3. Sicherheitsgewinn mit technologischen Innovationen (Schwerpunkt ITK)

J. Menno Harms

Ein Dialog über die sozialen Aspekte von Sicherheitstechnologien ist längst überfällig. Es gibt kaum eine Technologie, deren soziale Dimension nicht bereits an berufener Stelle diskutiert würde – ganz gleich, ob es um Biotechnologie, Gentechnik oder Energietechnik geht. Intelligente Sicherheitstechnologien greifen tief in unsere Gesellschaft, Wirtschaft und Privatsphäre ein. Sie bieten zwar enorme Chancen, doch mit der Digitalisierung wird auch vieles sichtbar, was vormals verborgen blieb. Digitale Fingerprints auf dem Personalausweis oder die elektronische Gesundheitskarte geben zwar mehr Sicherheit, sie sorgen aber auch für mehr Transparenz und einen Verlust an Privatheit. Ein Beispiel dafür sind die sogenannten »Nacktscanner«. Sie bringen mehr Sicherheit, aber auch mehr Transparenz – im wahrsten Sinne des Wortes! Die EU und die für ihre Toleranz bekannten Niederlande haben sich für den mit dieser Technologie verbundenen Sicherheitsgewinn entschieden. Die Bundesregierung dagegen favorisiert Privatheit gegenüber Transparenz. Das Spannungsverhältnis zwischen öffentlicher Sicherheit einerseits und privater Entfaltungsfreiheit wird durch moderne Sicherheitstechnologien ganz neu definiert. Es entstehen neue Fragen, auf die Antworten gefunden werden müssen.

Wie können Sicherheit und Freiheit zusammengedacht werden? Welche Rolle kann Spitzentechnologie dabei spielen? Und wie kann der Staat diese Spitzentechnologie einschlägig fördern? Die Frage nach Sicherheit in der digitalen Welt verweist zumeist auf komplexe Systeme. Ein Beispiel sind Logistiksysteme, die praktisch jedes Gut in kürzester Zeit an jeden beliebigen Ort der Erde bringen können. Neben modernen Transportmitteln leisten hier Informations- und Kommunikationssysteme einen wichtigen Beitrag. Sie stellen die notwendigen Daten für das *handling* vor Ort zeitgerecht und sicher zur Verfügung und ermöglichen das Zusammenspiel weltweit verteilter Logistikzentren und Verkehrsmittel. So

kann der Versender des Frachtstücks heute jederzeit und unabhängig von seinem eigenen Standort in Echtzeit den Status seiner Sendung nachvollziehen. Hochkomplexe und automatisierte Strukturen – auch im Verkehr, in der Energiewirtschaft oder im Gesundheitswesen – haben allerdings ein gemeinsames Problem: Jede noch so kleine Störung kann bei fehlender Robustheit der betroffenen Infrastruktur massive Beeinträchtigungen nach sich ziehen. Zwar ist das Internet per definitionem weniger anfällig, doch wurde es durch massive »Cyber-Attacken« in Estland 2007 und in Georgien 2009 zu großen Teilen stillgelegt. Die Situation ist zwiespältig: Hochtechnologie stellt ein wesentliches Element öffentlicher Sicherheit dar, führt aber gleichzeitig zu neuer Unsicherheit. Diese ›Janusköpfigkeit‹ technischer Lösungen erfordert, dass zeitgleich beide Seiten des ›Doppelkopfes‹ – die Chancen und Risiken technischer Lösungen betrachtet werden. Eine hundertprozentige Sicherheit gibt es auch in der digitalen Welt nicht. Wo immer Menschen mit technischen Systemen arbeiten, können durch fehlerhafte Nutzung, durch Unachtsamkeit oder Vorsatz, Gefahren entstehen. Fehlerquellen können aber auch systemimmanent vorliegen, zum Beispiel wenn zwei quasi-fehlerfreie Systeme im Zusammenwirken ein nicht vorhersehbares Verhalten erzeugen.

Im November 2006 kam es zu einem Stromausfall, der von Deutschland bis nach Spanien reichte. Das Kreuzfahrtschiff »Norwegian Pearl« wurde von der Meyer-Werft im niedersächsischen Emsland an die Küste überführt. Dafür wurde eine Hochspannungsleitung abgeschaltet, unter der das Schiff hindurchfahren sollte.

Die dabei entstehende Überlast führte zu einer prinzipiell richtigen Konsequenz: dem Abschalten eines überlasteten Teilnetzes. Nicht geplant war jedoch, dass dadurch die Energienetze in halb Europa kaskadenartig ausfielen. Intelligente Energienetze hätten dies verhindern können.

Der Branchenverband BITKOM begrüßt die Absicht der Bundesregierung, mit dem »Forschungsprogramm zur zivilen Sicherheit« über den technischen Tellerrand hinauszublicken und interdisziplinäre Ansätze zu verfolgen. Den Leitlinien, an denen das Programm ausgerichtet wird, wird zugestimmt.

Wesentlich ist *erstens*, dass eine ressortübergreifende Zusammenarbeit bei den Forschungsvorhaben der einzelnen Bundesministerien und nachgeordneten Behörden gestärkt wird. Die bislang teils stark fragmentierten Forschungsvorhaben des Bundes können so deutlich produktiver gestaltet werden.

Zweitens: Bei all den technischen Problemen, die in den einzelnen Vorhaben der Sicherheitsforschung zu lösen sind, dürfen die Menschen, ihre Bedürfnisse, ihr Verhalten und ihre Ängste nicht vergessen werden. Auf den griechischen Philosophen Epiktet geht der Aphorismus zurück »Nicht Tatsachen, sondern Meinungen über Tatsachen bestimmen das Zusammenleben«. Die Bedeutung der subjektiven und gesellschaftlichen Wahrnehmung von Technologien gilt es durch vertrauensvolle Aufklärung zu berücksichtigen. Daher sind neben Natur- und Ingenieurwissen-

schaften auch sozial- und geisteswissenschaftliche Erkenntnisse einzubeziehen. Dies kann an Beispielen verdeutlicht werden. Für die Evakuierung eines Flughafens im Notfall sind Lautsprecheranlagen, Fluchtwegkennzeichnungen und beste technische Ausstattung der Rettungskräfte absolut notwendig. Sie sind aber nicht hinreichend. Ein Sicherheitskonzept wird erst dann greifen, wenn die technischen Anlagen auf der Grundlage verhaltenspsychologischer Erkenntnisse errichtet werden und somit die Rettungskräfte zielgerichtet unterstützen können. Ein weiteres Beispiel sind vorbeugende Sicherheitstechnologien wie Videoüberwachung und Zutrittskontrollen durch Biometrie. Die zuverlässige Arbeit dieser Systeme hängt von ihrer Akzeptanz und einem Mindestmaß an Kooperation der Nutzer ab. Eine automatisierte Zutrittskontrolle mit Gesichtserkennung funktioniert beispielsweise nicht, wenn jemand mit einem Sturzhelm durch die Anlage geht.

Drittens müssen Forschungsvorhaben auch auf die Anforderungen der Endnutzer sowie auf zukünftige Marktchancen ausgerichtet werden. Insbesondere müssen Rettungskräfte und ihre Organisationen wie Feuerwehr, Polizei und Technisches Hilfswerk frühzeitig in die Forschungsvorhaben einbezogen werden. Hinzu kommt die notwendige Abschätzung des jeweiligen Kosten-Nutzen-Verhältnisses. Sicherheitstechnologien können sich – zunächst getrieben durch staatliche Nachfrage – zu massentauglichen Lösungen entwickeln. Dazu muss aber für die breite Bevölkerung ein konkreter Nutzen erkennbar sein. Im Zoo Hannover erfolgt beispielsweise die Zutrittskontrolle von Dauerkartenbesitzern mittels Biometrie. In vielen Unternehmen werden die Passwörter am PC per Stimmerkennung zurückgesetzt. Es gibt bereits Supermarktkassen, an denen per Fingerabdruck bezahlt werden kann. Weitere Praxisbeispiele für den Biometrie-Einsatz finden sich in der Biometrie-Referenzbroschüre von BITKOM.[1] Der endgültige Durchbruch der Biometrie als breit eingesetzte Sicherheitstechnologie ist bald zu erwarten. Daraus resultieren gute Aussichten für die vielen, zumeist noch jungen deutschen Unternehmen in diesem Anwendungsfeld. Die neuen Reisepässe enthalten bereits biometrische Gesichtsdaten und Fingerabdrücke. Wenn diese schnell lesbaren Biometriedaten bei Grenzkontrollen zum Einsatz kommen, kann eine beschleunigte Abfertigung viel zur Akzeptanz der Technologie beitragen.

Viertens und letztens gilt es, die europäische Zusammenarbeit zu stärken und damit internationale Forschungsallianzen voranzubringen. Zivile Sicherheit lässt sich heute – weniger denn je – im nationalen Kontext betreiben.

Wichtige Beiträge zur Gewährleistung von Sicherheit sind mit Hilfe der ITK-Technologien zu leisten; vier Haupteinsatzgebiete der ITK-Technologien sind zu unterscheiden:

1 | Siehe BITKOM (Hg.), Biometrie. Referenzprojekte, 2. Auflage, Berlin 2009.

1. Die Erfassung und Weiterleitung relevanter Daten durch Sensoren, Scanner und Bildanalyse;
2. Die Verdichtung, Auswertung und Präsentation von Informationen, etwa zur Visualisierung von Lage-Informationen in Gebäuden;
3. Die Unterstützung bei der Risikobewertung und –entscheidung; Weiterleitung an Rettungskräfte;
4. Die Unterstützung präventiver Maßnahmen, etwa bei umfangreichen Risiko-Simulationen.

Ihre Bedeutung lässt sich wiederum am Beispiel der Flughäfen verdeutlichen, die wie Tunnel, Häfen und Bahnhöfe zu den kritischen Verkehrsinfrastrukturen gehören und ein besonders hohes Sicherheitsniveau verlangen. In den vergangenen 30 Jahren haben terroristische Aktivitäten schrittweise zu einer Verschärfung der Sicherheitsauflagen und zu einem intensiven Einsatz von Sicherheitstechnologien im Luftverkehr geführt. Im Zuge der spektakulären Flugzeugentführungen der 1970er Jahre wurden drastische Passagier- und Gepäckkontrollen eingeführt. Seit dem Bombenanschlag auf den PAN AM Jumbo Jet im Jahr 1988 wird abgeglichen, ob zu jedem eingeladenen Gepäckstück tatsächlich der richtige Passagier eingestiegen ist. Dieses so genannte *baggage reconciliation* ist nur durch ITK-Technologien schnell und effizient möglich. Seit den Anschlägen auf das World Trade Center 2001 müssen alle Gepäckstücke auch auf Explosivstoffe untersucht werden. Diese Bilanz liest sich wie eine Liste des Schreckens. Gleichwohl sagt die Statistik, dass das Flugzeug noch immer eines der sichersten Transportmittel ist und Fliegen nie so sicher war wie heute. Und die Herausforderungen wachsen. Der Boom der Luftverkehrsbranche mit weltweit knapp fünf Milliarden Reisenden im Jahr 2007 wird weitergehen und mit ihm potenzieren sich die Anforderungen an die Sicherheitstechnologien. Trotz der Sicherheitsauflagen bei gleichzeitig stark gestiegenen Passagierzahlen soll das Reiseerlebnis des einzelnen Passagiers insgesamt positiv bleiben. Die unangenehmen Eingriffe in die Privatsphäre an den Kontrollstellen sollen einerseits ein für die Passagiere erträgliches Maß nicht überschreiten. Andererseits müssen Fluggesellschaften, Flughäfen und Behörden mit einem vertretbaren Aufwand für das notwendige Sicherheitsniveau sorgen. Die zivile Sicherheitsforschung soll zur Erfüllung dieser Anforderungen signifikant beitragen.

In der Vergangenheit wurde in erster Linie auf Bedrohungen reagiert. In Zukunft kann die zivile Sicherheitsforschung helfen, proaktiv zu handeln und Bedrohungspotenziale zu antizipieren. Die Technologieentwicklung zeigt bereits erste Ergebnisse. Systeme zum schnellen und präzisen Aufspüren gefährlicher Gegenstände und Explosivstoffe werden kontinuierlich verbessert. Kamerasysteme sind flächendeckend im Einsatz. Durch sie kann das Sicherheitspersonal herrenlose Gepäckstücke und kritische Situationen erfassen. Intelligente Software wertet alle zur Verfügung stehenden Kameras automatisch aus, entdeckt Gefahrensituationen und meldet sie. Ohne den Einsatz leistungsfähiger ITK-Systeme

sind solche Innovationen in der zivilen Sicherheit nicht denkbar. Damit die Sicherheitstechnologien der ITK wirksam werden können, brauchen sie aber eine breite Akzeptanz. Im Luftverkehr haben sich die Passagiere mit den Sicherheitsregelungen arrangiert und diese akzeptiert. Ähnliches gilt für die passive und aktive Sicherheit von PKWs, die in den vergangenen 50 Jahren massiv weiterentwickelt wurde. Erfolgte die Anschnallpflicht in den 1970er Jahren noch gegen den Widerstand vieler Autofahrer, sind heute Seitenaufprallschutz, Airbag, ABS und Elektronisches Stabilitätsprogramm bewusst nachgefragte Sicherheitsfunktionen. Die Zahl der Verkehrstoten ging zwischen 1970 und 2007 von 21.300 auf weniger als 5.000 zurück.

Während beim Flug- und Autoverkehr kaum Widerstand gegen Sicherheitstechnologien zu beobachten ist, entzünden sich immer wieder Diskussionen um die Akzeptanz von Informations- und Telekommunikationssicherheitstechnologien. Soll alles technisch Machbare tatsächlich umgesetzt werden? Hier gilt es genau abzuwägen – und gelegentlich die Bürger zu fragen. So hat BITKOM in diesem Jahr eine repräsentative Umfrage zur Kameraüberwachung öffentlicher Plätze in Auftrag gegeben. Das Ergebnis zeigt, dass eine große Mehrheit der Bundesbürger eine stärkere Video-Überwachung öffentlicher Plätze befürwortet. Drei von vier Befragten gaben an, sie seien für mehr Kameraüberwachung. 20 % lehnten eine stärkere Überwachung öffentlicher Plätze ab. Ein anderes Beispiel ist die elektronische Gesundheitskarte. Sie wird von 96 % oftmals als technikskeptisch eingeschätzten Bevölkerung begrüßt. Dieses Ergebnis ist überraschend, da auf der Gesundheitskarte hoch sensible Daten gespeichert werden.

Zuweilen scheint die Bevölkerung ihren Vordenkern in Politik, Wissenschaft und Presse einen Schritt voraus zu sein. Das sollte bei aller Notwendigkeit der Risikoabwägung neuer Technologien nicht vergessen werden. Der Spannungsbogen zwischen den Antipoden Sicherheit und Freiheit wird in diesen Jahren gelegentlich überzogen. Das Motto dieser Konferenz – »Mit Sicherheit: für Freiheit« – kann dazu beitragen, Entspannung in dieses Verhältnis zu tragen.