

## 10. Europäischer Polizeikongress Berlin – 13. und 14. Februar 2007

Vortrag von Dr. Markus Hellenthal

(Senior Vice President EADS - Global Security, Special Advisor)

### EFFIZIENTE TERRORISMUSBEKÄMPFUNG

#### Eine Frage der Bedrohungswahrnehmung

Ladies and Gentlemen:

Meine sehr geehrten Damen und Herren:

Ich freue mich auch in diesem Jahr über die Gelegenheit zum Gedanken- und Erfahrungsaustausch anlässlich des Europäischen Polizeikongresses, der im Jubiläumsjahr unter dem Leitgedanken steht: 'Die Europäische Sicherheitsstrategie – Konzepte und Technologien gegen Terrorismus'. In meinem Diskussionsbeitrag möchte ich mich mit den Herausforderungen globaler Sicherheitsfragen unter Berücksichtigung einer zunehmend globalisierten Bedrohungswahrnehmung auseinandersetzen.

Meine Damen und Herren:

Die Bundesregierung hat das innenpolitische Arbeitsprogramm ihrer EU-Ratspräsidentschaft unter den Anspruch: „Europa sicher leben“ gestellt. Die anhaltende Bedrohungssituation der westlichen Wertegemeinschaft sowie allgemeine Sicherheitsfragen, die im Zusammenhang mit dem fortdauernden Kampf gegen den internationalen Terrorismus und die organisierte Kriminalität stehen, aber auch die Herangehensweise und etwaige Bewältigung aktueller internationaler Konflikte wurden damit einmal mehr in den Mittelpunkt des Interesses gestellt.

Dies erscheint nicht zuletzt deswegen angebracht, weil sich viele Europäer mehr als anderthalb Jahre nach den vorerst letzten, realisierten Terroranschlägen auf den öffentlichen Personennahverkehr von London in einem Gefühl relativer Ruhe und Sicherheit wähnen. Wie trügerisch und gefährlich diese Fehlperzeption ist, zeigen nicht zuletzt die glücklicherweise gescheiterten Kofferbombenanschläge in Deutschland im August 2006 oder die in London und Birmingham im vergangenen Herbst festgenommenen Selbstmordattentäter. Darüber hinaus lässt sich das Auseinanderfallen von kollektiver Bedrohungswahrnehmung und tatsächlicher Gefahrensituation im Meinungsbild gerade der deutschen Öffentlichkeit aus dem Umstand erklären, „das(s) wir uns“, um mit den Worten von Bundesinnenminister Wolfgang Schäuble zu sprechen, „nicht existentiell betroffen glauben“.

Einerseits lässt ein solch dramatisches Missverhältnis auf eine eher zurückhaltende Bedrohungswahrnehmung schließen, zum anderen ist sie Ausdruck eines Spannungsverhältnisses zwischen Freiheit und Sicherheit, das gerade in Deutschland besonders stark ausgeprägt zu sein scheint. Eine Grundlagenstudie zum Freiheitsverständnis der Deutschen, die durch das Institut für Demoskopie Allensbach durchgeführt wurde, zeigt, dass die Deutschen der Sicherheit zwar einen vergleichsweise hohen Stellenwert zumessen, dennoch wird Sicherheit vorrangig als mit Lasten und

Pflichten verbundene Einschränkung verstanden. Dem entgegen ist Sicherheit jedoch vielmehr die Voraussetzung für Freiheit und anhaltenden Wohlstand und wird in dieser Konnotation von führenden Staatsrechtlern als Vorbedingung aller Grundrechte definiert.

Während die Politik sich allenthalben darauf konzentriert, das Spannungsverhältnis zwischen Freiheit und Sicherheit durch staatliche Intervention unter Kontrolle zu halten, legt die Industrie ihren Unternehmungen ein differenziert positives Sicherheitsverständnis zugrunde. In diesem Zusammenhang steht der Slogan: "*Facilitation Without Compromizing Security*" für eine Grundhaltung, bei der Sicherheitsmaßnahmen neben dem selbstverständlichen Gebot der Wirksamkeit und Nachhaltigkeit zuallererst auf die Ermöglichung bzw. Erleichterung der ihr zugrundeliegenden Aktivität gerichtet sind.

Fünf Jahre nach den Anschlägen auf New York und Washington ist der Terror im Alltagsbild der Europäer angekommen. Zwar ist die Intensität der Bedrohungswahrnehmung bei Amerikanern in allen relevanten Bereichen, mit Ausnahme der globalen Erwärmung, durchweg deutlich höher als bei Europäern; in ihrem Sicherheitsbedürfnis stimmen beide Seiten jedoch grundsätzlich überein. Die nach wie vor akute Gefahrensituation hat sich zu der unausweichlichen Gewissheit verdichtet, dass der internationale Terrorismus, insbesondere der 'Global Jihad' kein auf die Vereinigten Staaten von Amerika und den Mittleren Osten beschränktes Phänomen ist, sondern sich vielmehr gegen die gesamte freie Welt, und damit eben auch gegen Europa richtet. Die Terrorakte in den USA, in Madrid und London, sowie die erst kürzlich vereitelten Anschläge in London und Deutschland haben in ihrer Menschenverachtung der gesamten Weltöffentlichkeit den im wahrsten Sinne des Wortes 'grenzenlosen' Vernichtungswillen der islamistischen Täter und ihrer Anführer vor Augen geführt.

Als ebenso dramatisch haben sich die sicherheitspolitischen, militärischen und völkerrechtlichen Folgen dieser neuen Sicherheitsherausforderungen auf die Weltpolitik und das Verhältnis von Freiheit und innerer Sicherheit erwiesen. Damit ist die Grenze zwischen innerer und äußerer Sicherheit zwar nicht obsolet geworden, es ist jedoch nicht mehr von der Hand zu weisen, dass zivile und militärische Sicherheitsorgane ganz anders miteinander zusammenarbeiten müssen, als dies bislang weithin der Fall war. Das gilt im Übrigen auch für die Zusammenarbeit der Sicherheitsbehörden untereinander, sowohl national wie international. Es gilt aber schließlich auch für einen mehr bedarfsorientierten Umgang mit Technologien, welche die Produktivität der Sicherheitsorgane deutlich erhöhen können, ohne zugleich die Freiheit über Bord zu werfen. Beispiele dafür sind zum einen die Nutzung von Ressourcen, die ansonsten in Diensten des Militärs stehen. Es grenzt schon an Verschwendung von Potentialen, wenn diese im Notfall nicht auch eingesetzt werden, um Schaden zu vermeiden, zu vermindern, oder möglichst schnell wieder einen geordneten Stand zu erreichen. Ein anderes Beispiel sind moderne Kommunikationsmittel und übergreifende Lage- und Einsatzzentralen, in denen alle Sicherheitsbehörden gemeinsam arbeiten können. Ist es wirklich nötig, dass wir in Deutschland über 1.600 Lage- und Einsatzzentralen betreiben, mit all den Sach- und Personalkosten? Mit der nunmehr bevorstehenden Einführung des Digitalfunks in Deutschland wird es auch möglich sein, Lage- und Einsatzzentralen wesentlich effizienter zu strukturieren und ihre Zahl bei gleichzeitiger Produktivitätssteigerung drastisch zu senken.

Sicherheit ist heute mehr denn je globale Herausforderung aller EU Staaten. Mit der zunehmenden Globalisierung, Durchlässigkeit und Vernetzung unserer Gesellschaften wachsen auch die damit einhergehenden Gefahren. Diesen müssen wir adäquat begegnen. Zusätzlich zum vorherrschenden Kampf gegen den Terrorismus, sehen wir uns weiteren, schwerwiegenden Bedrohungen ausgesetzt. Die Europäische Sicherheitsstrategie hat bereits 2003 zutreffenderweise darauf hingewiesen, dass es sich hierbei um 'vernetzte Bedrohungen' handelt, welche aus den Interdependenzen einer mehr und mehr grenzenlosen bzw. entgrenzten Welt resultieren und die Möglichkeiten bzw. Ressourcen eines einzelnen Staates zur adäquaten Gegenwehr übersteigen. Vernetzte Bedrohungen bedürfen kollektiver Anstrengungen und zwingen uns zu struktur- und länderübergreifender Sicherheitskooperation.

Letztendlich besteht unsere größte Herausforderung in Zeiten des "Information Overkill" nicht mehr in der Informationsgewinnung, sondern vielmehr in der Informationsauswertung, sowie der Bereitstellung, dem Austausch und der Weitergabe von Erkenntnissen in Echtzeit. Sie muß nahtlos und umfassend genug sein, um diejenigen, die mit Vorbeugung, Bewältigung und Abschreckung betraut sind, in die Lage zu versetzen, notwendige und angemessene Maßnahmen anhand eines umfassenden und vernetzten Lagebildes, eines sogenannten 'Common Relevant Operational Picture', zu ergreifen. Ob wir uns mit symmetrischen oder asymmetrischen Bedrohungen konfrontiert sehen, die Wirksamkeit und Nachhaltigkeit unserer Maßnahmen hängt ganz wesentlich davon ab, in wie weit wir im Vorfeld einer Risikorealisation hinreichende, präventive Maßnahmen unternommen haben. Wenn das Unvorhersehbare passiert, und wir können sicher sein, dass es passiert, hängt sowohl die Wirksamkeit unserer Abwehrmaßnahmen, als auch die Effizienz unseres Krisenmanagements von unserer Fähigkeit ab, zügig, angemessen und umfassend agieren zu können. Notwendig ist hierzu ein konstant hohes Maß an Aufmerksamkeit und Wachsamkeit der zuständigen polizeilichen Führungsorganisationen sowie die Modernisierung und Verknüpfung bestehender Kommunikationsmittel, welche allen Einsatzkräften: Polizei, Spezialeinheiten, Feuerwehr, Rettungsdienst, Krankenhäuser und falls erforderlich auch Militärverbänden zur Verfügung stehen bzw. diese miteinander koordiniert. Im Verbund mehrerer Maßnahmen trägt das bereits im Dezember 2004 ins Leben gerufene Terrorismusabwehrzentrum in Treptow (GTAZ) diesem nachdrücklichen Erfordernis eines beschleunigten Informationsaustausches und der Stärkung und Zusammenführung unterschiedlicher Analysekompetenzen Rechnung.

Barrierefreie Kommunikationsnetzwerke sowie integrierte grenzüberschreitende Lage- und Einsatzzentralen sind die Basis für jedes Zusammenwirken von inneren und äußeren Sicherheitskräften und damit für eine effektive, umfassende Sicherheit. Die zukunftsgerichtete Sicherheitsarchitektur bedarf der nahtlosen Kommunikation über bestehende geographische und organisatorische Grenzen hinweg. Hierzu müssen sowohl die rechtlichen als auch die operativen Voraussetzungen häufig erst noch geschaffen werden. Zurecht hat sich die laufende EU-Trio-Präsidentschaft der Innen- und Justizminister Deutschlands, Portugals und Sloweniens dem umfassenden Ausbau der europäischen Sicherheitsarchitektur verschrieben. Die aus dem mittelfristigen Arbeitsprogramm hervorgehende Stärkung der europäischen Grenzschutzagentur FRONTEX mit Blick auf die Abschaffung der Kontrollen an den EU-Binnengrenzen zum 31. Dezember 2007; die Verstärkung der grenzüberschreitenden polizeilichen Zusammenarbeit durch die Überführung des Vertrages von Prüm in den EU-Rechtsrahmen; die Befugnisausweitung

von EUROPOL sowie die Einführung des Schengener Informationssystems der 2. Generation sind richtige und dringend erforderliche Weiterentwicklungen.

Damit verbunden ist ein ganzheitlicher Ansatz beim Thema Lagebild und Einsatzführung, damit die Einsatzkräfte vor Ort besser und effektiver eingebunden und unterstützt werden können. Es ist kein Geheimnis mehr, dass effektives Sicherheits- und Krisenmanagement eine zunehmend komplexe Aufgabe darstellen, welche durch die bloße Bereitstellung technologischer Applikationen nicht mehr angemessen bewältigt werden kann. Aus diesem Grund verstehen und positionieren sich traditionelle Technologieanbieter heute über die selbstverständliche Bereitstellung von Hochleistungstechnologien hinaus, vordringlich als langfristiger Sicherheitspartner, der in Anbetracht der spezifischen Bedarfe und in enger Kooperation mit dem Kunden adäquate Fähigkeiten realisieren. Der Systemintegration kommt dabei eine Kernkompetenz zu, denn vernetzte Systemlösungen sind prädestiniert dafür, einen nachhaltigen Sicherheitsmehrwert zu generieren. Die anachronistisch anmutende Sandkastenplanung kann den Herausforderungen strukturübergreifender Sicherheits- bzw. Risikofelder längst nicht mehr gerecht werden. Zurecht richtet sich die Anspruchshaltung des Kunden heute mehr denn je auf umfassende und zugleich flexible Fähigkeiten, die den veränderten Sicherheitsrealitäten ebenso umfassend wie kontinuierlich angepasst werden können. Dem Know-how einer bedarfsbezogenen Konstruktion, Auswertung und Demonstration von Konzepten und Systemen der vernetzten Operationsführung kommt dabei die Bedeutung eines differenzierenden Wettbewerbsfaktors zu. 'Network Centric Operations' kombinieren und verknüpfen Modelle, Simulationen, sowie bedienergesteuerte („Man-in-the-Loop“) reale Systeme in einer künstlichen Umgebung. Was diese Umgebung so innovativ und bedeutsam macht, ist ihre Fähigkeit zur Erstellung virtueller, doch höchst realistischer Bedarfssfelder unter Einbindung eines umfassenden Lage- und Einsatzbildes (Common Relevant Operational Picture) einschließlich aller Führungs- und Informationsnetze. Dadurch wird es möglich, interaktive Szenarien zu erzeugen, um Leistungen und Interoperabilität bestehender und zukünftiger Sicherheitssysteme in vernetzten Systemarchitekturen vorab zu bewerten. Nichtsdestotrotz erweist sich eine abschließende Klassifizierung der Bedarfsbereiche als kompliziert, da die Übergänge zwischen den Segmenten fließend sind und es zudem erforderlich ist, spezifische Grundanforderungen sicherzustellen, welche die gesamte Sicherheitsstruktur betreffen. So diversifiziert die Markteinteilung der einzelnen Sicherheitsanbieter auch sein mag, im wesentlichen lassen sich alle Bemühungen auf den Schutz kritischer Infrastrukturen, den Schutz der Bevölkerung sowie auf die Überwachung und Sicherung der Land-, Luft-, und Seegrenzen zurückführen. Darüber hinaus kommt dem sogenannten Identitätsmanagement eine systemübergreifende, zentrale Funktion zu.

Der Schutz kritischer Infrastrukturen stellt wahrscheinlich die größte Herausforderung dar. Die jüngsten Ereignisse haben uns die Verletzlichkeit unserer westlichen Gesellschaften gegenüber Angriffen auf wichtige Infrastrukturen vor Augen geführt. Hilflos mussten wir mit ansehen, wie Passagierflugzeuge und andere Transportmittel des öffentlichen Personenverkehrs als todbringende Waffen missbraucht wurden. Der Schutz dieser 'neuralgischen Punkte' ist von herausragender Bedeutung für unser Gemeinwesen, denn sie sind im wahrsten Sinne des Wortes überlebenswichtig und daher ebenso schützenswert wie gefährdet. Es fällt schwer, sich das ganze Ausmaß einer etwaigen Beeinträchtigung oder gar Zerstörung der öffentlichen Wasserversorgung, von Öl- bzw. Kerosinraffinerien oder zentraler Verkehrsinfrastrukturen vorzustellen. Nichtsdestotrotz sind diese Bedrohungen real! Verschiedene Staaten haben begonnen, kritische Infrastrukturen zu erfassen oder

planen dies. In Deutschland wird dem Schutz kritischer Infrastrukturen, dies belegen sowohl das KRITIS Programm als auch das darauf aufbauende Basisschutzkonzept, eine herausgehobene Bedeutung zugeschrieben. Eine der wesentlichen Erkenntnisse ist dabei, dass in vielen Fällen kritischen Infrastrukturen in privatem Eigentum liegen, und die Eigner ein lediglich eingeschränktes Interesse haben, die erforderlichen Mittel für notwendige Schutzmassnahmen aufzubringen.

Wesentlicher Aufgabenbereich infrastruktureller Sicherheit, insbesondere im Hinblick auf Flughäfen und industrielle Einrichtungen, besteht in der Einlass-, Zugangs- bzw. Durchgangskontrolle, mit anderen Worten in der Identifikation und Authentifizierung von Personen und Gegenständen. Identitätsmanagement von Menschen, Organisationen und öffentlichen Einrichtungen stellt seit Jahrtausenden eine zentrale Herausforderung für Regierungen bzw. für die betreffenden Sicherheitsorganisationen und Unternehmen dar. In diesem Zusammenhang sind alle europäischen Staaten derzeit bemüht, neue Identitätsdokumente einzuführen. Auch global operierende Unternehmen sehen sich im Zuge einer zunehmend internationalisierten Standardisierung gezwungen, ihre Sicherheitsstrukturen den wachsenden Erfordernissen anzupassen. So nutzt beispielsweise die skandinavische Airline SAS – als erste Fluggesellschaft weltweit – biometrische Daten, um Passagiere und Gepäck zweifelsfrei einander zuordnen zu können. Dafür geben Reisende an schwedischen Flughäfen beim Check-in und am Gate ihren Fingerabdruck ab. Das beschleunigt den Abfertigungsvorgang und garantiert zudem, dass dieselbe Person, die ein Gepäckstück aufgegeben hat, auch tatsächlich an Bord der Maschine geht.

Auch hinsichtlich der Einführung biometrischer Daten sind netzwerkzentrierte Lösungen zielführender als Inselsysteme. Doch stellt ihre Implementierung die öffentliche Verwaltung vor enorme Herausforderungen. Hier bieten professionelle Systemintegratoren, zumal wenn sie im Sicherheitssektor beheimatet sind, eine dauerhafte, service-orientierte Unterstützung bei der Umsetzung aller Entwicklungsstufen: von der Registrierung von Bürgern bis hin zur funktionsfähigen Bereitstellung intelligenter Identifikationstechnologien und von der Erfassung, Auswertung und Bereitstellung von personenbezogenen Daten bis hin zur technologischen und operativen Ausbildung von Service- und Sicherheitskräften.

In Anbetracht verfügbarer, innovativer Technologien, welche erhöhte Sicherheit bei steigender Durchlaufleistung garantieren, stellt sich darüber hinaus die Frage, ob es nicht sinnvoll wäre, vorbereitende Sicherheits- und Kontrollmaßnahmen bereits vor Reiseantritt, beispielsweise durch zertifizierte Reisebüromitarbeiter, als Teil grenzübergreifender Sicherheitskooperationen durchzuführen. Diese Maßnahme könnte zur Begrenzung und Vermeidung von Bedrohungen beitragen, insbesondere weil durch sie Personen mit Sicherheitsrisiko identifiziert und aufgehalten würden noch bevor diese unsere Grenzen überschreiten, ja bevor sie unsere Grenzen überhaupt erreichen. Indem wir Terroristen, Kriminelle, illegale Einwanderer aber auch Schmuggel- und Gefahrgüter wirksam bekämpfen und aufhalten, bevor sie unsere Grenzen erreichen, verhindern wir deren möglicherweise katastrophale Entfaltung in der Mitte unserer Gesellschaften.

Dies gilt in besonderer Weise für Reise- und Frachtgüter. Hier gewinnt, in Anlehnung an die biometrische Datenerfassung bei Personen, der Begriff der 'objectmetric data' zunehmend an Bedeutung. Damit sind jene Objektmerkmale gemeint, welche einen spezifischen Gegenstand eindeutig beschreiben. Einer versiegelten Ware bzw. Warengruppe werden damit bestimmte Eigenschaften in Form einer künstlich generierten Objektidentität

zugeschrieben. In Kombination mit innovativen RFID-Applikationen lassen sich somit die berührungslose Identifikation, Steuerung und Verfolgung beliebig vieler Waren und Objekte über die gesamte Wertschöpfungskette realisieren. Wurde eine Ware oder ein Reisekoffer einmal in die Versendung gegeben und ihm eine eigenständige Objektkennung zuerkannt, so lässt sich sein Weg von der Aufgabe bis zum Abhol- oder Zustellort, sein aktueller Aufenthalts- bzw. Lagerort, der jeweils aktuelle Warencumzustand sowie jegliche inhaltliche oder merkmalspezifische Manipulation in Echtzeit nach- bzw. mitverfolgen. Von herausragender Bedeutung ist hierbei die Definition und Ermittlung der objektspezifischen Erkennungsmerkmale. Neben banal anmutenden Faktoren wie Form, Größe und Gewicht sind innovative Merkmale hinzuzunehmen. Dazu gehören beispielsweise Gattungseigenschaften (Holz, Metall, Kunststoff), molekulare Zusammensetzung aber auch Duftsignaturen.

Derzeit werden Flugpassagiere vor allem auf metallische Gegenstände untersucht, welche auf Waffen oder Sprengzünder hindeuten könnten. Beim Gepäck verhält es sich letztlich nicht viel besser. Frachtgut wird in Deutschland und vielen anderen Staaten, wenn überhaupt, nur stichprobenartig untersucht. Hinsichtlich der Detektion von Gefahrgütern kommt es an Flughäfen und Grenzkontrollpunkten bisweilen zum Einsatz von Spürhunden. Doch das jahrelange Training, der notwendige Hundeführer und die relativ kurze Einsatzdauer von höchstens 30-40 Minuten sind jedoch nicht vernachlässigbare Kosten- und Risikofaktoren. Bereits heute sind an Flughäfen Geräte mit so genannten 'künstlichen Nasen' im Einsatz. Diese werden jedoch durch mangelnde Sicherheitsbestimmungen lediglich im konkreten Verdachtsfall oder nur stichprobenartig eingesetzt. Darüber hinaus ist die gängige Wischprobentechnik anfällig gegenüber Fehlbedienung durch das Sicherheitspersonal. Das Forschungszentrum der EADS hat die 'künstliche Nase' im vergangenen Jahr entscheidend weiterentwickelt. Basierend auf dem Prinzip der Ionen-Mobilitäts-Spektrometrie (IMS), hebt sie sich gegenüber bekannten Detektoren und herkömmlichen Sensoren durch eine höhere Genauigkeit, Schnelligkeit und eine weitaus geringere Fehlerquote ab. Hierzu werden Laser- und spektroskopische Verfahren kombiniert, die es gestatten, schon kleinste Partikelspuren zu erkennen. Mit diesem durch den Bundesverband der Deutschen Industrie prämierten Verfahren ist es nunmehr möglich, sowohl bekannte als auch neuartige Sprengstoffe, wie sie die terroristische Szene kontinuierlich entwickelt, zuverlässig zu detektieren. Der bei den versuchten Anschlägen auf den Flughafen London-Heathrow im vergangenen Jahr verwendete Flüssigsprengstoff wäre mit dieser neuentwickelten Technologie sehr wahrscheinlich zu erkennen gewesen. Langfristig erscheint es zwingend, die Sicherheitsbestimmungen an Flughäfen, an Grenzkontrollpunkten wie auch bei Großveranstaltungen dahingehend auszurichten, dass moderne, zuverlässige Verfahren zur Detektion von Gefahrenstoffen zur Anwendung kommen. Hier dürfte Handlungsbedarf beim Gesetzgeber liegen, zumal, wie bereits erwähnt, sich viele der kritischen Infrastrukturen im privaten Eigentum befinden. Bedingt durch die erst vor wenigen Monaten glücklicherweise gescheiterten Kofferbombenanschläge auf zwei Züge des öffentlichen Personenverkehrs hat der Gesetzgeber seinen Handlungsbedarf erkannt und Konsequenzen angekündigt. Dabei geht es vor allem um die Ausweitung der öffentlichen Videoüberwachung an Bahnhöfen, Flughäfen, öffentlichen Plätzen und Einrichtungen; aber auch um die seit langem kontrovers diskutierte Anti-Terror-Datei.

Beide Maßnahmen, Videoüberwachung und Anti-Terrordatei, schaffen jedoch nicht automatisch oder notwendigerweise ein Mehr an Sicherheit. Das Ausweiten der Videoüberwachung hat zunächst lediglich unmittelbare Auswirkungen auf das subjektive Sicherheits- und Freiheitsempfinden der Öffentlichkeit. Dennoch gibt es Beispiele, wie die Kofferbombenanschläge, bei denen mehr Videotechnik tatsächlich den Fahndungserfolg beschleunigt oder überhaupt erst ermöglicht hat. Um im Kampf gegen internationalen Terrorismus und die organisierte Kriminalität Angriffe und Straftaten wirksam verhindern zu können, müsste man theoretisch gemäß der Formel "Mehr Technik = mehr Erfolg" ganz Deutschland bzw. ganz Europa flächendeckend mit Überwachungstechnik ausrüsten. Abgesehen von den rechtlichen Implikationen ist dies praktisch nicht machbar und darüber hinaus finanziell völlig unrealistisch. Die Formel "Mehr Technik = mehr Erfolg" vernachlässigt zudem einen weiteren Gesichtspunkt. Eine Videokamera allein garantiert noch keinen Erfolg. Die größte Herausforderung besteht heute wie auch zukünftig in der Informationsauswertung sowie dem Austausch und der Weitergabe von Erkenntnissen – fehlerfrei und in Echtzeit. Nur so werden schnelle Reaktionen und damit auch präventives Handeln möglich. Dabei ist die Videoüberwachung eine Maßnahme, die in ein umfassendes Gesamtsystem integriert sein muss, um ihre Wirksamkeit überhaupt entfalten zu können.

In Spanien gibt es beispielsweise in allen Parkhäusern Kameras mit angeschlossenen Bildvergleichssystemen zur Kennzeichenüberprüfung. Ein gestohlenen Kraftfahrzeug kommt aus dem Parkhaus nicht heraus, da sich die Schranke erst gar nicht öffnet. Hinter diesem vergleichbar simplen Sicherheitssystem stehen eine präzise Datengewinnung mittels Kamera, die fehlerfreie Auswertung und eine Reaktion in Echtzeit: Die Schranke bleibt zu! Dieses System kann beliebig mit anderen technischen Komponenten wie beispielsweise dem Ticketing vernetzt und damit erweitert werden. Dieses Bildvergleichssystem in Parkhäusern ist in Spanien bereits Normalität.

Videotechnologie wird als Dokumentationsmedium für Polizei und Staatsanwaltschaft auch in Zukunft eine herausgehobene Rolle spielen. Die Schwierigkeit für einen präventiven Einsatz von Videodaten liegt in dem Umstand begründet, dass Bilder und Informationen von Menschen kontinuierlich evaluiert werden müssen. Bei den derzeitigen und noch mehr bei den künftigen Datenmengen ist dies nicht mehr möglich, was nicht zuletzt die Terroranschläge vom 11. September 2001 gezeigt haben. Die Herausforderung besteht somit darin, Videotechnik intelligent zu machen. Dies kann beispielsweise mittels Videosensorik erfolgen: Ein Videobild wird erst dann aufgeschaltet, wenn das System auf Grund von bestimmten Vorgaben im überwachten Gebiet eine Abweichung vom Soll-Wert festgestellt hat. Dieses System muss zudem fehlerfrei und schnell entscheiden, welche Informationen in der ganzen Datenflut für die Verhinderung einer Straftat oder eines terroristischen Angriffs tatsächlich relevant sind. Es muss darüber hinaus entscheiden, wer diese Informationen benötigt, um schnell reagieren zu können, und wohin sie deshalb versendet werden müssen.

Die technologische Machbarkeit stellt aber nur eine Seite der Sicherheitsmedaille dar. Letztendlich liegt es an den politischen Entscheidungsträgern, die rechtlichen Voraussetzungen für den Einsatz derartiger Technologien und innovativer Sicherheitslösungen zu schaffen. Dies kann allein im Einvernehmen bzw. auf Grundlage eines umfassenden Rückhaltes in der Bevölkerung erfolgen. Daher sind eine realistische Bedrohungswahrnehmung wie auch fähigkeitenorientierte Maßnahmen von übergeordneter Bedeutung.

Zusammenfassend bleibt festzuhalten, dass der Umfang unserer anhaltenden Verwundbarkeit verdeutlicht, dass wir uns Defizite hinsichtlich der Implementierung umfassender Sicherheit nicht leisten können. Der Preis unzureichender Sicherheitskapazitäten und Einsatzmöglichkeiten ist einfach zu hoch! Zudem liegt es an allen Sicherheitsakteuren bewusst zu machen, dass Freiheit ohne Sicherheit weder auf individueller noch auf kollektiver Ebene realisierbar ist. Nur in einer von Sicherheit geprägten Umwelt kann Fortschritt stattfinden und Wohlstand nachhaltig gesichert werden.

Für all jene Sicherheitsdienstleister, die auch zukünftig professionell und nachhaltig erfolgreich am Markt operieren möchten ist es angebracht, neben der selbstverständlichen Verpflichtung gegenüber dem Kunden, Anspruch und Selbstverständnis von der Erkenntnis leiten zu lassen:

- dass selbst das umfassendste und hochtechnisierteste Sicherheitssystem letztlich überwindbar sein wird und wir deshalb nicht nur unseren Kampf gegen organisierte Kriminalität und internationalen Terrorismus ausweiten müssen, sondern auch unsere Bemühungen, die Ursachen für diese Bedrohungen nach Möglichkeit zu beseitigen,
- dass unsere Verantwortung und Verpflichtung, obgleich technologisch optimiert und fähigkeitenbezogen, dem Menschen und seinem fundamentalen Bedürfnis nach einem Leben in Freiheit und Sicherheit gilt,
- und dass wir zwangsläufig auf struktur- und grenzübergreifende Kooperation, auf Interoperabilität und Interkonnektivität angewiesen sind, da kein Staat, wie mächtig er sich auch seiner unbegrenzten Möglichkeiten versichert, allein in der Lage ist, globale Sicherheit dauerhaft und nachhaltig zu gewährleisten.

Der Titel der europäischen Sicherheitsstrategie: "A secure Europe in a better world" sollte zum Leitgedanken aller Sicherheitsakteure werden. An ihm müssen wir unser Engagement messen lassen.

Ich bedanke mich für Ihre Aufmerksamkeit!