

# Nacktscanner? Der BDK ist für mehr menschliche statt künstliche Intelligenz!

10.01.2010

**Es ist erstaunlich, mit welcher Vehemenz die Politik momentan Techniken forciert, die weder besonders effizient sind noch das versprochene Allheilmittel gegen die terroristische Bedrohung darstellen. Körperscanner sind nicht die Lösung des Luftsicherheitsproblems!**

Nach dem versuchten Anschlag im Dezember auf ein Verkehrsluftfahrzeug in den USA wird der sogenannte "Nacktscanner" von vielen Politikern und Sicherheitsexperten als eine Lösung des Sicherheitsproblems propagiert. Dieser Scanner kann das eigentliche Sicherheitsproblem jedoch nicht lösen: Kleine, aber hochwirksame und gut getarnte Sprengsätze im Körper (oral, vaginal oder rektal eingeführt) kann das Gerät nur schlecht oder gar nicht detektieren!

Der BDK fordert daher, die politische Debatte auf das Kernproblem der bundesdeutschen Luftsicherheits-Philosophie auszurichten. Diese ist auf die ineffiziente Suche nach der Bombe und nicht auf die gezielte Suche nach dem potentiellen Attentäter unter den Fluggästen ausgerichtet. Die damit verbundene breite Streuung von Kontrollmaßnahmen führt zwangsläufig zu einer langsamen Abfertigung der Passagiere.

Es wäre wesentlich effizienter und würde damit auch die Warteschlangen vor den Kontrollstellen verkürzen, wenn unter den Fluggästen mit Hilfe einer Datenbank potentielle Gefährder identifiziert und dann einer intensiven Kontrolle zugeführt werden. Es ist völlig unverständlich, warum eine 70-jährige Großmutter mit der gleichen Intensität einer Luftsicherheitskontrolle unterzogen wird wie ein Reisender, der bereits in nachrichtendienstlichen und polizeilichen Dateien einschlägig erfasst ist. Alle Flugzeugattentäter der jüngsten Vergangenheit waren junge muslimische Männer und nicht Rentner.

Der BDK fordert daher eine grundlegende Änderung der Sicherheitsstrategie im Luftsicherheitsbereich mit dem Ziel, mehr Einheitlichkeit und hohe Qualitätsstandards auf allen deutschen Verkehrsflughäfen zu erreichen. Die israelische Luftsicherheitsstrategie ist hier vorbildlich. Auch Ansätze wie HAMLeT<sup>1</sup> und **Preborderlane** sind seriös zu prüfen! Es gilt, diese Erfahrungen zu nutzen und an das europäische Rechtssystem anzupassen.

---

## Nacktscanner

*Der öffentlichkeitswirksame aber unsachliche Begriff "Nacktscanner" beflügelt offenbar ungeahnte Phantasien in der Politik, der Berichterstattung und unter Karikaturisten. Der BDK fordert eine sachliche Debatte.*

---

Mehr Effizienz verspricht sich der BDK durch ein Maßnahmenbündel, dass für sich in der Gesamtheit ein Netzsystem darstellt. Das System filtert erst grob, wird dann feiner und führt zuletzt verdächtige Personen einer intensiven Befragung und Kontrolle zu:

- Automatisierter Abgleich der Passagierdaten durch die BPOL unmittelbar nachdem Ticketkauf mit allen polizeilichen Verbunddateien!
- Kopplung der Antiterrordatei (ATD) mit dem polizeilichen Fahndungssystem INPOL mit dem Ziel, den kontrollierenden Beamten zumindest den automatisierten Hinweis zu geben, dass gegen die Person luftsicherheitsrelevante Erkenntnisse vorliegen. Die weitere Bearbeitung sollte im Trefferfall im Rahmen des ersten Angriffs durch Kriminalbeamte der BPOL übernommen werden.
- Schulung ausgewählter Bundespolizisten in Befragungstechniken, um ggf. erste Verdachtsmomente, die bei der Kontrolle entstehen, gezielt überprüfen zu können.
- Beobachtung der wartenden Fluggäste durch psychologisch geschulte Beamte (auch unter Einsatz von Videotechnik) anhand eines zu entwickelnden Profils, um frühzeitig potentielle Verdächtige zu identifizieren, die dann intensiv kontrolliert und befragt werden.
- Verstärkte Fahndung durch besonders geschulte Zivilfahnder auch im Vorfeld der eigentlichen Luftsicherheitskontrollen. Mit Betreten des Flughafens sollten sich die Besucher bereits in einem gesicherten Bereich befinden<sup>2</sup>. Unübersichtliche Bereiche, die u.U. von Insidern zur Umgehung der Kontrollen genutzt werden, sind umzubauen oder ggf. durch in Zivil eingesetzte Beamte zu überwachen.

## EasyPass -eine weitere teure, aber wirkungslose Wunderwaffe mehr!

An den langen Wartezeiten auf den Flughäfen sind allein die langsam arbeitenden Beamten schuld. Diesen Satz hat der mittlerweile geschasste Staatssekretär Dr. Hanning zwar nicht gesagt, als er am 16. Oktober 2009 den Testlauf von "EasyPass" am Frankfurter Flughafen startete. Es drängt sich aber mehr und mehr der Verdacht auf, dass die Passkontrollen in der jetzigen Form abgeschafft werden sollten und die Entscheidung, ob eine Person nach Schengen einreisen kann, künftig ein Automat trifft.

EasyPass ist eine automatische Personenschleuse, die aufgrund des Vergleichs der in den biometrischen Reisepässen gespeicherten Daten und den mittels Kamera und Scanner erfassten Daten die Entscheidung trifft, ob die Person tatsächlich ihren eigenen Ausweis vorlegt. Nach positivem Lichtbild-Vergleich und negativer Fahndungsabfrage öffnet sich die

Personenschleuse und der Eingang nach Schengen ist frei. Ein Beamter der Bundespolizei überwacht per Video das Geschehen in jeweils 4 Schleusen. Beispielsweise soll er erkennen, ob eine reelle Person von der Kamera gefilmt wird oder nur ein hochgehaltenes Lichtbild. Auch das Betreten der Schleuse durch mehrere Personen soll der Beamte erkennen. Ein weiterer Polizist steht bereit, um ggf. notwendige Nachkontrollen vorzunehmen. Teilnehmen dürfen nur volljährige Personen, so dass Familien mit Kindern vom Verfahren automatisch ausgenommen werden. Für Rollstuhlfahrer sind die Spuren zu eng, älteren Reisenden ist die Schleuse häufig zu kompliziert.

Zum Einsatz kommt keine wirklich neue Technik. In anderen europäischen Ländern ist man hier wesentlich weiter. Bei EasyPass wird konventionelle und damit für Überwindungsversuche anfällige 2D-Technik verwendet. Deswegen und wegen der fehlenden Lebenderkennung kann das System nicht unbeaufsichtigt eingesetzt werden. Auf dem überladenen Bildschirm des beaufsichtigenden Beamten erscheinen die Lichtbilder der vier Schleusenkameras, die gescannten Lichtbilder aus den Reisepässen und die Lichtbilder der Passinhaber, die auf dem RFID-Chip<sup>3</sup> des PASSES gespeichert sind. Nur wenn alle drei Lichtbilder nach Auffassung der Software identisch sind (der Schwellenwert kann angepasst werden) und nicht nach der Person gefahndet wird, öffnet sich die jeweilige Personenschleuse.

Die derzeitigen Abgleichmöglichkeiten reichen noch nicht aus, um mit hoher Wahrscheinlichkeit sicherzustellen, dass die vorstellig gewordene Person mit der im Pass gespeicherten Person identisch ist. Wesentliche unveränderliche Merkmale des Gesichtes werden nach wie vor nicht elektronisch erfasst. Bisher wird nur ein Frontfoto erfasst, bei dem wesentliche unveränderliche Merkmale des Äußeren nicht zu einer Prüfung herangezogen werden können. Auch das verwendete Ausweislesegerät ist nicht geeignet, um sicher auszuschließen, dass keine ver- oder gefälschten Dokumente verwendet werden. Den Lesegeräten fehlen die "Sinnesorgane des Menschen" mit dem sich z.B. bestimmte Druckarten oder die Beschaffenheit des Papiers erfüllen / ertasten lassen. Die Auswertung der wenigen maschinenlesbaren Elemente eines Reisedokumentes allein reicht nicht aus, um ein Reisedokument als echt einzustufen.

Wenn EasyPass zu Testzwecken eingesetzt wird, um weitere wissenschaftliche Erkenntnisse zum Zweck der Echtheitskontrolle von Dokumenten und/oder den Abgleich von biometrischen Daten zu erbringen, dann muss bis zur Realisierung einer 100%-igen Leistung definitiv eine manuelle Nachkontrolle erfolgen, um Fehler sofort erkennen und beseitigen zu können.

#### **Sicherheit nur bei Symbiose von Mensch und Maschine**

Dass der Druck seitens der Politik auf die Herstellerfirmen von Sicherheitstechnik groß ist, wird nicht übersehen. Es geht um die Geschwindigkeit des Verkehrsflusses von Passagieren und die Kürzung von Standzeiten der Verkehrsmaschinen. Aber mehr Sicherheit kann nur erreicht werden, wenn bei dem heutigen Stand der Technik eine Symbiose zwischen Mensch und Maschine gegeben ist. Grenzbeamte wünschen sich meist ganz bodenständige Dinge statt Hi-Tec-Spielerei. So zum Beispiel, dass erst einmal grundsätzliche Bedingungen von Personaldokumenten wie gute Fälschungsmerkmale, ausreichend große und scharfe (!) Lichtbilder, nichtspiegelnde Folien erfüllt werden. Die heutigen "ID-Cards" und Pässe haben oft nur noch daumnagelgroße Lichtbilder, sind falsch belichtet oder unscharf. Darüber hinaus müssen die Beamten besser in Urkundendelikten, Personenidentifizierung, Ausländerrecht und in Fremdsprachen fortgebildet werden. Sie müssen sich spezialisieren dürfen. Der omnipotente Beamte ist und bleibt Wunschdenken - das Multiplikatorensystem hat sich überlebt!

Der BDK empfiehlt der Politik und Wirtschaft im Bereich der Gesichtserkennung, den Weg zum 3D-face-Projekt zu gehen, um unter Verwendung eines Halbprofils des menschlichen Gesichts mehr Sicherheit zu erzielen. Die Verwendung des Halbprofils würde sowohl eine sichere manuelle als auch maschinelle Kontrolle ermöglichen. Dies gilt ebenso für die Echtheitskontrolle von Dokumenten. In der Erkennung von Nachahmungen, die mit dem geschulten menschlichen Auge einfach erkannt werden, weisen die Ausweislesegeräte der heutigen Generation noch hohe Fehlerquoten auf.

Bei aller Euphorie für neue Technologien gilt es erst einmal, sinnvolle, kostengünstige und somit effektive herkömmliche Verbesserungsmöglichkeiten zu nutzen.

- Wann werden endlich Höhenmaße in den Kontrollboxen angebracht, um die Größenangaben in den Pässen prüfen zu können?
- Wann gibt es überall Spiegel, um das "Unterlaufen" der Passkontrollen zu verhindern?
- Wann werden Schutzscheiben und Spiegelfolien angebracht, um den Reisenden den Blick auf Polizei-PC und Fahndungsunterlagen zu verbergen?
- Wann wird die Lupe (Fadenzähler) Standardausstattung bei Kontrollbeamten?
- Wann werden in den Kontrollboxen schnelle Rechner und vor allem schnelle und fehlerfreie Ausweislesegeräte installiert?
- Wann werden endlich die verschiedenen und komplizierten Informationen zu Einreisemodalitäten, internationalen Pässen und Fahndungshinweisen in einem funktionierenden, schnellen und intuitiven System zusammengeführt?
- Wann werden die meist nur spärlichen Fremdsprachenkenntnisse der Beamten durch kontinuierliche Lehrgangsangebote verbessert?
- Wann wird das vorhandene Fremdsprachenpotential überhaupt einmal erhoben und dieses Wissen einheitlich auf dem Flughafen zugänglich gemacht? Hotel-, Supermarkt- und Backshop-Mitarbeiter tragen häufig Schilder mit den Flaggen ihrer Sprachkenntnisse - bei der Bundespolizei Fehlanzeige!
- Wissen die Verantwortlichen, dass die PC in den Kontrollboxen oft älter als 10 Jahre sind, die Mäuse älter als 15 Jahre, die Tastaturen oft noch nicht mal Windows95- Tastaturen und meist klemmende Tasten haben?
- Was plant die Bundespolizei eigentlich mit den durch die geplante Technikoffensive freigesetzten Beamtinnen und Beamten? Werden zukünftig noch mehr uniformierte Beamte im öffentlichen Bereich Streife laufen - die wohl ineffektivste Methode, um Anschläge zu verhindern!?

Die Bundespolizei hat viele Möglichkeiten, ihre Arbeit an den Flughäfen zu professionalisieren. Teure und schlecht funktionierende Technik gaukelt aber nur Sicherheit vor! Auch das permanente Schreien nach mehr Personal für die Flughäfen ist keine Art von effektiver Lösungsstrategie, solange das bereits jetzt üppig vorhandene Personal nach dem Gießkannenprinzip eingesetzt wird. Nicht Masse, sondern Klasse macht den Unterschied. Zieht man ein Fazit aus der derzeitigen Technikdiskussion, bleibt festzustellen: Eingesetzte Technik muss der Sicherheit dienen und sich praktisch bewährt

haben. Die Fehlertoleranzen müssen sehr gering sein. **Maschinen sind notwendig und sinnvoll, sollen jedoch nur unterstützen und keine Entscheidungen treffen. Dazu bedarf es gut ausgebildeter und klug eingesetzter Mitarbeiter!**

<sup>1</sup> Hazardous Material Localization and Person Tracking

<sup>2</sup> auch hier ist an den verstärkten Einsatz von Videotechnik zu denken, wobei eine Videoüberwachung nur dann Sinn macht, wenn gut ausgebildete und speziell geschulte Polizeibeamte diese "live" begleiten

<sup>3</sup> <http://de.wikipedia.org/wiki/RFID>

## Dateien zur Nachricht

- [2010-01-10\\_download\\_flyer.pdf](#)
- [2010-01-10\\_download\\_flyer-2blatt-Version.pdf](#)