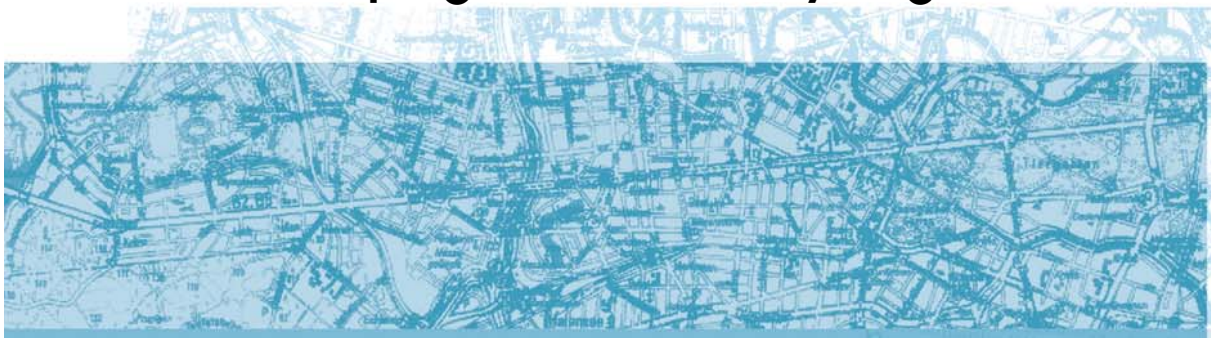
Can Technology Keep Us Safe?

New Security Systems, Technological-Organizational Convergence, Developing Urban Security Regimes



Holger Floeting

Deutsches Institut für Urbanistik

Difu-Papers

February 2007

Contents

Abstract

The terrorist attacks in New York, Madrid and London have made central, local authorities and the public acutely aware that urban agglomerations, with their high-rise office blocks, concentrated mixed-use and residential areas and major technological infrastructures, are particularly vulnerable to this type of threat. Although this is not the first time towns and cities have had to face such dangers, the number of terrorist attacks has increased significantly since the 1990s. Real and suspected threats are not confined to catastrophic incidents affecting world metropolises and megalopolises; they also include every-day crime. Security systems using information and communication technology (e.g. video surveillance, biometrics and radio frequency identification) have the potential to avert these dangers, minimize their impact or, at the very least, reinforce crime fighting efforts. However, many are concerned about the Orwellian nature of such technologies and the social exclusion they may cause. Despite a current lack of integrated urban security policies with dedicated security resources, new urban security regimes are developing to meet specific threats. Urban policy-makers and councils must assess the potential benefits and risks of ICT-supported security technology impartially and on the basis of hard facts. This Difu paper[1] will contribute to the debate by defining urban security as a public responsibility, describing promising ICT-supported security technologies and technological-organizational convergence in an urban setting, and by sketching the future of city life under new security regimes.

Keywords: Security, Urban Policy, Video Surveillance, Biometrics, RFID

1. Changing Conditions – Time for New Approaches?

1.1 New threats?

Following the terrorist attacks in the United States on 11 September 2001 and the subsequent attacks in Madrid and London, the public is more aware than ever that towns and cities, with their densely built-up areas and sophisticated infrastructures, are extremely vulnerable.

A quick glance around the world to Latin America, Asia or the Middle East shows that the terrorist threat to towns and cities is by no means a recent development. Urban Europe has itself long been subject to attacks from groups such as ETA[2] and the IRA[3]. Since the 1990s, however, terrorist attacks on urban areas have been on the increase (Savitch 2005) and will continue to be an issue in the future. Yet,

1 The paper is based largely on Floeting 2006.
2 Euskadi Ta Askatasuna.
3 Irish Republican Army.

whether real or suspected, threats to the urban fibre are not confined to mass attacks aimed at „global cities“ and megalopolises; the worries commence with everyday crime.

Urban security is the subject of increasing public debate, which often leads to the assumption that towns and cities are unsafe per se.

A number of myths must be dispelled. For example, „the fear of crime is influenced less by the 'objective' crime rate than by problematic social situations in residential areas.“ (Oberwittler 2003, p. 31). Nevertheless, around 40% of Germans fear a sharp rise in crime rates and are concerned by increased vandalism (around 30%), graffiti (20% of West Germans and 29% of East Germans) and begging (18% of west Germans and 21% of east Germans) (Opaschowski 2005, cited in Stegemann 2005). No one disputes the fact that in some urban areas security, once taken for granted „as a by-product“ (e.g. platform staff at train stations, bus and train conductors etc.), has fallen victim to staff cuts and must now be painstakingly „repurchased“. Thus, the increase in private security services[4] cannot be attributed exclusively to declining safety levels in urban areas. „To at least some extent, this figure is due to a statistical manipulation related to increased outsourcing“ (Siebel/Wehrheim 2003, p. 24) and to „security as a by-product“ having been curtailed. Even the use of security technologies cannot automatically be interpreted as a reaction to growing urban insecurity. „Nor can any conclusions about surveillance in cities be drawn from [increased] sales of CCTV[5] systems. […] Cameras are often simply used to regulate traffic flow“ (ibid.).

In a fictional speech on the 10th anniversary of the September 11 attacks, Richard A. Clarke – until 2003 the U.S. National Coordinator for Security, Infrastructure Protection and Counter-terrorism – depicted a terrorist threat to cities that would demand security measures extending far beyond anything we have experienced thus far. Not only the critical infrastructure was at risk, he explained, but also casinos, theme parks, hotels, shopping malls, etc. (Clarke 2005). If there is no such thing as total security, then just how much protection can be guaranteed, how much must we and can we afford and how great a risk are we willing to take?

4 Since the 1990s the number of people working for private security providers in Germany has risen by 50% to around 145,000 (v. Landenberg 2004).

5 Closed circuit television.

1.2 New approaches to improved safety?

Until now, academic debate has rarely explored the interplay of domestic security and urban development. The sparse discussions of the issue have focused on the historical perspective[6]. Experts, the public and the media assess threats to security very differently. Even expertises are inconsistent[7]. Tailoring precautionary measures requires precise, objective risk assessments.

Security plans – not just for terrorist threats – primarily focus on so-called critical infrastructures. These include „organizations and facilities of key importance to the urban community whose destruction or impairment would result in long-term supply bottlenecks, considerable disturbances to public safety or other dramatic consequences“ (DStGB 2006, p. 6). In Germany they are categorized as follows: energy supply; drinking water supply; food; health services; telecommunication and information technology; passenger and freight systems; handling of hazardous materials; finance and insurance; administrative bodies and public authorities; other fields, such as protection of cultural heritage, landmark buildings, major research facilities, media etc. Since these infrastructures are mutually dependent, damage to any one of them would significantly affect every aspect of urban life – power cuts amply illustrate this interconnection. Restructuring in recent years, including continuing internationalization of networks (e.g. energy and telecommunications), privatization and partition of state infrastructure (e.g. passenger and freight systems) and increasing dependence on information technology, has necessitated inclusion of new players and a general overhaul of existing security plans.

Locally, security policy is seen „as a matter for higher government authorities and international defence alliances“ (Lenk 2006, p. 1). Although risks and threats clearly affect people at a local level and,

6 Traditionally, „organized [...] politically motivated violence targeting urban areas, their populations and supply systems has been persistently neglected in critical academic debates about cities and urbanization“ (Graham 2004: p. 58). „Since the Second World War“ contemporary urban research has had a tendency „to avoid broaching the subject, because the notion of destroyed cities directly conflicts with optimistic images of progress, order and modernization“ (ibid., p. 59).

7 „Dangers which the public find most frightening and shocking are not necessarily those which (statistically speaking) cause the most deaths. […] In many instances, public alarm over dangers does not reflect scientific risk assessment. […] Often, it is impossible to find any definitive scientific assessment of a given risk“ (Schütz/Peters 2002, p. 40).

more importantly, are felt locally („crime hotspots", „critical infrastructure", „no-go areas" are just three terms which highlight the local relevance of security issues), we still do not have a comprehensive local security policy. Currently, responsibility for local risk management „as a whole does not fall under overall municipal policy" and „is relegated to the various departments: emergency medicine, fire fighting, police" (ibid.). Even cautious analysts would say that local risk control, measured against the local fallout of global risks and threats, does not yet seem „particularly mobilized" (ibid.).

Dealing with threats demands realistic assessment, prevention – insofar as this is possible – and concerted action when damage occurs. Increasingly, this can only be achieved by cooperation among the departments. The wider the damage, the more apparent this need becomes. Even minor disasters require a considerable amount of coordination, and a collaborative approach to prevention makes sense.

Security technologies can increasingly be applied to every phase of danger and damage control. Although their potential is rated highly, their actual use is „widely unplanned, due to vague conjecture about the usefulness of particular technologies" (ibid.).

So far, little has been said about the relationship between employing security technologies, assuring domestic security and urban planning. At the same time, it would appear that more diffuse threats increase willingness to resort to technological solutions. In his fictional speech, Clarke says that „smart" video surveillance cameras are to be installed „throughout public areas", that all video monitoring will be linked „to a central emergency management site where police officers and sophisticated software programs could track suspicious activity on main traffic arteries" and that „security identity cards" would be needed to use local public transport (Clarke 2005).

2. Security as a Public Task

2.1 Duties and responsibilities

A key task of government is „protecting the public from dangers which cannot be averted individually" (Weber 2004, p. 1) and „guaranteeing security and public order" (DST 2004, p. 1). In Germany, the police are the principle guardians of law and order. They are supported by other enforcement agencies. Civil defence in Germany is structured hierarchically; the federal government and Länder work together. Civil defence is a national responsibility, while the states handle disaster control. Germany's civil defence relies largely on a safety and rescue system provided by honorary and voluntary organizations (volunteer fire brigades, the Deutsche Lebens-Rettungs-Gesellschaft e.V., German Red Cross, the Arbeiter-Samariter-Bund, etc.). In particular, local governments in Germany are entrusted with ensuring law and order. „When city walls became redundant, external security [...] ceased to be a municipal responsibility, and since the Munich police force, the last to be re-established after the Second World War, was nationalized in 1975 (Lange 1998, p. 83), internal security has also been a federal and Land obligation" (v. Kodolitsch 2003, p. 5). Municipal security focuses are:

- risk prevention (granting and withdrawing pub/restaurant/amusement arcade licences etc., establishing prohibited zones, monitoring immigrant organizations etc., sheltering the homeless, imposing curfews, protecting minors and restricting the right of assembly),
- urban development measures (establishing use criteria, preventing emergence of architectural no-go areas etc.) and
- designing social, youth, family, housing, education, culture, employment and other policies to support crime prevention.

Security and preventative measures as tasks in themselves are only slowly entering discussions in these areas[8].

It was not until the early 1990s that municipalities recognized security as an interdepartmental responsibility and developed integrated approaches, generally grouped under the heading „local crime prevention" (cf. DST 2004, p. 2 ff.). New local security tools (ibid.) include:

- public order and security partnerships between police and the municipality: they aim to curb the tendency to „place responsibility for security exclusively with the police and public order with the city" (DST 2004, p. 2),
- crime prevention councils to integrate citizen involvement and contribute to developing neighbourhood solutions,
- municipal security services to assume security duties which, due to cutbacks in state budgets, can no longer be performed by the police or which are no longer provided by local depart-

8 „The impact [of these areas] on security and crime prevention was, with the exception of a few departments, not the explicit aim of local government practice, and was often not even recognized as a side effect of the actual function performed." (v. Kodolitsch 2003, p. 6)

ments (e.g. Inspection duties traditionally carried out by parking attendants, conductors etc.).

Urban areas are increasingly depicted as crime zones and debates are often fuelled by a growing fear of crime rather than being founded on actual crime rates. The security situation in Germany's conurbations is, however, „far less critical than in most other cities in Europe and the world" (DST 2004, p. 1). Yet within metropolitan regions, there are „clear signs that our security systems must be refined and extended" (ibid.) to meet emerging demands. Concerns include:

- organized crime and corruption,
- new security issues in areas with negative demographic trends,
- growing citizen expectations in the sphere of public order and general risk protection (ibid.).

Additionally, debates on urban security are focusing more on terrorist threats. Metropolitan regions are at their most vulnerable when staging major events or developing existing infrastructures.

2.2 Changes in the security architecture

German federal security policy has been restructred considerably since 2001. The line between internal and external security has become blurred; risks and threats can no longer be unequivocally categorized as one or the other. Players active in the two fields rely increasingly on cooperation to solve new security problems[9]. The German federal government and the Länder have formulated a joint New Strategy for Civil Protection in exceedingly threatening situations which emphasizes collaboration within the security community. It harmonizes the existing resources of the federal government, Länder, municipalities and relief organizations, and develops new coordination instruments.

The perceived deterioration of the security situation has made citizens more willing to accept restrictions to their personal freedom. For instance, 90% of British citizens endorse video surveillance of public places, 44% of Germans feel antiterrorist security precautions are insufficient, and more than 60% would like to see the German armed forces deployed for law enforcement and border protection duties (Allensbach survey, cf. BPB 2004, p. 2). In German cities internal security measures influence different spheres and constitute new security regimes. Measures include legislation (amending security and public order acts, threat protection regulations), organizational intervention (replacing informal arrangements with government agencies or private enterprise) and symbolic alterations to the cityscape (closing off certain areas, enhancing visibility, beautification) (Wehrheim 2004). Technology upgrades are essential to inner security in cities.

3. Is Security Technology the Solution?

Security technology can facilitate risk avoidance and security measures in every phase:

- analysis of dangerous and threatening situations,
- prevention support,
- security situation assessment,
- coordination of disaster management and response activities and
- disaster area rehabilitation.

The security technology sector offers an array of solutions equal to the complex task which are being implemented in municipalities or may be introduced in the future. Commonly praised advantages of security technology include (cf. DStGB 2003, p. 17):

- programmability and configurability, which ensure reliable operation,
- efficiency, thanks to availability, durability, technical efficiency and precision,
- innovativeness,
- high cost-benefit ratio, in particular when incorporating the potential damage averted, lower insurance costs, etc.

The advantages are weighed against misgivings regarding ubiquitous technological surveillance and social exclusion and scepticism towards security promises. Nonetheless, security authorities are willing to resort to technology, particularly when faced with imminent or suspected threats. In most cases this occurs before thorough analysis has been performed or integrated action plans synergizing technology, strategies, concepts and non-technological measures have been devised. Such solutions appear to appease technology users, or at least decision-

9 „Throughout the Cold War internal and external security were separated politically, and, most importantly, by constitutional law following prevailing international security paradigms; today, the far-reaching consequences of the terrorist attacks on 11 September 2001 have led to a confluence of the demands on both branches of government security policy. […] Current threat and vulnerability analyses and the short, mid and long-term measures which result from them must be pursued in a concerted effort by threat prevention organs, i.e. intelligence services, police authorities, state civil defence and armed forces." (Weber 2004: p. 2)

makers, who are at least able to demonstrate the ability to react in critical situations, and technology providers who „portray an immature technological application as a panacea“ (Lenk 2006, p. 2).

The security market is booming. In the United States the Department of Homeland Security alone has a budget of roughly $40 billion. The German federal government, Länder and municipalities spend approximately 30 billion euros annually on internal security (v. Landenberg 2004). Since the 9/11 attacks „the market for access control and video surveillance systems has tripled“ (ibid., p. 44). In Germany, private security service sales have risen from 1.9 billion euros in the early 1990s to 3.6 billion euros (v. Landenberg 2004). These figures clearly show that the employment of security technologies and urban security restructuring not only involve security considerations, but are also economically motivated.

3.1 Examples of security technology implementation in cities

This section expounds upon only a few examples of new security technology application in municipalities. The cases described below focus on „visible“ front-end applications. They illustrate how commonplace security technologies already are in spheres which do not incontestably fall under „internal security“. Apart from concrete examples, some common areas of application can be identified:

- information systems (for players and residents),
- expert systems (decision support),
- workflow management systems (to facilitate cooperation between a disparate cast of players),
- help systems (for players and citizens),
- monitoring networks (information gathering and early warning),
- GIS applications (spatial analysis and forecasting potential and imminent disasters),
- data mining (to generate detailed profiles),
- augmented reality (to aid decision-makers and their support staff) and
- ubiquitous computing (comprehensive networking).

3.1.1 Video surveillance

The topic of video surveillance is not new to municipalities. It is considered „the most significant innovation for internal security in cities“ (Wehrheim 2004, p. 23) in recent years. Video cameras are widely used to monitor traffic. Video surveillance systems have also become an established component of facility security (for government agencies, stadiums, public transport etc.). For years now video surveillance systems have been used to prevent crime on city streets and in public spaces, e.g. to police drug-related criminality. This development was spearheaded by British municipalities, some of which have proceeded to implement CCTV systems extensively in shopping streets, busy public places and elsewhere so individuals can be traced throughout larger areas of cities.

Surveillance of this sort can be automated with the support of biometric and behavioural characteristics. One possible use would be „filtering out“ people who are considered likely to do property damage (e.g. graffiti tagging) on the basis of route tracking.

Alongside permanent surveillance systems, mobile video surveillance has become more widespread. In Britain „many municipalities […] have introduced CCTV vans equipped with digital cameras and control rooms“ (Hempel 2003). German Länder plan to deploy more mobile surveillance units (e.g. Baden-Württemberg and Bavaria).

Video surveillance was first allowed in Germany after 2000 as a result of Länder police law amendments. There has been no attempt to establish a nationwide surveillance scheme like the one in the UK. Cities argue that video surveillance activities should be restricted to crime hotspots. Surveillance can complement other crime prevention measures, but is not a substitute for them (DST 2004, p. 5). The number of permanently installed video cameras is estimated at 500,000. Video surveillance has only been used sporadically to monitor crime in German cities. For the most part crime-ridden areas were observed with two to three cameras (Wehrheim 2004, p. 23). The London terror attacks, the train bombs found in North Rhine-Westphalia and daily reports of vandalism and violence on public transport and in public spaces in general have spurred further debate on substantially broadening the scale of video surveillance.

Because constant surveillance of public places often leads to profound invasions of personal privacy (the right to one's own image, the right to informational self-determination) its implementation is limited; private monitoring of public spaces is restricted, time limits have been set for data storage, the use of hidden cameras is prohibited and notices of surveillance activities must be posted. Nonetheless, there continue to be grey areas, infringements and inconsistencies which have incited public debate on video

surveillance[10]. The use of surveillance data in borderline cases continues to be a hot topic[11].

Video surveillance data analysis has proven particularly effective in solving crimes. It is used more and more to identify offenders (e.g. following the attacks in the London Underground, in combatting ordinary crimes, vandalism etc.). A wide range of opinions have been expressed regarding how effectively video surveillance deters crime. Its preventive impact in high crime areas is commonly mentioned as a positive outcome along with its provision of evidence for criminal prosecution. Measurable crime reduction in areas monitored with CCTV is sometimes offset by increased crime rates in other areas, the so-called displacement effect.

The scale of surveillance has expanded significantly in recent years and will continue to grow in the midterm. In addition to the proliferation of cameras in public spaces, various surveillance techniques are being networked, and private und public security measures are being coordinated, e.g. to create security alliances (cf. Hempel 2003).

3.1.2 Biometric access systems

Using biometric identification in counterterrorism has been discussed frequently in recent years. The debate centres on integrating biometric data in identification documents and using biometric traits for identification and access control. The number of operational biometric ID systems in Europe has skyrocketed from around 8,500 (1996) to over 150,000 (2004) (European Commission Joint Research Center – JRC, cf. Horvath 2005). The biometrics industry is expected to grow considerably. Unfortunately, no official revenue or employment statistics are kept for this sector. It is difficult to distinguish exactly what proportion of security technology implements biometrics, and the companies involved tend to have prohibitive information policies (cf. Petermann/ Sauter 2002, p. 6). We must therefore rely on market studies conducted by interest groups and private institutions. These studies indicate that sales in the biometrics sector will soar from $600 million (2002) to $4 billion (2007). Biometric technologies are considered „the most important IT innovations in the near future“ (BITE 2005). In 2004 the entire biometrics market in Germany was estimated at 12 million euros. Large federal government contracts are expected to push market volume to 377 million euros by 2009 (SOREON 2004, cf. http://www.heise.de/newsticker/meldung/48560). Despite the stated reservations, the figures suggest that the market is indeed still maturing. As is often the case when new technologies are first introduced, revenue forecasts are very optimistic. It is also evident that large government contracts have been driving the market.

Biometric systems tested to date use facial recognition, fingerprinting and iris scans:

- Facial recognition systems analyze specific facial features from a scanned image. The individual traits analyzed are used to create a biometric signature. Two and three-dimensional facial recognition systems are available.
- Finger printing systems generate individual fingerprint images. Various types of sensors are employed (pressure, ultrasonic, optical, thermal, electric and capacitive[12]). The image is used to detect characteristic peculiarities (arches, loops and whorls) which are compared with existing data.
- Iris recognition systems illuminate the eyes of the person being identified with infrared light to create a high-resolution, near-infrared image which is then examined for specific features (corona, depressions, muscle fibres, pigment spots, scars, radial furrows, striations). Idiosyncratic traits are then used to generate an iris code which is compared to records in a database.
- Forensics identify people using DNA characteristics[13].

An array of unsolved problems remains. Some individuals cannot be detected with fingerprint and iris recognition because their traits cannot be recognized or are not sufficiently distinctive. With age, recogni-

10 Some instances involving municipalities include the video surveillance of a men's changing room at a public swimming pool in Freiburg („Videoüberwachung überraschend gestoppt“ [Video Surveillance Unexpectedly Halted]), *Badische Zeitung*, 8 November 2003) and the video monitoring of waste collection areas as part of the campaign „Unser sauberes Braunschweig“ (Keeping Our Braunschweig Tidy), Braunschweig im Putzwahn (Braunschweig in a Cleaning Frenzy), *taz Nord*, 15 March 2004.

11 One example is the German Border Patrol/German Federal Police's use of the Deutsche Bahn AG's video surveillance system in and around train stations (Bundesdatenschutzbeauftragter [Federal Commissioner for Data Protection] 2005, p. 63).

12 Capacitive sensors use conductor plates (capacitor) which measure the flow of DC currents between the surface of the capacitor and the finger (dielectric) to generate greyscale images. This can sometimes be used to chart the characteristics of living skin underneath the external layer, reducing the distorting effects of injuries and similar inconsistencies on biometric measurements (cf. Petermann/Sauter 2002, p. 25).

13 Deoxyribonucleic acid is a nucleic acid stored in cell nuclei which forms a double helix and contains the genetic instructions for biological development.

tion methods become less reliable and some occupations (e.g. jobs in which finger injuries are common) hamper biometric recognition. Moreover, conditions at the time of recognition (e.g. lighting during facial scanning) can interfere with the system. Lastly, these systems are feared to have too many security loopholes, e.g. fingerprint recognition (Bundesdatenschutzbeauftragter 2005, p. 47 f.). In addition, no bioethical frame of reference has been established for the development and use of biometric technologies. Discussions on the acceptability of biometric technologies have focused mainly on cost-benefit aspects and security issues (BITE 2005).

The notion that such access systems are only employed in high security areas and at border control points is erroneous, as the entry system for Hanover Zoo season ticket holders illustrates. People wishing to subscribe to the zoo must first supply personal information which is recorded in a ticketing system. A digital photo is taken and saved the first time the ticket holder visits the zoo. Digital photographs are taken before entry on every subsequent visit and are compared with the stored data. Visitors may only enter after they have been positively identified. When requesting family tickets, purchasers must provide proof of familial relation (child benefit book, official family records, official ID, health insurance card). With more than 71,000 season ticket holders, this represents the largest application of biometric identification in Germany's service sector (DStGB 2003, Glitza 2004, Schiffhauer 2004). The first attempt to use biometric characteristics, in this case fingerprints, had failed because the system was thought unsanitary and had a poor child identification rate. In addition, the system was not waterproof (cf. Glitza 2004, Schiffhauer 2004). Municipalities could install biometric entry systems in places like museums and sports venues. Numerous other applications in the realm of security are conceivable.

3.1.3 RFID

Radio frequency identification (RFID) is microchip technology which enables contact-free data transfer. RFID systems include an antenna, a transceiver, a transponder and radio frequency technology. They can be employed to:

- recognize objects,
- authenticate documents and commercial goods
- optimize processes, i.e. automate logistics,
- support access control and track vehicles and
- monitor the environment etc.

Transponder systems are not entirely new. They have been used to identify animals for around 20 years; transponders are either injected or implanted as ear tags. Initially, these systems were only used extensively for livestock, they are now used for pets as well. Due to significant advances in silicon chip technology and radio transmission, and especially due to the improved integration of the two, RFID has become a focus of public debate. It is superior to other technologies employed for similar purposes:

- It offers a much broader range of features for access control technology than standard smart card and magnetic stripe systems. Non-contact data transmission is user-friendlier (no waiting periods, active registration process etc.).
- In the logistics field, bulk processing can replace the time and labour consuming individual registration of goods. This improves operational efficiency and increases resource utilization rates. RFID also has security advantages (e.g. asset tracking).
- Branches with high security requirements and extensive verification procedures benefit most from cost reduction (e.g. logistics and waste management companies).
- Businesses with self-contained supply chains (e.g. retailers) also expect to profit from this technology. In flow structures of this sort RFID transponders, which are still relatively costly, can be used repeatedly and continually. Retail giants Metro, Wal-Mart and Tesco were among the first to adopt RFID technology. The Metro Group's Future Store initiative in Rheinberg in North Rhine-Westphalia tests new technologies for use in retail sales. One plan is to replace individual barcode scanning at checkout with electronic bulk scanning while the goods are still in the shopping cart. The scanned data is stored in a mainframe computer. Individual links in the value-added chain (manufacturers, distributors, purchasing departments, warehouses) are networked with the central computer and have access to the database. Customer cards incorporating RFID transponders may be integrated into the system. The ultimate goal is to replace barcodes with RFID transponders (BSI 2004, p. 85 f.).

Cities are applying RFID technology to an ever greater degree. RFID applications already abound in public transport. Because about a fifth of ticket costs are spent to manage ticket sales, radio frequency identification is appealing to transit companies. Adopting this technology is expected to lower costs and improve transport operations. Germany's first smart-card project on public transport was launched

in Cologne in the early 1990s; the first project with contact-free cards was introduced in the mid-1990s (Cap 2005).

RFID applications are used in healthcare to clearly attribute medical information to patients. For instance, a Saarbrücken medical centre provides patients with RFID bracelets. RFID transponders will soon track blood supplies. Transponders are attached to blood bags when they arrive at the hospital and are programmed with a number which is linked to a database containing detailed information on the origin of blood donations and instructions regarding their intended use. PDAs[14] and readers enable hospital staff to retrieve the data from the RFID transponder and compare it to the data in the patient's wristband. The data is simultaneously incorporated in the centre's process work flow system and the patient's file[15].

Facility managers can use RFID to register supplies and maintain inventory. For example, the Berliner Wasserbetriebe are implementing RFID technology to supervise their facilities. The Wasserbetriebe's approximately 60,000 assets at 250 locations in Berlin and Brandenburg are being equipped with RFID transponders. Information can be downloaded to mobile data readers and is automatically recorded in the inventory system[16].

RFID can also facilitate municipal utilities. Waste management companies in the districts Hof, Erlangen-Höchstadt, Mühldorf am Inn, Kehlheim am Inn and Heiligenstadt mark their refuse containers with RFID transponders, each with an individual identification code. The arrangement provides information on waste pickup sites and container size. Waste disposal vehicles are equipped with readers. Rubbish collection is automatically recorded on a smart card in a computer installed in the vehicle. Following pickup, the data can be itemized and used in invoicing. Weighing systems on the vehicles assist in calculating the exact amount of rubbish collected and determining individual waste disposal fees (BSI 2004, p. 70).

RFID systems in Munich Public Libraries allow visitors to self-issue books and media. By 2009 Munich Public Libraries' freely accessible collection consisting of 3.15 million holdings will be equipped with RFID tags. Users can borrow library materials at self-service stations. Automated book depositories in the lobby and outside make it possible to return borrowed items when the libraries are closed. Data stored on RFID transponders is transmitted to the main system and library accounts are automatically updated. Sorting equipment built into the book return machines and a desktop interface which recognizes RFID technology assist in issuing and sorting items. Security gates at the exits equipped with detectors warn when materials which have not been issued are being taken from the library[17].

A major worry regarding RFID technology is that personal data may be manipulated because the processing stages lack transparency. Some systems allow data access from metres away. Both RFID and readers can be inconspicuously embedded in everyday objects. Data protection concerns are reinforced by awareness that „identifying individuals, including linking this technology with video cameras, […] has already been tested on the market" (Bundesdatenschutzbeauftragter 2005, p. 46). A number of everyday viability issues remain[18].

RFID chips continue to make inroads. On April Fools' Day in 2004 the computer magazine c't could still joke that RFID chips were being embedded in number plates – a year later Britain did just that. To encumber forgery of officially issued plates, authorities began tagging them with RFID chips. Tagging also made it possible to record movement patterns, a bonus – or drawback – depending on the perspective[19]. Another example of extensive use of RFID technologies is New Songdo, a city in South Korea 40 miles southwest of Seoul. This real-estate development scheme is conceived as a free trade area which will accommodate 65,000 inhabitants and 300,000 workers; English will be the lingua franca and various international currencies will be accepted[20]. The developers plan to network the prin-

14 Personal digital assistant, small, hand-held computer.

15 „Erster Deutscher Kongress für Patientensicherheit, Bundesweites Medienecho" (Nationwide Media Coverage of the First German Patient Safety Convention), http://www.klinikum-saarbruecken.de/kliniknews/index.php3?tid=256&a=NEWS, 13 November 2006.

16 „Berliner Wasserbetriebe now using RFID to help manage facilities", http://www.esg.de/en/press/pressreleases/?tid=755, 13 November 2006.

17 „Bücher aus dem Automat" (Books from a Machine), *Süddeutsche Zeitung*, 12 January 2006.

18 At the Confederations Cup in Germany in 2005 many fans had pinned their tickets to pin boards, destroying the RFID chips in their tickets and complicating the admission process. A warning not to bend tickets was printed on the tickets, but no one planned on fans posting their tickets on pin boards (cf. WM-Tickets bitte nicht knicken (Please Do Not Bend Your World Cup Tickets), http://www.heise.de/newsticker/meldung/61251, 31 August 2005).

19 „Briten testen funkende Autokennzeichen" (The British Test Electronic Number Plates), *Spiegel Online*, 11 August 2005, http://www.spiegel.de/netzwelt/technologie/0,1518,369248,00.html, 26 August 2005.

20 The developers provide a detailed description at http://www.new-songdocity.co.kr/, 7 November 2005.

cipal information systems, allowing seamless data exchange. Data protection issues are practically ignored; backers appear to have no misgivings whatsoever about the prospect of creating an „Orwellian state". The project is predominantly viewed as an opportunity to demonstrate technological prowess and to attract foreign investors (O'Connell 2005)[21].

3.2 Technical-organizational convergence of security technologies

New security technologies can be utilized in a variety of ways in urban areas. The combination of a range of technologies, such as video surveillance, biometric profiling and non-contact data transfer is enabling the development of complex identification, entry and surveillance systems. These can control access to and use of certain areas (city centres, local public transport, embassies, ministries, government agencies etc.) and larger parts of a city. Convergent technology systems like these are already in place.

Economic changes (e.g. the fall in the price of computer memory) and technological developments (e.g. higher capacity storage media) are making it easier to manage data. Storing information without specific justification or purpose is becoming an increasingly popular precautionary measure (particularly in security circles). It is also maintained that the public is more inclined to allow their personal data to be filed, possibly as a trade-off for heightened security. On the basis of this assumption, there have been efforts from some quarters to facilitate the process of gaining ex post access to data which was originally gathered for different purposes. The debate on using road toll data to combat crime and terrorism demonstrates the issues at hand. The gradual spread of the practice of using data retroactively for objectives other than those originally intended is one of the main reasons for public opposition to storing personal data in any form.

On the one hand, we must take full advantage of all technologies which can be employed to contain threats. On the other hand, the growing practice of collecting personal data and information that can be traced back to individuals within their particular urban setting and the possibility to link this data will take surveillance to a whole new level. Organizational as well as technical convergence has a particular role to play in this domain. The opportunity to link data, combined with factors such as the increased overlapping of internal and external security countermeasures and a desire to assess the situation comprehensively based on the available facts, will make it possible to develop ever more detailed profiles of individuals. Without wanting to dramatize the situation by conjuring an image of the „transparent citizen", technical-organizational convergence will make it easier than ever to obtain details on private citizens. Closer integration of technical and organizational resources will also increase the danger of data being misappropriated at a later date.

4. Urban Life under Changing Security Conditions

The use of information and communication security technologies involves dangers and potential benefits which must be considered and weighed up. Surveillance technology, for example, has preventative potential as it lowers the detection threshold (e.g. of minor violations and crimes) and of potentially dangerous situations. The subsequent growth in intelligence on particular security matters could theoretically enable early intervention. Empirical findings however, taking the situation as a whole into account, demonstrate that the potential of these technologies is not being exploited and cannot be exploited[22]. On the other hand, there is a danger that surveillance which is focused too heavily on certain areas will lead to exclusion or crime displacement.

The implementation of ICT security technologies can improve a city's accessibility if, for example, permanent security measures such as fences, security margins and protection devices are replaced by technological control systems and temporary measures. However, these technologies can also reduce the accessibility of certain city areas if that is the purpose of the system or if its implementation targets certain social groups too heavily (cf. Graham 2005).

It is always difficult to assess the impact of a technology. Security technology, too, can only be properly judged once in a specific application. The grow-

21 Examples of possible applications are: „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; cell phones that store health records and can be used to pay for prescriptions" (O'Connell 2005).

22 „In 2002, the British Home Office published its findings from an evaluation of 22 rigorous surveys on the impact of video surveillance in the U.S and the U.K. […] According to the report, the number of cars stolen and broken into fell by 40 percent, pickpocketing, however, went down by only two to four percent and there was barely any change in the level of violent crime." (Wehrheim 2004, p. 24)

ing use of security technologies must be considered in the context of real and perceived threats and the security regime which has been set up to counter them[23].

The changing nature of the threat, the increasing use of security technology in particular parts of the city and the growing significance of security issues for city life could have a variety of repercussions. These include a fundamental shift in the image of cities, the long-term transformation of urban architecture and space and adjustments in the use of urban sites.

The public may increasingly view cities as unsafe places, giving rise to a new type of „urban fear". Cities are comparatively „unmanageable areas" and are therefore suspected of harbouring every type of security threat: from „common criminals" to terrorists planning attacks. These fears are already being voiced in international urban studies literature[24]. Are we reverting back to fortified cities and easily controllable Hausmannian boulevards? Will the electronic portal become the new barricade in the information and communication technology age? (cf. Virilio 2004)

A growing or lasting threat could lead to cities becoming more heavily „armed" through the step-by-step introduction of security measures, security technologies and architectural features which promote safety. First, authorities and the public begin to pay more attention to what is happening around them, thus creating a kind of informal surveillance system. Then security technology is upgraded and regulations controlling activities in public places are tightened. Fences, barricades and gates are constructed and an „architecture of fortification" begins to distort the face of the city[25]. In security circles, this is referred to as „target hardening" (Oc/Tiesdell 2000). Even private cars are becoming citadels. This includes not only „armouring" the body of the car[26] but, in keeping with the current security trend, also equipping it with information and communication technology systems[27].

Supposed „archipelagos of safety" such as shopping malls, train stations, central squares, business improvement districts and gated communities could proliferate (cf. Wehrheim 2002)[28], leading to the categorization of urban spaces according to their level of security. Polarization would result with areas viewed either as safe or unsafe. A further factor to be considered here is the existence of „undefined areas" which are becoming increasingly common as a result of demographic developments, gradual technological changes and economic restructuring. Due to their frequent recycling, these areas could also be labelled as unsafe. „Ethnic profiling" is one tool used to prevent attacks, particularly when previous attacks can be attributed to certain ethnic groups (cf. Savitch 2005). As a result, neighbourhoods predominantly populated by a particular ethnic group become a target for security services. Security consciousness could intensify the debate on the threat posed by so-called parallel societies, created by the spatial concentration of one particular ethnic group, and mobilize support for methods such as restricting settling for specific groups in certain districts. Suburban areas, on the other hand, are considered to be relatively secure[29]. However, if we are to take stock in

23 „The way in which surveillance is used more and more in locations which originally had nothing to do with the „Big Brother" phenomenon, but have infrastructures which lend themselves well to the implementation of surveillance technologies, is alarming." (Rötzer 2004)

24 „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, p. 362)

25 Oc and Tiesdell developed the concept of a step-by-step fortification of the city and defined these steps as animated presence, panoptic devices, regulatory measures, fortress construction (Oc/Tiesdell 2000).

26 The hummer, tried and tested during the Golf War, is not the only car designed to withstand all. The Ford SYNUS, based on the Fiesta model, also has a tough design: („Fords Tresor-Auto. Es muss nicht immer Hummer sein" [Ford's mean machine. It Doesn't Have to Be a Hummer]), *Manager-Magazin*, 17 January 2005).

27 The Volvo S80, for example, comes with a „Personal Car Communicator", enabling drivers to check whether their car is secure by remote control. This function not only tells the driver if the car is locked and the alarm is activated. Using a heartbeat sensor, it can also detect if there is someone in the car: „100 Prozent Angst" [100 Percent Fear]), *Handelsblatt,* 29 March 2006).

28 A literal „island of safety" is being constructed on the 62-acre Ayers Island in Maine. The island's owners plan to transform it into an „intelligent island with sensors monitoring the entire area including the buildings in order to detect 'suspicious behaviour'" (Rötzer 2004). Another example of an attempt to create small pockets of security is a project in the East London district of Shoreditch. 20,000 residents are able to receive images from local CCTV cameras via their cabel connection enabling them to spot people behaving suspiciously and anonymously report their activities to the police. Residents are aided in their identification of suspicious characters by a „rogues gallery" („ASBO-TV helps residents watch out" *The Sunday Times*, 8 January 2006).

29 „Many of the more secure places resemble the protected spaces of suburban malls as well as lower-

Clarke's previously cited fictional speech, this haven will probably become a thing of the past (cf. Clarke 2005).

„Control zones" or „security zones" could be constructed on boundaries of undesirable neighbourhoods[30]. Large cities could develop an island system made up of overlapping milieus (localized poverty milieus, the working, leisure and residential areas of the various lifestyle groups and the milieu of cosmopolitan, highly skilled workers) who strive to control and minimize contact with each other (cf. Wehrheim 2004, p. 26). „Security zones" around „institutions under threat" may be expanded to residential buildings[31]. Depending on the level of security required, temporary entrance restrictions may be imposed on particular parts of a city, combined with technological surveillance of these areas. Measures temporarily restricting access are already in use. These range from police orders (declaring an area off limits to certain individuals) and constructing barricades at events to longer-term entry bans for specific areas[32]. Technological surveillance will considerably extend the feasibility of such entry restrictions.

The growing use of technological surveillance could transform the nature of public space, ultimately resulting in the loss of certain spaces and the merging of public and private spheres. Some fear, for example, that public spaces could become „elite consumer enclaves governed by private law" (cf. Hamedinger 2005).

Urban security regimes could have an impact on infrastructure planning. It may be considered necessary, for example, to change the design of entrance areas to public transport (as has already been done to some extent in airports) and limit transfers between the different carriers. The development of screening corridors equipped with explosive detectors or sensors which can remotely recognize hidden explosives will revolutionize existing transport infrastructure[33]. In the final analysis, we have to consider the possibility that the infrastructure of major airports and train stations with adjoining shopping centres and office complexes may simply be too vast to ensure security. For security reasons, it may make sense to decentralize facilities. This could entail the disintegration of shopping and transport facilities (e.g. at airports or train stations) and the introduction of size limitations or the concentration of these facilities (depending on what is more suitable for control measures).

Security considerations may strongly influence town planning – at least at vulnerable locations. This would significantly change the face of city centres where such sites are concentrated (e.g. Berlin or Frankfurt am Main)[34].

The solution could be implementing a comprehensive security plan. By looking at London we can see where this development would take us. IRA attacks in the City at the beginning of the 1990s prompted construction of a „ring of steel", like Belfast's. The number of entry points to the financial district were reduced and road blocks were erected, making it possible to temporarily cordon off the area if necessary. Thousands of video cameras were installed, security plans were devised for financial institutions and they were advised to limit the number of entrance points to each building. Buildings were fitted with more security technology and back-up premises

density, suburban housing complexes" (Savitch 2005, p. 383).

30 For example, the draft of the new French anti-terror law provides for automated surveillance of car number plates and their occupants in „high risk" zones. The chief of police has the powers to order the installation of cameras in a particular area if there is „founded evidence of suspicious activity" without a court order (Streck 2005b).

31 For example, the security zone surrounding a diplomat's house in Vienna (cf. Jänicke 2004).

32 The entry ban imposed on the Madrid's Colonia Marconi de Villaverde to combat prostitution is a particularly extreme example of this type of restriction. This area can only be entered between 11 p.m. and 6 a.m. with a pass. A total of 3,000 passes have been issued (Streck 2005a).

33 „To make such a measure truly effective, walkthrough detectors would need to be installed and staffed at every entrance, as is already the case in airports. Aside from the cost this would incur, it would inevitably cause severe commuting disruption. Ensuing long queues are also ideal targets for potential attackers, as has been demonstrated clearly in Iraq (Rötzer 2005). London underground is said to be planning „to test several passive millimetre wave scanners to allay public fears. These devices are able to see through passenger's clothes and detect concealed objects" (ibid.).

34 The reconstruction work on Ground Zero in New York illustrates with particular clarity how security considerations can affect architectural design. The Freedom Tower will meet security requirements which go far beyond normal building security standards. „The square base will be constructed of impermeable concrete and titanium steel [...] one metre thick and clad in shimmering metalwork [...] the bottom ten metres of the tower will have no windows at all". The design responds „to fears of car or lorry bombings. Police security experts insisted on the tower being constructed according to the standards required for federal buildings such as American embassies or the Pentagon. In addition to this, it was stipulated that the tower be at least 30 metres away from the next public thoroughfare. There are, of course, chemical and biological filters, elaborate fire precautions, extra wide steps, a network of interconnected exits and specially protected lifts" (Böhnel 2005).

of the original sites were created for an emergency. Police patrols increased significantly (cf. Coaffee 2003).

Changing security conditions also have implications for the organization of mass gatherings, which have become a favourite tool of modern urban planners in their endeavours to market public space. For example, growing security demands have led to the increasing use of personalized tickets, which can prove extremely inconvenient for the eventgoer. Extensive security measures (road blocks, flyover bans etc.) can also disable large parts of a city.

The relationship between material and virtual space could change permanently. The „space of flows" (Castells 1989) could expand significantly. Partly unnoticed, data from everyday activities could be generated, selected and stored. Numerous new links between the expanded „space of flows" and material space could emerge. One example is the spread of data-based admission controls at events (with personalized tickets), for border crossing (with machine-readable ID which automatically detects biometric characteristics) and for security zones (in public and private buildings). The technological developments behind this trend range from individual and isolated applications to complete sustainable networks. The catchwords in this discussion are „augmented reality", „ubiquitous computing", „pervasive computing" and „ambient intelligence".

Ultimately, these feelings of insecurity could lead to a relocation of certain activities to cyber space, at least in the short term. For example, Clarke's fictional speech describes the growing number of Internet shoppers following attacks on shopping malls (Clarke 2005).

Finally, in view of their shrinking financial means, one must ask how cities will be able to respond to increase investment in security infrastructures[35]. There is a danger that architectural, technological and regulatory security measures in cities will successfully combat the threat of attacks, but, in doing so, will impair urban living spaces and disrupt city life, thereby achieving one of the terrorists' objectives.

5. Conclusion

The public debate on using technology to improve urban security has provoked a very polarized response from decision-makers as well as city residents: security technology is either demonized or uncritically espoused as the solution to all the security challenges facing the city. Up until now, the potential benefits and risks of security technology have hardly ever been evaluated in specific contexts. Instead of deciding whether to implement security technology on the basis of vague speculation about its virtues, we should conduct more empirical research into the specific effects of individual security technologies and their collective impact in their interfaces. Conversely, to achieve this, we must refrain from automatically condemning every move to introduce security technology as an attempt to establish a „totalitarian State". We should continue to explore the risks associated with these technologies – assuming that this dialogue has indeed begun, a point which itself is open to debate – in order to obtain a more balanced assessment of the situation. Nobody disputes the fact that we are working towards a common goal: to make our cities safer. What must still be debated is how much security we need and how best to achieve it. The crux is not the implementation of technology itself, but how to combine it with a security plan which addresses the social origins of crime. Prevention should not be reduced to intervening to stop „disruptive" behaviour when it occurs, but focus on schemes which aim to nip these behavioural patterns in the bud.

In the future, security looms as a vital issue for cities and their residents. Urban security regimes are developing – more in response to events and ad hoc security demands than as well thought-out, integrative programmes. Urban impact analyses are also necessary to mould this blossoming security regime into an integrated local security policy in the medium term. These analyses should not only resolve urgent issues, i.e. how to manage dangerous and threatening situations and disasters, but must also assess the long-term impact of internal security measures on urban life. These issues must be addressed by town planning and technological impact researchers, as well as city residents, technology users and developers. Studying the development of security technologies and urban security regimes is therefore a central task of modern urban technology management.

35 Equipping the underground with passive millimetre-wave scanners would cost „up to three million euros per station" for the machines alone (Rötzer 2005).

Bibliography

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

Bone, Max (2005): Hochsicherheitsklotz statt Freiheitsturm, in: Telepolis, 6 July 2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20459&mode=print, 26 August 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, slides from the „Smart Cards, Smart Labels, Smart Devices" lecture, Chair for Information and Communication Services, University of Rostock, http://www.iuk.informatik.uni-rostock.de/sites/lehre/lehrveranstaltungen/vl_smartx/rfid-applications.pdf, 9 May 2005.

Castells, M. (1989): The Informational City. Information Technology, Information Restructuring and the Urban Regional Process, Oxford/Cambridge, MA.

Clarke, Richard A. (2005): Zehn Jahre danach (Originally published in English under the title „Ten Years Later".) Vortragsmanuskript zum zehnten Jahrestag des 11. September 2001, in: Frankfurter Allgemeine Sonntagszeitung, 6 March 2005.

Coaffee, Jon (2003): Terrorism, Risk and the City: the making of a contemporary urban landscape, Aldershot.

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

DST – Deutscher Städtetag (2004): Positionspapier Sicherheit und Ordnung in der Stadt.

DStGB – Deutscher Städte- und Gemeindebund (2003): Kommune schafft Sicherheit. Trends und Konzepte kommunaler Sicherheitsvorsorge. Editorial supplement „Stadt und Gemeinde interaktiv", vol. 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, editorial supplement „Stadt und Gemeinde interaktiv", no. 5.

Floeting, Holger (2006): Sicherheitstechnologien und neue urbane Sicherheitsregimes, Institut für Technikfolgenabschätzung, Österreichische Akademie der Wissenschaften, ITAmanu:script, Wien.

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 October 2005, pp. 562-580.

Graham, Stephen (2004): Postmortem City. Plädoyer für eine Geopolitik des Urbanen, in: Informationen zur modernen Stadtgeschichte (IMS), no. 2, pp. 54-71.

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

Hempel, Leon (2003): Verdrängen statt Vorbeugen, in: Telepolis, 15 January 2003, http://www.heise.de/tp/r4/artikel/13/13928/1.html, 9 May 2005.

Horvath, John (2005): Prepare to be scanned, in: Telepolis, 2 August 2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20635&mode=print, 13 November 2006.

Jänicke, Ekkehard (2004): Sicherheitszone für US-Bürger in Wien, in: Telepolis, 15 August 2004, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?mode=html&artikelnr=18121, 9 May 2005.

v. Kodolitsch, Paul (2003): Einführung: Sicherheit in der Stadt, in: Deutsche Zeitschrift für Kommunalwissenschaften (DfK), no. I, pp. 5-10.

v. Landenberg, Markus (2004): Mit Sicherheit mehr Jobs, in: Stern Spezial „Campus & Karriere", 1 October 2004, pp. 42-44.

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

Lenk, Klaus (2006): Öffentliche Risikovorsorge und gesellschaftliche Sicherheitsbedürfnisse als Gegenstand der Politik. Lecture given at the German Association of Towns and Cities and the Alcatel SEL Foundation symposium on „Municipal Security Communication Systems", 31 May 2006, Berlin.

Oberwittler, Dietrich (2003): Die Entwicklung von Kriminalität und Kriminalitätsfurcht in Deutschland – Konsequenzen für die Kriminalprävention, in: Deutsche Zeitschrift für Kommunalwissenschaften, no. I, pp. 31-52.

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

O'Connell, Pamela (2005): Korea's High-Tech Utopia. Where Everything Is Observed, in: New York Times, 5 October 2005.

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

Rötzer, Florian (2005): Politiker fordern mehr Überwachung zur Verhinderung von Terror, in: Telepolis, 11 May 2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20490&mode=print, 26 August 2005.

Rötzer, Florian (2004): Insel der Überwachung, in: Telepolis, 2 June 2004, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=17451&mode=print, 9 May 2005.

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

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

Schütz, Holger, and Hans Peter Peters (2002): Risiken aus der Perspektive von Wissenschaft, Medien und Öffentlichkeit, in: Aus Politik und Zeitgeschichte, no. B 10/11, pp. 40-45.

Siebel, Walter, and Jan Wehrheim (2003): Sicherheit und urbane Öffentlichkeit, in: Deutsche Zeitschrift für Kommunalwissenschaften (DfK), vol. I, pp. 11-30.

SOREON Research (2004): The Biometrics Market in Germany 2004-2009.

Stegemann, Thorsten (2005): Auf der Suche nach der Stadt der Zukunft, in: Telepolis, 19 October 2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=21143&mode=print, 4 November 2005.

Streck, Ralf (2005a): Eingangsverbote statt Ausgangssperre, in: Telepolis, 9 August 2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20689&mode=print, 26 August 2005.

Streck, Ralf (2005b): Volle Überwachung in Frankreich, in: Telepolis, 27 October 2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=21229&mode=print, 4 November 2005.

Virilio, Paul (2004): Die überbelichtete Stadt, in: Aus Politik und Zeitgeschichte, no. B 44, pp. 3-4.

Weber, Wolfgang (2004): Die neue Sicherheitsarchitektur Deutschlands – Neue Strategie von Bund und Ländern zum Schutz der Bevölkerung. Lecture given at the German Association of Towns and Cities symposium on „Improving security to make our municipalities better places to live in", 4 March 2004 in Mainz.

Wehrheim, Jan (2004): Städte im Blickpunkt Innerer Sicherheit, in: Aus Politik und Zeitgeschichte, no. B 44, pp. 21-27.

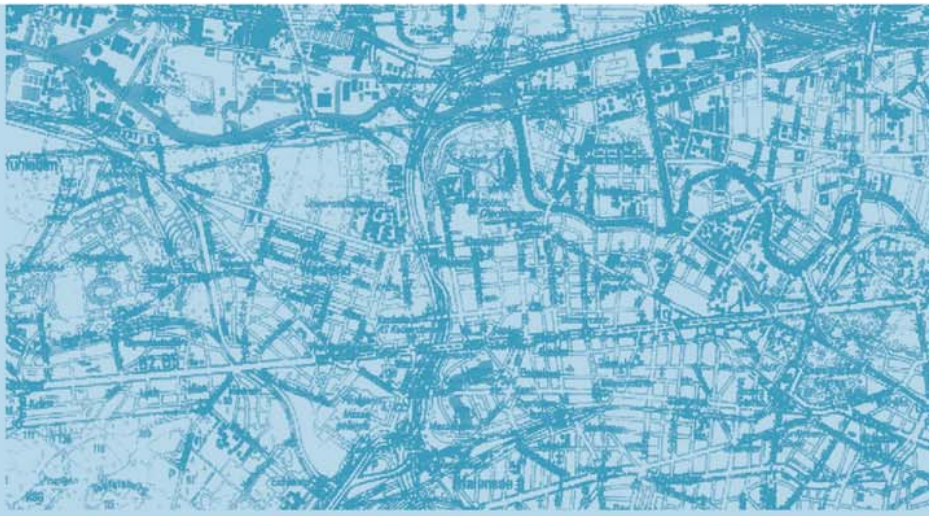
Wehrheim, Jan (2002): Die überwachte Stadt. Sicherheit, Segregation und Ausgrenzung, Opladen.

Winsemann, Bettina (2005): Alles, was noch krauchen kann, muss persönlich ins Stadion, in: Telepolis, 22 October 2005, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=21189&mode=print, 4 November 2005.

Zusammenfassung

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. Informations- und Kommunikationstechnik 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. Dieses Difu-Paper möchte zu diesem Thema einen Beitrag leisten, indem es städtische Sicherheit als öffentliche Aufgabe beschreibt, beispielhaft IuK-gestützte Sicherheitstechniken sowie die technologischen und organisatorischen Konvergenzprozesse im urbanen Anwendungskontext beschreibt und mögliche städtische Zukünfte unter veränderten städtischen Sicherheitsregimes skizziert.

Schlagwörter: Sicherheit, Stadtpolitik, Videoüberwachung, Biometrie, RFID



Citation/Zitierweise: Holger Floeting: **Can Technology Keep Us Safe?** New Security Systems, Technological-Organizational Convergence, Developing Urban Security Regimes, Berlin 2007 (Difu-Paper)

Published by/Herausgeber:
Deutsches Institut für Urbanistik (German Institute of Urban Affairs)
Straße des 17. Juni 110 • 10623 Berlin
Phone/Telefon: +49(0)30/39001-0, Fax/Telefax: +49(0)30/39001-100
E-Mail: difu@difu.de • Internet: http://www.difu.de

Author/Autor: Dipl.-Geogr. Holger Floeting
Editor/Redaktion: Patrick Diekelmann
DTP: Christina Blödorn

ISSN 1864-2853