BMBF-Konferenz: „… mit Sicherheit: für Freiheit - die gesellschaftlichen Dimension der Sicherheitsforschung“

Prof. J. Menno Harms, Mitglied des BITKOM-Hauptvorstands
Vortrag: „Sicherheitsgewinn mit technologischen Innovationen (Schwerpunkt ITK)"
Berlin, 5.November 2008 (ca. 13.30 bis 14.00 Uhr)

Sehr verehrte Frau Ministerin Schavan,

Monsieur le Professor Grosser,

meine sehr geehrten Damen und Herren,

zunächst ein herzliches Dankeschön an Sie, Frau Ministerin, dass Sie das Thema „Gesellschaftliche Dimension der Sicherheitsforschung“ auf die Agenda gehoben haben. Es ist längst überfällig, dass wir einen Dialog auch über die sozialen Aspekte von Sicherheitstechnologien beginnen. 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 – und ich spreche nicht über das Verteidigungswesen – 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 wunderbares Beispiel sind die sogenannten „Nacktscanner“. Mehr Sicherheit? Ganz sicher Ja! Aber auch mehr Transparenz? Im wahrsten Sinne! Die EU und zum Beispiel die für ihre Toleranz bekannten Niederländer haben sich hier für mehr Sicherheit entschieden. Die Bundesregierung entschied sich für mehr Privatheit und gegen Transparenz. Das Spannungsverhältnis zwischen öffentlicher Sicherheit einerseits und privater Entfaltungsfreiheit wird durch moderne Sicherheitstechnologien ganz neu definiert. Es entstehen neue Fragen und darauf müssen wir neue, möglichst richtige Antworten finden.

Meine Damen und Herren, im Programm bin ich als Aufsichtsratsvorsitzender der Hewlett-Packard GmbH geführt. Angesprochen wurde ich für diesen Beitrag als langjähriger Vizepräsident und Hauptvorstand des Hightech-Verbandes BITKOM. Aus dessen Perspektive möchte ich heute zu Ihnen sprechen, für die in Deutschland tätige Hightech-Industrie und nicht für ein einzelnes Unternehmen.

Sicherheit und Freiheit. Geht das zusammen? Welche Rolle kann Spitzentechnologie dabei spielen? Und wie kann der Staat diese Spitzentechnologie einschlägig fördern? Wenn wir über Sicherheit in der digitalen Welt sprechen, dann sprechen wir zumeist über komplexe Systeme. Es geht zum Beispiel um 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

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10
10117 Berlin
+49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner:
Lutz Neugebauer
Bereichsleiter Sicherheit
Tel +49. 30. 27576-242
Fax +49. 30. 27576-51-242
l.neugebauer@bitkom.org

Präsident
Prof. Dr. Dr. h.c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer
Dr. Bernhard Rohleder

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 diesem Jahr in Georgien lahmgelegt. Die Situation ist zwiespältig: Hochtechnologie stellt ein wesentliches Element öffentlicher Sicherheit dar, führt aber gleichzeitig zu neuer Unsicherheit. Diese 'Janusköpfigkeit' technischer Lösungen erfordert, dass wir uns zeitgleich mit beiden Seiten des ‚Doppelkopfes' oder - wie die Asiaten sagen - mit TaiChi, mit Chancen und Risiken technischer Lösungen beschäftigen. Hundertprozentige Sicherheit gibt es nicht, auch nicht in der digitalen Welt. Wo immer Menschen mit technischen Systemen arbeiten, können durch fehlerhafte Nutzung – seien es Unachtsamkeit oder Vorsatz – Gefahren entstehen. Auf der anderen Seite können Fehlerquellen auch systemimmanent vorliegen, zum Beispiel wenn zwei quasi-fehlerfreie Systeme im Zusammenwirken ein nicht vorhersehbares Verhalten erzeugen.
Sie erinnern sich vielleicht noch an den Stromausfall im November 2006. Er reichte von Deutschland bis nach Spanien. Was war passiert? Das Kreuzfahrtschiff „Norwegian Pearl" wollte die Meyer-Werft im niedersächsischen Emsland verlassen. 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, dass dadurch die Energienetze in halb Europa kaskadenartig lahmgelegt wurden. Mehr IT-Intelligenz in den Energienetzen hätte dies verhindern können.

Verehrte Frau Ministerin, die Absicht der Bundesregierung, mit dem „Forschungsprogramm zur zivilen Sicherheit" über den technischen Tellerrand hinauszublicken und interdisziplinäre Ansätze zu verfolgen, begrüßen wir sehr. Die Leitlinien, an denen Sie dieses Programm ausrichten, sind aus unserer Sicht genau richtig:

Wesentlich ist erstens, dass eine ressort-übergreifende Zusammenarbeit bei den Forschungsvorhaben der einzelnen Bundesministerien und nachgeordneten Behörden gestärkt wird. Die unseres Erachtens teils stark fragmentierten Forschungsvorhaben des Bundes können so deutlich produktiver ausfallen. Das ist eine sicher nicht einfache Führungsaufgabe, wie ich aus eigener Erfahrung weiß.

Zweitens: Bei all den technischen Problemen, die in den einzelnen Vorhaben der Sicherheitsforschung zu lösen sind, dürfen wir die Menschen, ihre Bedürfnisse, ihr Verhalten und ihre Ängste nicht vergessen. „Nicht Tatsachen beunruhigen die Menschen sondern die Vorstellung von den Tatsachen" soll der Grieche Epiktet bereits gesagt haben. Auch dies gilt es durch vertrauensvolle Aufklärung zu berücksichtigen. Somit sind neben Natur- und Ingenieurwissenschaften auch sozial- und geisteswissenschaftliche Erkenntnisse einzubeziehen. Ein Beispiel macht dies deutlich: „Evakuierung eines Flughafens". Dafür sind Lautsprecheranlagen,

Fluchtwegkennzeichnungen und beste technische Ausstattung der Rettungskräfte absolut notwendig. Aber sie sind eben nicht hinreichend. Das 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 begrüßen wir sehr, die Forschungsvorhaben auch auf die Anforderungen der Endnutzer sowie auf zukünftige Marktchancen auszurichten. Insbesondere müssen Rettungskräfte und ihre Organisationen wie Feuerwehr, Polizei und Technisches Hilfswerk frühzeitig in die Forschungsvorhaben einbezogen werden. Daneben müssen sicher auch die Kosten-Nutzen-Verhältnisse geklärt werden. Sicherheitstechnologien können sich – zunächst getrieben durch staatliche Nachfrage – zu massentauglichen Lösungen entwickeln. Dazu muss aber für die breite Bevölkerung ein konkreter Nutzen erlebbar sein. Im Zoo Hannover funktioniert beispielsweise die Zutrittskontrolle von Dauerkartenbesitzern mittels Biometrie. In vielen Unternehmen werden die Passwörter am PC per Stimmerkennung zurückgesetzt. Es gibt bereits Supermarktkassen, an denen man per Fingerabdruck bezahlen kann. BITKOM hat eine umfangreiche Broschüre veröffentlicht, in der rund 25 Praxisbeispiele für den Biometrie-Einsatz beschrieben werden. Ihr endgültiger Durchbruch als breit eingesetzte Sicherheitstechnologie ist bald zu erwarten. Gute Aussichten auch für die vielen, zumeist noch jungen deutschen Unternehmen dieses Anwendungsfeldes. 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: Wir unterstützen ausdrücklich das Ziel, die europäische Zusammenarbeit zu stärken und damit internationale Forschungsallianzen voranzubringen. Zivile Sicherheit lässt sich heute
- weniger denn je - im nationalen Kontext betreiben.

Meine Damen und Herren, wie können ITK-Technologien zu mehr Sicherheit beitragen? Ihre Haupteinsatzgebiete bei Sicherheitslösungen sind: 1. Erfassung und Weiterleitung relevanter Daten durch Sensoren, Scanner und Bildanalyse. 2. Verdichtung, Auswertung und Präsentation von Informationen, etwa zur Visualisierung von Lage-Informationen in Gebäuden. 3. Unterstützung bei der Risikobewertung und -entscheidung. Weiterleitung an Rettungskräfte. 4. Unterstützung präventiver Maßnahmen, etwa bei umfangreichen Risiko-Simulationen.

Als Beispiel nehmen wir wieder die Flughäfen, die - wie Tunnel, Häfen, Bahnhöfe auch - zu den kritischen Verkehrsinfrastrukturen gehören und ein besonders hohes Schutzniveau 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. Mit den spektakulären Flugzeugentführungen der 70er 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 5 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 für die Passagiere in einem erträglichen Maß liegen. Andererseits müssen Fluggesellschaften, Flughäfen und Behörden mit einem vertretbaren Aufwand für das notwendige Sicherheitsniveau sorgen. Die zivile Sicherheitsforschung muss diese Anforderungen umfassend erfüllen!

Meine Damen und Herren, in der Vergangenheit haben wir auf Bedrohung in erster Linie reagiert.
In Zukunft soll die zivile Sicherheitsforschung helfen, auch proaktiv zu handeln und Bedrohungs-potenziale zu antizipieren. In der Forschung hat man sich bereits auf den Weg gemacht. So werden Systeme zum schnellen und präzisen Aufspüren gefährlicher Gegenstände und Explosivstoffe 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 eine breite Akzeptanz. Im Luftverkehr hat sich der Passagier mit den Sicherheitsregelungen arrangiert und diese akzeptiert. Ähnliches gilt für die passive und aktive Sicherheit von PKW's, die sich in den vergangenen 50 Jahren massiv weiterentwickelt hat. Wurde die Anschnallpflicht in den 70er Jahren noch gegen den Widerstand vieler Autofahrer, eingeführt, sind heute Seitenaufprallschutz, Airbag, ABS und Elektronisches Stabilitätsprogramm bewusst nachgefragte Sicherheitsfunktionen. Die Zahl der Verkehrstoten ging zwischen 1970 und 2007 von 21300 auf weniger als 5000 zurück.

Beim Flug- und Autoverkehr scheint der Fall klar zu sein. Doch gibt es immer wieder Diskussionen um die Akzeptanz von Informations- und Telekommunikationssicher-

heitstechnologien. Sollen wir alles technisch Machbare wirklich einsetzen? 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: Eine große Mehrheit der Bundesbürger befürwortet eine stärkere Video-Überwachung öffentlicher Plätze. 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 Prozent unserer vorgeblich so technik-skeptischen Bevölkerung begrüßt. Und dies, obwohl die Karte die sensibelsten Daten überhaupt enthält.

Zuweilen scheint mir die Bevölkerung ihren Vordenkern in Politik, Wissenschaft und Presse einen Schritt voraus zu sein. Das sollten wir bei aller Notwendigkeit der Risikoabwägung neuer Technologien nicht vergessen.
Sicherheit und Freiheit. Der Spannungsbogen zwischen diesen beiden Antipoden wird in diesen Jahren ganz offensichtlich etwas überzogen. Durch das Motto dieser Konferenz „Mit Sicherheit: für Freiheit“ sollte wieder mehr Entspannung angesagt sein. In diesem Sinne wünsche ich der Veranstaltung viel Erfolg und danke für Ihre Aufmerksamkeit.