



Prof. Dieter Kempf
Mitglied des BITKOM-Präsidiums

Innere Sicherheit und Hightech

BITKOM - Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

München, 24. Oktober 2007

Bereitstellung von Sicherheitselektronik

Videoüberwachung

Biometrie, z.B. E-Pass

Verteidigung u.a.

Staatliche Überwachung von Kommunikation

Vorratsdatenspeicherung

TK-/Internetüberwachung

Online-Durchsuchung

Anwender-Schutz gegen Gefahren

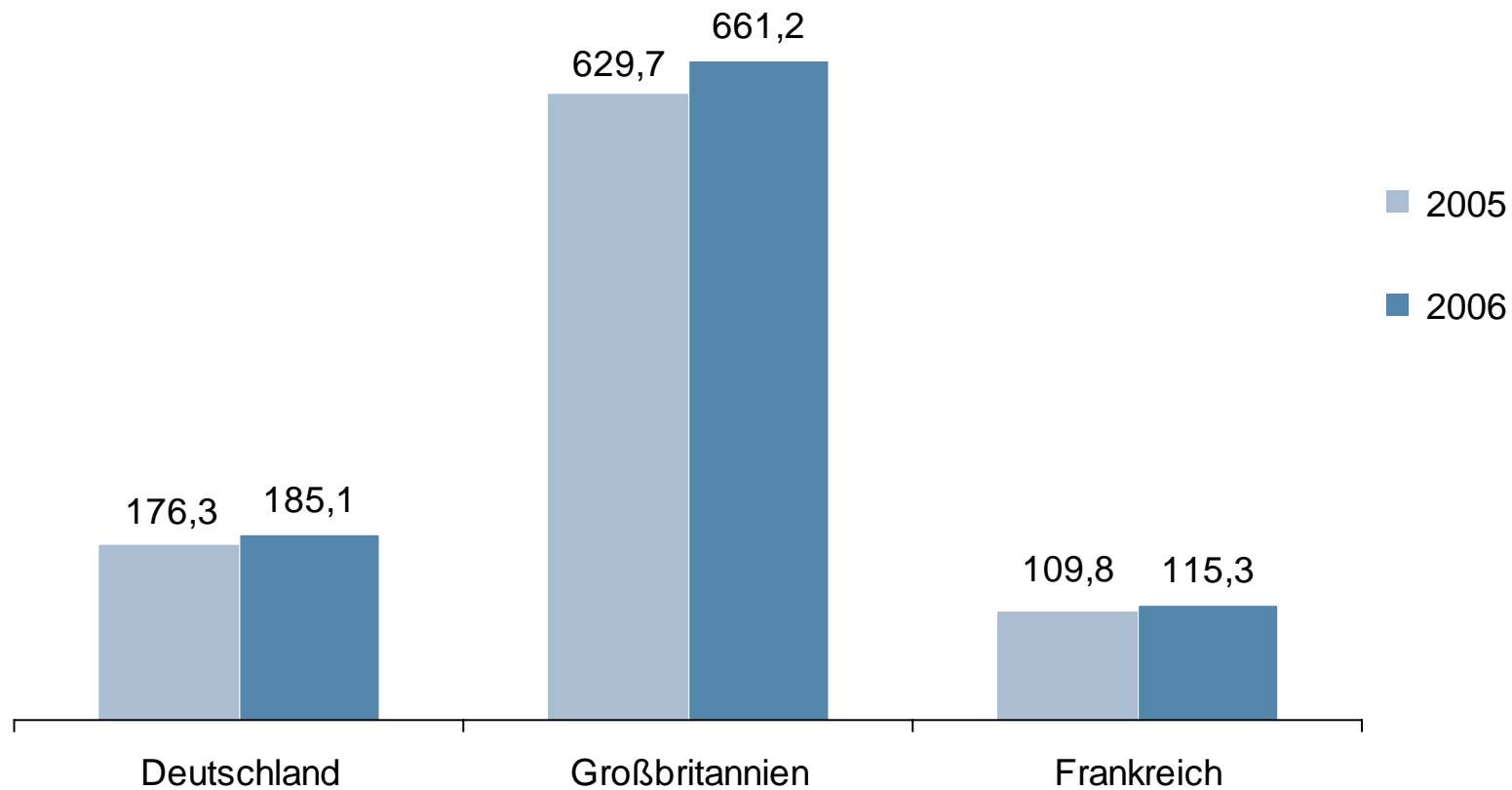
Schadprogramme/Viren

Phishing

Hacker

Sicherheitselektronik: Videoüberwachung

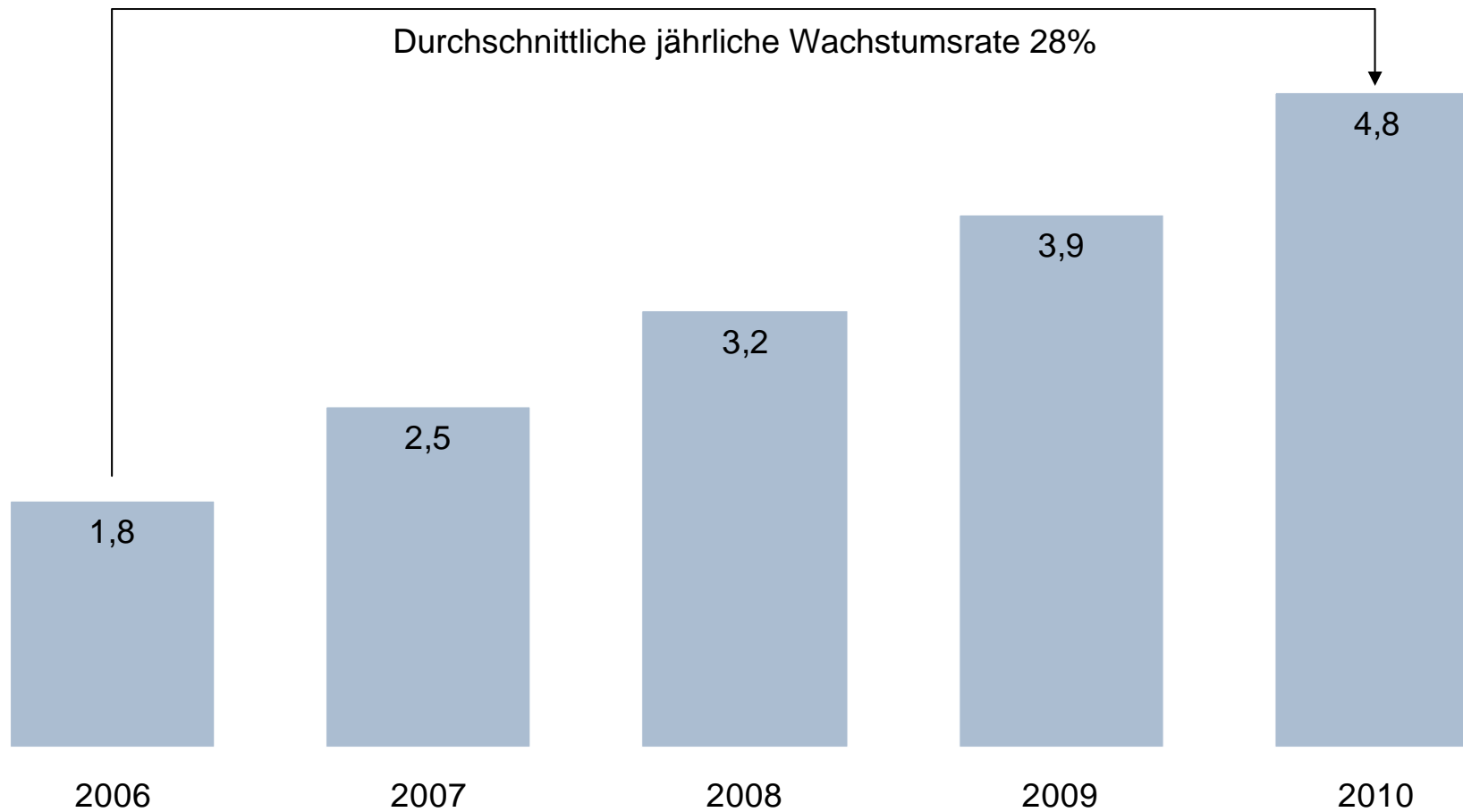
Märkte ausgewählter Länder, in Mio. Euro



Quelle: BITKOM

Sicherheitselektronik: Wachstumsmarkt Biometrie

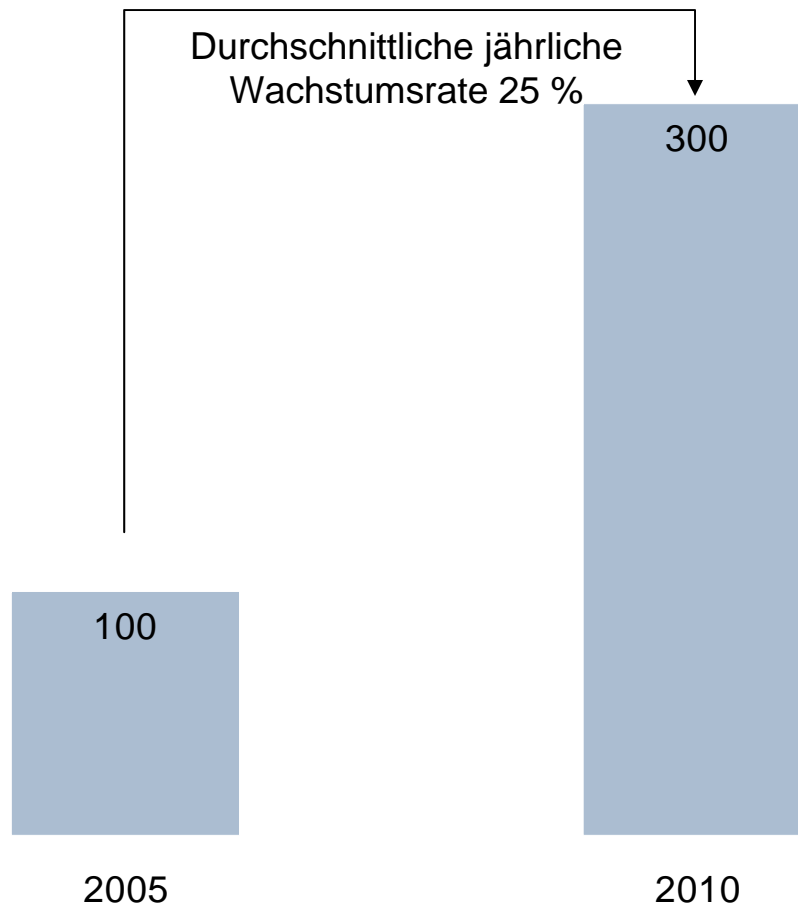
Umsatzentwicklung weltweit in Mrd. Euro



Quelle: International Biometric Group 2006

Sicherheitselektronik: Wachstumsmarkt Biometrie

Umsatzentwicklung in Deutschland in Mio. Euro



Quelle: BITKOM/Roland Berger

Sicherheitselektronik: Biometrie

Technologien und Anwendungsfelder



Wichtigste Technologien

- Erkennung von Fingerabdrücken (48 % Marktanteil)
- Gesichtserkennung (22 % Marktanteil)

Anwendungsfelder

- Absicherung von Datenspeichern (z.B. USB-Sticks) mit sensiblen Daten
- Gesicherte Anmeldung in Unternehmensnetzen
- Zugriffskontrolle bei wichtigen Dokumenten
- Zutrittskontrolle als Schlüssellersatz
- Bezahlen im Einzelhandel (Pilotprojekt: Edeka-Markt in Ingolstadt)

Beispiel: Elektronischer Reisepass

- 4,3 Millionen Deutsche haben einen Chip mit Foto im Pass
- Ab November 2007 Fingerabdrücke mit Datenschutzmechanismus
- Nächster Schritt: Elektronischer Personalausweis

Kommunikation: Speicherung Verbindungsdaten

Gesetzliche Bedingungen bei Telefon und Internet



	Bisher	Künftig (geplant für 1.1.2008)
Telefon, Handy, VoIP, SMS	<ul style="list-style-type: none"> ▪ Keine generelle Speicherpflicht ▪ Max. 6 Mon. Speicherung für Rechnungszwecke ▪ Auf Kundenwunsch Löschung mit Re.-Versand ▪ Auskunft an Ermittler bei erheblichen Straftaten 	<ul style="list-style-type: none"> ▪ Generelle Speicherpflicht 6 Mon. ▪ Inkl. Standortdaten und IP-Adressen ▪ Auskunft an Ermittler bei mehr Straftaten ▪ Entschädigung der Anbieter noch offen
Internet-Zugang, E-Mail	<ul style="list-style-type: none"> ▪ Keine generelle Speicherpflicht f. IP-Adressen ▪ Auch nicht für E-Mail-Verbindungsdaten ▪ Max. 6 Mon. Speicherung für Rechnungszwecke ▪ Auskunft an Ermittler bei erheblichen Straftaten 	<ul style="list-style-type: none"> ▪ Internet-Einwahldaten 6 Mon. speichern ▪ Inkl. IP-Adresse und Anschlusskennung ▪ Mail-Verbindungsdaten 6 Mon. speichern ▪ Inkl. Mail-Adressen, Absender-IP, Zeiten ▪ Auskunft an Ermittler bei mehr Straftaten

Unterstützung für Ermittler

- Bekämpfung von Kriminalität und Terror ohne Branchen-Mitarbeit undenkbar
- Verlässlicher Kooperationspartner auf gesetzlicher Basis

Pragmatischer Ansatz

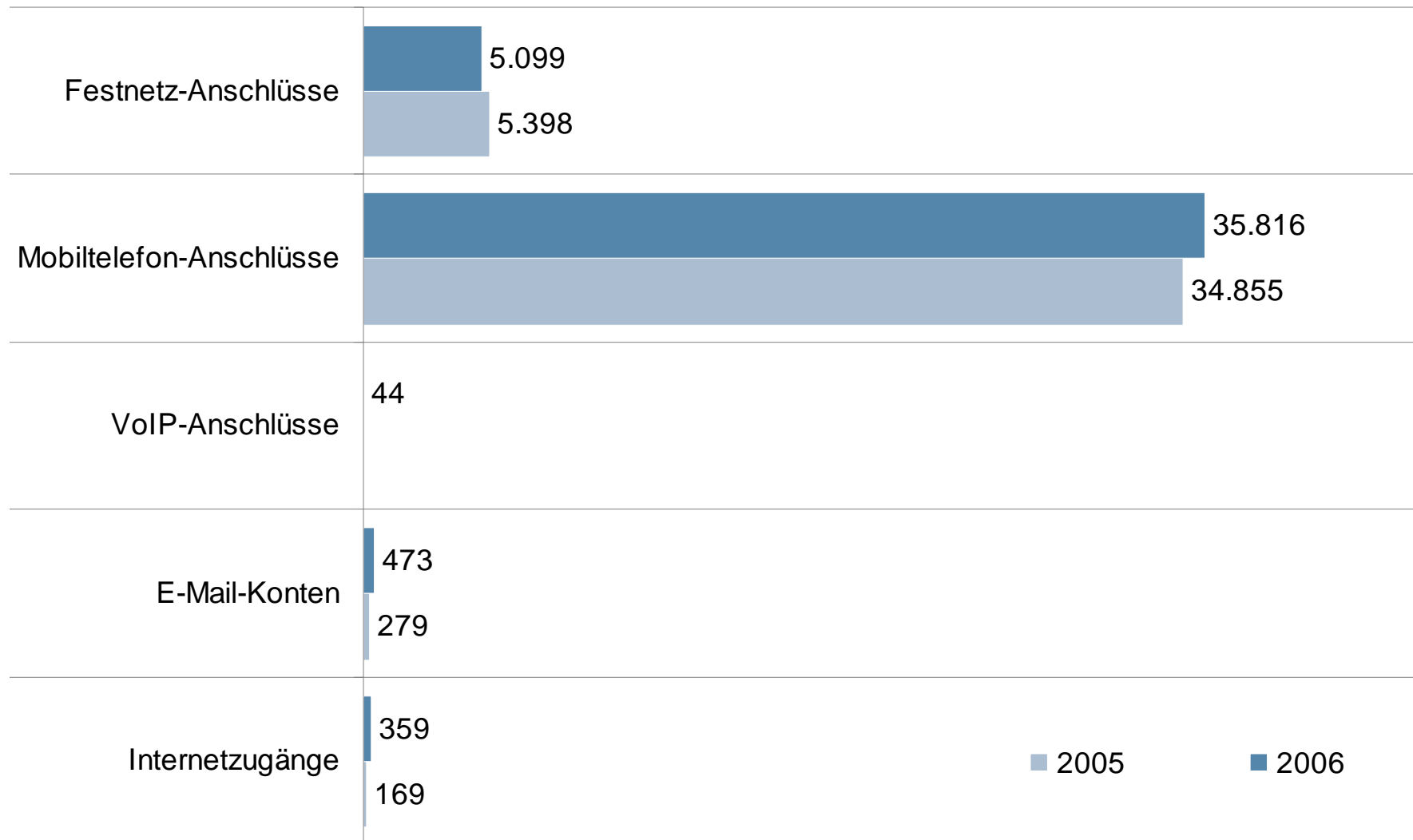
- Balance zwischen Schutz der Gesellschaft und Schutz der Privatsphäre
- EU-Vorgaben sind sinnvolle Richtschnur
- Straftatenkatalog überprüfen (z.B. Beleidigung per Telefon/Internet)

Faire Bedingungen

- Branche braucht Übergangsfrist bis 2009 für technische und personelle Umstellung
- Entschädigung für Investitionen in Technik von 50 bis 75 Millionen Euro
- Entschädigung für jährliche Betriebskosten in zweistelliger Millionen-Höhe

Der Staat hört mit

Überwachung zur Strafverfolgung, § 110 Abs. 8 TKG



Quelle: Bundesnetzagentur

Überwachung von Gesprächsinhalten und Daten

Gesetzliche Bedingungen nach §§ 100 ff. StPO



	Bisher	Künftig
Telefon, Handy, VoIP, SMS, E-Mails	<ul style="list-style-type: none"> ▪ Enger Straftatenkatalog ▪ Nur wenn andere Wege aussichtslos ▪ Irrelevantes löschen, Betroffene informieren ▪ Richtervorbehalt, bei Gefahr im Verzug StA 	<ul style="list-style-type: none"> ▪ Erweiterter Straftatenkatalog ▪ Z.B. Steuerdelikte, Menschenhandel, Doping ▪ Geplant ab 01.01.2008
PCs u. Festplatten	<ul style="list-style-type: none"> ▪ Kein Bundesgesetz f. Online-Durchsuchung ▪ Zugriff nur bei Hausdurchsuchung ▪ Hausdurchsuchung bei allen Straftaten mögl. ▪ Richtervorbehalt, bei Gefahr im Verzug StA 	<ul style="list-style-type: none"> ▪ Informeller Entwurf zur Online-Durchsuchung ▪ Alle Endgeräte und Mail-Server mögl. Ziel ▪ Abwehr „dringender Gefahren“/Terrorismus ▪ Richtervorbehalt, notfalls durch BKA-Präsid.
Wohnung	<ul style="list-style-type: none"> ▪ Großer Lauschangriff (Gespräche innerhalb) ▪ Enger Straftatenkatalog, bes. hohe Hürden ▪ Pers. Kernbereich muss ausgeschlossen sein ▪ Strenger Richtervorbehalt, nicht durch StA 	<ul style="list-style-type: none"> ▪ Keine Änderungen in Sicht

Eng begrenzter Einsatzbereich

- Hohe Hürden wie bei der Wohnraumüberwachung
- Orientierung an Leitlinien des BVerfG zum Großen Lauschangriff
- Wenige Fälle pro Jahr (Gefahrenabwehr/Terrorismus)

Problematisch bei Software-Schnittstellen

- Nationaler Ansatz für Hintertüren wenig sinnvoll
- Nachteile für Anbieter in Deutschland
- Bei wenigen Fällen pro Jahr besser individueller Zugriff

Problematisch bei E-Mail-Servern

- Nationaler Ansatz wenig sinnvoll
- Nutzer können auf ausländische Anbieter ausweichen

Online-Durchsuchung

Varianten und offene Fragen



Technisch

- Programm: Trojaner, Key-Logger oder andere Technik
- Zugriff: Individuell oder über obligatorische Software-Schnittstelle
- Installation: Direkt/manuell, über E-Mail-Anhang, Webseite oder Software-Update
- Sog. „Bundestrojaner“ müsste Firewalls und Virens Scanner umgehen
- Programm soll nicht irrtümlich auf weitere Rechner übertragen werden

Rechtlich

- Gelten für Festplatten ähnliche Schutzkriterien wie für Wohnräume?
- Lassen sich strafrechtlich Relevantes und persönlicher Kernbereich trennen?
- Sind Erkenntnisse auch vor Gericht zur Strafverfolgung nutzbar?
- Dürfen Firmen in Deutschland Schutzprogramme gegen Online-Durchs. anbieten?

Online-Durchsuchung

Beispiele aus dem Ausland



Österreich

- Kabinett hat Regelung beschlossen, gilt voraussichtlich ab Herbst 2008
- Nicht nur zur Gefahrenabwehr, sondern auch zur Strafverfolgung
- Straftaten mit 10 Jahren Mindestfreiheitsstrafe und dringender Tatverdacht
- Richtervorbehalt und gesonderte Beobachtung durch Rechtsschutzbeauftragten
- Nach Angaben des Justizministeriums ein bis zwei Einsätze jährlich geplant

Schweiz

- Gesetzliche Regelung zur Gefahrenabwehr geplant
- Einsatzfelder: Terrorismus, Spionage, Waffenhandel, illegaler Technologietransfer
- Richtervorbehalt, bei Gefahr im Verzug Anordnung durch zuständiges Bundesamt

USA

- FBI hat bisher in Einzelfällen Spähprogramme eingesetzt, die namentlich bekannt sind
- Funktionen: Ausspähen von Systemdaten, besuchten Webseiten sowie IP-Adressen
- Laut FBI keine Erfassung von Kommunikationsinhalten



Prof. Dieter Kempf
Mitglied des BITKOM-Präsidiums

Innere Sicherheit und Hightech

Pressekonferenz auf der Systems 2007

BITKOM - Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

München, 24. Oktober 2007