IT-abhängige kritische Infrastrukturen

Reinhard W. Hutter

Leiter des Geschäftsbereichs
InfoKom
hutter@iabg.de
+49 89 6088 2524
+49 89 6088 2460

Inhalt

- **Die Informationsgesellschaft**:
  - Risiken
  - Bedrohungen
  - Folgen
- **Szenarien:**
  - Realität
  - Prognose
  - Fiktion
- **Lösungsansätze:**
  - Methoden
  - Strategie
  - Management
  - Technologie

IABG

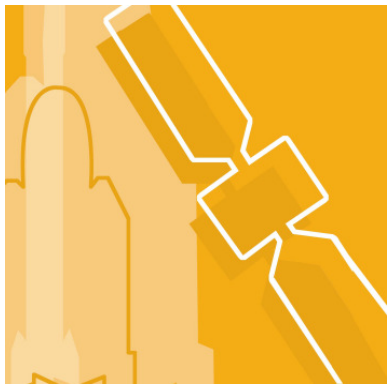
Geschäftsfelder der IABG

Automotive

Information & Kommunikation

Verkehr & Umwelt

Luftfahrt



Raumfahrt

Verteidigung

www.iabg.de

Informationsgesellschaft

Grundlegende Trends

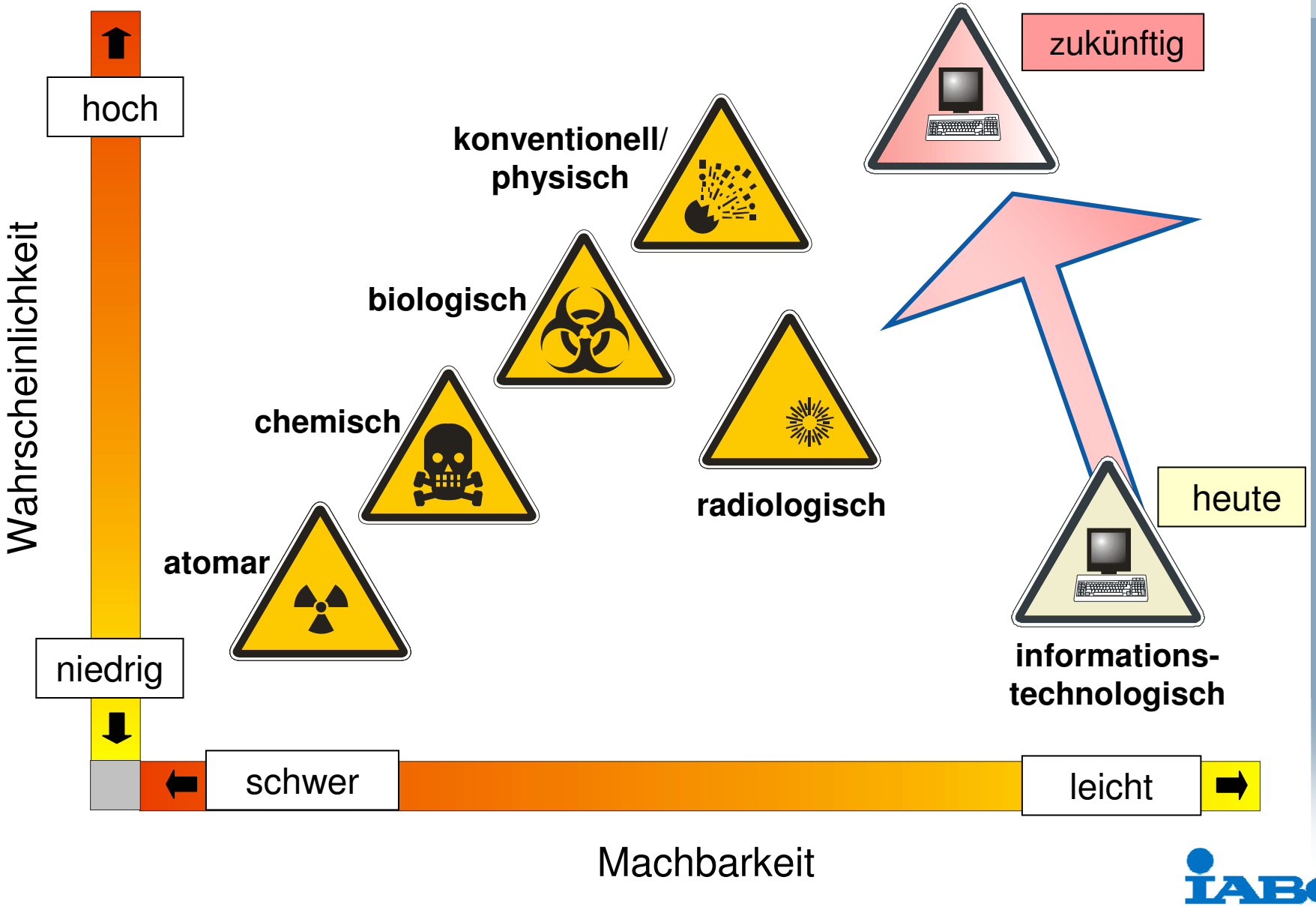
- De-Industrialisierung
- Generierung von Wohlstand durch informationsbasierte Prozesse
- Weltweite, unmittelbare und permanente Kommunikation
- Information als Quelle von Wohlstand und Armut (digital divide)
- Prozessoptimierung durch Einsatz von IT in allen wirtschaftlichen, sozialen und politischen Sektoren wissensbasierter Gesellschaften

IABG

Infrastrukturen als Risikofaktor

www.aksis.de

Bedrohungstrends



Risikofaktoren der Informationstechnologie (1)

Kriterien	Eigenschaften & Folgen
1. Vernetzung	Weltweit und nicht verfolgbar
2. Abhängigkeit	Versorgungsengpässe, Inhalte unbekannt
3. Innovation	Schneller als Sicherheitsvorsorge
4. Komplexität	Beherrschbarkeit & Überschaubarkeit
5. Verfügbarkeit	Weltweit verbreitet & leichter Zugang

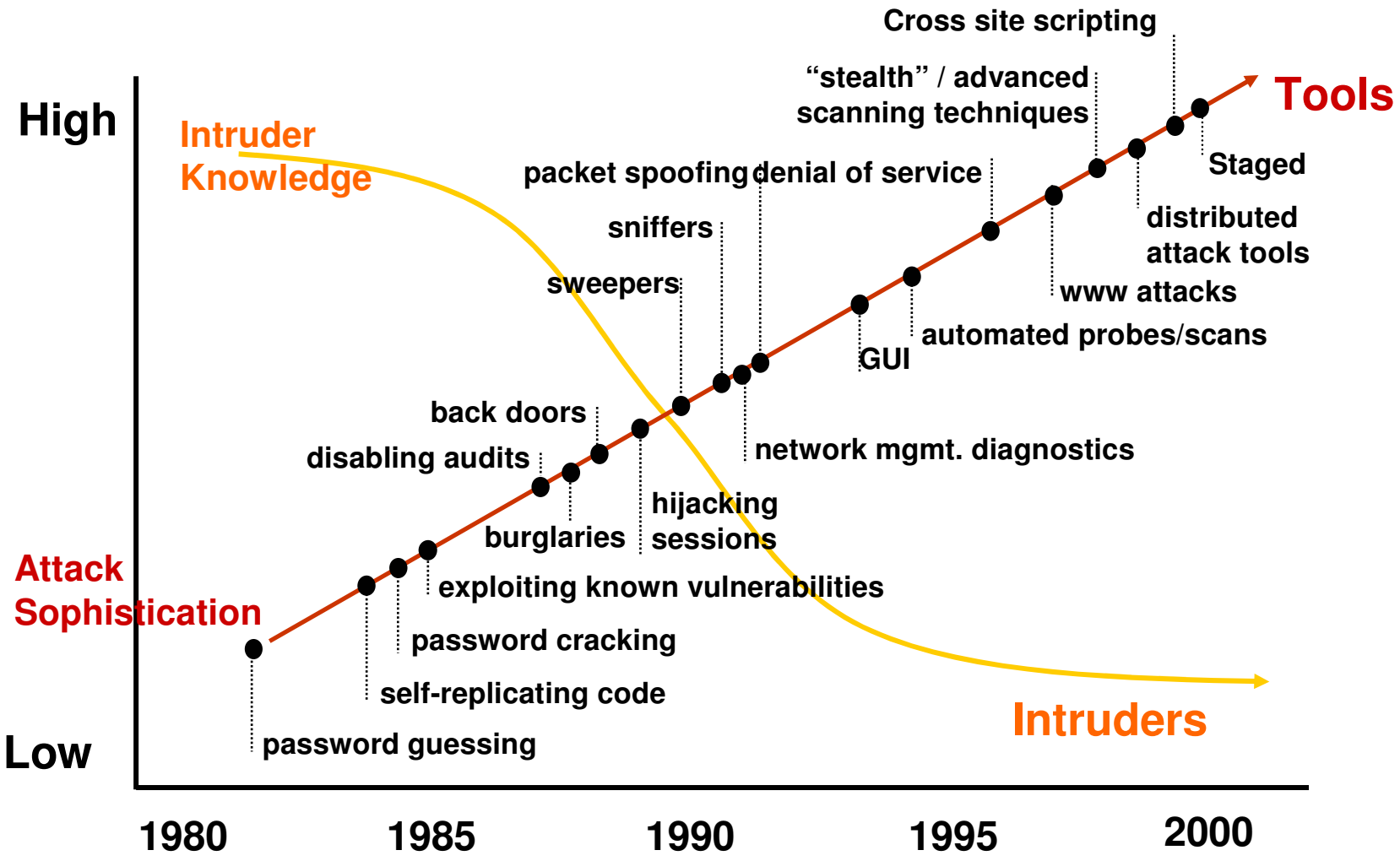
IABG

Risikofaktoren der Informationstechnologie (2)

Kriterien	Eigenschaften & Folgen
6. Asymmetrie	Geringer Aufwand & große Wirkung
7. Verwundbarkeit	Großes Spektrum & ständiger Wandel
8. Angriffe	Großes Spektrum an Arten & Optionen
9. Rechtslage	Lücken, international unabgestimmt
10. Zuständigkeiten für Reaktion & Prävention	Größtenteils unklar

IABG

Technisches Wissen im Verhältnis zu Angriffsqualität



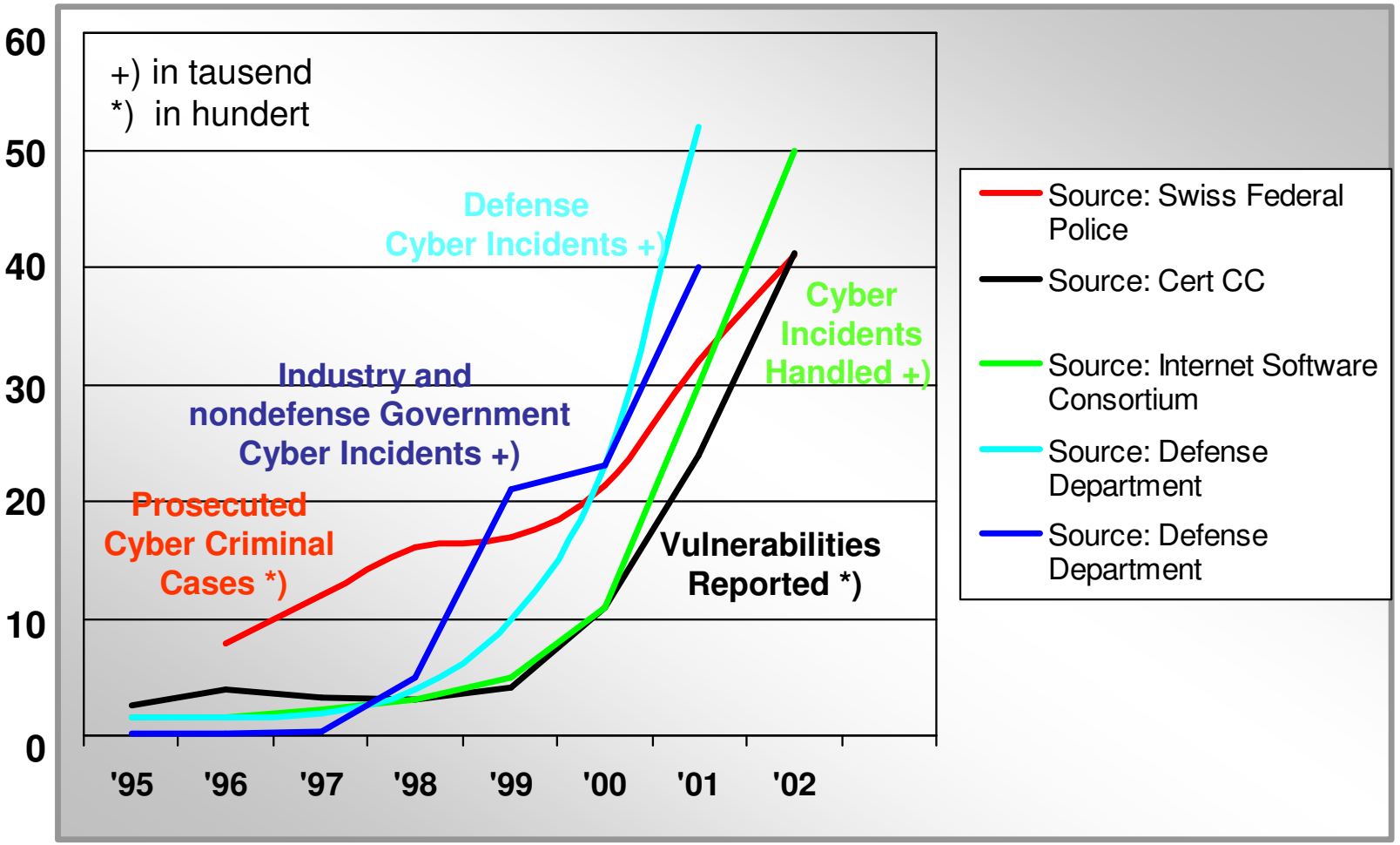
http://www.niscc.gov.uk/NISCC_Monthly.htm

Gefärdungstrends

- **Automatisierung** von Angriffswerkzeugen
- **Ausgefeilt**ere Werkzeuge
- **Schneller**es Erkennen von Verwundbarkeiten durch Angreifer
- Anstieg **asymmetrisch**er Gefahren
- Anstieg der Gefahr von **Infrastruktur**angriffen
- Umstellung proprietärer auf **standardisierte** Systeme
- Leichtere **Verfügbarkeit** und Nutzung

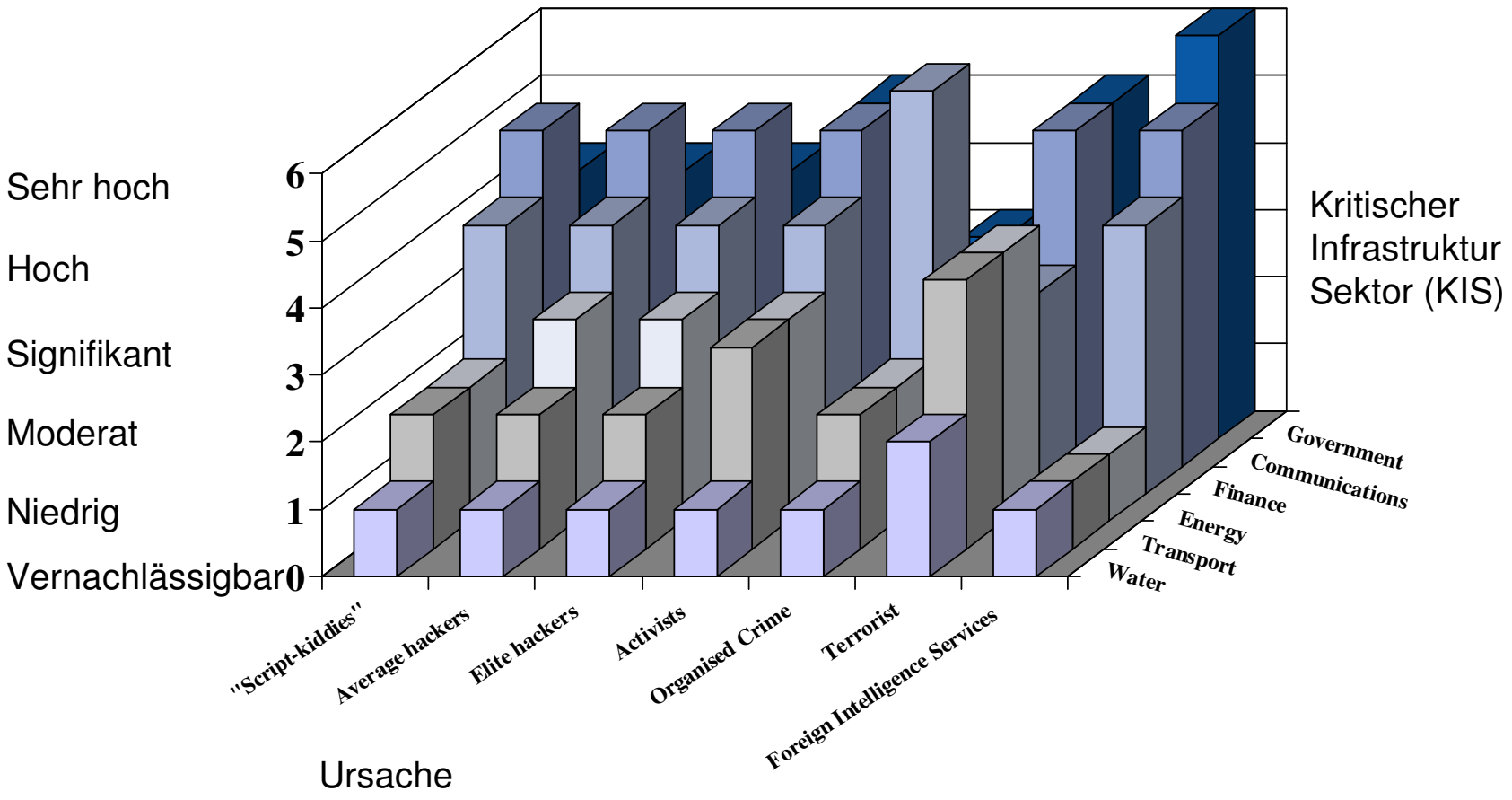
Kritische Infrastrukturen – Trends in Cybersecurity

(Ereignisanzahl)



IABG

Bedrohungsspektrum & Ziele elektronischer Angriffe

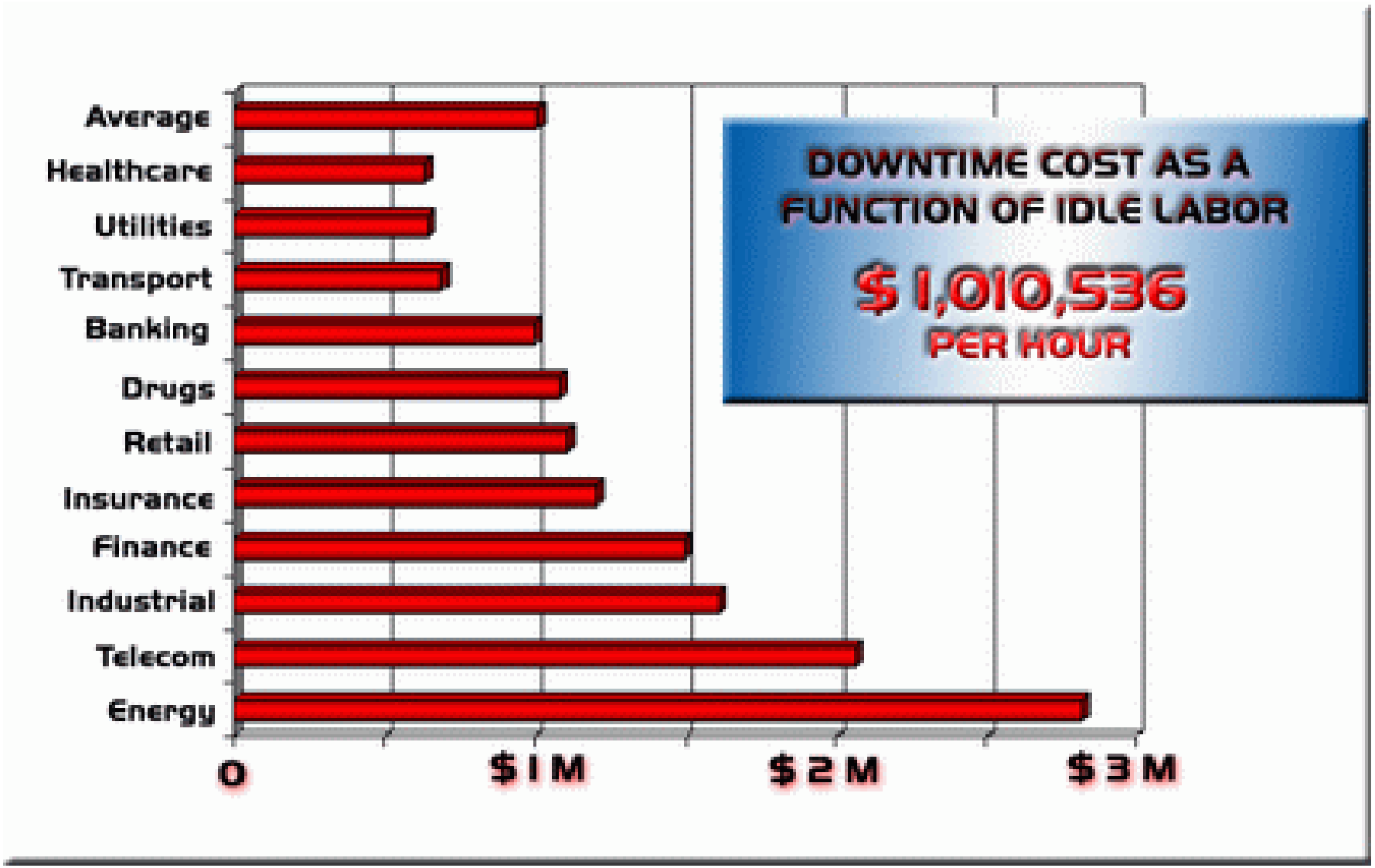


NISCC Monthly

http://www.niscc.gov.uk/NISCC_Monthly.htm

IABG

Wirtschaftliche Schäden durch IT-Ausfälle



IABG

Gefährdungsszenario - Atomkraftwerk

Slammer Worm crashed Ohio nuke plant network

The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall.

The breach did not post a safety hazard. The troubled plant had been offline since February, 2002, when workers discovered a 6-by-5-inch hole in the plant's reactor head.

http://www.securityfocus.com/news/6767

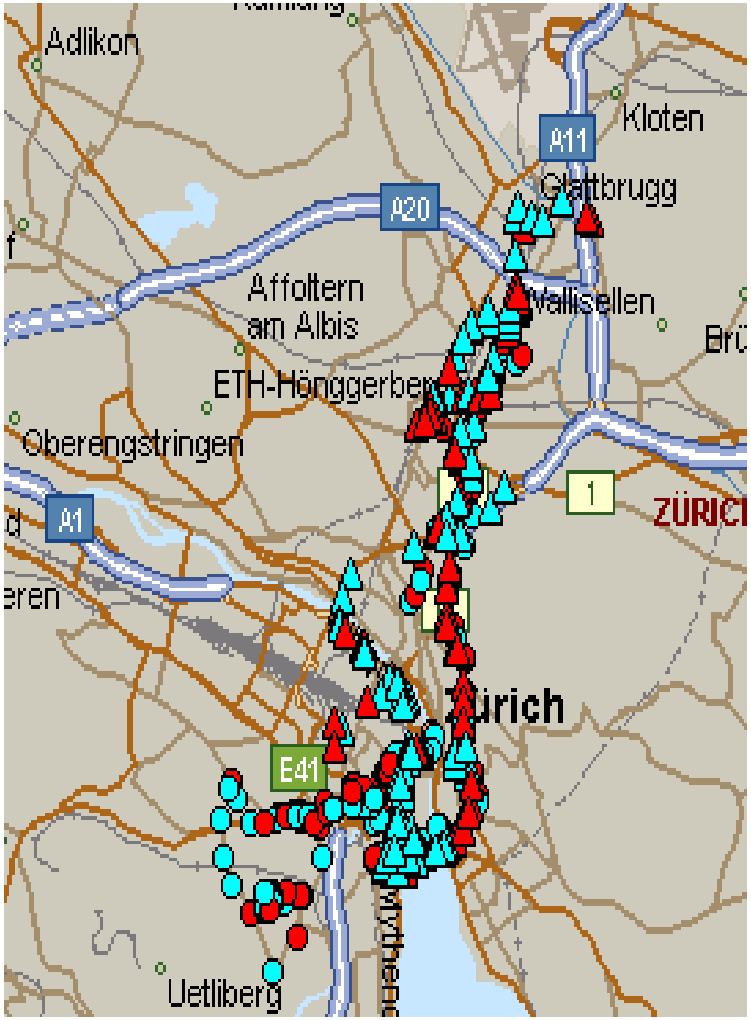
IABG

Gefährdungsszenario: Datendiebstahl/Spionage/Kostenbeeinflussung in WLANs

„Wardriving“

Necessary Equipment:

- Laptop Computer - At least a pentium 100 with a free PCMCIA slot and serial port for GPS.
- 802.11b-compliant wireless ethernet card
- The Software, Linux, BSD, Windows, Mac, everyone is supported.
- Optional: GPS receiver for location tracking.
- A way to get around, a car, bus, subway, walking, bike.



680 Wireless Netzwerke mit 2 Team‘s in 75 Minuten

http://www.bsi.bund.de/literat/doc/wlan/wlan.pdf http://www.wardriving.ch/index2.html

IABG

Gefährdungsszenario - Militärnetzwerk

Edwards Air Force Base shut down

Computer systems at Edwards Air Force Base, Calif., were shut down this week as a result of the „Blaster“ computer worm.
The desert base is home to the Air Force Flight Test Center, which conducts work on the B-2 and B-1B bombers, the airborne laser, the Global Hawk unmanned aerial vehicle, the new F-22 Raptor jet fighter, the Joint Strike Fighter and other high-tech weapons.

„We stopped access to our base computer network Monday about 2 p.m. because of the Blaster worm,“ said Air Force Lt. Col. Kerry Humphrey, a base spokeswoman. „We don't know how much damage was done, but we're slowly but surely getting our system back on line.“

The Washington Times, 2003-08-17
http://washtimes.com/national/inring.htm

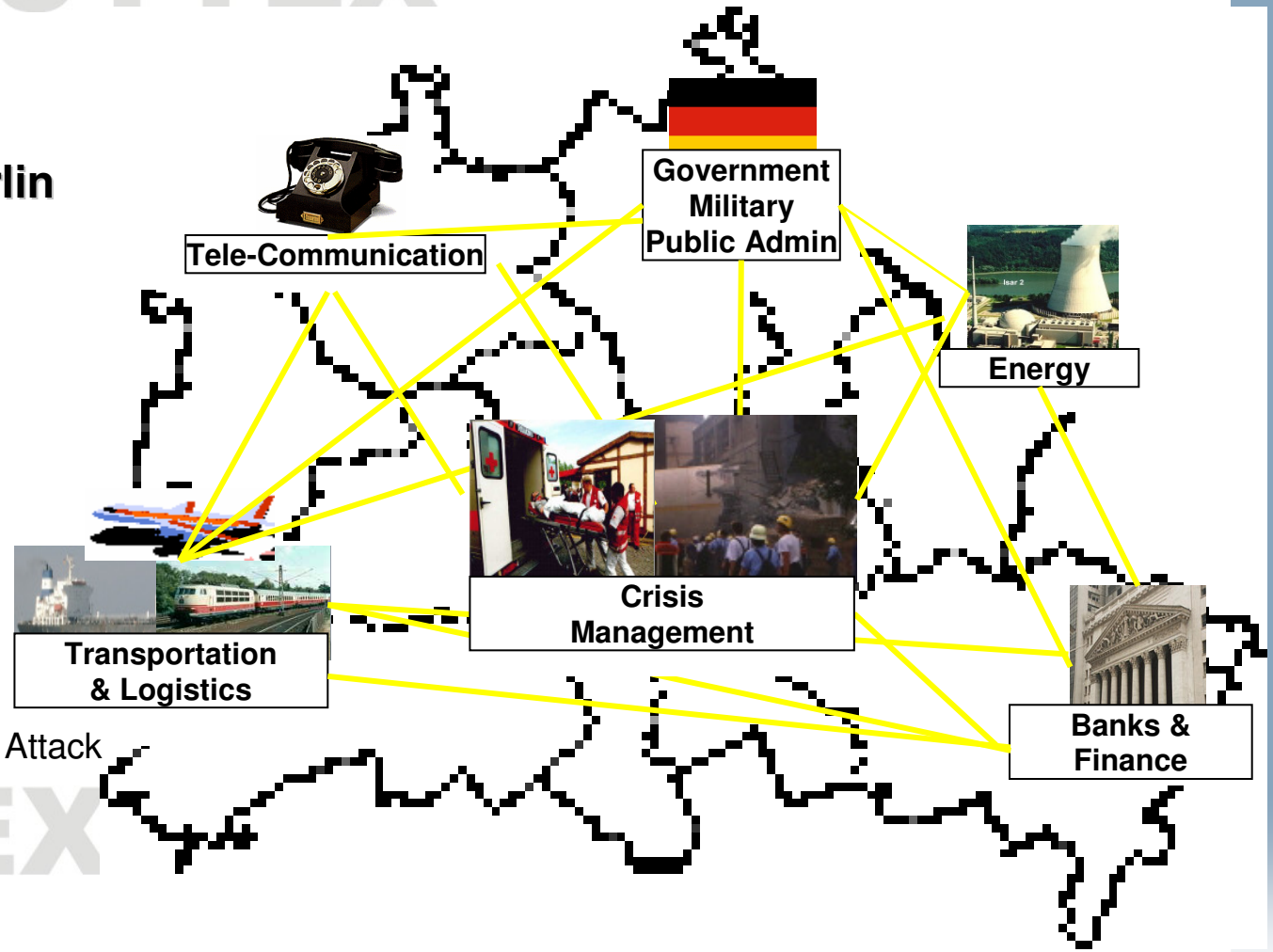
IABG

Gefährdungsszenario Cyber Attack auf Berlin

CYTEX CYTEX AKSIS

Year 200X City of Berlin

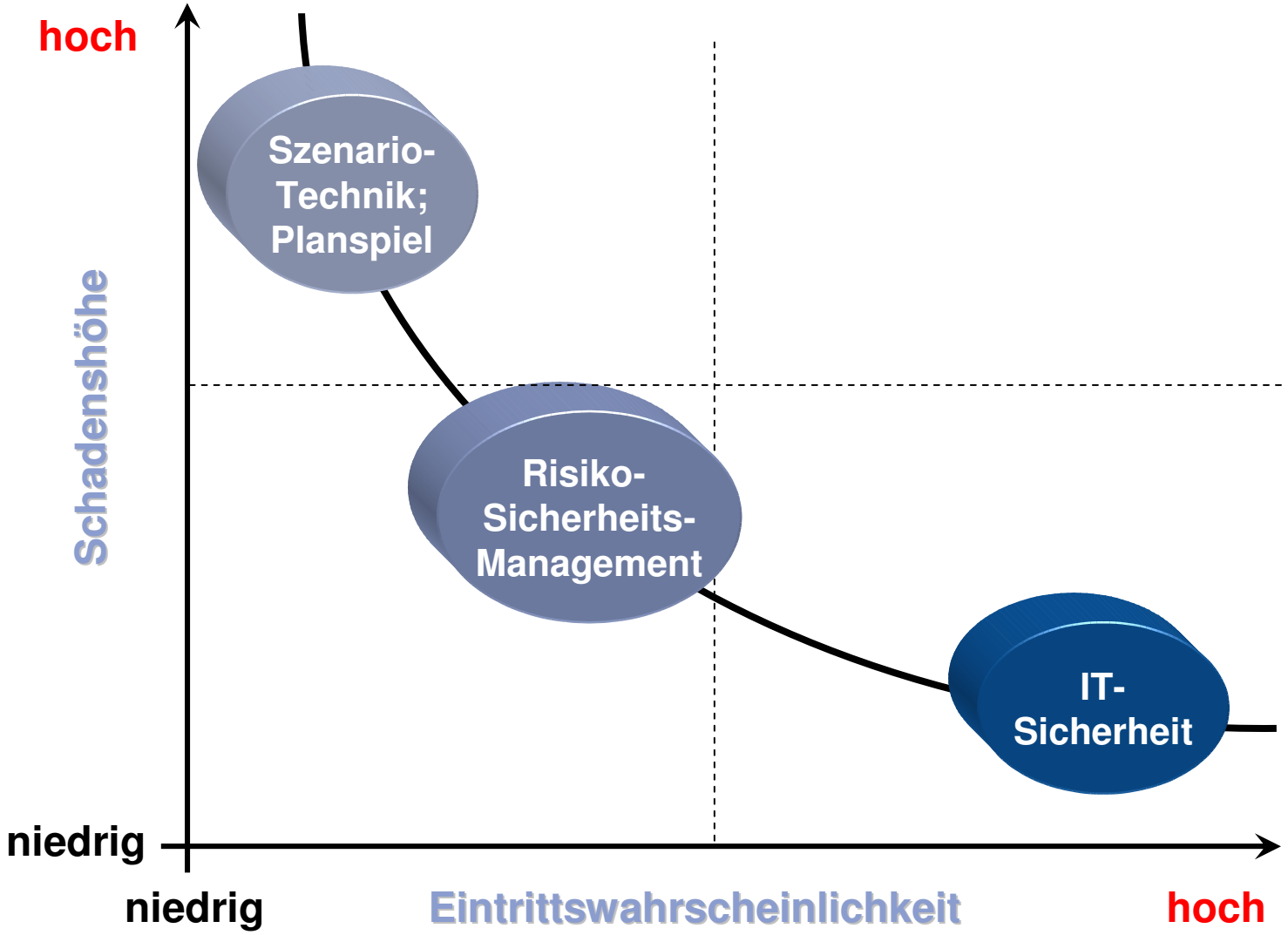
28 Jan	G8 Summit
21 Jan	Terror. Manifesto
22 Jan	Intelligence Ass. Gov't Task Force
23 Jan	Chancellor's Crisis Meeting
24 Jan	Gov't Press Conf.
24-28 Jan	Replanning of Safety & Security Forces
28 Jan	08:00 a.m. Start of Attack



CYTEX

IABG

Risikobewertung und prinzipielle Lösungsansätze



Möglichkeiten der Problembehandlung

Bedrohungsmodell

Angriff

Übungsangriff

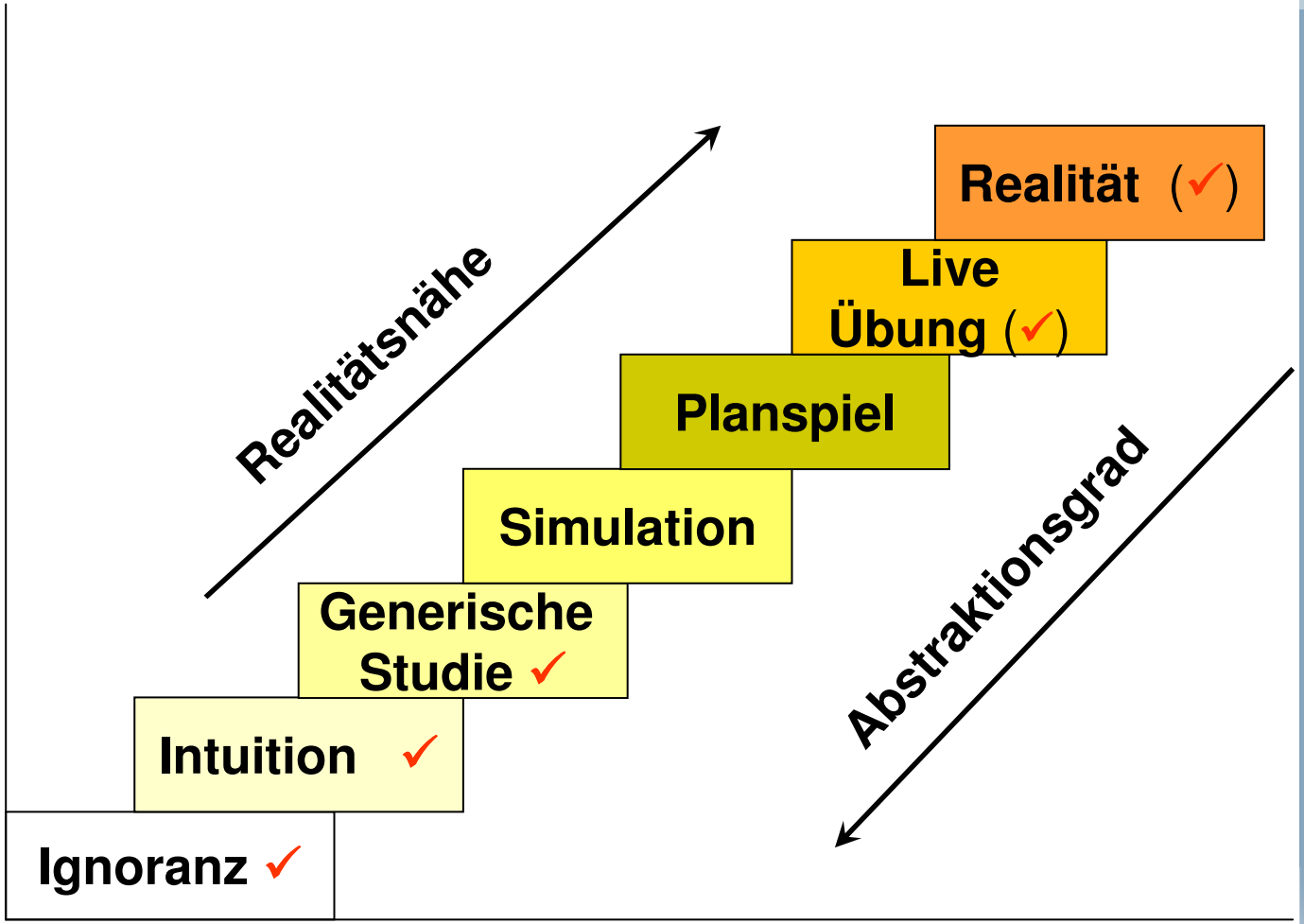
Simulierter Angriff

Computer basiertes Szenario

Gedachtes Szenario

Vorstellungen

Wer weiss?



IABG

Lösungsansätze

Public-Private-Partnerships (PPP)

- Staatliche **Anreize** für Schutzkonzepte in & von Unternehmen
- Wirtschafts-, Standort- & Industrie**politik** zugunsten ganzheitlicher Sicherheit
- Gegenseitiges **Fordern & Fördern** aller Partner in Politik und Wirtschaft
- **Regularien** nur als letzter Anker jeder staatlichen Sicherheitsstrategie
- Risiken bei **Outsourcing und Privatisierung** im Vergleich zu rein fiskalisch-monetären und wirtschaftlichen Effekten bewerten
- Höherer Stellenwert in **Forschung** & Ausbildung
- **Sensibilisierung** der Bevölkerung / Management / Politik
- **Internationale** Zusammenarbeit und Harmonisierung

IABG

Nutzen durch Infrastrukturschutz

Prävention vor Reaktion

- Minimierung direkter **Schäden**
- Konstruktiver **Umgang** mit Medien und öffentlicher Meinung
- Sicherstellen der „**Business Continuity**“
- Gesteigerte **Reputation** bei Geschäftspartnern und Kunden
- **Entlastung** von Entscheidungsträgern (KontraG, Basel II)
- Verbesserte **Einstufung** an Kapitalmärkten (?)
- **Standortvorteile** (?)
- Verbesserte **Versicherung**skonditionen
- **Technologietreiber**

Die „weichen“ Faktoren für Wirtschaft / Öffentlichkeit / Medien

- **Informationspolitik** gegenüber der Bevölkerung
- **Versachlichung** der öffentlichen Diskussion
- Abmildern von **Überreaktionen**
  - Medien-Politik-Konsens für Kritische Situationen
  - Verhindern von Panikreaktionen
  - Verhindern von Falschinformationen
- Vermittlung einer (realistischen) **positiven Grundstimmung** über die Sicherheitsvorkehrungen in Deutschland
- Vergrößerung der **Halbwertszeit** im öffentlichen und politischen Bewusstsein
- **Transnationale** Effekte

Staatliche Aufgaben im Rahmen von PPPs

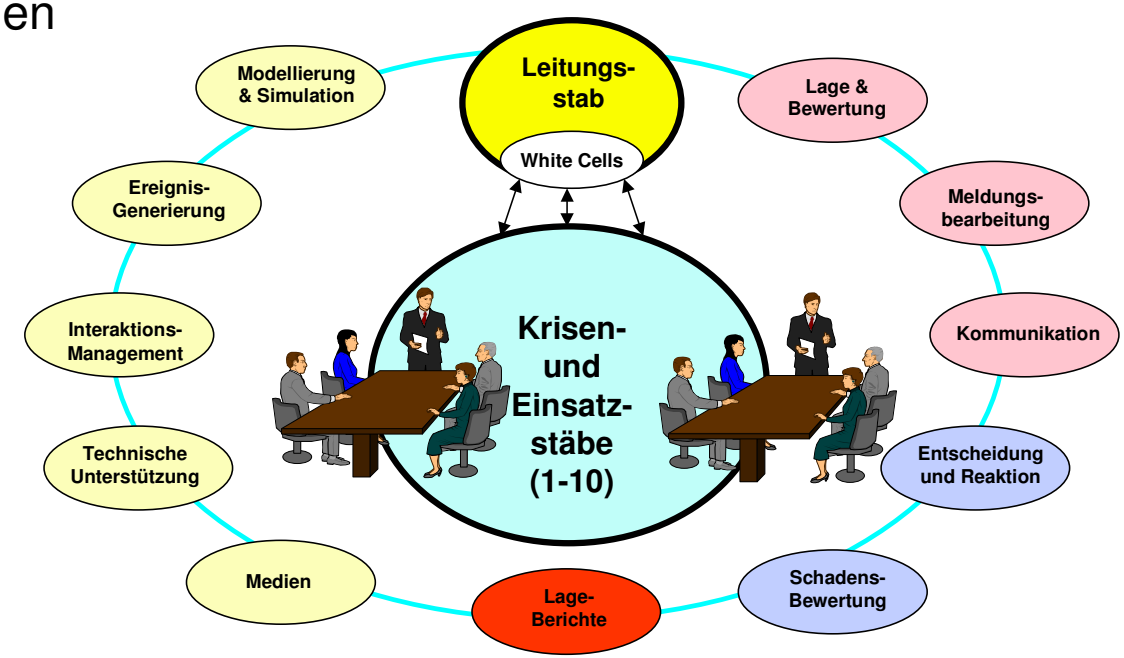
- Gesamtgesellschaftliche **Strategie**entwicklung
- Sicherheitspolitische **Bewertung** von Bedrohung und denkbaren Szenarien
- Kontinuierliche B**edrohungsanalyse** und -prognose
- Üben von **Szenarien**
- **Gesetzgebung**/Rechtsnormen anpassen
- **Kontroll**- und **Aufsicht**sverfahren und –organe überarbeiten (vgl. DHS)
- **Ausrüstung** BOS
- Zielsetzung und **Rahmen**bedingungen für PPPs schaffen
- Einwirken auf die Wirtschaft/**Dialog** mit der Wirtschaft / Selbstverpflichtungen
- **Technologieförderung**
- **Sensibilisierung** von Management/Politik/Öffentlichkeit
- **Internationale Kooperation**

IABG

Drei Beispiele für Prävention

(1) Strategieentwicklung

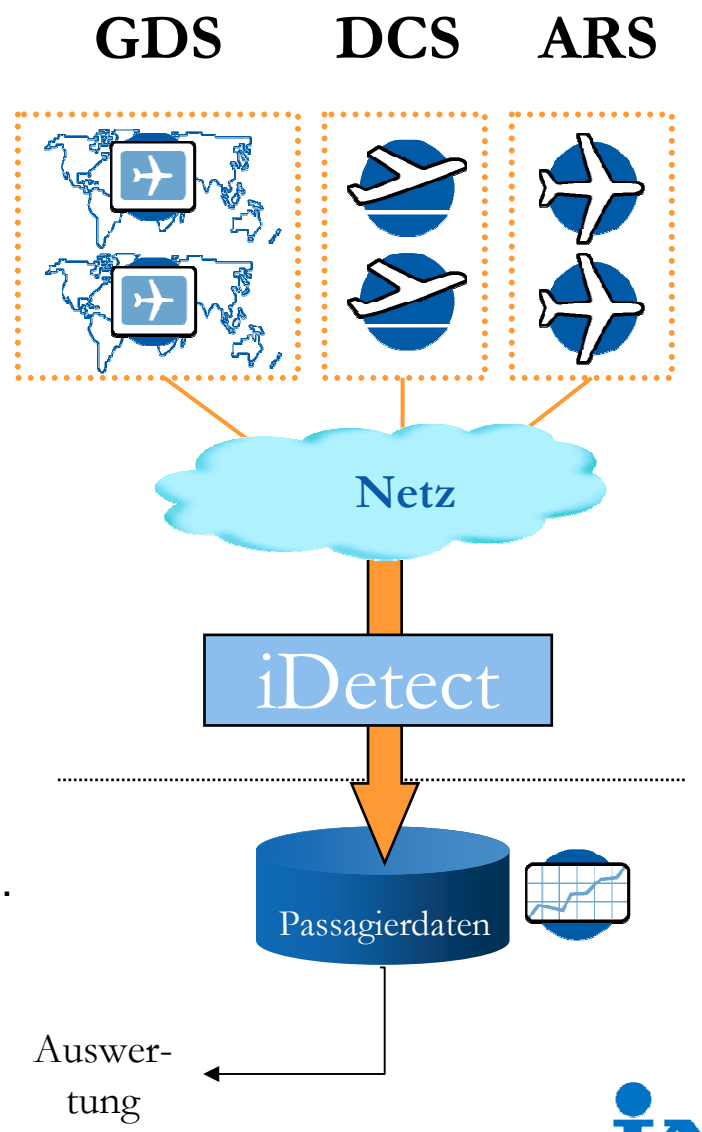
- Vordenken von **Szenarien** („Futures“)
- Leistungsfähige **Methoden** wie Planspiele und Simulationen
- **Üben** und **Bewerten** von
  - **Präventions**strategien
  - **Reaktions**strategien
- **Auswerten**
- **Umsetzten**
  der Erkenntnisse



Drei Beispiele für Prävention

(2) Management: Beispiel Flugreiseüberwachung

- Verbesserter **Schutz** der Grenzen
- Effiziente **Identifikation** verdächtiger Personen
- **Einsatz** bei Rasterfahndung
- Effizientere Fluggast **Abfertigung**
- **Zugriff** auf Reservierungs**daten**banken
  - Global Distribution Systems, z.B. AMADEUS
  - Airline Reservation Systems, z.B. Reservierungssystem LH
  - Departure Control Systems, z.B. Check-In System am MUC
- **Zugriff** auf Länderdatenbanken
- Ergänzbarkeit bei IT-basiertem **Check-In** inkl. Auswertung **biometrischer** Merkmale



Drei Beispiele für Prävention

(3) Ausrüstung: Der digitale BOS-Funk

- Anachronistische **analoge** Systeme
- Einsatz **digitaler Funksysteme** während der Oderflut zur Etablierung von Kommunikation vor **Ort und** mit Berliner Krisenstab (Ausfall der gesamten Infrastruktur)
- **Schengen** Abkommen
- Realisierung eines **deutschlandweiten** digitalen Funksystems
- Einheitlich, **Abhörsicher, Datenaustausch,** Fault Tolerant
- Geleitzugprinzip
- Ausschreibung Anfang 2004?
- **Systemoffenes** Ausschreibungsverfahren
- Technik, Vergaberecht, Betreibermodelle, **Wirtschaftlichkeit,** Finanzierung
- Erfolgreiche **Referenzprojekte**

IABG

Resume

- **Die Informationsgesellschaft**:
  - Birgt zunehmende neue **Risiken**
  - Ist neuen **Bedrohungen** ausgesetzt
  - Mit z.T. unbekannten **Folgen**

- **Szenarien:**
  - **Realität** nicht abwarten
  - **Prognose** wagen
  - **Fiktionen** vermeiden

- **Lösungsansätze:**
  - **Methoden** entwickeln und anwenden
  - **Strategien** erstellen und umsetzen
  - **Management** sensibilisieren/verbessern
  - **Technologien** entwickeln und **Ausrüstung** adäquat gestalten

IABG

Vielen Dank für Ihre Aufmerksamkeit!

www.aksis.de

www.eu-acip.de

www.edag.info

www.iabg.de