthammer verkündete „unipolar moment“, das von der Bush-Administration für unilaterale Außenpolitik benutzt worden war, geht nun zu Ende. Wie die neue Welt aussehen wird, ist offen. Fest steht, dass die USA einer der wichtigsten Akteure auf der Weltbühne bleiben wird, andere wichtige staatliche, regionale, kontinentale und nichtstaatliche Kräfte werden aber hinzukommen. Der Begriff „Multipolarität“ beschreibt die neue Situation nur mangelhaft. Sie impliziert Polarisierung, die aber im Zeitalter der Globalisierung und internationalen Verflechtung nicht im Interesse der meisten Akteure ist. Alle großen Teilnehmer in der neuen Welt haben Interesse daran teilzuhaben, an der Weltwirtschaft beteiligt zu sein, den Terrorismus zu bekämpfen, und nukleare Proliferation zu verhindern. Sie werden nicht automatisch den Vorgaben der USA folgen, wie das George W. Bush hoffte, aber sich auch nicht prinzipiell gegen die USA stellen, wie das während der ideologischen Teilung der Welt in Kommunismus und Kapitalismus der Fall war. Verschiedene Autoren haben unterschiedliche Begrifflichkeiten für die entstehende

neue Welt vorgeschlagen, wie „Nichtpolare Welt“ (Richard Haas), „Die postamerikanische Welt: Der Aufstieg des Restes“ (Fareed Zakaria), „Der Aufstieg der Zweiten Welt“ (Khanna). Die Vielfältigkeit der Ideen demonstriert nur die Unsicherheit über die Beschaffenheit der künftigen Welt. Es werden sich viele Kooperationsmöglichkeiten aber auch zahlreiche Verwundbarkeiten ergeben. Joseph Nye hat als Antwort eine flexible Strategie vorgeschlagen. Die Akteure sollen sowohl „hard power“ als auch „soft power“ in Form einer „smart power“ anwenden, die sich aber verändernden Kontexten anpassen muss. Übersetzt bedeutet das, dass sie politische, ökonomische und militärische Fähigkeiten mit Strategien der Bedrohungsverminderung (Diplomatie, Anreize zur Erbringung einer Vorbildwirkung) verbinden und flexibel gestalten.

Über Jahrhunderte bauten Staaten militärische Kapazitäten auf, um sich gegen andere Staaten zu verteidigen, sie anzugreifen oder sie gar zu vernichten. Die Welt erschien anarchisch, jeweils andere Staaten wurden als potentielle Feinde angesehen. Mit den Petersberg-Aufgaben der Europäischen Union hat ein Umdenken begonnen. Krisenmanagement, Abrüstung, Friedenserhaltung, Friedensschaffung und Wiederaufbau zerstörter Gesellschaften stehen im Vordergrund. Der Bericht der „International Commission on Intervention and State Sovereignty“ von 2001 über „The Responsibility to Protect“ geht noch einen Schritt weiter: Es sei Pflicht der Staaten die eigene Bevölkerung vor massiver Verletzung der Menschenrechte, Genozid und anderen verheerenden Ereignissen zu schützen. Wenn sie diese unterlassen oder dazu nicht in der Lage sind, sollen internationale Organisationen, allen voran der Sicherheitsrat der Vereinten Nationen, diese Rolle übernehmen. Nicht mehr die Zerstörung von Feinden und die Eroberung von Territorium stehen im Zentrum von Sicherheit, sondern der Schutz von Menschen und Individuen. Technische Fähigkeiten der Zukunft (wie Fernaufklärung) müssen sich künftig an diesen Erfordernissen menschlicher Sicherheit orientieren.

Professor Dr. phil. Heinz Gärtner
Österreichisches Institut für Internationale Politik (OIIP), Wien
a. o. Universitätsprofessor am OIIP und Lehrbeauftragter
an den Universitäten Wien, Innsbruck und Salzburg

Literaturverzeichnis

Haass RN, „The Age of Nonpolarity: What Will Follow U.S. Dominance“, in: Foreign Affairs, May/June 2008

International Commission on Intervention and State Sovereignty, Responsibility to Protect, Report, December 2001

Khanna P, The Second World: Empires and Influence in the New Global Order, New York 2008

Nye JS, The Powers to Lead, Oxford 2008

Zakaria F, The Post-American World, New York 2008

Rahmenbedigungen zur Realisierung des EU-Programms „Global Monitoring for Environment and Security GMES“

Peter Knopf

1 Die gemeinsame Entwicklung der europäischen Raumfahrtprogramme der ESA und der EU

1.1 Entstehungsgeschichte der Raumfahrtprogramme der EU und von GMES

Im Mai 1998 erging während des Zusammentreffens zur Gründung von GMES in Baveno am Lago Maggiore von den Teilnehmern der Aufruf an Europa, zusammen zu agieren, um die Erdbeobachtung vom Weltraum aus in einer gemeinsamen Strategie zu vereinen. Der Aufruf kam zustande, weil evident wurde, dass Europa ein globales satellitenbasiertes Erdbeobachtungssystem für die Beobachtung des Kontinents brauchte. Dieser Aufruf entwickelte schon ab 2000 ein politisches Momentum im Rahmen der EU, das von der Europäischen Kommission gemeinsam mit der ESA aufgegriffen wurde. In der Folge erschien auf der Agenda der verschiedenen EU-Präsidentschaften der Aufbau eines Programms „Global Monitoring for Environment and Security (GMES)“. Gleichzeitig entwickelte die Europäische Kommission zunehmend das Bewusstsein, dass Europa seine eigenen Raumfahrtprogramme entwickeln muss. Dazu war natürlich die Zusammenarbeit mit den bereits existierenden European Space Agency (ESA), EUMETSAT (Betreiberagentur der europäischen Wettersatelliten) und nationalen Raumfahrtagenturen der EU-Mitgliedsländer erforderlich. Zunächst wurde als erstes „Flagship programme“ Galileo angegangen, um im vor allem zivilen Navigations- bereich unabhängig vom GPS und GLONASS zu werden, den beiden militärischen Satelliten-Navigationssysteme der USA und Russlands, die jedoch die zivile Nutzung zuließen, aber im Falle militärischer Konflikte für zivile Nutzer auch jederzeit gesperrt werden könnten. Parallel zu Galileo wurde auch GMES durch verschiedene GMES-Foren als zweites „Flagship programme“ der EU entwickelt. Ebenfalls parallel zur Entwicklung dieser beiden Raumfahrtprogramme, wurde unter der Federführung der Europäischen Kommissi-

on auch eine eigentliche europäische Raumfahrtpolitik formuliert. Als Beteiligter und Beobachter in diesen Prozessen sind im folgenden einige evaluierende Anmerkungen zur Qualität der Umsetzung der genannten Vorhaben Galileo und GMES durch die Europäische Kommission angebracht. Gérard Brachet, vormaliger Chef des CNES (französisches Raumfahrtzentrum), fasst den Werdegang von GMES von der Baveno Deklaration bis zum eigentlichen europäischen Programm im Folgenden in konziser Sprache zusammen:

> **From initial ideas to a European plan:**
> **GMES as an exemplar of European space strategy**
>
> Gérard Brachet[1]
>
> Global Monitoring for Environment and Security (GMES) is an idea which originated during a meeting in Baveno, Italy, in May 1998, which generated a call for Europe to get its act together in the field of environmental monitoring from space, to define a well articulated strategy in this area and to build upon its excellent scientific research community, its proven technical prowess in Earth observation from space and its nascent political will to express its objectives in international fora related to climate change and other global environment topics. While Europe was already active in the most advanced areas of global monitoring, its rather uncoordinated efforts (even within the European Commission) lacked visibility and did not appear to fit into a clearly established strategy. The 'Baveno initiative' was an attempt to remedy this situation and find a place within a developing 'European Strategy for Space', which requires ESA and the European Union to work more closely together. GMES was extended to include the 'security' (in its wider sense) aspects of global monitoring, a move that produced a number of questions and misunderstandings, but which allowed many in Europe to realize that monitoring the activities of the Earth' land masses, oceans and atmosphere do include a security dimension. GMES will eventually incorporate an implementation plan which will call upon various monitoring techniques, ambitious modelling projects and connections with society's more urgent requirements with respect to environmental protection and prevention or reduction of risks related to natural hazards. This will entail significant efforts to inform the user communities and to convince them of the relevance and usefulness of this initiative. It will also provide a sound basis for the European contribution to the new initiative for improved coordination of strategies and systems for Earth observations called for by the July 2003 Earth Observation Summit.

---

[1] Gérard Brachet, 37 rue Tournefort, Paris 75005, France. http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V52-4BG3S26-1&_user=10&_coverDate=02%2F29%2F2004&_rdoc=1&_fmt=full&_orig=search&_cdi=5774&_sort=d&_docanchor=&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=6160453621ebd40e0c8395a27c34f100#fn1 (15. Januar 2004).

1.2 Einige evaluierende Bemerkungen zur Umsetzung von Galileo, GMES und dem europäischen Raumfahrtprogramm

Eine differenzierte Evaluation der Implementierung von Galileo und GMES wird hier nicht beansprucht, aber einige Beobachtungen über die Entwicklung und Implementierung der Programme sollen im Folgenden gleichwohl gemacht werden.

- Ein erster Verdienst der Europäischen Kommission ist zweifellos die Aufnahme von Galileo und GMES in die politische Agenda der EU und die so genannte „Federation of User Requirements", die eine pragmatische Implementierung von Programm- modulen erlaubte. Unterstützend wurden auch viele Entwicklungen von Diensten im Rahmen des Europäischen Rahmenprogramms Forschung und Technologie- entwicklung vorangetrieben, nebst den erheblichen Beiträgen der ESA und EUMETSAT.
- Es zeigte sich jedoch schnell, dass die Europäische Kommission, wie bereits bei Galileo, von der Implementierung komplexer technologischer Programme wie GMES überfordert war. Zweifellos überstieg der Machtwille der Europäischen Kommission ihre Sachkompetenz. Man überlässt ja die Konstruktion komplexer Autos auch nicht den Politikern. Diesen Mangel an Sachkompetenz machte die Europäische Kommission gegenüber den anderen involvierten Organisationen ESA und EUMETSAT durch teilweise unerträgliche Arroganz wett, was angesichts der Aufteilung der Kosten je hälftig auf ESA und EU keinesfalls gerechtfertigt war. Immerhin gelang es 2005 die Zuständigkeiten zu regeln, wobei die ESA die technische Entwicklung der Raumfahrtkomponenten und die Europäische Kommission die Verwaltung und Entwicklung der GMES-Dienste übernahm.
- Diese Arroganz der EU gipfelte auch im Versuch, die ESA und auch das CERN als gut verwaltete multilaterale Organisationen (wie die EU selbst) wohl aus Machtgier zu übernehmen. Glücklicherweise scheiterten diese Vorhaben an einer Mehrheit der Mitgliedsländer der beiden Organisationen, die das ablehnten. Es ist auch nicht einzusehen, weshalb die Basis gut verwalteter und funktionierender multilateraler Organisationen aus willkürlicher Machtgier in Frage gestellt werden soll.
- Der Implementierungsprozess von Galileo wie auch von GMES ging unter EU-Leitung sehr langsam und mit einigen Pannen vor sich. Auch hier zeigte sich die weitgehende Inkompetenz der Europäischen Kommission beim Aufbau komplexer technologischer/wissenschaftlicher Programme, was auch der Ver-

gleich mit der doch schnellen Implementierung des IGOS-P (Integrated Global Observing Strategy Partnership) nahe legt. Dieses Programm startete gleichzeitig mit GMES, wobei heute im Gegensatz zu GMES fünf Module operationell sind: Global Carbon Cycle, Geohazards, Ocean, Water Cycle, Athmospheric Chemistry. Dabei zeigt sich, dass diese Module doch eher grundlagenorientiert angelegt sind und deshalb auch für GMES Ergänzungen in Form von komplementärer Forschung erbracht hätten.

– In der internationalen Zusammenarbeit hat die Europäische Kommission gravierende Fehler gemacht: statt mit IGOS-P mit seinen öffentlichen Träger-Organisationen (ESA, UNCOPUOS, UNEP, NOAA etc.) zusammenzuarbeiten, hat sie die Kooperation mit GEOSS (eine amerikanische Initiative mit allerdings sehr vielen Mitgliedsländern) gesucht, die bis heute kein Geld für konkrete Projekte/Module hat, jedoch die globale Koordination im Erdbeobachtungsbereich beansprucht (um jene der UNCOPUOS zu torpedieren) und nach Gerüchten zufolge von den USA wohl auch zur Verhinderung, respektive Verlangsamung, von GMES gegründet wurde – wie wenn letzteres die Europäische Kommission nicht selbst gründlich getan hätte.
– Immerhin zeigt die 5th Space Council Resolution bedeutende Lernfortschritte in Bezug auf eine nachhaltige Raumfahrtpolitik der EU. Die Europäische Kommission erkannte letztlich aus Einsicht COPUOS offiziell als Partner in der Space Debris Mitigation an, ebenso die ESA selbst mit ihren Mitgliedsländern und deren nationalen Raumfahrt-Agenturen sowie EUMETSAT als Partner in der Europäischen Raumfahrtpolitik und will sich im Sinne einer Arbeitsteilung speziell auf die Belange der Raumfahrtapplikationen für ihre Politik konzentrieren – wohl nachdem der Übernahmeversuch der ESA durch die Europäische Kommission misslang.

1.3 Einige methodologische Schwächen von GMES

GMES ist zweifellos eines der umfangreichsten und teuersten Umweltprogramme, die je geplant wurden. GMES umfasst vier Hauptkomponenten: Dienste, Erdbeobachtung *in situ* und Space sowie umfangreiches Datenmanagement. In diesem Zusammenhang wurde auch frühzeitig gefordert, dass Ausbildung in der Handhabung der angebotenen Dienste ein wichtiges Element von GMES sein müsse. Ferner gingen mittlerweile auch einzelne noch aufgeführte Gebiete mit den gravie-

rendsten Umweltveränderungen – die Gebirgsregionen (Alpenraum) – mit der Entwicklung und Formulierung als Module wieder weitgehend verloren. Es scheint, als wäre für GMES die europäische Topologie total flach.

Eine weitere Schwäche betrifft die fast ausschließlich pragmatische Konstruktion von GMES, was in gewisser Weise auch eine Stärke sein mag, weil es weitgehend den über Jahre eruierten Bedürfnissen an Diensten der EU-Mitgliedsländer in GMES entspricht. Setzt man voraus, dass GMES der Führung einer nachhaltigen Politik in Europa dienen soll, so wären theoretische Konzepte dieser Nachhaltigkeit der zukünftigen EU-Politik und der Ableitung entsprechender Dienste als Ergänzung nützlich oder gar erforderlich. Ein solches Konzept, der sog. Ecological Footprint, scheint sich seit Kurzem durchzusetzen und wäre ein solches Nachhaltigkeitskonzept.

2 Ecological Footprint als Ansatz einer nachhaltigen Politik

Als Basis einer Nachhaltigkeitspolitik braucht es neue, verlässliche Ansätze, die messbare Kriterien für die Nachhaltigkeit auf einer wissenschaftlich anerkannten Basis liefern. Ein solches Konzept für erneuerbare Ressourcen scheint der „Ecological Footprint“ (EF) zu sein, der als „notwendige Land- und Wasserressourcen des Ökosystems zur Produktion erneuerbarer Ressourcen (Nahrung) für die Versorgung der Bevölkerung“ definiert ist. Im Grunde misst der EF den Durchsatz an erneuerbaren Ressourcen für verschiedene Produkte/Dienstleistungen und entsprechenden Landflächengebrauch. Das verheerende Resultat entsprechender Berechnungen des EF ist, dass die Menschheit schon im Jahr 2000 das 1.2-fache der Erde für ihren Bedarf verbraucht – mit stark steigender Tendenz. Entsprechende Berechnungen aus dem Jahr 2001 ergaben, dass der EF der USA doppelt so hoch wie der von Europa ist. Die USA sind die Verschwendernation par excellence und die Menschheit lebt seit 2003 mit dem 1.25-fachen der Erde bereits deutlich über ihrem Verhältnis, was unser Planet an erneuerbaren Ressourcen überhaupt hergibt. Die Regenerationsfähigkeit der Erde ist somit um 25% überschritten, was wahrscheinlich in nur zwei Jahrzehnten zum ökologischen Kollaps der Erde und unabsehbaren Folgen für die Menschheit führen wird. Zweifellos sind Hungersnöte und Ausrottung vieler Spezies in Fauna (inklusive Menschen) und Flora hoch wahrscheinlich und treten bereits vermehrt auf. Ein durchaus ähnli-

ches Bild gibt ein alltäglich gebrauchtes Instrument, das Auto, ab. Man wusste seit geraumer Zeit ziemlich genau, dass bereits in ca. zehn Jahren die leicht und günstig erschließbaren Erdölressourcen mit größtmöglicher Fördermenge (bekannt als „Oil peak") erreicht sein würden. Danach gehen die Fördermengen rasch zur Neige. Weder hat die Autoindustrie genügend verbrauchsarme Autos auf Benzinbasis (etwa Hybridautos) noch solche mit alternativen elektrischen Antrieben (Brennstoffzellen) rechtzeitig entwickelt. Dass dabei die entsprechenden Innovationsdefizite der Autobauer mit den sehr hohen Investitionskosten in die Fertigungsstraßen gerechtfertigt wird, lässt erwarten, dass die Verfügbarkeit elektrischer Antriebe etwa durch Brennstoffzellen noch Jahre (bis diese finanziell amortisiert sind!) beanspruchen wird, obwohl die Technologien bekannt sind und teilweise verfügbar wären. Die Unvernunft des Menschen hat also System, weshalb die Aussage, dass die Bevölkerungszahl der Menschheit für deren Rettung halbiert werden sollte, mehr als nur ein Scherz ist.

Viele dieser relativ neuen Erkenntnisse sind nicht zuletzt den vielen operationellen Erdbeobachtungs- und Meteosatelliten zu verdanken, die bereits operationell im Orbit sind und auch in GMES mit Sentinel 1 bis 5 in näherer Zukunft zusätzlich geplant sind. Es bleibt zu hoffen, dass ein Kollaps der Ökosysteme der Erde rechtzeitig erforscht und auch dokumentiert wird und so vielleicht doch noch verhindert werden kann. So gesehen ist GMES zweifellos ein extrem wichtiger Beitrag für die zivile Sicherheit Europas und darüber hinaus. Das Bild der Titanic, die ungebremst auf den Eisberg zufährt, drängt sich heute dennoch für die Situation der gesamten Menschheit auf. „Learning by disaster" ist wohl die einzige Lernart, welche die Menschheit „versteht", auch wenn eine steigende Anzahl Menschen, hoffentlich auch die Politiker, den Ernst der menschlichen Situation heute begriffen haben.

3 Weltraumsicherheit global betrachtet

Bisher haben die Kanadier die Problematik der „Space Security" am weitgehendsten analysiert und mit ihren jährlichen Berichten im Internet unter www.spacesecurity.org zugänglich gemacht. Auch haben kanadische Vertreter im Council und im International Relation Committee der ESA ihre Überlegungen über Inhalt und Governance der „Space Security" dargelegt und darüber berichtet. Mit einem

wissensbasierten Ansatz werden die verschiedenen Aspekte von „Space Security" dargestellt und jährlich analysiert, was für diesen sich rasch wandelnden Bereich wichtig ist.

Thematisch geschieht diese Analyse in den folgenden Bereichen:

- Space Environment
- Space laws, politics and doctrines
- Civil space programs and global utilities
- Commercial space
- Space support for terrestrial military operations
- Space system protection
- Space systems negation (Verhinderung)
- Space based strike systems

Es würde zu weit führen, hier eine vollständige Zusammenfassung dieser jeweils komplexen Bereiche der Space Security zu liefern. Adressaten dieser jährlichen Berichte sind Raumfahrt-Experten. Zunächst unterscheidet sich „Space environment" von der Umwelt auf der Erdoberfläche und ist wohl nicht weniger komplex als die Interaktionen der verschiedenen Ökosysteme der Erde untereinander: Land, Meer, Atmosphäre, wobei letztere mit dem erdnahen Weltraum ebenfalls in komplexer Wechselwirkung steht. Man denke etwa an den Zusammenhang zwischen Sonnenwind und der gesamten Raumfahrt, ob bemannt (etwa ISS) oder unbemannt bei üblichen Satelliten (Erdbeobachtung, Telekommunikation). Sonnenwind kann nicht nur die Astronauten, sondern auch die Elektronik von Satelliten schädigen bzw. zerstören. Deshalb ist die kontinuierliche Überwachung des so genannten „Space Weather" enorm wichtig für die „Space Security" im Orbit. Europa hinkt in diesem Bereich beträchtlich hinterher und hat nur ungenügende Kapazität mit einhergehender Abhängigkeit von USA und Russland. Dasselbe gilt auch für die „Space debris" (Weltraummüll aus Raketen-Endstufen und ausgedienten Satelliten). Das Entsetzen in UNCOPUOS über den unverantwortlichen Abschuss eines Satelliten durch das chinesische Militär im Frühjahr 2007 war unübersehbar. Dass die USA kurz darauf eine ebensolche Demonstration veranstalteten, zeigt die Unvernunft des Militärs in grundsätzlicher Weise auf. Die Anhäufung von Space debris im vor allem erdnahen Orbit macht die Sicherheit in der Raumfahrt auf absehbare Zeit unmöglich. Zwar werden Maßnahmen zur Verringerung des „Space debris" vorgeschlagen, ja sogar ratifiziert, aber dessen

Zunahme wird noch zu wenig begrenzt. Dass in den USA die Budgets der militärischen Raumfahrt jene der NASA weit übersteigen, zeigt auch hier die enorme Unvernunft auf, trotz der Konventionen von UNCOPUOS zu den „peaceful uses of outer space".

Zusammenfassend kann wohl gesagt werden, dass zivile Sicherheit der Menschheit ohne kontinuierliche Erdbeobachtung nicht mehr machbar ist. Nur mit den Mitteln der synoptischen Übersicht der Raumfahrt zum Zustand der Ökosysteme der Erde kann eine dauerhafte Nachhaltigkeit in der Entwicklung und Bewahrung der menschlichen Zivilisation gewährleisten.

Dipl.-Phys. Peter Knopf
ehem. Berater für Wissenschaft und Raumfahrt des Eidgenössischen Departements für auswärtige Angelegenheiten, Bern
Schweizer Delegierter im Rat der ESA und des CERN, Delegationsleiter in COPUOS UNO Wien sowie Mitglied verschiedener Programmausschüsse von ESA-EU-Programmen

Wirtschaftliche Hindernisse beim Einsatz satellitengestützter Sicherheitstechnologien

Jürgen K. von der Lippe

Hintergründe

Sicherheit ist eines der höchsten Güter für die Menschheit, für die es sich lohnt, die besten Mittel (Technologien) zum Erhalt einzusetzen. Die aktuelle politische Diskussion über die richtigen Anti-Terror-Maßnahmen wird vom Streben nach immer mehr Sicherheit dominiert, um den perfekten Schutz zu erreichen.

Sicherheitsmaßnahmen jedweder Art zur Abwehr terroristischer Anschläge sind mit hohen Kosten für Forschung und Entwicklung sowie Herstellung verbunden. Die Umsetzung dieser Maßnahmen senkt die Produktivität von Wirtschaft und Verwaltung. Ein erfolgreicher Transfer in operationelle Systeme erfordert daher eine begleitende Untersuchung der Wirtschaftlichkeit. Seit den Ereignissen des 11.9.2001 und mit den Erkenntnissen zur globalen Erwärmung ist die Nachfrage nach Sicherheitstechnologien stark gestiegen. Neue Forschungs- und Technologieentwicklungsprogramme sind mit umfangreichen Budgets entstanden: in den USA sind das die Programme des „Department of Homeland Security" (DHS), in Europa ist es das „European Security Research Programme" (ESRP) im 7. Rahmenforschungsprogramm (FP7), sowie verschiedene nationale Sicherheitsforschungsprogramme. Der Schwerpunkt liegt auf der Entwicklung neuer Sicherheitstechnologien, die wirtschaftlichen Aspekte werden dabei nur unwesentlich erforscht.

Besonders eindeutig wurde über die Folgen unsystematischen Handelns in der „New York Times" vom 5. Mai 2005 unter der Überschrift „U.S. to Spend Billions More To Alter Security Systems" berichtet:

> After spending more than $4.5 billion on screening devices to monitor the nation's ports, borders, airports, mail and air, the federal government is moving to replace or alter much of the antiterrorism equipment, concluding that it is ineffective, unreliable or too expensive to operate. Many of the monitoring tools – intended to detect guns, explosives, and nuclear and biological weapons – *were bought during the blitz in security spending after the attacks of Sept. 11, 2001.*

Investitionen und Risikoabschätzung

Die Investitionen für die Anschaffung eines Sicherheitssystems durchlaufen einen Genehmigungsprozess, deren wichtigste Kriterien für öffentliche Organisationen und private Unternehmen ähnlich sind. Nur gesetzlich vorgeschriebene Sicherheitsmaßnahmen bilden eine Ausnahme. Es gilt zunächst, den Nutzen zu bestimmen und damit besonders die Wirtschaftlichkeit. Ein Kernproblem für die Entscheidung, die zur Anschaffung eines Sicherheitssystems führt, ist die Bewertung des Risikos, das heißt der Bestimmung der Eintrittswahrscheinlichkeit der abzuwendenden Gefahr. Dabei ist zu berücksichtigen:

– Sicherheitstechnologien werden für einen zeitlich nicht bestimmbaren Einsatz konzipiert;
– Der Mitteleinsatz allein für den unbestimmten Katastrophenfall kann oft nicht begründet werden (nach der Maßgabe: Lieber ein neues Feuerwehrfahrzeug als aktuelle Satellitenbilder);
– Eine kontinuierliche Wertschöpfung ist erforderlich, d.h. die Verwendung für eine Mehrfachnutzung („dual use“) ist anzustreben.

Der Wertschöpfung stehen die Kosten für die Anschaffung, den Betrieb und die mögliche Senkung der Produktivität gegenüber. Für den Budget-Verantwortlichen ist daher eine kontinuierliche Wertschöpfung (multipler Einsatz) anzustreben.

Maßnahmen zum Abbau der Hindernisse – „Dual use“ Konzept

Nicht zu verwechseln, mit dem herkömmlichen Verständnis, welches eine Verwendbarkeit einer Technik sowohl zu zivilen als auch militärischen Zwecken definiert. Gemeint ist hier die Nutzung im zivilen Bereich für die Abwendung eines Schadensfalles bei gleichzeitigem Einsatz im kontinuierlichen Betrieb zur Erzielung einer Wertschöpfung. Ein Beispiel einer dualen Nutzung ist:

– Hochwasser- und Sturmflutvorhersagen durch Satellitenaufnahmen bei gleichzeitiger Verwendung für den Küsten- und Deichschutz (Zustand, Veränderungen, Planung, …);
– Waldbrandüberwachung durch Satellitenbeobachtung bei gleichzeitiger Nutzung für Waldmanagement.

Integrierte Produkte

Eine weitere Möglichkeit zur Förderung des Einsatzes von satellitengestützten Sicherheitssystemen ist das Angebot von integrierten Systemen wie die gleichzeitige Nutzung von Satellitenfernerkundung (SAR und optisch/thermal), -navigation, und -kommunikation sowie terrestrischen Systemen. Dieser Ansatz wurde von Staatsrat Heiner Heseler (Senatskanzlei Bremen) im Rahmen der Aktivitäten des CEON (Promotion Center for Communication, Earth Observation and Navigation satellite based Services") aufgezeigt:

> Durch satellitengestützte Dienstleistungen, insbesondere durch die Integration von Diensten aus der satellitengestützten Erdbobachtung (zukünftiges System KOPERNIKUS), Navigation (aktuell GPS, ab 2013 GALILEO) und Kommunikation werden erhebliche Verbesserungen, insbesondere bei der Identifikation und der Zustandüberwachung von Schiffen und der Routenplanung (Tracing and Tracking) erwartet.
> (Beitrag zur Podiumsdiskussion der Konferenz „Globale Fernerkundungssysteme und Sicherheit" vom 9.–10. Oktober 2008 in Wien).

Regionale Anwendungen

Für die Vermarktung von satellitengestützten Sicherheitssystemen ist zu berücksichtigen, dass neben den globalen Großschadenslagen auch viele regionale Katastrophenfälle den Einsatz von Fernerkundungsprodukten erfordern. Die mediale Aufmerksamkeit konzentriert sich jedoch im Wesentlichen auf die großen globalen Katastrophen. Zur Erhöhung der Akzeptanz im regionalen Bereich ist es daher notwendig, integrierte Produkte anzubieten, und dabei zu berücksichtigen, dass der potentielle Nutzer in einem konventionellen Umfeld lösungsorientierte Informationen benötigt.

Marktentwicklung

Das ESA Department für Earth Observation (EO) berichtet im EO Market Development (EOMD) Report: „There is a perceived difficulty in gaining widespread acceptance of EO products and services in the target markets." Und: „There is a history of overselling the capabilities of EO based services."

Ein wünschenswerter wachsender Einsatz von satellitengestützten Produkten erfordert daher eine nutzerfokussierte Entwicklung und Information, d.h. eine

gezielte Marktentwicklung ist erforderlich, da ein „Market Pull“ nicht besteht. Das gilt sowohl für die konventionelle EO-Nutzung wie auch besonders für EO als Sicherheitssystem.

Um dieses Ziel zu unterstützen, hat die ESA ein Marktentwicklungsprogramm eingeführt: „EOMD provides the first opportunity for specific programmatic support within ESA for activities related to the market development and business phase in the overall evolution of EO-based products and services.”

Eine Auswahl der „Market Development“-Projekte der ESA mit Sicherheitsrelevanz und damit Beispiele für die duale Nutzung sind:

- COASTCHART, Coastal mapping Service;
- FAME, Flood Risk and Damage Assessment (Modelling);
- TIDAL, Tidal information service;
- BALU, Burned Area Land use change detection;
- ITALSCAR, Burned Forest Mapping from Space;
- ALPSLOPE, Monitoring of unstable slopes;
- SLAM, Service for Landslide Monitoring;
- SEVESEO, Support industrial/technological risk management.

Schlussbetrachtung

Die satellitengestützten Sicherheitssysteme haben ein großes Potential in der Gefahrenabwehr von Naturkatastrophen, industriellen Großschadenslagen und terroristischen Anschlägen. Die besonders durch die Ereignisse des 11. September 2001 gestiegene Nachfrage nach Sicherheitssystemen setzt jedoch nicht die Marktgesetze außer Kraft. Die Investitionsentscheidung für ein Sicherheitssystem unterliegt immer der Frage nach dem zu schaffenden Mehrwert. Dieser ist oft nur schwer für eine potentielle Gefahrenabwehr zu bestimmen.

Eine intensivere Nutzung von satellitengestützten Satellitensystemen erfordert nutzerorientierte Lösungen und eine erweiterte Wertschöpfung für die Produkte. Die notwendigen Maßnahmen sind:

- Mehrzweckprodukte (dual use);
- Integrierte Produkte (Bündelung von Funktionen);
- Marktentwicklungsprogramme (Demonstrationsprojekte);
- Lösungsorientierte Informationen.

Die damit möglich werdende breitere Nutzung der satellitengestützten Sicherheitssysteme verbessert die allgemeine Sicherheitslage bei ausgewogenem Einfluss zwischen Sicherheit und Produktivität.

Dipl.-Ing. Jürgen K. von der Lippe
vdl consult, Hannover
Ingenieur und Manager in der Industrie mit dem Schwerpunkt
Raumfahrt und kommerzielle Geschäftsentwicklungen

Globale Fernerkundungssysteme und Sicherheit. Resümee und Ausblick

Stephan Lingner und Wolfgang Rathgeber

Für eine synoptische Beurteilung der Sicherheitsrelevanz globaler Fernerkundungssysteme sind sowohl ihre technischen Potentiale als auch Rechtfertigungsfragen hinsichtlich der Nutzung entsprechender Datenprodukte sowie deren praktische Bedeutung darzustellen. Die folgenden Abschnitte fassen die Ergebnisse der vorstehenden Beiträge zum Thema zusammen.

1 Potentiale und Limitierungen

Besonders ist hier das europäische System GMES (Global Monitoring for Environment and Security) hervorzuheben, das auf eine Konsolidierung und Integration von Erdbeobachtungsdiensten zur Verifikation ziviler Gefahrensituationen, humanitärer Notlagen und zum Schutz vor Umwelt- und Erdbebengefahren abzielt. Der Anlass von Frühwarnung und Krisenbewältigung erfordert dabei eine schnelle Prozessierung entlang der Datenkette unter Einbeziehung des Bodensegments und nutzerorientierter Einsatzstrategien, wie sie u.a. das deutsche Zentrum für satellitenbasierte Kriseninformation (ZKI) anbietet.

Von GMES-Seite wird grundsätzlich eine offene Datenpolitik verfolgt, die allen interessierten Stellen Zugang verspricht. Diese an sich wünschbare Politik und die Möglichkeit der militärischen Nutzung von GMES-Daten bergen allerdings auch Risiken des Missbrauchs (Geiger 2005). Über die internationalen Verabredungen der „Petersberger Beschlüsse“ hinaus wird daher noch eine geeignete Klassifizierung und Verschlüsselung sensibler Daten bzw. Datenflüsse unter den beteiligten Staaten abzustimmen sein.

2 Sicherheits- und Regulierungsfragen

Fernerkundungsdaten erscheinen aufgrund ihrer Aktualität grundsätzlich attraktiv für Sicherheitsanwendungen. Ihre problemspezifische Aufbereitung ist aber zumeist mit hohen Kosten verbunden, die in diesen Fällen nur bei hohen Schadensrisiken gerechtfertigt sind. Das gegenwärtig noch begrenzte Potential

sicherheitsrelevanter Fernerkundungsdienste erfährt durch Implementierung in geographische Informationssysteme (GIS) bereits einen Bedeutungsgewinn, der voraussichtlich durch konvergente Entwicklungen mit IKT-getragenen Sicherheitsinfrastrukturen weiter anhalten wird. Aus planerischer Sicht sind geeignete integrierte Sicherheitsregimes – statt kurzlebige *ad hoc*-Lösungen – anzustreben, um Orte nicht unnötig als unsicher erscheinen zu lassen und um etwaigen sozialen Polarisierungstendenzen entgegenzuwirken. Für die Konzeption angemessener Sicherheitsstrategien sollte neben der „objektiven" Risikolage auch auf subjektive Einschätzungen der Betroffenen insoweit eingegangen werden, dass Einbußen an Lebensqualität, z.B. durch die Furcht vor terroristischen Anschlägen (trotz geringer statistischer Fallzahlen), entgegengewirkt werden kann. Hierbei sind allerdings auch die geäußerten Sicherheitserwartungen selbst kritisch zu hinterfragen, um einen Rigorismus im Umgang mit entsprechenden Risiken zu vermeiden. Angesichts der o.g. Konvergenzthese gilt es für eine legitime Implementierung fernerkundlicher Verfahren vielmehr, die Robustheit und Flexibilität der Gesellschaft gegenüber den vielfältigen Sicherheitsrisiken wirksam zu erhöhen, ohne berechtigte individuelle Ansprüche an Privatheit in ihrem Kern zu gefährden, die z.B. durch unnötige Erhebung personenbeziehbarer Daten und ihre nachträgliche kommerzielle Nutzung verletzt werden könnten. Der Umgang mit Sicherheitsproblemen erfordert einerseits auch präventive, nicht-technische Maßnahmen sowie die Bereitschaft, mit „Rest-Risiken" der Moderne zu leben, andererseits das Vertrauen in sich entwickelnde sicherheitstechnische Infrastrukturen, soweit diese dezentral organisiert sind und unter legitimierbarer Kontrolle stehen.

Aus *rechtlicher Sicht* ist bei der Gewinnung und Nutzung von Fernerkundungsinformation ein Paradigmenwechsel hin zu einer Übertragung staatlicher Ziele und Aufgaben auf private bzw. kommerzielle Dienstleister zu konstatieren. Dies führt zwangsläufig zu einem „Hinterherlaufen" und Zeitverzug ausstehender Regulierungen auf den verschiedenen Ebenen des nationalen und internationalen Rechts. Die derzeitige Regelung der Interessen staatlicher und nicht-staatlicher Rechtssubjekte stellt sich dabei folgendermaßen dar: Primär gilt international ein diskriminierungsfreier Zugang zu Fernerkundungsdaten. Die „UN Remote Sensing Principles" sehen in der Fassung von 1986 eine Erkundungsfreiheit auch über Drittstaaten vor, was allerdings hinsichtlich ihrer Rechte an den Daten umstritten ist.

Auf nationaler Ebene erlauben z.B. entsprechende Regelungen der USA seit einigen Jahrzehnten die kommerzielle Verbreitung von Fernerkundungsinformation – allerdings ohne einklagbare Rechte der Vertreiber. Das deutsche Satellitendaten-Sicherheitsgesetz (SatDSiG) regelt seit 2007 den Schutz des Landes vor Gefährdung der Sicherheit durch Verbreitung von „hochwertigen Fernerkundungsdaten". Hier gilt ein Genehmigungsvorbehalt für Betrieb und Nutzung entsprechender Systeme durch Dritte, der bei Gefährdung der nationalen Sicherheit (sowie bei völkerrechtlichen Bedenken) in ein Verbot münden kann. Dagegen birgt die explizit freizügige europäische Datenpolitik der GMES-Mitgliedsländer die oben erwähnten Proliferationsrisiken. Hier wären Friktionen zwischen den Rechtsebenen beispielsweise durch Klassifizierung von Fernerkundungsdaten zu mindern. Zu klären bleiben derzeit insbesondere Fragen zur Dienstleistungs-, Produkt- und Systemhaftung (z.B. bei Galileo) sowie zur Kommunikationshaftung bei Verletzung von Persönlichkeitsrechten.

3 Perspektiven für satellitengestützte Sicherheitsdienstleistungen

Trotz vielfältiger Potentiale wird die satellitengestützte Erdbeobachtung nur einige – wenn auch wichtige – Teile des sicherheitsrelevanten Erkundungsbedarfs abdecken können. Ohne komplementäre Maßnahmen am Boden wird der konkrete Erkenntnisgewinn ausbleiben oder unzureichend sein. Im Rahmen langfristig wirksamer Sicherheitskonzepte werden in dem Zusammenhang auch nicht-technische, konfliktvermeidende Strategien sowie das kontinuierliche Monitoring globaler Umweltveränderungen, die sich auch auf die zivile Sicherheit auswirken können, vorzusehen sein. Kurzfristig erfolgversprechende und teilweise bereits genutzte Einsatzgebiete der Fernerkundung liegen in der Überwachung des Schiffsverkehrs, der Hafensicherheit und des Küstenschutzes sowie in der Kontrolle murengefährdeter Gebirgsregionen.

Die dem Erkundungsbedarf entsprechende Planung, Errichtung und Nutzung von Erdbeobachtungssystemen erfordert konkrete Anpassungen in technischer und ökonomischer Hinsicht. So ist einerseits das Problem der Frequenzinterferenzen zu lösen, die den ungestörten Datentransfer zunehmend gefährden. Andererseits sind aufgrund der hohen Investitions- und Betriebskosten wirtschaftlich effiziente Nutzungen zu ermöglichen. „Dual-use-Fähigkeit" und Bündelung der Funktio-

nen entsprechender Systeme sowie ihre nachgewiesene Nutzerorientierung und die Standardisierung ihrer Datenprodukte würden ihre breite Anwendung zum Vorteil der zivilen Sicherheit erleichtern.

Literaturverzeichnis

Geiger G, Europas weltraumgestützte Sicherheit. Aufgaben und Probleme der Satellitensysteme Galileo und GMES, SWP-Studie, Stiftung Wissenschaft und Politik, Berlin 2005

Bisher erschienene Bände der Grauen Reihe:

1 Carl Friedrich Gethmann, Armin Grunwald, *Technikfolgenabschätzung: Konzeptionen im Überblick,* 9/96, 2. Aufl. 7/98

2 Carl Friedrich Gethmann, *Umweltprobleme und globaler Wandel als Thema der Ethik in Deutschland,* 9/96, 2. Aufl. 10/98

3 Armin Grunwald, *Sozialverträgliche Technikgestaltung: Kritik des deskriptivistischen Verständnisses,* 10/96

4 Arbeitsgruppe Neue Materialien, *Technikfolgenbeurteilung der Erforschung und Entwicklung neuer Materialien. Perspektiven in der Verkehrstechnik.* Endbericht zum Vorprojekt, 1/97

5 Mathias Gutmann, Peter Janich, *Zur Wissenschaftstheorie der Genetik. Materialien zum Genbegriff,* 4/97

6 Stephan Lingner, Carl Friedrich Gethmann, *Klimavorhersage und -vorsorge,* 7/97

7 Jan P. Beckmann, *Xenotransplantation. Ethische Fragen und Probleme,* 7/97

8 Michael Decker, *Perspektiven der Robotik. Überlegungen zur Ersetzbarkeit des Menschen,* 11/97

9 Carl Friedrich Gethmann, Nikolaj Plotnikov, *Philosophie in Rußland. Tendenzen und Perspektiven,* 5/98

10 Gerhard Banse (Hrsg.), *Technikfolgenbeurteilung in Ländern Mittel- und Osteuropas,* 6/98

11 Mathias Gutmann, Wilhelm Barthlott (Hrsg.), *Biodiversitätsforschung in Deutschland. Potentiale und Perspektiven,* 11/98, 2. Aufl. 4/00

12 Thorsten Galert, *Biodiversität als Problem der Naturethik. Literaturreview und Bibliographie,* 12/98

13 Gerhard Banse, Christian J. Langenbach (Hrsg.), *Geistiges Eigentum und Copyright im multimedialen Zeitalter.* Positionen, Probleme, Perspektiven, 2/99

14 Karl-Michael Nigge, *Materials Science in Europe,* 3/99

15 Meinhard Schröder, Stephan Lingner (eds.), *Modelling Climate Change and its Economic Consequences. A review,* 6/99

16 Michael Decker (Hrsg.), Robotik. *Einführung in eine interdisziplinäre Diskussion,* 9/99

17 Otto Ulrich, *„Protection Profile" – Ein industriepolitischer Ansatz zur Förderung des „neuen Datenschutzes",* 11/99

18 Ulrich Müller-Herold, Martin Scheringer, *Zur Umweltgefährdungsbewertung von Schadstoffen und Schadstoffkombinationen durch Reichweiten- und Persistenzanalyse,* 12/99

19 Christian Streffer et al., Environmental Standards. *Combined Exposures and their Effects on Human Beings and their Environment (Summary),* 1/00

20 Felix Thiele (Hrsg.), *Genetische Diagnostik und Versicherungsschutz. Die Situation in Deutschland,* 1/00, 2. Aufl. 2/01

21 Michael Weingarten, *Entwicklung und Innovation,* 4/00

22 Ramon Rosselló-Mora, Rudolf Amann, *The Species Concepts in Prokaryotic Taxonomy,* 8/00

23 Stephan Lingner, Erik Borg, *Präventiver Bodenschutz. Problemdimensionen und normative Grundlagen,* 9/00

24 Minou Bernadette Friele (Hrsg.), *Embryo Experimentation in Europe,* 2/01

25 Felix Thiele (Hrsg.), *Tierschutz als Staatsziel? Naturwissenschaftliche, rechtliche und ethische Aspekte,* 2/01

26 Vitaly G. Gorokhov, *Technikphilosophie und Technikfolgenforschung in Russland,* 2/01

27 Chris W. Backes, *Klimaschutz in den Niederlanden,* 3/01

28 G. Hanekamp, U. Steger (Hrsg.), *Nachhaltige Entwicklung und Innovation im Energiebereich,* 7/01

29 Thomas Christaller, Michael Decker (Hrsg.), *Robotik. Perspektiven für menschliches Handeln in der zukünftigen Gesellschaft. Materialienband,* 11/01

30 Michael J. Selgelid, *Societal Decision Making and the New Eugenics,* 4/02

31 Bernhard Irrgang, *Humangenetik auf dem Weg in eine neue Eugenik von unten?,* 2/02

32 Meinhard Schröder et al., *Climate Prediction and Climate Precautions,* 6/02

33 Ulrich Steger et al., *Sustainable Development and Innovation in the Energy Sector. Executive Summary,* 2/03

34 Carl Friedrich Gethmann, Stephan Lingner, *Zukünftige Klimaänderungen als Herausforderung für die deutsche Wirtschaft,* 7/03

35 Günter Schmid et al., *Small Dimensions and Material Properties. A Definition of Nanotechnology,* 11/03

36 Jorge Guerra González (ed.), *Environmental Noise. Main Focus: Aircraft Noise,* 3/04

37 Konrad Ott, Gernot Klepper, Stephan Lingner, Achim Schäfer, Jürgen Scheffran, Detlef Sprinz (mit einem Beitrag von Meinhard Schröder), *Konkretisierungsstrategien für Art. 2 der UN-Klimarahmenkonvention,* 7/04

38 Annemarie Gethmann-Siefert, Stefan Huster (Hrsg.), *Recht und Ethik in der Präimplantationsdiagnostik,* 7/05

39 Friedrich Breyer, Margret Engelhard (Hrsg.), *Anreize zur Organspende,* 11/06

40 Carl Friedrich Gethmann, Nicola Rohner, Kai-Uwe Schrogl (Hrsg.), *Die Zukunft der Raumfahrt. Ihr Nutzen und ihr Wert,* 1/07

41 Michael Decker, *Angewandte interdisziplinäre Forschung in der Technikfolgenabschätzung,* 1/07

42 Stephan Lingner, Simone Allin, Gerhard Steinebach (Hrsg.), *Gesellschaftliche Randbedingungen der Virtualisierung urbaner Lebenswelten,* 5/07

43 Margret Engelhard, Kristin Hagen, Felix Thiele (eds), *Pharming – A New Branch of Biotechnology,* 11/07

44 Ulrich Steger, Ulrich Büdenbender, Eberhard Feess, Dieter Nelles, *The Regulation of Electricity Networks. Open Questions and Methods of Solution. Executive Summary,* 7/08

45 Jan A. Bollinger, *Profilierung und Qualitätsentwicklung von Schulen durch Bildung für eine nachhaltige und gerechte Entwicklung,* 9/08

46 Felix Thiele, Jörg Fegert, Günter Stock (eds), *Clinical research in minors and the mentally ill,* 11/08

47 Bert Droste-Franke, Holger Berg, Annette Kötter, Jörg Krüger, Karsten Mause, Johann-Christian Pielow, Ingo Romey, Thomas Ziesemer, *Fuel Cells and Virtual Power Plants. Energy, Environmental, and Technology Policy Aspects of an Efficient Domestic Energy Supply. Executive Summary,* 11/08

48 Laura Martignon, Winfried Sander, *Der Weg zu einer Nachhaltigkeitskultur in der Schule. Zwei empirische Studien,* 3/09

49 Stephan Lingner, Wolfgang Rathgeber (Hrsg.), *Globale Fernerkundungssysteme und Sicherheit. Beiträge durch neue Sicherheitsdienstleistungen?* 6/09

GRAUE REIHE · NR. 49 · JUNI 2009