ITA manu:script

INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG

Sicherheitstechnologien und neue urbane Sicherheitsregimes

Holger Floeting

ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

Wien, Nov./2006
ITA-06-05
ISSN 1681-9187

http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_05.pdf

November/2006
(ITA-06-05)

Sicherheitstechnologien und neue urbane Sicherheitsregimes

Holger Floeting

Keywords

Sicherheit, Stadtpolitik, Videoüberwachung, Biometrie, RFID
Public safety, urban policy, video surveillance, biometrics, RFID

Abstract

Nach den Terroranschlägen in New York, Madrid und London haben Öffentlichkeit ebenso wie Regierungsstellen und öffentliche Verwaltungen erkannt, dass städtische Verdichtungsräume mit ihren Bürohochhäusern, verdichteten Misch- und Wohngebieten und technischen Großinfrastrukturen besonders verwundbar für derartige Bedrohungen sind. Selbst wenn Terroranschläge für Städte keine völlig neue Bedrohung sind, so hat ihre Zahl seit den 1990er Jahren doch deutlich zugenommen. Tatsächliche und vermeintliche Bedrohungen gehen aber nicht nur von einzelnen Großschadensereignissen, die Weltstädte und Megametropolen betreffen, aus, sondern auch von alltäglicher Kriminalität. IuK-Technik gestützte Sicherheitstechnik (z. B. Videoüberwachung, Biometrie, RFID) soll derartige Gefahren abwenden, deren Auswirkungen abschwächen oder wenigsten die Verbrechensbekämpfung unterstützen. Demgegenüber stehen Befürchtungen von allgegenwärtiger Überwachung oder sozialer Ausgrenzung durch den Einsatz dieser Techniken. Obwohl es immer noch an einheitlicher städtischer Sicherheitspolitik mangelt, die die Anwendungsmöglichkeiten von Sicherheitstechnik gezielt einbezieht, entwickeln sich doch aus dem pragmatischen Handeln neue urbane Sicherheitsregimes. Stadtpolitik und Stadtverwaltung müssen vorurteilsfrei und gestützt auf Fakten zwischen den Potenzialen und Risiken der IuK-gestützten Sicherheitstechnik abwägen. Der Artikel möchte zu diesem Thema einen Beitrag leisten, indem er städtische Sicherheit als öffentliche Aufgabe beschreibt, beispielhaft IuK-gestützte Sicherheitstechniken sowie die technologischen und organisatorischen Konvergenzprozesse im urbanen Anwendungskontext darlegt und mögliche städtische Zukünfte unter veränderten städtischen Sicherheitsregimes skizziert.

After the terrorists' attacks in New York, Madrid and London the public as well as governmental agencies and public administrations recognized that urban agglomerations accommodating high-rise office buildings, high-density mixed-use and residential areas and large-scale technical infrastructures are particularly vulnerable for these threats. Even if terrorists' attacks are no new threats for urban areas their number has increased significantly since the 1990s. But actual or pretended threats for urban safety are not only caused by singular damaging events concerning global cities and mega metropolises but also by everyday crime. ICT based safety features and equipment (e.g. video surveillance, biometrics, RFID) should avert such dangers, mitigate their impact or at least help to fight against crime. On the other hand these technologies raise the fear of omnipresent control and social marginalisation. Despite a lack of consistent urban safety policies that aim at the integration of the specific potentials of ICT based safety features and equipment, new urban safety regimes are developing from pragmatic actions. Urban politics and municipal administration have to deliberate open-minded and based on factual knowledge about the potentials and risks of ICT based safety features and equipment. This article will contribute to this topic by describing the public tasks regarding urban safety. It exemplifies ICT based safety features and equipment as well as the technological and organisational convergence processes in their urban application and outlines possible urban futures under the terms of changed urban safety regimes.

IMPRESSUM

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

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

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

ITA-manuscript Nr.: ITA-06-05 (November/2006)
ISSN-online: 1818-6556
http://epub.oeaw.ac.at/ita/ita-manuscript/ita_06_05.pdf

Inhalt

Glossar

ASB ..... Arbeiter-Samariter-Bund
BITE ..... Biometric Information Technology Ethics
BPB..... Bundeszentrale für politische Bildung
BSI..... Bundesamt für Sicherheit in der Informationstechnik
CCTV..... Closed Circuit Television
DB AG..... Deutsche Bahn AG
BGS ..... Bundesgrenzschutz, Bundespolizei
DLRG ..... Deutsche Lebens-Rettungs-Gesellschaft e.V.
DNA..... Deoxyribonucleic acid, Desoxyribonukleinsäure
DRK..... Deutsches Rotes Kreuz
DST..... Deutscher Städtetag
DStGB ..... Deutscher Städte- und Gemeindebund
ETA ..... Euskadi Ta Askatasuna
IRA ..... Irish Republican Army
IKT-Ausstattung ..... Informations- und Kommunikationstechnikausstattung
IuK-Technik..... Informations- und Kommunikationstechnik
ÖPNV ..... Öffentlicher Personennahverkehr
PDA ..... Personal Digital Assistant
RFID ..... Radio Frequency Identification
TA..... Technikfolgenabschätzung
TÜV..... Technischer Überwachungs-Verein

1 Veränderte Rahmenbedingungen – neue Handlungserfordernisse?

1.1 Neue Bedrohungssituationen?

Nach dem Terroranschlag vom 11. September 2001 in den USA und den späteren Anschlägen in Madrid und London ist die Verwundbarkeit von Städten mit ihren konzentrierten Baumassen und Großinfrastrukturen stärker in das Bewusstsein der Öffentlichkeit gerückt.

Die Bedrohung von Städten durch terroristische Anschläge ist allerdings keine neue Entwicklung, wie ein Blick nach Lateinamerika, Asien oder in den Nahen Osten zeigt, und auch in Europa gibt es schon lange terroristische Bedrohungen von Städten wie etwa die Beispiele der ETA oder der IRA zeigen. Seit den 1990er Jahren gab es allerdings eine Zunahme von Terroranschlägen in Städten (Savitch 2005) und auch zukünftig werden Städte mit dieser Bedrohung umgehen müssen. Tatsächliche oder vermeintliche Bedrohungen gehen aber nicht nur von singulären Schadensereignissen aus, die „global cities" und Megametropolen betreffen, sondern auch von alltäglicher Kriminalität.

Dass Sicherheitsfragen von Städten in der Öffentlichkeit stärker diskutiert werden, führt manchmal zu dem Kurzschluss, dass die Städte selbst unsicher seien. Dabei gibt es einige Mythen zu dekonstruieren. So ist beispielsweise „die Kriminalitätsfurcht weniger durch die ‚objektive' Kriminalitätslage als vielmehr durch soziale Problemlagen im Wohnquartier beeinflusst" (Oberwittler 2003, 31). Dennoch befürchten mittlerweile rund 40 % der Deutschen einen deutlichen Anstieg der Kriminalitätsrate und fühlen sich unbehaglich angesichts von wachsendem Vandalismus (rund 30 %), Graffitis (20 % der Westdeutschen und 29 % der Ostdeutschen) oder Bettlern (18 % der Westdeutschen und 21 % der Ostdeutschen) (Opaschowski 2005, zit. n. Stegemann 2005). Es ist allerdings unbestreitbar, dass an vielen Orten in den Städten Sicherheit, die quasi „nebenbei" produziert wurde (z. B. durch Abfertigungspersonal auf Bahnhöfen, Schaffner in Bussen und Bahnen usw.), Personaleinsparungen zum Opfer gefallen ist und nun mühsam „erkauft" werden muss. So lässt sich die Zunahme privater Sicherheitsdienste[1] nicht zwangsläufig als ein Ausdruck für eine höhere Unsicherheit in den Städten erklären, sondern „verdankt sich zumindest teilweise einem statistischen Artefakt, das sich durch den wachsenden Umfang von Outsourcing-Prozessen erklären lässt" (Siebel/ Wehrheim 2003, 24) und die Wegrationalisierung von „Nebenbei-Sicherheit". Auch im Bezug auf den Einsatz von Sicherheitstechnik kann man nicht zwangsläufig auf eine Zunahme von Unsicherheit in Städten schließen. Aus der Zunahme der „Verkaufszahlen von CCTV-Anlagen [kann nicht] automatisch auf die Überwachung in den Städten geschlossen werden …. Oft werden Kameras tatsächlich nur für die Regulierung des Verkehrsflusses … eingesetzt" (ebd.).

In einer fiktiven Rede zum zehnten Jahrestag des 11. September zeichnet Richard A. Clarke – bis 2003 nationaler Koordinator für Sicherheit, Infrastrukturschutz und Antiterrorpolitik beim US-amerikanischen Präsidenten – ein Bild der Bedrohung gerade von Städten durch Terrorismus, das Sicherheitskonzepte erfordern würde, die noch weit über das bisherige Maß hinausgingen. Seien doch nicht nur die kritischen Infrastrukturen bedroht, sondern auch Casinos und Themenparks, Hotels, Einkaufszentren usw. (Clarke 2005). Wenn es keine absolute Sicherheit gibt, stellt sich grundsätzlich die Frage, wie viel Schutz gewährleistet werden kann, wie viel wir uns leisten müssen und können und wie viel Risiko wir bereit sind zu tragen.

[1] In Deutschland arbeiten mittlerweile rund 145.000 Menschen bei privaten Sicherheitsdienstleistern, allein seit Anfang der 1990er Jahren ist deren Zahl um etwa 50 Prozent gestiegen (v. Landenberg 2004) .

1.2 Neue Wege zu mehr Sicherheit?

Die wissenschaftliche Auseinandersetzung mit Fragen des Zusammenspiels von Innerer Sicherheit und der Entwicklung von Städten wurde bisher kaum und wenn, dann meist unter historischer Perspektive geführt[2]. Risiken werden nicht nur unter Experten, Laien und Medien sehr unterschiedlich eingeschätzt, auch die Experteneinschätzungen gehen häufig auseinander.[3] Dennoch bedarf es einer möglichst objektivierten Risikoeinschätzung, will man Schutzmaßnahmen gezielt entwickeln.

Schutzkonzepte – nicht nur vor terroristischen Bedrohungen – konzentrieren sich vor allem auf die sogenannten kritischen Infrastrukturen. Dazu zählen „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (DStGB 2006, 6). Sie werden in Deutschland nach folgenden Bereichen gegliedert: Energieversorgung, Versorgung mit Trinkwasser, Ernährung, Gesundheitsleistungen, Telekommunikation und Informationstechnik, Transport- und Verkehrswesen, Umgang mit Gefahrenstoffen, Finanz-, Geld- und Versicherungswesen, Behörden und öffentliche Verwaltung und sonstige Bereiche wie der Schutz von Kulturgut, symbolträchtigen Bauwerken, Großforschungseinrichtungen, Medien usw. Vor allem die wechselseitige Abhängigkeit dieser Infrastrukturen untereinander kann im Schadensfall mit erheblichen Folgewirkungen für alle Bereiche des Lebens verbunden sein – das Beispiel einer Störung der Stromversorgung macht dies besonders deutlich. Strukturelle Veränderungen der letzten Jahre wie die fortschreitende internationale Vernetzung (z. B. im Energie- und Telekommunikationsbereich), die Privatisierung und Aufteilung ehemals staatlicher Infrastrukturen (z. B. im Transport- und Verkehrswesen) und die zunehmende Abhängigkeit von Informationstechnik machen die Einbeziehung neuer Akteure und insgesamt eine Neuformulierung von Schutzkonzepten nötig.

Auf kommunaler Seite wird „Sicherheitspolitik als Angelegenheit von übergeordneten staatlichen Instanzen und von internationalen Verteidigungsbündnissen“ (Lenk 2006, 1) angesehen. Obwohl Risiken und Bedrohungen sich natürlich lokal auswirken und Unsicherheitsgefühle vor allem lokal wahrgenommen werden („Kriminalitätsschwerpunkte“, „kritische Infrastrukturen“, „No-Go-Areas“ sind nur drei Begriffe, die die örtliche Verankerung von Sicherheitsfragen deutlich machen), gibt es bisher keine umfassende kommunale Sicherheitspolitik. Die lokale Risikovorsorge wird „in ihrer Gesamtheit nicht politisch verantwortet“ und „geschieht spartenweise aus der Sicht der Professionen: Notfallmedizin, Feuerwehr, Polizei“ (ebd.). Insgesamt erscheint die lokale Risikovorsorge angesichts der lokalen Auswirkungen globaler Risiken und Bedrohungen vorsichtig formuliert „noch nicht sehr beeindruckt“ (ebd.).

Zum Umgang mit Bedrohungen bedarf es jedoch der realistischen Einschätzung, der Prävention – soweit dies möglich ist – und des sicheren Handelns, sobald Schadensfälle eintreten. Dies kann in zunehmendem Maß nur im Zusammenwirken der Professionen geschehen. Mit der Größe des Schadenser-

[2] Bisher wurde die „auf den Raum, auf die Bevölkerung und auf die Versorgungssysteme von Städten gerichtete … organisierte politische Gewalt in den kritischen sozialwissenschaftlichen Debatten über Städte und Urbanisierung beharrlich vernachlässigt“ (Graham 2004, 58). Die moderne Stadtforschung tendiere „seit dem Zweiten Weltkrieg dazu, der Behandlung … auszuweichen, weil die vollständige Zerstörung von Städten in Konflikt zur aufklärerischen Vorstellung von Fortschritt, Ordnung und Modernisierung steht“ (Graham 2004, 59).

[3] „Die Risiken, die Menschen ängstigen und empören, sind nicht unbedingt die Risiken, an denen sie (statistisch gesehen) am häufigsten sterben. … Die öffentliche Aufregung über Risiken entspricht in vielen Fällen nicht der wissenschaftlichen Risikoeinschätzung. … Häufig lässt sich gar keine einheitliche wissenschaftliche Bewertung eines Risikos mehr finden“ (Schütz/Peters 2002, 40).

eignisses wird dies um so deutlicher, auch wenn bereits kleine Schadensereignisse ein erhebliches Maß an Koordination benötigen und integriertes Handeln bereits im Rahmen der Prävention sinnvoll ist.

Sicherheitstechnik soll den Umgang mit Gefahrensituationen und Schadensereignissen in allen Phasen in zunehmendem Maß unterstützen. Obwohl viel Vertrauen in die Unterstützungspotenziale von Sicherheitstechnik besteht, erfolgt ihr Einsatz „weithin ungeplant, auf Grund vager Vermutungen über die Nützlichkeit einer bestimmten Technik“ (ebd.).

Über die Zusammenhänge des Einsatzes von Sicherheitstechnik, der Entwicklung der Inneren Sicherheit und der Stadtentwicklung wird dabei bisher wenig diskutiert. Dabei scheint die Bereitschaft, auf technische Problemlösungen zu setzen, in dem Maß zu wachsen, wie die Bedrohungen diffuser werden: „Intelligente“ Überwachungskameras sollen in Clarke’s eingangs zitiertem Szenario „an allen öffentlichen Plätzen“ installiert, die Videoüberwachung „mit einem zentralen Notfallmanagement“ vernetzt werden, „mit Hilfe elaborierter Softwareprogramme sollten Polizeibeamte verdächtige Aktivitäten entlang der Hauptverkehrsadern aufspüren“ und für die Benutzung des öffentlichen Personennahverkehrs würden „Security Identity Cards“ notwendig (Clarke 2005).

2 Sicherheit als öffentliche Aufgabe

2.1 Aufgaben und Zuständigkeiten

Zu den öffentlichen Aufgaben von herausragender Bedeutung gehört „der Schutz der Bevölkerung vor besonderen Gefahren, die nicht aus eigener Kraft abzuwehren sind“ (Weber 2004, 1) und „die Gewährleistung der Sicherheit und Ordnung“ (DST 2004, 1). Schutz und Sicherheit der Bürger werden in Deutschland in erster Linie durch die Polizei gewährleistet. Daneben bestehen Einrichtungen der nicht-polizeilichen Gefahrenabwehr. Der zivile Bevölkerungsschutz ist in Deutschland vertikal gegliedert; Bund und Länder arbeiten zusammen. Aufgaben des Zivilschutzes werden auf nationaler Ebene wahrgenommen, auf die Länder entfällt die Verantwortung für den Katastrophenschutz. Der zivile Bevölkerungsschutz in Deutschland stützt sich in hohem Maß auf ein Sicherheits- und Hilfeleistungssystem, das auf ehrenamtlichen und Freiwilligenorganisationen beruht (freiwillige Feuerwehren, DLRG, DRK, ASB usw.). Die kommunale Ebene nimmt in Deutschland vor allem Aufgaben zur Gewährleistung der Sicherheit und Ordnung war. „Seit die Stadtmauern ihre Funktion verloren haben, ist die äußere Sicherheit … keine kommunale Angelegenheit mehr, und seit 1975 die Münchner Polizei als letzte der nach 1945 wieder eingerichteten Großstadtpolizeien verstaatlicht worden ist (Lange 1998, 83), ist auch die innere Sicherheit endgültig zur staatlichen Aufgabe geworden“ (v. Kodolitsch 2003, 5). Die kommunalen Aufgaben in Bezug auf die Sicherheit in der Stadt konzentrieren sich im Wesentlichen auf

- die 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),
- 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.).

Sicherheits- und Präventionsmaßnahmen als eigenständige Aufgaben werden in diesen Kontexten erst langsam thematisiert.[4]

Erst seit Beginn der 1990er Jahre haben die Kommunen Sicherheit als Querschnittsaufgabe entdeckt und integrierte Ansätze zum Umgang mit dem Thema Sicherheit entwickelt, die meist unter dem Leitbegriff „kommunale Kriminalprävention" zusammengefasst werden (vgl. DST 2004, 2 ff.). Zu den neueren Instrumenten kommunaler Sicherheitspolitik (ebd.) zählen z. B.

- *Ordnungs- und Sicherheitspartnerschaften zwischen Polizei und Stadt:* Sie sollen der Tendenz entgegenwirken „die alleinige Verantwortung für die Sicherheit bei der Polizei, für die öffentliche Ordnung aber bei den Städten anzusiedeln" (DST 2004, 2).
- *Kriminalpräventive Räte:* Sie sollen bürgerschaftliches Engagement einbinden und zur Entwicklung kleinteiliger Lösungen beitragen.
- *Kommunale Ordnungsdienste:* Sie übernehmen Ordnungsaufgaben, die von der Polizei aufgrund von Sparzwängen in den Landeshaushalten nicht mehr wahrgenommen werden bzw. von den Städten nicht mehr anderweitig erledigt werden (z. B. Kontrollaufgaben, die früher durch Parkwächter, Schaffner usw. erledigt wurden).

Städte werden immer wieder als Brennpunkte der Kriminalität dargestellt. Zunehmende Kriminalitätsfurcht bestimmt die Argumentation oft in stärkerem Maß als die tatsächliche Kriminalitätsentwicklung. Die Sicherheitslage in den deutschen Verdichtungsräumen ist aber „weit weniger kritisch als in den meisten Städten Europas und der Welt" (DST 2004, 1). Gerade im Bereich der Metropolregionen gibt es „klare Signale dafür, dass unser Sicherheitssystem weiterentwickelt und ausgebaut werden muss" (ebd.), um neuen Sicherheitsanforderungen gerecht zu werden. Zu den neuen Problemlagen werden beispielsweise gezählt:

- organisierte Kriminalität und Korruption,
- neue Sicherheitsprobleme in Gebieten mit negativer demographischer Entwicklung,
- eine gewachsene Erwartungshaltung der Bürgerinnen und Bürger im Bereich der öffentlichen Ordnung und der allgemeinen Gefahrenabwehr (ebd.).

In zunehmendem Maß wird aber auch die Bedrohung durch terroristische Aktionen im Rahmen der Sicherheitsüberlegungen von Städten thematisiert. Gerade in den Metropolregionen, im Zusammenhang mit der Durchführung von Großveranstaltungen und im Kontext des Infrastrukturausbaus spielt dies eine wichtige Rolle.

[4] „Was dabei an sicherheitsspezifischen und kriminalpräventiven Wirkungen entsteht, wurde jedoch von der kommunalen Praxis über lange Zeit, von wenigen Teilbereichen abgesehen, keineswegs ausdrücklich angestrebt, oft genug nicht einmal als Nebenwirkung der eigentlichen Aufgabenerfüllung zur Kenntnis genommen" (v. Kodolitsch 2003, 6).

2.2 Veränderungen in der Sicherheitsarchitektur

Der Zuschnitt staatlicher Sicherheitspolitik in Deutschland hat sich nach 2001 erheblich verändert: Innere und äußere Sicherheit vermischen sich. Risiken und Bedrohungen lassen sich nicht mehr automatisch eindeutig dem einen oder dem anderen Bereich zuordnen. Die Akteure aus den beiden Bereichen sind in stärkerem Maß auf das Zusammenwirken bei der Lösung neuer Sicherheitsaufgaben angewiesen.[5] In Deutschland haben Bund und Länder eine gemeinsame „Neue Strategie zum Schutz der Bevölkerung" bei außergewöhnlichen Schadenslagen entwickelt, in deren Mittelpunkt das partnerschaftliche Zusammenwirken der Akteure steht. Dies umfasst eine engere Abstimmung vorhandener Hilfspotenziale von Bund, Ländern, Gemeinden und Hilfsorganisationen und die Entwicklung neuer Koordinierungsinstrumente.

Unter dem Eindruck einer veränderten Bedrohungs- und Gefahrensituation sind Bürger eher bereit Einschränkungen persönlicher Freiheit in Kauf zu nehmen. So befürworten beispielsweise mittlerweile 90 % der Briten die Kameraüberwachung auf öffentlichen Plätzen, 44 % der Deutschen reichen die Sicherheitsvorkehrungen gegen Terroranschläge nicht aus und über 60 % würden die Bundeswehr gern auch für Polizei- und Grenzschutzaufgaben im Innern eingesetzt sehen (Allensbach-Erhebung, zit. n. BPB 2004, 2). Maßnahmen der Inneren Sicherheit greifen in deutschen Städten auf unterschiedlichen Ebenen und führen zu neuen Sicherheitsregimes. Die Maßnahmen umfassen rechtliche Veränderungen (Novellierung der Sicherheits- und Ordnungsgesetze, Gefahrenabwehrverordnungen), organisatorische Eingriffe (Ersatz informeller Organisationsformen durch staatliche bzw. privatwirtschaftliche) und die symbolisch-materielle Gestaltung der Stadt (Schließung von Räumen, Herstellung von Einsehbarkeit, Ästhetisierung) (Wehrheim 2004). Ein zentraler Bereich der Umsetzung von Maßnahmen der Inneren Sicherheit in den Städten ist die technische Aufrüstung.

[5] „Waren in Zeiten des Kalten Krieges innere und äußere Sicherheit aufgrund der damals geltenden internationalen sicherheitspolitischen Paradigmen nicht nur politisch, sondern vor allem auch verfassungsrechtlich streng getrennt, haben die Terroranschläge vom 11. September 2001 und deren weit reichende Folgen zu einer tendenziellen Überschneidung in den Anforderungen an die beiden Teilbereiche staatlicher Sicherheitspolitik geführt. … Aktuelle Bedrohungs- und Gefährdungsanalysen und aus ihnen abzuleitende kurz-, mittel- und langfristige Maßnahmen müssen von allen Organen der Gefahrenabwehr, d. h. den Nachrichtendiensten, den Polizeibehörden, dem staatlichen Bevölkerungsschutz und den Streitkräften in enger Kooperation erfolgen" (Weber 2004, 2).

3 Sicherheitstechnik als Problemlöser?

Sicherheitstechnik kann die Gefahrenabwehr sowie Maßnahmen zur Herstellung von Sicherheit und Ordnung in allen Phasen unterstützen:

- Sie kann zur Analyse von Gefahren- und Bedrohungssituationen eingesetzt werden,
- sie kann der Prävention dienen,
- die Lagebeurteilung kann durch technische Systeme erleichtert werden,
- die Komplexität von Intervention und Management bei Schadensereignissen kann handhabbarer gemacht werden und
- bei der Rehabilitation von Schadensräumen wirkt Sicherheitstechnik unterstützend.

Der komplexen Aufgabe entsprechend bietet die Industrie eine breite Palette von sicherheitstechnischen Produkten, die im kommunalen Bereich bereits Anwendung finden oder zukünftig in Anwendung kommen könnten. Als Vorteile des Einsatzes von Sicherheitstechnik werden immer wieder genannt (vgl. u. a. DStGB 2003, 17):

- 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.

Demgegenüber stehen Befürchtungen hinsichtlich allgegenwärtiger technischer Überwachung und Ausgrenzung und Skepsis gegenüber Sicherheitsversprechen. Dennoch sind die für Sicherheit Verantwortlichen bereit, besonders bei akuten tatsächlichen oder vermeintlichen Bedrohungssituationen, zur technischen Lösung zu greifen, zumeist ohne dass umfassendere Analysen oder integrierte Einsatzkonzepte vorliegen, die das Zusammenwirken von Technik, Strategien, Konzepten und nichttechnischen Maßnahmen beinhalten. Technikanwender, zumindest deren Entscheider, die unter Handlungsdruck zeigen konnten, dass Maßnahmen ergriffen werden, und Technikanbieter, die „eine gerade fertige oder halbfertige Technikanwendung als Problemlösung darstellen und behaupten, mit ihr seien alle Probleme gelöst“ (Lenk 2006, 2), scheinen damit zufrieden gestellt.

Sicherheit ist ein wachsender Markt. In den USA hat allein das Heimatschutzministerium ein Budget von rund 40 Milliarden Dollar. In Deutschland wenden Bund, Länder und Kommunen etwa 30 Milliarden Euro jährlich für Innere Sicherheit auf (v. Landenberg 2004). Seit den Anschlägen in New York sei „der Markt für Zutrittskontrollen und Videoüberwachungsanlagen um jeweils ein Drittel gewachsen“ (v. Landenberg 2004, 44). Der Umsatz privater Sicherheitsdienstleister in Deutschland ist von 1,9 Milliarden Euro Anfang der 1990er Jahre auf mittlerweile 3,6 Milliarden Euro gestiegen (v. Landenberg 2004). Zahlen, die deutlich machen, dass es im Kontext des Einsatzes neuer Sicherheitstechnologien und der Etablierung neuer urbaner Sicherheitsregimes nicht nur um Sicherheitserwägungen, sondern auch um ökonomisches Kalkül geht.

3.1 Beispiele für den Einsatz von Sicherheitstechnik in den Städten

An dieser Stelle können nur einige wenige Beispiele für die Anwendung neuer Sicherheitstechniken im kommunalen Bereich ausgeführt werden. Die nachfolgenden Ausführungen konzentrieren sich auf „sichtbare" Frontend-Anwendungen. Sie zeigen, wie alltäglich Sicherheitstechnologien bereits heute in Bereichen eingesetzt werden, die nicht zwangsläufig zum Aufgabenbereich „Innere Sicherheit" gehören. Über die konkreteren Beispiele hinaus lassen sich grundsätzliche Anwendungsfelder auch in folgenden Bereichen identifizieren:

- Informationssysteme (für Akteure und Bürger),
- 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) und
- Ubiquitous Computing (zur umfassenden Vernetzung).

3.1.1 Videoüberwachung

Mit dem Thema Videoüberwachung befassen sich die Kommunen schon seit längerer Zeit. Videoüberwachung wird als „die bedeutendste Neuerung auf dem Feld der Inneren Sicherheit in Städten" (Wehrheim 2004, 23) der vergangenen Jahre angesehen. Im Rahmen der Verkehrsüberwachung sind Kamerasysteme bereits weit verbreitet. Auch zur Gebäudesicherung (z. B. Behörden, Fußballstadien, im öffentlichen Personennahverkehr usw.) sind Kamerasysteme mittlerweile eine gängige Unterstützung. Seit einer Reihe von Jahren werden Videoüberwachungssysteme auch im Rahmen der Kriminalprävention auf öffentlichen Plätzen und Straßen eingesetzt, z. B. zur Kontrolle von Drogenkriminalität. Vorreiter dieser Entwicklung waren Kommunen in Großbritannien, die Videotechnik mittlerweile z. T. flächendeckend in Geschäftsstraßen, an zentralen öffentlichen Plätzen usw. einsetzen und damit z. T. auch eine videotechnische Verfolgung von Einzelpersonen in größeren Stadtbereichen ermöglichen.

Neuere technische Entwicklungen erlauben − gestützt auf biometrische und Verhaltensmerkmale − eine Automatisierung dieser Überwachung. So besteht beispielsweise die Möglichkeit Verdachtspersonen von denen angenommen wird, sie werden eine Sachbeschädigung (z. B. das Anbringen von Graffiti) begehen, anhand spezifischer Bewegungsmuster „auszufiltern".

Neben ortsfesten Anlagen schreitet auch der Einsatz mobiler Videoüberwachung voran. In Großbritannien haben „zahlreiche Kommunen … inzwischen sogenannte ‚CCTV-Vans' eingeführt, die mit Digitalkameras und Kontrollräumen ausgestattet sind" (Hempel 2003). Auch in Deutschland sollen mobile Systeme zukünftig stärker eingesetzt werden, so etwa in Baden-Württemberg und Bayern.

In Deutschland ist die Überwachung öffentlicher Straßen und Plätze durch die Änderung der Polizeigesetze der Länder erst seit den 2000er Jahren möglich. Eine flächendeckende Überwachung nach britischem Muster wurde bisher allerdings nicht angestrebt. Nach Auffassung der Städte sollte Videoüberwachung auf Kriminalitätsschwerpunkte beschränkt sein. Sie kann andere Maßnahmen der Kriminalprävention ergänzen, aber nicht ersetzen (DST 2004, 5f.). Die Zahl der stationierten Videokameras wird auf 500.000 geschätzt. Zur Kriminalitätskontrolle wurde Videoüberwachung in deutschen Städten bisher nur vereinzelt eingesetzt. Meist wurden Kriminalitätsschwerpunkte nur durch zwei bis drei Kameras überwacht (Wehrheim 2004, 23). Die Terroranschläge in London, die Bombenfunde in Regionalzügen in Nordrhein-Westfalen, aber auch die Meldungen über alltäglichen Vandalismus und Gewalt in öffentlichen Verkehrsmitteln und im öffentlichen Raum allgemein haben aber die Diskussion um eine erhebliche Ausweitung der Videoüberwachung erneut angefacht.

Da eine ständige Überwachung von öffentlichen Plätzen mit tiefen Eingriffen in die Persönlichkeitsrechte (Recht am eigenen Bild, Recht auf informationelle Selbstbestimmung) des Einzelnen verbunden sein kann, sind die Einsatzmöglichkeiten begrenzt. So ist etwa die Überwachung öffentlicher Plätze durch Private eingeschränkt, die Speicherung von Daten zeitlich begrenzt, die heimliche Videoüberwachung ist untersagt und die Überwachung muss deutlich angezeigt werden. Dennoch ergeben sich immer wieder Grenzfälle, Überschreitungen und Skurrilitäten, die zu heftigen öffentlichen Diskussionen der Videoüberwachung führen.[6] Immer wieder werden auch Grenzfälle der Nutzung von Überwachungsdaten thematisiert.[7]

Videoüberwachung hat sich insbesondere bei der Aufklärung von Straftaten als erfolgreich erwiesen. Die Identifizierung von Tätern (z. B. nach den Anschlägen auf die Londoner U-Bahn, aber auch bei alltäglicher Kriminalität, Vandalismus usw.) stützt sich immer häufiger auch auf die Auswertung von Videoüberwachungsdaten. Über die Effektivität der Videoüberwachung hinsichtlich ihrer kriminalpräventiven Wirkung gibt es sehr unterschiedliche Aussagen. Die präventive Wirkung an Kriminalitätsschwerpunkten wird ebenso häufig als positiver Effekt genannt wie die Unterstützung der Strafverfolgung. Messbare Rückgänge der Zahl von Straftaten in videoüberwachten Bereichen sind z. T. aber auch mit Verdrängungsprozessen in andere Stadtbereiche verbunden.

Ohne Zweifel hat die Überwachungsintensität in den letzten Jahren erheblich zugenommen und wird mittelfristig weiter zunehmen. Dabei geht es nicht nur um die steigende Zahl der Kameras im öffentlichen Raum, sondern auch um die technische Verknüpfung unterschiedlicher Überwachungstechniken und die organisatorische Vernetzung von privaten und öffentlichen Sicherheitsmaßnahmen z. B. im Rahmen von Sicherheitspartnerschaften (vgl. Hempel 2003).

[6] Beispiele aus dem kommunalen Bereich dafür sind etwa die wieder aufgegebene Videoüberwachung der Männerumkleidebereiche in einem Freiburger Schwimmbad („Videoüberwachung überraschend gestoppt“, Badische Zeitung 8.11.2003) oder die Videoüberwachung von Müllsammelstellen im Rahmen der Kampagne „Unser sauberes Braunschweig“ („Braunschweig im Putzwahn“, taz Nord 15. März 2004).

[7] So z. B. die Nutzung der Videoüberwachung der DB AG durch den BGS auf Bahnhöfen und in Bahnhofsbereichen (Bundesdatenschutzbeauftragter 2005, 63).

3.1.2 Biometrische Zugangssysteme

Im Zuge der Diskussion um die Terrorabwehr wurde in den letzten Jahren häufig über die Nutzung von biometrischen Merkmalen im Rahmen neuer Sicherheitskonzepte diskutiert. Dabei geht es einerseits um die Integration von biometrischen Merkmalen in Personaldokumente, andererseits um deren Nutzung im Rahmen von Identitäts- und Zugangskontrollen. Die Zahl der eingesetzten biometrisch gestützten Systeme in Europa ist von rund 8.500 (1996) auf mehr als 150.000 (2004) gestiegen (European Commission Joint Research Center – JRC, zit. n. Horvath 2005). Erhebliche Wachstumsraten für die „Biometrieindustrie" werden vorausgesagt. Die amtliche Statistik liefert leider keine Angaben zu Umsätzen oder Beschäftigten in diesem Bereich. Der Biometrie-Anteil an der Gesamttechnologie ist auch nur bedingt abgrenzbar und die Informationspolitik der beteiligten Unternehmen ist eher restriktiv (vgl. Petermann/Sauter 2002, 6). So ist man auf Marktstudien privater Institute und Interessengruppen angewiesen. Danach soll der Umsatz der „Biometrieindustrie" von 600 Millionen Dollar (2002) auf 4 Milliarden Dollar (2007) steigen. Biometrie-Technologien werden als die „wichtigsten Innovationen in der IT-Industrie in den nächsten Jahren" (BITE 2005) angesehen. In Deutschland wurde der Biometrie-Gesamtmarkt im Jahr 2004 auf 12 Millionen Euro geschätzt. Insbesondere Großaufträge des Bundes sollen das Marktvolumen bis 2009 auf 377 Millionen Euro erhöhen (SOREON 2004, zit. n. http://www.heise.de/newsticker/meldung/48560). Auch wenn die Zahlen unter den dargestellten Vorbehalten stehen, so liefern sie doch einen Eindruck davon, dass der Markt sich erst entwickelt. Wie so häufig bei der Einführung neuer Technologien werden hohe Umsatzerwartungen für die Zukunft formuliert. Deutlich wird auch, dass der Markt zumindest bisher – in hohem Maß durch staatliche Großaufträge getrieben wird.

Bisher getestete Systeme setzen Gesicht, Fingerabdruck und Iriserkennung als biometrische Merkmale ein:

- Bei auf Gesichtserkennung beruhenden Systemen wird das Gesicht einer Person durch einen Scanner aufgenommen und Software gestützt hinsichtlich spezifischer Merkmale analysiert. Aus den analysierten Individualmerkmalen wird eine biometrische Signatur erzeugt. Zu unterscheiden sind zwei- und dreidimensionale Gesichtserkennungssysteme.
- Bei Fingerabdrucksystemen werden individuelle Bilder des Fingerabdrucks erstellt. Dafür werden unterschiedliche Arten von Sensoren genutzt (Drucksensoren, Ultraschallsensoren, optische, thermische, elektrische und kapazitive Sensoren[8]). Das Bild wird nach charakteristischen Merkmalsausprägungen (Bögen, Schleifen und Wirbel) analysiert und mit vorhandenen Daten verglichen.
- Bei Iriserkennungssystemen werden die Augen der zu erkennenden Person mit Infrarotlicht bestrahlt und eine Makroaufnahme des Auges im nahen Infrarotbereich erzeugt, die auf spezifische Muster (Corona, Krypten, Fasern, Flecke, Narben, radiale Furchen, Streifen) hin analysiert wird. Aus der individuellen Merkmalsausprägung wird ein spezifischer Iriscode erzeugt, der mit den gespeicherten Daten abgeglichen wird.
- In der Forensik bzw. Gerichtsmedizin werden daneben DNA-Merkmale zur Identifizierung genutzt.

Es besteht noch eine Reihe weitgehend ungelöster Probleme. So können einige Personen grundsätzlich von derartigen Systemen nicht erfasst werden (bei Fingerabdruck-, Iriserkennung), da Merkmale nicht erkannt werden oder nicht ausgeprägt sind. Mit dem Alter der zu erkennenden Person nimmt die Erkennungsleistung ab und für bestimmte Berufsgruppen (z. B. solche mit erhöhter Verletzungsgefährdung der Finger) ist sie eingeschränkt (Fingerabdruckerkennung). Darüber hinaus

[8] Kapazitative Sensoren sind Chips, die durch Messung der Gleichstromkapazität zwischen der Chipoberfläche und der Fingeroberfläche digitale Graustufenbilder erzeugen. Zum Teil kann dabei sogar die lebende Schicht des Fingers unter der Oberfläche vermessen werden, sodass sich z. B. Verletzungen weniger auf die Messung auswirken (vgl. Petermann/Sauter 2002, 25).

können umgebungsbedingte Erkennungsschwierigkeiten (z. B. aufgrund bestimmter Lichtverhältnisse bei der Gesichtserkennung) die Systeme behindern. Schließlich wird die geringe Überwindungssicherheit (Fingerabdruckerkennung) derartiger Systeme bemängelt (Bundesdatenschutzbeauftragter 2005, 47f.). Darüber hinaus gibt es bisher kein eindeutiges bioethisches Bezugssystem für die Entwicklung und Nutzung biometrischer Technologien. Diskussionen über die Akzeptanz biometrischer Technologien konzentrieren sich bisher vor allem auf Kosten-Nutzen-Aspekte und Sicherheitsfragen (BITE 2005).

Wer bisher gedacht hat, derartige Zugangssysteme seien beschränkt auf Hochsicherheitsbereiche und Grenzübertritte, irrt, wie das Beispiel des Zugangssystems für Dauerkartenbesitzer des Zoos Hannover zeigt. Wer für den Zoo eine Dauerkarte erwerben will, muss zunächst seine Personalien zur Aufnahme in ein Ticketing-System angeben. Beim ersten Zoobesuch wird ein digitales Foto des Kartenbesitzers aufgenommen und gespeichert. Bei weiteren Besuchen wird an der Zugangskontrolle erneut ein digitales Bild erstellt und mit den gespeicherten Daten verglichen. Ein Zugang ist nur nach positiver Prüfung möglich. Für die Beantragung von Familien-Karten benötigt man zusätzlich einen Familiennachweis (Kindergeldnachweis, Auszug aus dem Stammbuch, amtlicher Ausweis, Krankenkassenkarte). Mit mehr als 71.000 Dauerkarten handelt es sich um die größte biometrische Anwendung im sog. Convenience-Bereich in Deutschland (DStGB 2003, Glitza 2004, Schiffhauer 2004). Der erste Versuch, biometrische Merkmale – den Fingerabdruck – zur Zugangskontrolle zu nutzen, war zuvor daran gescheitert, dass hygienische Bedenken das System ebenso aushebelten wie die schlechte Erkennungsrate bei Kindern, und weil der langsame Durchgang sowie die mangelnde Wetterfestigkeit des Systems sich als Problem erwiesen (vgl. Glitza 2004, Schiffhauer 2004). Mögliche weitere kommunale Einsatzfelder von Zugangssystemen mit biometrischen Merkmalen sind z. B. Museen oder Sporteinrichtungen. Darüber hinaus lassen sich natürlich zahlreiche Anwendungen in sicherheitsrelevanten Bereichen vorstellen.

3.1.3 RFID

Hinter der Abkürzung RFID (Radio Frequency Identification) verbirgt sich eine Mikrochiptechnologie zur kontaktlosen Datenübermittlung. RFID-Systeme bestehen aus RFID-Schreib- und Lesegerät, einem Transponder und dem Einsatz von Radiofrequenztechnologie. RFID-Systeme können genutzt werden zur

- Objektkennzeichnung,
- Echtheitsprüfung von Dokumenten und Waren,
- Prozessoptimierung bzw. zur Automatisierung von logistischen Abläufen,
- Unterstützung von Zugangskontrollen und Routenüberwachungen, oder
- Umweltbeobachtung usw.

Transpondersysteme werden bereits seit längerem eingesetzt. Zur Tieridentifikation werden beispielsweise seit etwa 20 Jahren Transpondersysteme genutzt, die injiziert oder als elektronische Ohrmarke angebracht werden. Während diese Systeme zunächst in der Nutztierhaltung Verbreitung fanden, werden sie mittlerweile auch bei Haustieren genutzt. RFID-Systeme sind aufgrund der erheblichen Fortschritte in der Speichertechnologie und der Funkübertragungstechnologie − und besonders deren Zusammenwirken − in den Blickpunkt der öffentlichen Diskussion gelangt. So bieten sie erhebliche Vorteile gegenüber anderen Technologien, die in gleichen Einsatzfeldern Anwendung finden:

- Beispielsweise erweitern sich bei der Zugangskontrolle die Leistungsmerkmale deutlich gegenüber traditionellen Chipkartensystemen oder Magnetkartensystemen. So erhöht die kontaktlose Übermittlung der Daten die Bequemlichkeit für den Benutzer erheblich (keine Wartezeiten, kein aktiver Eincheckvorgang usw.).

- Im Logistikbereich erübrigt sich die arbeits- und zeitaufwendige Einzelerfassung von Waren zugunsten einer Pulkerfassung von Lieferungen. Damit kann die operative Effizienz gesteigert werden und die Auslastung der Betriebsmittel kann erhöht werden. Auch sind Sicherheitsvorteile (z. B. im Bezug auf die Warenverfolgung) mit dem RFID-Einsatz verbunden.
- Kostenvorteile entstehen gerade in Branchen mit hohen Anforderungen an die Prozesssicherheit wegen umfassender Nachweispflichten (z. B. Logistikunternehmen, Entsorgungsunternehmen).
- Auch Unternehmen mit geschlossenen Logistikkreisläufen (z. B. Einzelhandelsunternehmen) versprechen sich erhebliche Vorteile von der Technologie. Geschlossene Logistikkreisläufe erlauben die Wieder- oder Dauerverwendung des – heute in der Herstellung noch vergleichsweise teuren – RFID-Transponders. Zu den Vorreitern der Nutzung von RFID-Technologie gehören die Einzelhandelsunternehmen Metro, Wal-Mart und Tesco. Im „Future Store" der Metro Gruppe im nordrhein-westfälischen Rheinberg werden neue Technologien für den Einzelhandel getestet. Die manuelle Barcode-Erfassung von Waren an der Kasse soll durch die elektronische Erfassung im Einkaufswagen unter Nutzung von RFID-Technologie ersetzt werden. Die ausgelesenen Daten werden dann in einem Zentralrechner gesammelt. Die einzelnen Unternehmen der Wertschöpfungskette (Hersteller, Zwischenhändler, Zentraleinkauf, Warenlager) sind mit dem Zentralrechner vernetzt und haben Zugriff auf die Datenbank. Eine Kombination mit Kundenkartensystemen, die mit RFID-Transpondern ausgestattet sind, ist möglich. Geplant ist die vollständige Umrüstung von Barcodes auf RFID-Transponder (BSI 2004, 85f.).

RFID-Technologie wird in den Städten in immer mehr Einsatzfeldern genutzt. In zunehmendem Maß finden RFID-Anwendungen Eingang in den öffentlichen Personennahverkehr. Für die Nahverkehrsunternehmen sind RFID interessant, entfallen doch etwa ein Fünftel der Ticketkosten auf das Management des Ticketverkaufs. Hier verspricht man sich erhebliche Kostenvorteile und Verbesserungen im Transportablauf. Das erste Chipkarten-Projekt im ÖPNV gab es in Deutschland zu Beginn der 1990er Jahre in Köln, das erste Projekt mit kontaktlosen Karten Mitte der 1990er Jahre (Cap 2005).

Im Gesundheitsbereich werden RFID-Anwendungen eingesetzt, um Patientendaten eindeutig mit dem betreffenden Patienten zu verknüpfen. Im Klinikum Saarbrücken beispielsweise werden zu diesem Zweck Patienten mit RFID-Armbändern ausgestattet. Demnächst werden auch Blutkonserven über RFID-Transponder identifiziert. Bei der Anlieferung ins Klinikum erhält der Beutel mit der Blutspende einen RFID-Transponder, auf dem eine Nummer gespeichert ist, die mithilfe einer Datenbank die eindeutige Zuordnung zu Herkunfts-, Verwendungs- und Empfängerdaten der Blutspende ermöglicht. Das Pflegepersonal ist mit PDAs und Lesegerät ausgestattet und kann so die Daten des RFID-Transponders an der Blutkonserve und des Patientenchips auslesen und vergleichen. Die Daten werden gleichzeitig in die Prozesserfassungssysteme und den Datensatz des Patienten aufgenommen.[9]

Das Facility Management kann RFID-Technologie zur Kennzeichnung und Bestandsführung nutzen. Die Berliner Wasserbetriebe beispielsweise stellen ihr mobiles Anlagenmanagement auf RFID um. Die rund 60.000 Wirtschaftsgüter der Wasserbetriebe an 250 Standorten im Verdichtungsraum Berlin-Brandenburg werden mit RFID-Transpondern ausgestattet. Mit mobilen Datenerfassungsgeräten können alle Informationen vor Ort eingelesen und automatisch ins Inventursystem eingespielt werden.[10]

[9] „Erster Deutscher Kongress für Patientensicherheit, Bundesweites Medienecho", http://www.klinikum-saarbruecken.de/kliniknews/index.php3?tid=256&a=NEWS, 13.11.2006.

[10] „Berliner Wasserbetriebe verwalten Anlagen künftig mit Hilfe von RFID", http://www.esg.de/presse/archiv/?tid=751, 13.11.2006.

Kommunale Dienstleitungen können durch RFID-Technologie unterstützt werden. Die Entsorgungsbetriebe beispielweise in den Kreisen Hof, Erlangen-Höchstadt, Mühldorf am Inn, Kehlheim am Inn und Heiligenstadt kennzeichnen ihre Mülltonnen mit RFID-Transpondern, die eine einmalige Kennziffer speichern. Sie erlaubt die eindeutige Zuordnung zu Grundstücksdaten und Behältergröße. Die Müllfahrzeuge sind mit Lesegeräten ausgestattet, die entsprechenden Leerungsdaten werden auf einer Chipkarte im Bordrechner des Fahrzeugs automatisch gespeichert. Nach der Müllsammlung werden die Daten des Bordrechners ausgelesen und zur Gebührenberechnung genutzt. In Kombination mit Wiegesystemen an den Fahrzeugen können genaue Müllmengenberechnungen vorgenommen werden, auf deren Grundlage die Gebühren individuell berechnet werden können (BSI 2004, 70). Ein anderes Beispiel ist die Einführung eines RFID-gestützten Systems zur Selbstverbuchung von Medien in den Münchner Stadtbibliotheken. Bis 2009 soll von den 3,15 Millionen Medien der Münchner Stadtbibliotheken der gesamte Freihandbestand von 1,5 Millionen mit RFID-Transpondern ausgestattet sein. Die Leser können ihre Medien an Selbstbedienungsstationen ausleihen. Über Rückgabeautomaten in den Eingangs- oder Außenbereichen der Bibliotheken können Medien auch außerhalb der Öffnungszeiten zurückgegeben werden. Die auf den RFID-Transpondern gespeicherten Daten werden an den Ausleih- und Rückgabestationen kontaktlos ausgelesen und automatisch mit dem Bibliothekskonto abgeglichen. Sortieranlagen im Hintergrund der Rückgabeautomaten und RFID-Initialisierungsdesktops unterstützen die Verbuchung und Sortierung der Medien. Mit Lesegeräten ausgestattete Sicherungsgates an den Ausgängen signalisieren, wenn nicht verbuchte Medien aus der Bibliothek entfernt werden sollen [11].

Insgesamt ist die RFID-Technik mit der Gefahr der Verarbeitung personenbeziehbarer Daten ohne ausreichende Transparenz der Verarbeitungsvorgänge verbunden. Bei einigen Systemen ist der Zugriff bis auf einige Meter Entfernung möglich. Sowohl RFID als auch Lesegeräte können unerkannt in alltägliche Gegenstände eingearbeitet werden. Die aus datenschutzrechtlicher Sicht kritischen Potenziale werden auch daran deutlich, dass „ein Personenbezug, z. B. bis hin zur Kopplung mit Videokameras, … bereits Gegenstand von Feldversuchen im Handel“ war (Bundesdatenschutzbeauftragter 2005, 46). Es besteht weiterhin eine Reihe von technischen Problemen und Problemen mit der Alltagstauglichkeit der Systeme.[12]

Die Verbreitung von RFID-Chips schreitet weiter voran. Was in der Computerzeitschrift „c’t“ im Frühjahr 2004 noch als Aprilscherz „durchging“ – die angebliche Ausstattung von TÜV-Prüfplaketten mit RFID-Chips – soll in Großbritannien gut ein Jahr später Realität werden. Um das Fälschen von Nummernschildern zu erschweren, sollen sie mit RFID-Chips ausgerüstet werden. Als Nebeneffekt oder „Kollateralschaden“ – je nach Ansicht – würde damit die Aufzeichnung von Bewegungsprofilen möglich.[13] Ein weiteres Beispiel für die breite Anwendung von RFID-Technologien ist die südkoreanische Stadt New Songdo, 40 Meilen südwestlich von Seoul: Eine als Freihandelszone konzipierte großflächige Immobilienentwicklung, in der 65.000 Menschen wohnen und 300.000 Menschen arbeiten sollen, in der Englisch die Verkehrssprache sein soll und unterschiedliche internationale Währungen in Gebrauch sind.[14] Teil des Entwicklungskonzepts ist die Vernetzung und der Datenaustausch zwischen allen wesentlichen Informationssystemen. Datenschutzpro-

[11] „Bücher aus dem Automat“, Süddeutsche Zeitung vom 12. Januar 2006.

[12] So war ein Problem bei der Eingangskontrolle zu den Spielen des Confederation Cup in Deutschland 2005 die Angewohnheit von Fans Eintrittskarten an der Pinnwand zu befestigen und damit zum Teil die RFID-Chips zu zerstören. Vor dem Knicken der Eintrittskarten war auf den Karten gewarnt worden, an die „Pinnwand-Falle“ dachte keiner (vgl. „WM-Tickets bitte nicht knicken“, http://www.heise.de/newsticker/meldung/61251; 31.8.2005).

[13] „Briten testen funkende Autokennzeichen“, Spiegel Online, 11. August 2005, http://www.spiegel.de/netzwelt/technologie/0,1518,369248,00.html, 26.8.2005.

[14] Eine ausführlichere Darstellung der Entwickler findet sich in: http://www.new-songdocity.co.kr/; 7.11.2005.

bleme werden dabei kaum thematisiert, Skepsis vor dem „Überwachungsstaat“ scheint den Entwicklern völlig fremd zu sein. Das Projekt wird vielmehr als Möglichkeit gesehen, technologische Führerschaft zu beweisen und ausländische Investitionen anzuziehen (O’Connell 2005)[15].

3.2 Technische und organisatorische Konvergenz der Sicherheitstechnologien

In den Städten ist eine Vielzahl von Anwendungsmöglichkeiten denkbar. Vor allem die Kombination unterschiedlicher Sicherheitstechniken wie die Videoüberwachung, die Nutzung biometrischer Merkmale für die Identifikation und die kontaktlose Datenübermittlung 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 individueller Nutzung ermöglichen. Schon heute werden derartige konvergente Technologien genutzt. 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. Neben der technischen Konvergenz spielt in diesem Zusammenhang die organisatorische Konvergenz eine besondere Rolle. Mit der zunehmenden Vermischung von Aufgaben der Gefahrenabwehr der inneren und der 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. 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.

[15] Mögliche Anwendungen wären beispielsweise: „public recycling bins that use radio-frequency identification technology to credit recyclers every time they toss in a bottle; pressure-sensitive floors in the homes of older people that can detect the impact of a fall and immediately contact help; cellphones that store health records and can be used to pay for prescriptions” (O’Connell 2005).

4 Urbanität unter veränderten Sicherheitsbedingungen

Die Nutzung von IuK-gestützter Sicherheitstechnik ist mit Potenzialen und Gefahren verbunden, die es gegeneinander abzuwägen gilt. So bietet beispielsweise der Einsatz von Überwachungstechnologien grundsätzlich den Vorteil einer möglichen präventiven Wirkung, da das Entdeckungsrisiko (z. B. von Ordnungswidrigkeiten oder Straftaten) bzw. die Entdeckungswahrscheinlichkeit (von Gefahrensituationen) steigt und damit die Möglichkeit einer frühzeitigen Intervention, da sich die Informationsbasis über spezifische Sicherheitslagen vergrößert. Empirische Ergebnisse[16] deuten jedoch darauf hin, dass diese grundsätzlichen Potenziale in der Realität unter Einbeziehung der Gesamtsituation nicht ausgeschöpft werden bzw. nicht ausgeschöpft werden können. Demgegenüber stehen die Gefahren von übermäßiger punktueller Überwachung, die z. B. mit Ausgrenzungs- oder Verdrängungsprozessen verbunden sein kann.

Die Nutzung von IuK-gestützten Sicherheitstechniken kann die Zugänglichkeit der Stadt verbessern, wenn beispielsweise bauliche Sicherheitsmaßnahmen wie Zäune, Sicherheitsabstände und Verbauungen durch technische Kontrollsysteme und temporäre Intervention ersetzt werden können. Sie kann die Zugänglichkeit von bestimmten Bereichen der Stadt aber auch verringern, wenn über technische Systeme Zugangsrestriktionen durchgesetzt werden, und sie kann in erheblichem Maß sozial selektiv eingesetzt werden (vgl. Graham 2005). Technik ist immer ambivalent. Auch Sicherheitstechnik muss dabei immer in ihrem Einsatzkontext betrachtet werden. Der zunehmende Einsatz von Sicherheitstechnik muss auch vor dem Hintergrund tatsächlicher oder vermeintlicher Bedrohungen und des damit in Zusammenhang stehenden Sicherheitsregimes betrachtet werden.[17]

Mit einer veränderten Gefahrensituation, des zunehmenden 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.

Städte könnten zunehmend als unsichere Orte wahrgenommen werden. Damit würde einer neuen „Stadtfeindlichkeit“ Vorschub geleistet. Grundsätzlich sind Städte vergleichsweise „unübersichtliche Orte“ und könnten damit unter den Generalverdacht geraten, Versteck für alle möglichen Formen von Sicherheitsbedrohung zu sein: vom Versteck „gewöhnlicher Krimineller“ bis hin zum Rückzugsraum zur Vorbereitung terroristischer Aktivitäten. Schon jetzt werden diese Befürchtungen in der internationalen Stadtforschungsliteratur geäußert.[18] Sind wir also auf dem Rückweg in die befestigten Städte und die sicherheitspolitisch beherrschbaren Hausmann’schen Boulevards? Folgt im Zeitalter der Informations- und Kommunikationstechnik der Festungsmauer das elektronische Portal? (vgl. Virilio 2004)

[16] „Das britische Innenministerium legte 2002 die Ergebnisse einer Auswertung von 22 methodisch aufwendigen Studien zur Wirkung von Videoüberwachung in den USA und Großbritannien vor. … Demnach reduzierte sich die Zahl der Diebstähle von und aus Kraftfahrzeugen um gut 40 Prozent, Taschendiebstähle nahmen aber nur um zwei bis vier Prozent ab, und auf die Häufigkeit von Gewaltdelikten gab es keinerlei Auswirkungen“ (Wehrheim 2004, 24).

[17] „Das Fatale ist, dass sich Überwachung an vielen Stellen ausbreitet, die erst einmal mit dem ‚Großen Bruder’ nichts zu tun haben, aber doch eine Infrastruktur herstellen, die leicht anzueignen wäre“ (Rötzer 2004).

[18] „Cities are especially well suited for furnishing terrorists with anonymity, safe houses and supply depots in order to prepare attacks as well as gain access to potential targets. … Terrorists can more easily become invisible in overcrowded neighborhoods; they can hide weapons and explosives in obscure places and they can freely conduct themselves in a maze of twisting streets” (Savitch 2005, 362).

Die zunehmende oder lang anhaltende Bedrohung könnte mit einer verstärkten „Aufrüstung“ mit Sicherheitsmaßnahmen, -technologien und -architekturen verbunden sein. Die „Aufrüstung“ zeigt sich als schleichender Prozess der „Befestigung“ von Städten. Zunächst nimmt die Aufmerksamkeit für die Geschehnisse im öffentlichen Raum zu und eine informelle Überwachung etabliert sich. Die sicherheitstechnische Ausrüstung wird verbessert. Regelungen, die den Aufenthalt in öffentlichen Räumen regulieren, werden verschärft. Bauliche Veränderungen wie die Errichtung von Zäunen und Wällen, Zugangstoren und die Entwicklung „wehrhafter Architekturen“ finden Einzug in die Städte.[19] Unter Sicherheitsgesichtspunkten spricht man vom „target hardening“ (Oc/Tiesdell 2000). Selbst das eigene Auto wird zur Sicherheitszone ausgebaut. Nicht nur das Karosserie-Design wird „wehrhafter“[20] auch die IKT-Ausstattung der Automobile wird dem Sicherheitstrend angepasst.[21]

Vermeintliche „Archipele der Sicherheit“ wie Shopping Malls, Bahnhöfe, innerstädtische Plätze, Business Improvement Districts, Gated Communities könnten entstehen (vgl. Wehrheim 2002).[22]

Stadträume könnten nach ihrem Sicherheitsstatus unterschiedlich bewertet werden. 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. „Ethnic profiling“ ist eine der Sicherheitsinstrumente zur Prävention von Anschlägen, besonders, wenn vorhergehende Anschläge bestimmten ethnischen Gruppen zugeordnet werden konnten (vgl. Savitch, 2005). Damit geraten Wohnquartiere spezifischer ethnischer Gruppen in das sicherheitspolitische Visier. Auch die Diskussion um die Bedrohung durch vermeintliche Parallelgesellschaften, die bei einer engen räumlichen Konzentration einzelner ethnischer Gruppen in den Städten entstünden, und Instrumente wie kleinräumige Zuzugssperren bekämen unter sicherheitspolitischen Erwägungen einen verschärften Zungenschlag. Als eher sicher gelten dagegen suburbane Räume.[23] Nach Clarkes eingangs vorgestelltem Szenario müsste man sich von diesem Gedanken aber vermutlich ebenfalls verabschieden (vgl. Clarke 2005).

[19] Oc und Tiesdell entwickeln die Vorstellung eines gestuften Prozesses der Stadtbefestigung und bezeichnen diese Stufen der Entwicklung als animated presence, panoptic devices, regulatory measures, fortress construction (Oc/Tiesdell 2000).

[20] Nicht nur der während des Golfkriegs bewährte „Hummer“ auch die auf dem Modell „Fiesta“ aufbauende Stadtauto-Studie „Synus“ von Ford erscheint im „tough design“ („Fords Tresor-Auto. Es muss nicht immer Hummer sein“, Manager-Magazin, 17.1.2005).

[21] So bietet beispielsweise der neue Volvo S80 einen „Personal Car Communicator“, der es ermöglicht den Sicherheitsstatus des Fahrzeugs per Fernbedienung zu überwachen. Dabei wird nicht nur angezeigt, ob der Wagen verschlossen und die Alarmanlage angeschaltet ist, über einen Herzschlagsensor im Fahrzeug kann das System außerdem erkennen, ob sich eine Person im Innenraum des Fahrzeugs befindet („100 Prozent Angst“, Handelsblatt, 29.3.2006).

[22] Wörtlich genommen wird ein derartiges „Archipel der Sicherheit“ beispielsweise gerade auf der 62 ha großen Ayers-Insel im US-Bundesstaat Maine errichtet, wo eine „intelligente Insel“ entwickelt werden soll, „deren Ziel es ist, die gesamte Insel mitsamt allen Gebäuden mit Sensoren so abzudecken, dass ‚jede verdächtige Bewegung’ erfasst werden kann“ (Rötzer 2004). Ein anderes Beispiel für den Versuch kleinteilige Zonen der Sicherheit zu schaffen ist der Ortsteil Shoreditch im Londoner East End, wo 20.000 Bewohner über ihren Kabelanschluss Bilder lokaler Überwachungskameras empfangen können und die Polizei über verdächtige Wahrnehmungen, die sie dabei machen, anonym informieren können. Unterstützt wird die Suche nach Verdächtigen durch eine Galerie von Verdächtigenbildern („ASBO-TV helps residents watch out”, The Sunday Times, 8.1.2006).

[23] „Many of the more secure places resemble the protected spaces of suburban malls as well as lower-density, suburban housing complexes” (Savitch 2005, 383).

Zwischen unerwünschten Nachbarschaften könnten „Kontrollzonen“ oder „Sicherheitszonen“ entstehen.[24] In den Großstädten entstünde ein Inselsystem von sich überlagernden Milieus (die ortsgebundenen Armutsmilieus, die Arbeits-, Freizeit- und Wohnorte der Lebensstilgruppen und das Milieu international orientierter, hoch qualifizierter Arbeitskräfte), die bestrebt sind, sich mit tiefer gehender sozialer Spaltung kontrolliert von einander abzugrenzen (vgl. Wehrheim 2004, 26). „Sicherheitszonen“ um „gefährdete Einrichtungen“ könnten entstehen, die über das bisher gekannte Maß hinausgehen, z. B. auch Wohngebäude betreffen.[25] Je nach gewünschtem Sicherheitsstatus könnten temporär begrenzbare Zugangsbeschränkungen für bestimmte Stadtbereiche ausgesprochen und technisch überwacht werden. Schon heute werden solche temporären Aufenthaltsbeschränkungen vorgenommen, die von polizeilichen Anordnungen (wie dem Platzverweis) über Sperrmaßnahmen (z. B. bei Veranstaltungen) bis hin zu Aufenthaltsverboten reichen.[26] Mit technischer Überwachung ließen sich derartige Zugangsbeschränkungen erheblich ausweiten.

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. Befürchtet wird beispielsweise, dass öffentliche Räume „zu privatrechtlich sanktionierten Enklaven des gehobenen Konsums“ werden (vgl. Hamedinger 2005).

Neue Sicherheitsregimes könnten Auswirkungen auf die Infrastrukturplanung haben, z. B. könnte es als 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. Der Aufbau von Schleusensystemen mit Detektoren für Sprengstoff oder Sensoren, die versteckten Sprengstoff auch aus der Entfernung erkennen können, würde eine völlige Umgestaltung der bestehenden Verkehrsinfrastruktur mit sich bringen.[27] Letztlich kommt die Frage auf, ob Megainfrastrukturen wie Großflughäfen, Großbahnhöfe mit angegliederten Shopping- und Bürokomplexen überhaupt zu sichern wären und ob nicht dezentrale Einrichtungen aus Sicherheitsüberlegungen sinnvoller wären. Die Desintegration von Einkaufs- und Verkehrseinrichtungen (z. B. bei Flug- oder Bahnhöfen) und Größenbeschränkungen oder Konzentrationen (abhängig von der besseren Zugänglichkeit für Kontrollmaßnahmen) könnten die Folgen sein.

[24] Der Entwurf des neuen Anti-Terror-Gesetzes in Frankreich sieht beispielsweise die automatisierte Überwachung von Autonummernschildern und Insassen in „Risikozonen“ vor. Auf Anordnung des Polizeichefs könnten bei „konkretem Verdacht“ überall, ohne richterliche Anordnung, bis zu vier Monate Kameras installiert werden (Streck 2005b).

[25] Beispielhaft dafür ist der Fall eines Diplomatenwohnhauses in Wien (vgl. Jänicke 2004).

[26] Ein besonders krasses Beispiel für derartige Zugangsbeschränkungen ist das Zutrittsverbot, das zur Prostitutionsbekämpfung für den Stadtteil Colonia Marconi de Villaverde in Madrid ausgesprochen wurde. Der Zugang zu diesem Stadtteil ist in der Zeit von 23 bis 6 Uhr nur mit einer der ausgegebenen 3.000 Zugangskarten möglich (Streck 2005a).

[27] „Sollte eine solche Maßnahme nützlich sein, müsste wie in einem Flughafen jeder Zugang mit solchen Schleusen und zusätzlich mit Personal ausgestattet sein. Abgesehen von den Kosten würde dies im Berufsverkehr unweigerlich zum Chaos führen. Lange Schlangen bilden, wie im Irak deutlich sichtbar, überdies gute Ziele für Anschläge“ (Rötzer 2005). In der Londoner U-Bahn sollen angeblich „zur Beruhigung oder zum Testen einige dieser ‚Passive Millimetre-wave Scanner’ im Eingangsbereich der U-Bahn [aufgebaut werden], die die Kleidung der Passanten durchleuchten und versteckte Gegenstände sichtbar machen können“ (Rötzer 2005).

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.).[28]

Umfassende stadträumliche Sicherheitskonzepte könnten implementiert werden. Am Londoner Beispiel lassen sich diese Entwicklungen schon heute teilweise ablesen. Nach den IRA-Anschlägen in der Londoner City in der ersten Hälfte der 1990er Jahre hatte man sich entschlossen, dem Belfaster Beispiel folgend einen „ring of steel" zu bilden, indem die Zahl der Zugangsmöglichkeiten in den Finanzdistrikt begrenzt und Barrieren aufgebaut wurden, die temporäre Zugangssperren möglich machen sollten. Es wurden Tausende von Videokameras installiert, Sicherheitspläne der Finanzinstitutionen überarbeitet und empfohlen, die Zahl der Zugänge zu einzelnen Gebäuden von Finanzinstitutionen zu begrenzen. Die Gebäude wurden sicherheitstechnisch verstärkt und „back-up sites" aufgebaut, die im Notfall die Funktion der ursprünglichen Standorte übernehmen sollten. Die Polizeipräsenz wurde massiv verstärkt (vgl. Coaffee 2003).

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. So führen erhöhte Sicherheitsanforderungen dazu, dass der Einlass zu Großveranstaltungen in zunehmendem Maß nur mit personalisierten Tickets möglich ist, was zu erheblichen Unbequemlichkeiten für Ticketinhaber führen kann. Umfangreiche Sicherheitsmaßnahmen (Straßensperrungen, Sperrungen des Luftraums usw.) können darüber hinaus große Teile der Stadt beeinträchtigen.

In letzter Konsequenz könnte das subjektive Unsicherheitsgefühl mit einer Verlagerung von Aktivitäten in den virtuellen Raum verbunden sein. So beschreibt beispielsweise Clarke in seinem Szenario die Verlagerung von Einkäufen ins Internet nach Anschlägen auf Einkaufszentren (Clarke 2005).

Schließlich stellt sich die Frage, wie Städte aussehen, die bei sinkenden finanziellen Mitteln zunehmende Anteile für Sicherheitsinfrastrukturen investieren müssen oder wollen.[29] Die Gefahr besteht, dass sich die baulichen, technischen und regulatorischen Sicherheitsmaßnahmen in den Städten als wirksam gegen Bedrohungen erweisen und dennoch dafür sorgen, dass urbane Lebensräume zerstört und städtisches Leben behindert wird − und damit letztlich ein Ziel des Terrors gegen Städte erreicht wird.

[28] Wie sich Sicherheitsüberlegungen auf die Gestaltung von Architektur auswirken, zeigt sich besonders deutlich am Beispiel des Wiederaufbaus am „Ground Zero" in New York. Der „Freedom Tower" soll spezifische Sicherheitskriterien erfüllen, die über das Maß der üblichen Gebäudesicherheit erheblich hinausgehen. So soll „das Betonpodest, eine Stahl-Titan-Mischung, … einen Meter dick und in schimmerndes Metall gekleidet sein …, auf den von der Strasse aus gerechnet ersten 10 Metern Höhe ganz und gar fensterlos [sein]". Die Konstruktion „ geht … auf die Furcht vor Auto- und LKW-Bombenanschlägen zurück. Sicherheitsexperten der Polizei hatten darauf bestanden, dass der Turm nach Kriterien errichtet werden sollte, die auch für Bundesgebäude gelten, etwa für US-Botschaften oder das Pentagon. Darüber hinaus wurden mindestens 30 Meter Abstand von der nächsten befahrenen Strasse angemahnt. Natürlich gibt es chemische und biologische Filter, massive Vorkehrungen für Brandschutz, extra breite Treppen, viele verbundene Ausgänge und besonders geschützte Lifte" (Böhnel 2005).

[29] Allein für die Ausstattung mit „Passive Millimetre-wave Scanner" würden „pro Station … bis zu drei Millionen Euro erforderlich sein" (Rötzer 2005).

5 Fazit

Der Einsatz von Technik zur Verbesserung der Sicherheit in den Städten wird bisher in der öffentlichen Diskussion, von Bürgern, aber auch von Entscheidungsträgern sehr polarisiert bewertet: Sicherheitstechnik wird verteufelt oder unkritisch als Problemlöser für alle Sicherheitsaufgaben in den Städten angesehen. Potenziale und Risiken, die mit dem Einsatz von Sicherheitstechnologien verbunden sind, werden dagegen bisher kaum kritisch im Anwendungskontext bewertet. Die spezifischen Wirkungen einzelner Sicherheitstechniken und deren Zusammenwirken im individuellen Anwendungszusammenhang sollten häufiger empirisch untersucht werden, statt den Einsatz von Sicherheitstechniken von vagen Nützlichkeitsvermutungen abhängig zu machen. Umgekehrt bedeutet dies, dass nicht jede Einsatzerwägung mit der Keule „Überwachungsstaat" totgeschlagen werden sollte. Der Risikodialog sollte auch in diesem Bereich – soweit er überhaupt schon besteht, was man bezweifeln kann – weiter vorangetrieben werden, um ein gegenseitiges Aufschaukeln ohnehin polarisierter Positionen zu vermeiden. Denn das gemeinsame Ziel, Städte sicher zu machen, ist unbestreitbar. Gestritten werden muss über das Maß der Sicherheit und wie man es erreicht. Im Mittelpunkt steht dabei nicht der Einsatz von Technik selbst, sondern um deren Einbettung in Sicherheitskonzepte, die den sozialen Kontext der Entwicklung von Kriminalität berücksichtigen. Prävention sollte dementsprechend nicht vorrangig auf restriktive Interventionen bei „störendem" Verhalten setzen, sondern gerade auch auf Angebote, die auf Vermeidung solcher Verhaltensweisen bereits im Vorfeld abzielt.

Städte und ihre Bürger werden sich in Zukunft in stärkerem Maß mit Sicherheitsfragen auseinandersetzen müssen. Es entwickeln sich − eher als Reaktion auf konkrete Anlässe und ad hoc formulierte Sicherheitsansprüche als auf Basis integrierender konzeptioneller Überlegungen − urbane Sicherheitsregimes. Auch um diese gewachsenen Sicherheitsregimes mittelfristig in eine integrierte lokale Sicherheitspolitik umzusetzen, bedarf es Wirkungsanalysen. 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. Fragen, denen sich Stadtforschung und Technologiefolgenforschung ebenso stellen sollten wie Bürger, Technikanwender und Technikentwickler. Die Befassung mit der Entwicklung von Sicherheitstechnologien und der Entwicklung neuer urbaner Sicherheitsregimes ist damit eine zentrale Aufgabe modernen Technologiemanagements im städtischen Kontext – also TA im besten Sinne.

6 Literatur

BITE – Biometric Information Technology Ethics: Press Release, January 2005.

Böhnel, Max, 2005, Hochsicherheitsklotz statt Freiheitsturm, Telepolis, 6.7.2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20459&mode=print, 26.8.2005.

BPB – Bundeszentrale für politische Bildung, 2004, Aus Politik und Zeitgeschichte, Editorial.

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2004, Risiken und Chancen des Einsatzes von RFID-Systemen, Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit, Bonn.

Cap, Clemens H., o. J., Anwendungen von RFID Identifikation, Folien zur Vorlesung „Smart Cards, Smart Labels, Smart Devices", Lehrstuhl für Informations- und Kommunikationsdienste der Universität Rostock, http://wwwiuk.informatik.uni-rostock.de/sites/lehre/lehrveranstaltungen/vl_smartx/rfid-applications.pdf, 9.5.2005.

Clarke, Richard A., 2005, Zehn Jahre danach. Vortragsmanuskript zum zehnten Jahrestag des 11. September 2001, Frankfurter Allgemeine Sonntagszeitung, 6. März 2005.

Coaffee, Jon, 2003, Terrorism, Risk and the City: The Making of a Contemporary Urban Landscape, Aldershot: Ashgate.

Der Bundesbeauftragte für den Datenschutz, 2005, Tätigkeitsbericht 2003-2004, 20. Tätigkeitsbericht, Bonn.

DST – Deutscher Städtetag, 2004, Positionspapier Sicherheit und Ordnung in der Stadt, http://www.staedtetag.de/imperia/md/content/pressedien/2004/7.pdf.

DStGB – Deutscher Städte- und Gemeindebund: Pressemeldung vom 1.7.2002.

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

DStGB – Deutscher Städte- und Gemeindebund, 2006, Sichere Städte und Gemeinden. Unterstützungs- und Dienstleistungsangebote des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe für Kommunen, DStGB Dokumentation 60, Verlagsbeilage „Stadt und Gemeinde interaktiv, Ausgabe 5.

Glitza, Klaus Henning, 2004, Mundwasser gegen einen Hauch von Toll Collect, CD Sicherheitsmanagement 4, 125-129.

Graham, Stephen, 2005, Software-sorted geographies, Progress in Human Geography, 29, Oktober, 562-580.

Graham, Stephen, 2004, Postmortem City. Plädoyer für eine Geopolitik des Urbanen, Informationen zur modernen Stadtgeschichte, 2, 54-71.

Hamedinger, Alexander, 2005, Privatisierung und soziale Kontrolle öffentlicher Räume in „sicheren Städten", in: Manfred Schrenk (Hrsg.): CORP 2005 & Geomultimedia05, Proceedings/Tagungsband. Wien, 547-554.

Hempel, Leon, 2003, Verdrängen statt Vorbeugen, Telepolis, 15.1.2003, http://www.heise.de/tp/r4/artikel/13/13928/1.html, 9.5.2005.

Horvath, John, 2005, Prepare to be scanned, Telepolis 2.8.2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20635&mode=print, 13.11.2006.

Jänicke, Ekkehard, 2004, Sicherheitszone für US-Bürger in Wien, Telepolis 15.8.2004 http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?mode=html&artikelnr=18121, 9.5.2005.

v. Kodolitsch, Paul, 2003, Einführung: Sicherheit in der Stadt, in: Deutsche Zeitschrift für Kommunalwissenschaften I, 5-10.

v. Landenberg, Markus, 2004, Mit Sicherheit mehr Jobs, in: Stern Spezial Campus & Karriere, 1.10.2004, 42-44.

Lange, Hans-Jürgen, 1998, Sicherheitskooperationen und Sicherheitsnetzwerke in der eingreifenden Verwaltung – Zum Verhältnis von Polizei und Ordnungsverwaltung, in: Klaus Lenk, Rainer Prätorius (Hrsg.), Eingriffsstaat und öffentliche Sicherheit, Beiträge zur Rückbesinnung auf hoheitliche Verwaltung, Baden-Baden, 82-93.

Lenk, Klaus, 2006, Öffentliche Risikovorsorge und gesellschaftliche Sicherheitsbedürfnisse als Gegenstand der Politik. Vortrag bei der Fachkonferenz des Deutschen Städte- und Gemeindebundes und der Alcatel SEL Stiftung „Sicherheitskommunikation für Städte und Gemeinden, 31.5.2006, Berlin.

Oberwittler, Dietrich, 2003, Die Entwicklung von Kriminalität und Kriminalitätsfurcht in Deutschland – Konsequenzen für die Kriminalprävention, in: Deutsche Zeitschrift für Kommunalwissenschaften I, 31-52.

Oc, Taner und Tiesdell, Steven, 2000, Urban design approaches to safer city centers: the fortress, the panoptic, the regulatory and the animated, in: J.R. Gold, G. Revill (eds.), Landscapes of Defense, Upper Saddle River: Prentice Hall, 188-208.

O'Connell, Pamela, 2005, Korea's High-Tech Utopia, Where Everything Is Observed, New York Times, 05.10.2005.

Petermann, Thomas und Sauter, Arnold, 2002, Biometrische Identifikationssysteme, Sachstandsbericht, Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), Arbeitsbericht Nr. 76.

Rötzer, Florian, 2004, Insel der Überwachung, Telepolis, 2.6.2004, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=17451&mode=print, 9.5.2005.

Rötzer, Florian, 2005, Politiker fordern mehr Überwachung zur Verhinderung von Terror, Telepolis, 11.7.2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20490&mode=print, 26.8.2005.

Savitch, H. V., 2005, An Anatomy of Urban Terror: Lessons from Jerusalem and Elsewhere, Urban Studies 42(3), March, 361-395.

Schiffhauer, Nils, 2004, Hinter dem Spiegel geht's weiter, in: GIT Sicherheit + Management 12, 12-13.

Schütz, Holger und Peters, Hans Peter, 2002, Risiken aus der Perspektive von Wissenschaft, Medien und Öffentlichkeit, Aus Politik und Zeitgeschichte, B10/11, 2002, 40-45.

Siebel, Walter und Wehrheim, Jan, 2003, Sicherheit und urbane Öffentlichkeit, in: Deutsche Zeitschrift für Kommunalwissenschaften I, 11-30.

SOREON Research, 2004, Biometriemarkt in Deutschland 2004-2009.

Stegemann, Thorsten, 2005, Auf der Suche nach der Stadt der Zukunft, Telepolis, 19.10.2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=21143&mode=print, 4.11.2005.

Streck, Ralf, 2005a, Eingangsverbote statt Ausgangssperre, Telepolis, 9.8.2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20689&mode=print, 26.8.2005.

Streck, Ralf, 2005b, Volle Überwachung in Frankreich, Telepolis, 27.10.2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=21229&mode=print, 4.11.2005.

Virilio, Paul, 2004, Die überbelichtete Stadt, Aus Politik und Zeitgeschichte, B44, 3-4.

Weber, Wolfgang, 2004, Die neue Sicherheitsarchitektur Deutschlands – Neue Strategie von Bund und Ländern zum Schutz der Bevölkerung. Vortrag anlässlich der Fachkonferenz des DStGB „Mehr Sicherheit für lebenswerte Städte und Gemeinden“ am 4.03.2004 in Mainz.

Wehrheim, Jan, 2002, Die überwachte Stadt. Sicherheit, Segregation und Ausgrenzung, Opladen: Leske + Budrich.

Wehrheim, Jan, 2004, Städte im Blickpunkt Innerer Sicherheit, Aus Politik und Zeitgeschichte, B44, 21-27.

Winsemann, Bettina, 2005, Alles, was noch krauchen kann, muss persönlich ins Stadion, Telepolis, 22.10.2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=21189&mode=print, 4.11.2005.

Bisher erschienene manu:scripte

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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