Dieser Vortrag wurde im Rahmen meiner früheren Tätigkeit bei der Fa. IABG gehalten und enthält entsprechende Quellen. Im Einvernehmen mit der IABG wurde auf detaillierte Quellenangaben im Einzelnen verzichtet

Kritische Infrastrukturen

- Eine neue Herausforderung -

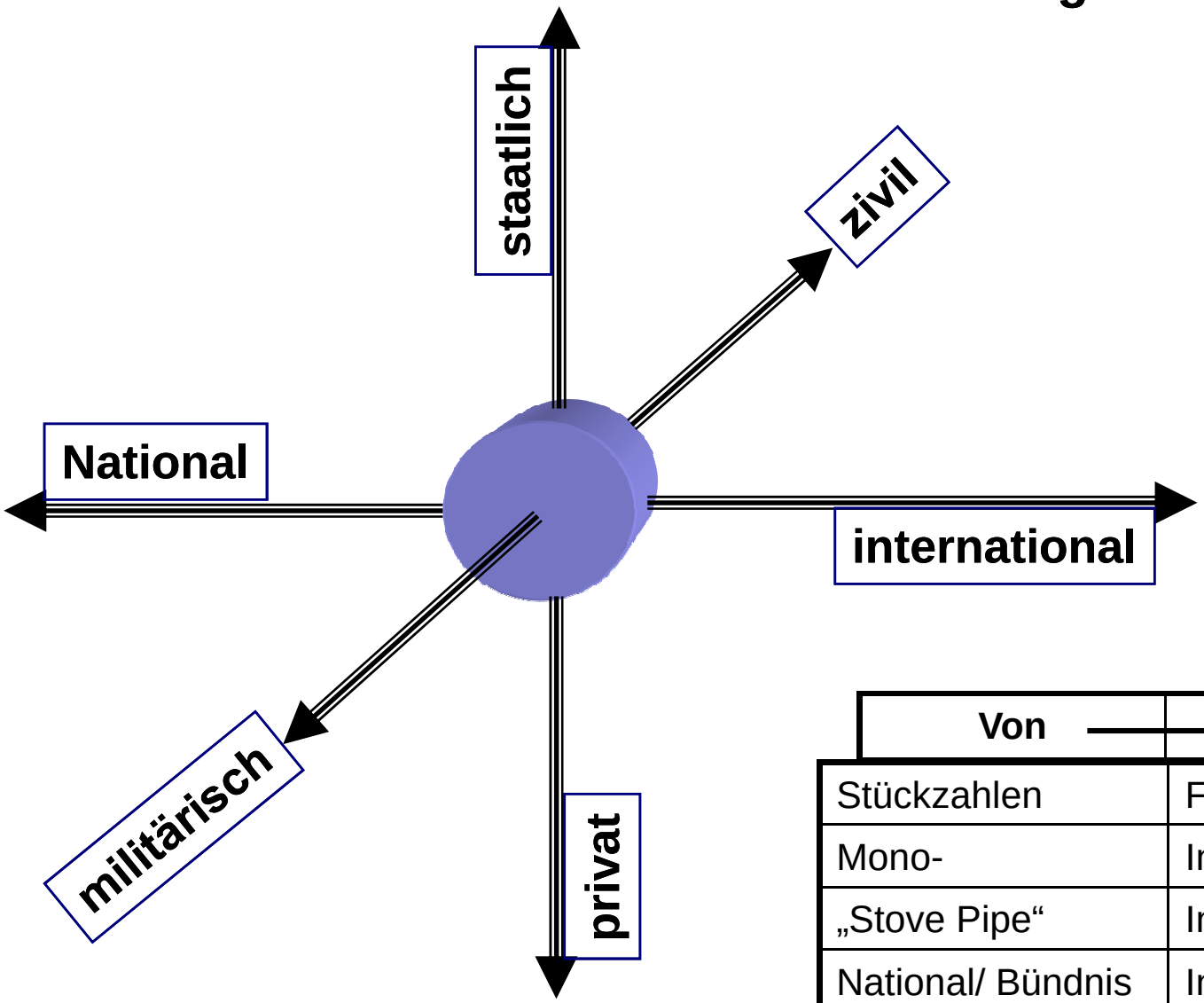
WimEsA
Universität der Bw München
9. Juni 2006

Reinhard W. Hutter
Sicherheitsberater
hutter@iabg.de
reinhard.hutter@gmx.de

Inhaltsübersicht

1. Das Problem
2. Besonderheiten der Kritischen Infrastrukturen
3. Programme und Maßnahmen
4. Beispiele
5. Resumé und Ausblick

Die neuen Dimensionen und Herausforderungen der Sicherheit



Von →	Zu
Stückzahlen	Fäh./ Wirkungen
Mono-	Interdisziplinär
„Stove Pipe“	Interoperabel
National/ Bündnis	Internat.Koalitionen
Schutz der Nation	Schutz der (Welt) - Bürger

Security Awareness

Where are we?

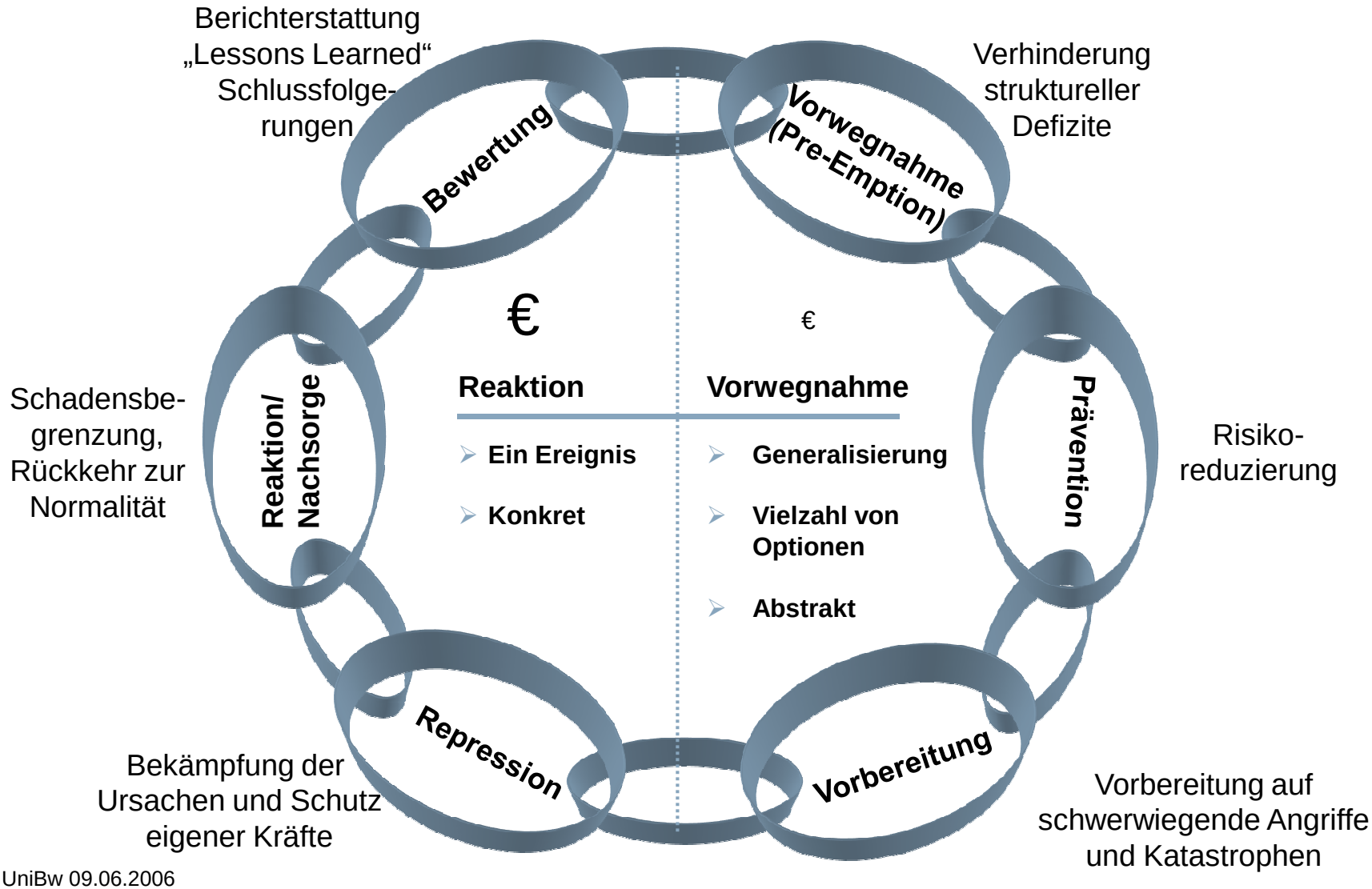
So far:

Society and Individuals	Tend to ignore
Politics and Public Admin.	Tend to prefer short-term fovours
Economy / Industry	Tend to save Money

However, there is

- Increasing Demand of Society and Individuals
- Upcoming Strategic Programs of Governments and International Organisations
- Security Awareness Programs of (some) major Industries

Die Sicherheitskette



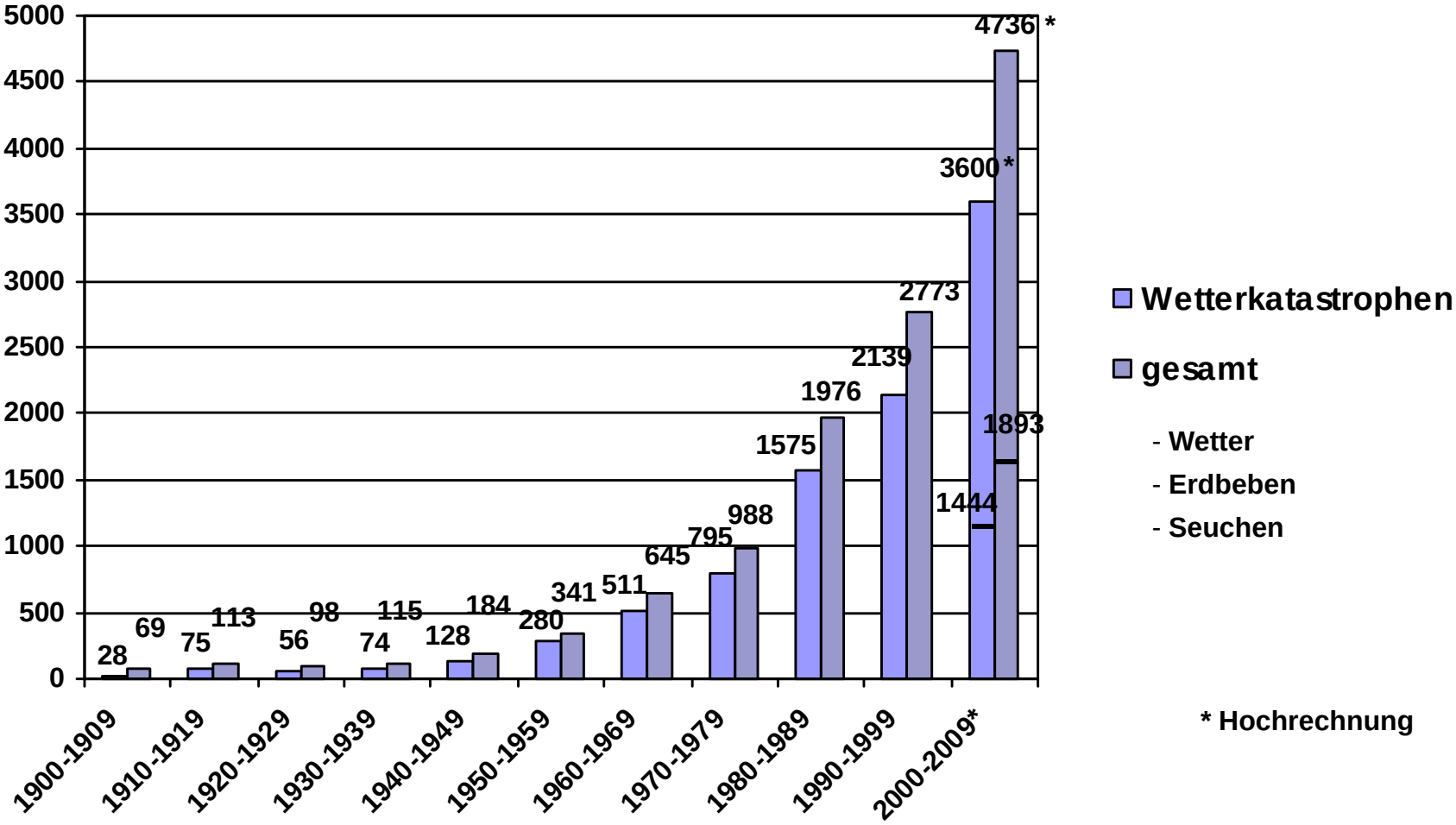
Quelle: TNO/IABG

Bedrohungen moderner Gesellschaften

Ursachen und Quellen

- Katastrophen
  - Natürliche: Umwelt; Klima
  - Künstliche: Industrien; Anlagen; Infrastukturen
- Pandemien
- Organisierte Kriminalität
- Terrorismus
- Instabile Staaten
- Proliferation
- Krieg

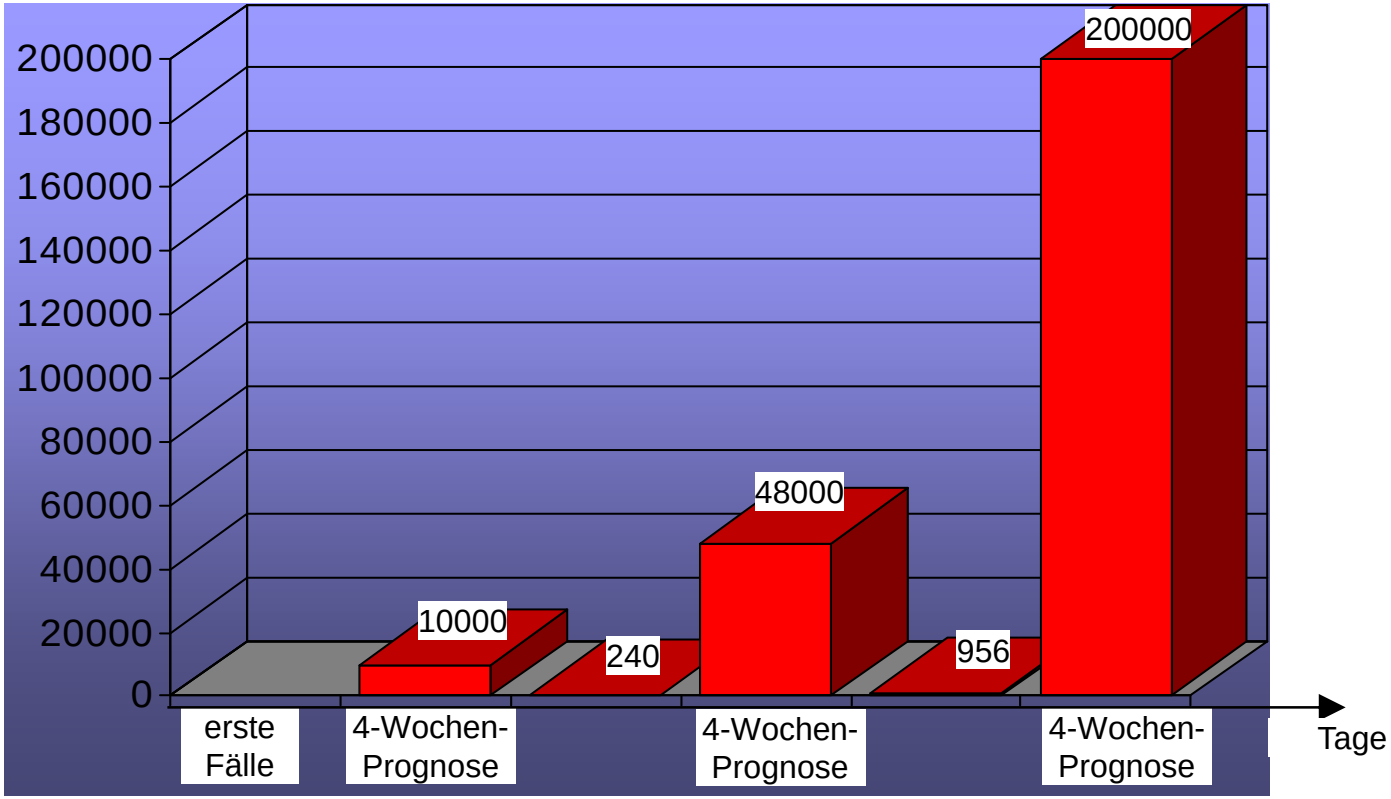
Naturkatastrophen



Quelle: EM-DAT: The OFDA/CRED International Disaster Database

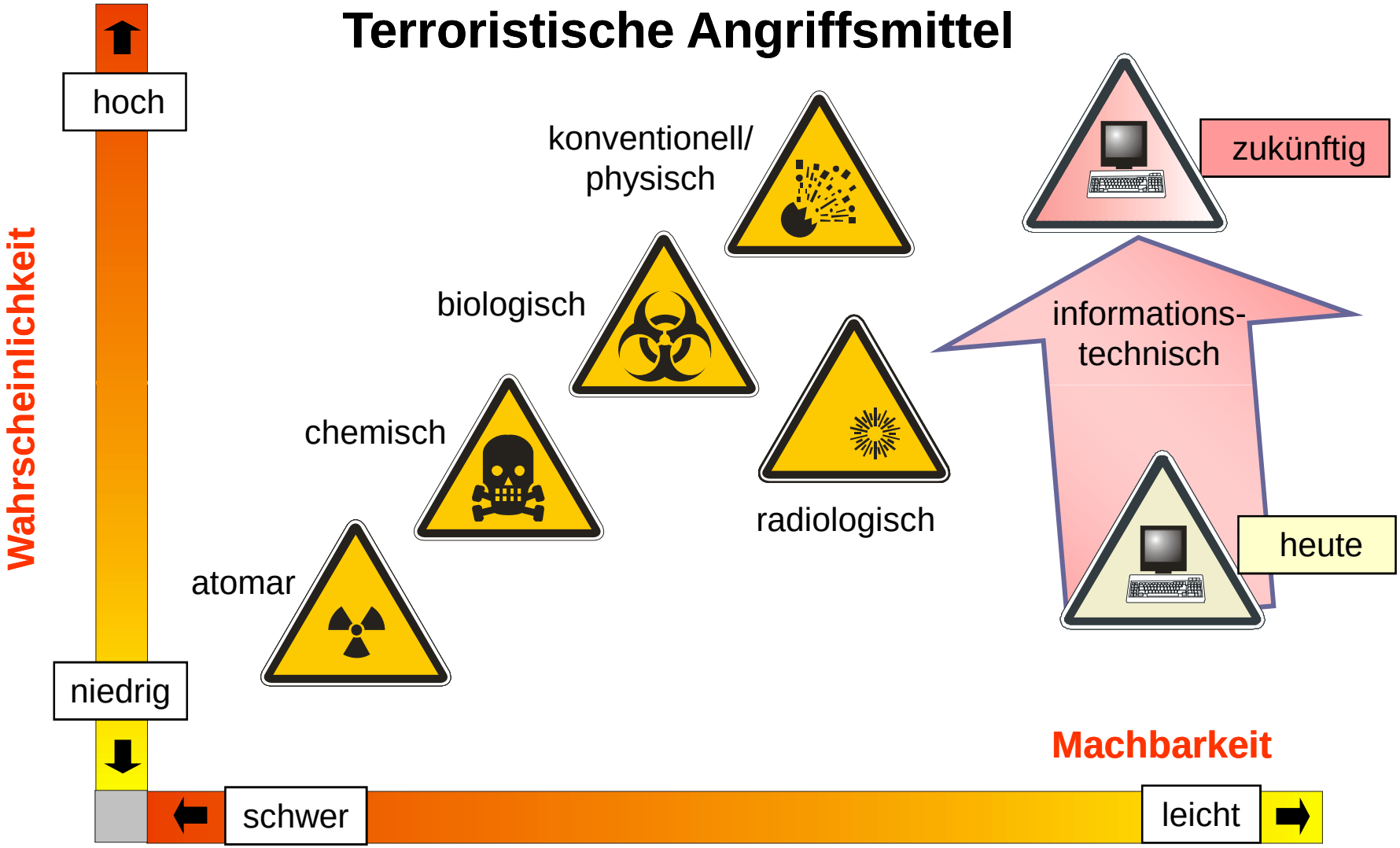
Angriff mit Pockenviren

Prognosen von Pockeninfektionen nach einem Angriff in Europa

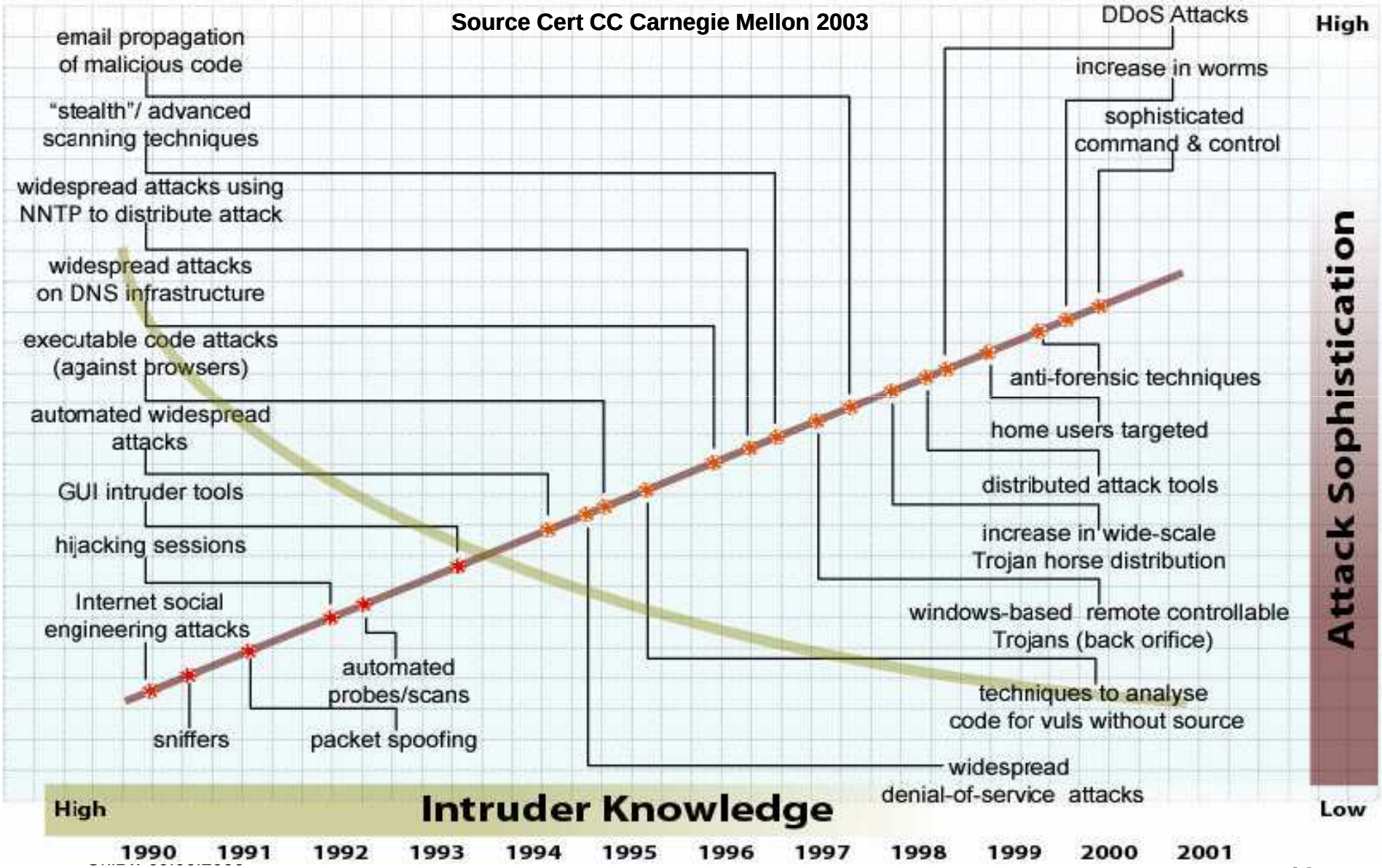


Quelle: Planspiel „Atlantic Storm“, Januar 2005

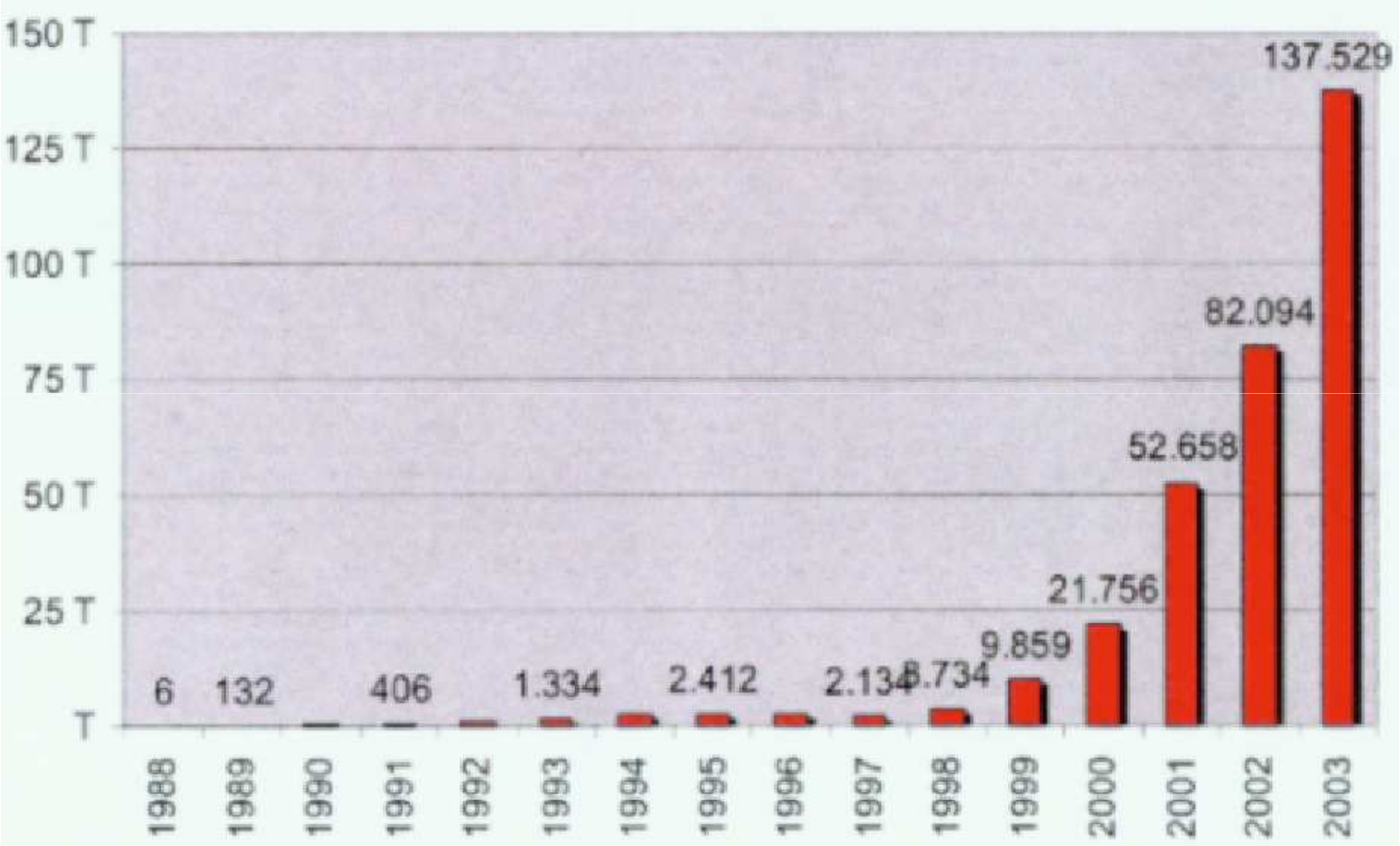
Bedrohungstrends: Terroristische Angriffsmittel



Attack Sophistication vs. Intruder Knowledge

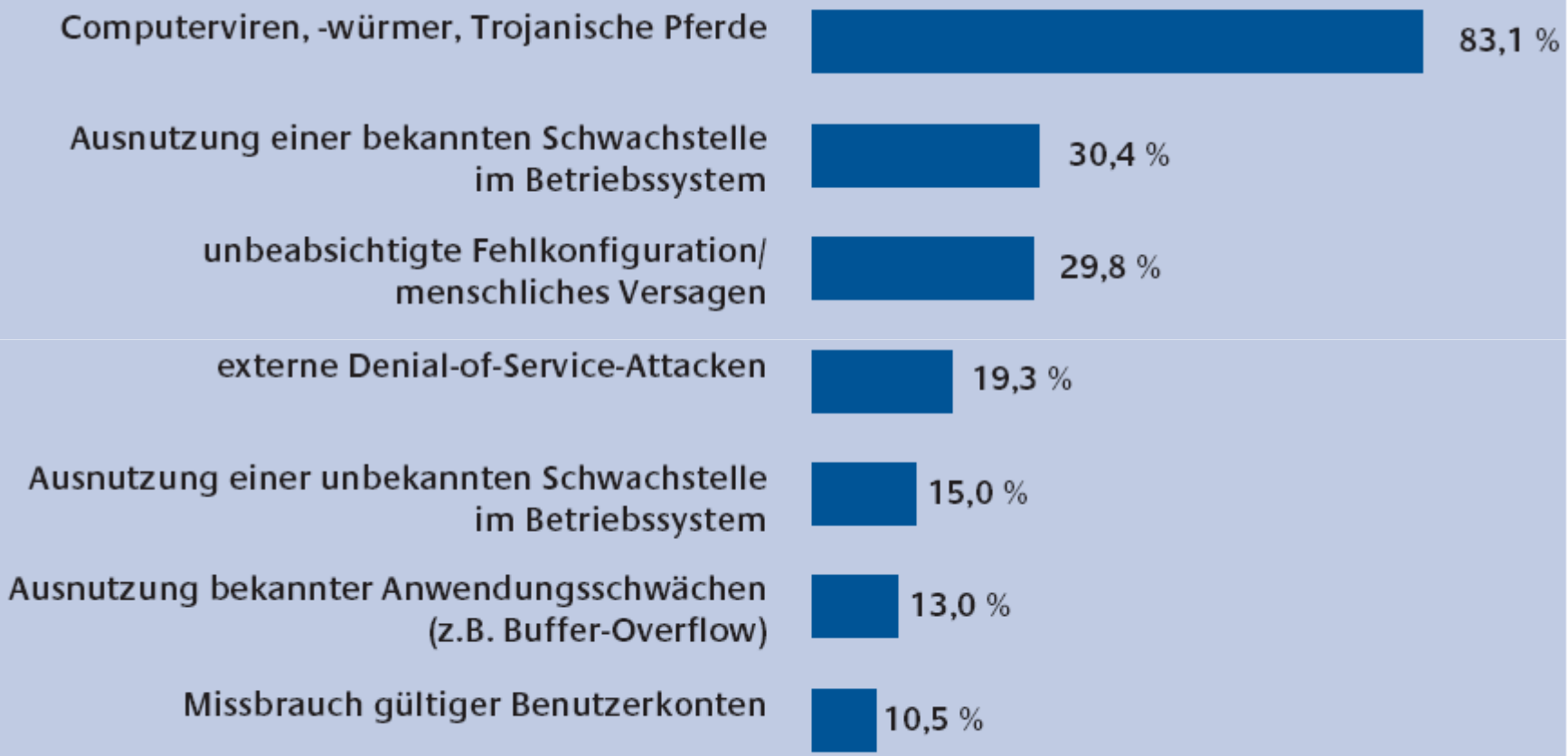


Cyber Security Incidents

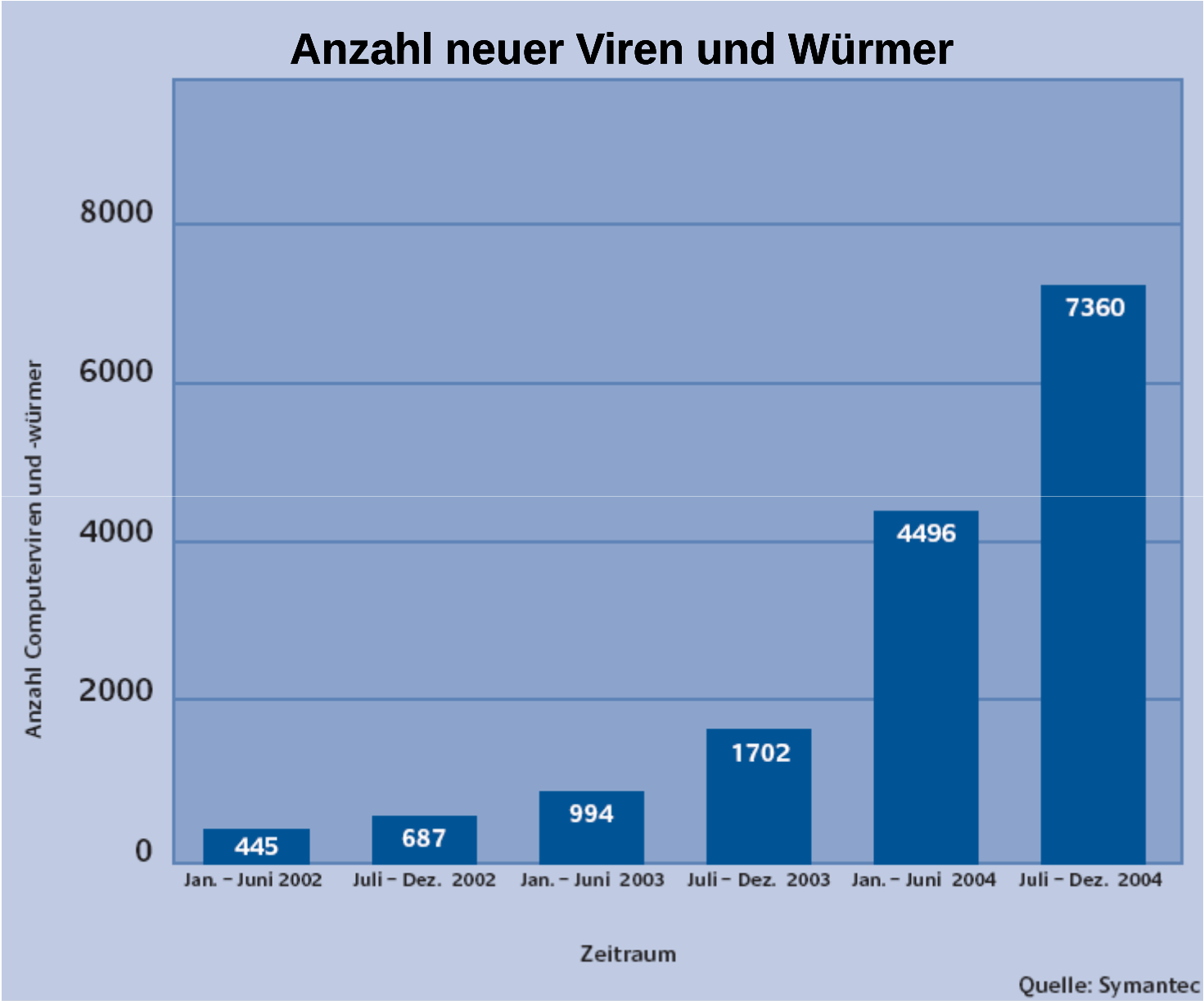


Source: CERT-CC, Carnegie Mellon University 22.01.04

Art der Sicherheitsverstöße / Angriffsmethoden

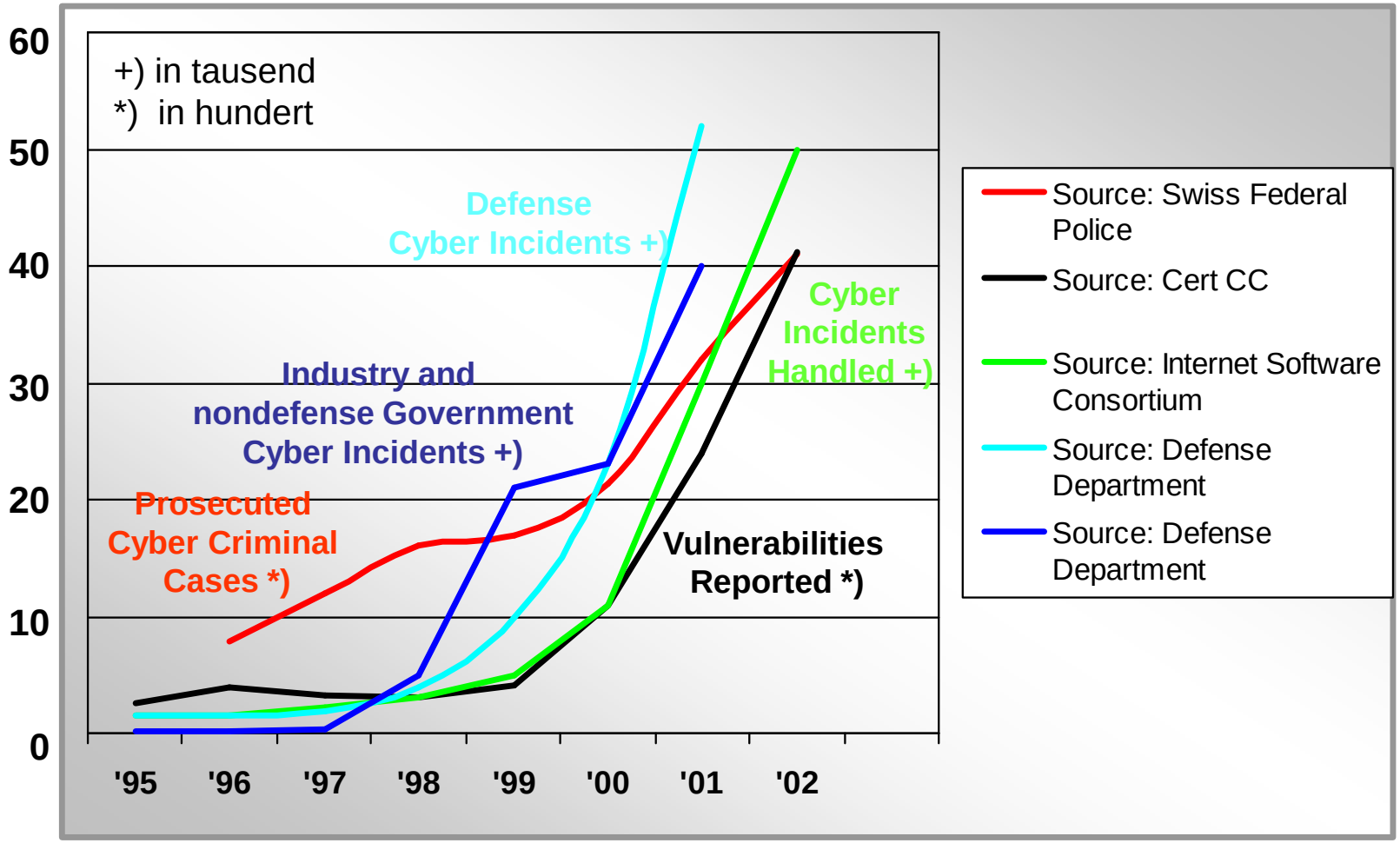


Quelle: InformationWeek


Anzahl neuer Viren und Würmer
Anzahl Computerviren und -würmer
8000
6000
4000
2000
0
445
687
994
1702
4496
7360
Jan. – Juni 2002
Juli – Dez. 2002
Jan. – Juni 2003
Juli – Dez. 2003
Jan. – Juni 2004
Juli – Dez. 2004
Zeitraum
Quelle: Symantec

Trends in Cyber Security

Ereignisanzahl



Akteure und Motivation

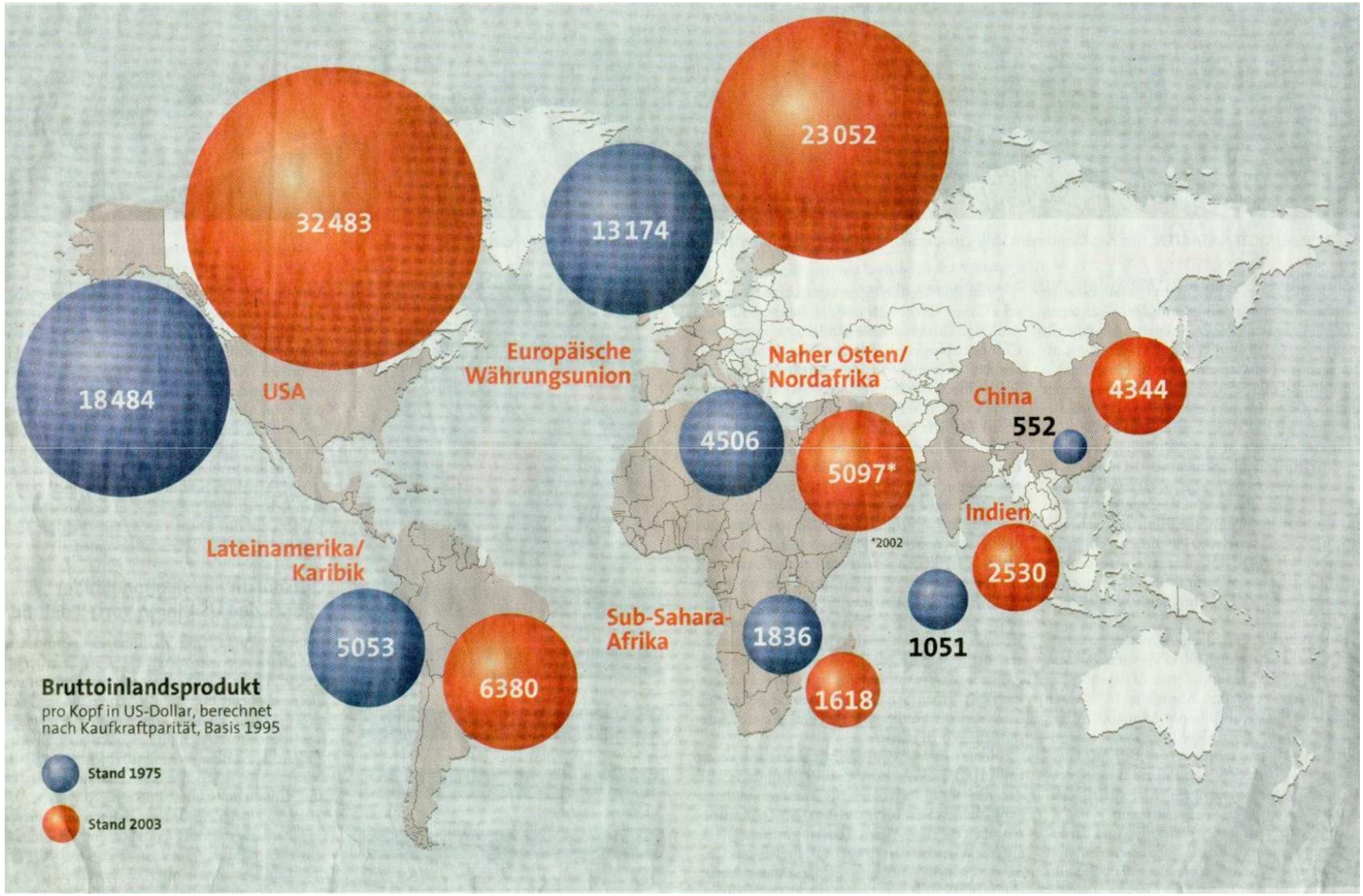
Akteur \ Absicht	Aussen-wirkung	Rache	Kon-trolle	Betrü-gen	Spio-nieren	Schä-digen	Er-pressen	Zer-stören
„Amateur“ Hacker	🔴	🟡	⚪	⚪		⚪		
Innentäter	🟡	🔴	🟡	🟡	🟡	🔴	⚪	🔴
Kriminelle Gruppen		⚪	🟡	🔴	🟡	🔴	🔴	🔴
Wirtschafts-Spionage			⚪	⚪	🔴	🔴	🟡	🟡
Ideologisch moti-vierte Terroristen	🔴	🔴	🟡	🟡	🟡	🔴	🟡	🔴
Strategischer Terrorismus	🔴	⚪	⚪	⚪	⚪	🔴	⚪	🔴
Terroristen im staatl. Auftrag	🟡	🟡	🟡	⚪	🔴	🔴	🔴	🔴
Staatliche Organe		🟡	🔴	⚪	🔴	🔴	🔴	🔴

🔴 Stark zutreffend 🟡 zutreffend ⚪ schwach zutreffend

Ursachen von Verwundbarkeiten

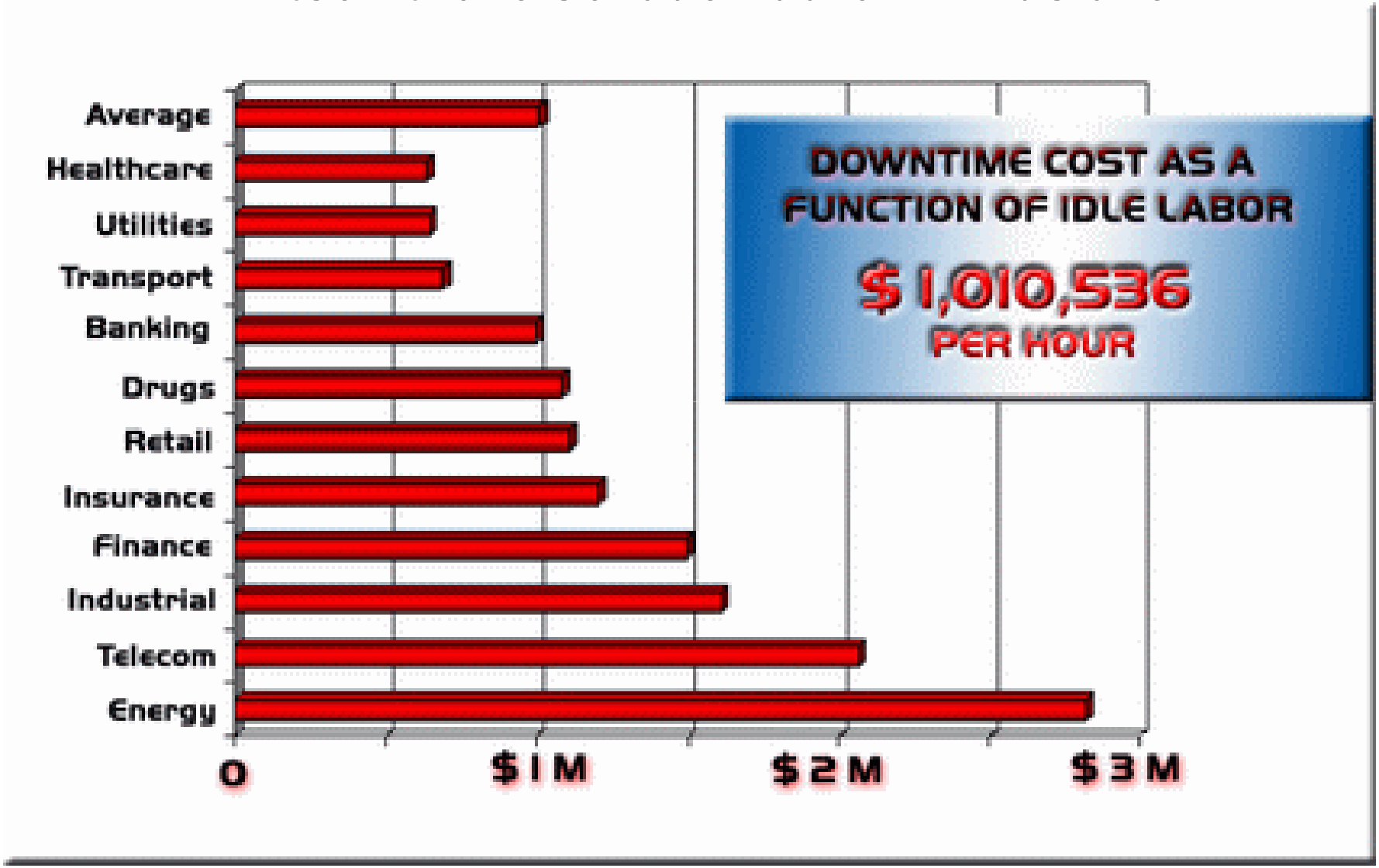
- Vernetzung und Abhängigkeiten in Wirtschaft und Gesellschaft
- Wohlstand und Armut
- Bevölkerungs - Konzentrationen
- Technische Komplexität und Empfindlichkeit
- Rohstoff – Begrenzung
- Umwelt und Klima
- Wahrnehmung und Kommunikation von Ereignissen
- Kritische Infrastukturen

Entwicklung Bruttosozialprodukt



Zeit-Grafik/Quelle: Weltbank

Wirtschftliche Schäden durch IT-Ausfälle



Source: NISCC (UK)

1. Inhaltsübersicht

1. Das Problem
2. Besonderheiten der Kritischen Infrastrukturen
3. Programme und Maßnahmen
4. Beispiele
5. Resumé und Ausblick

Definition Kritische Infrastrukturen

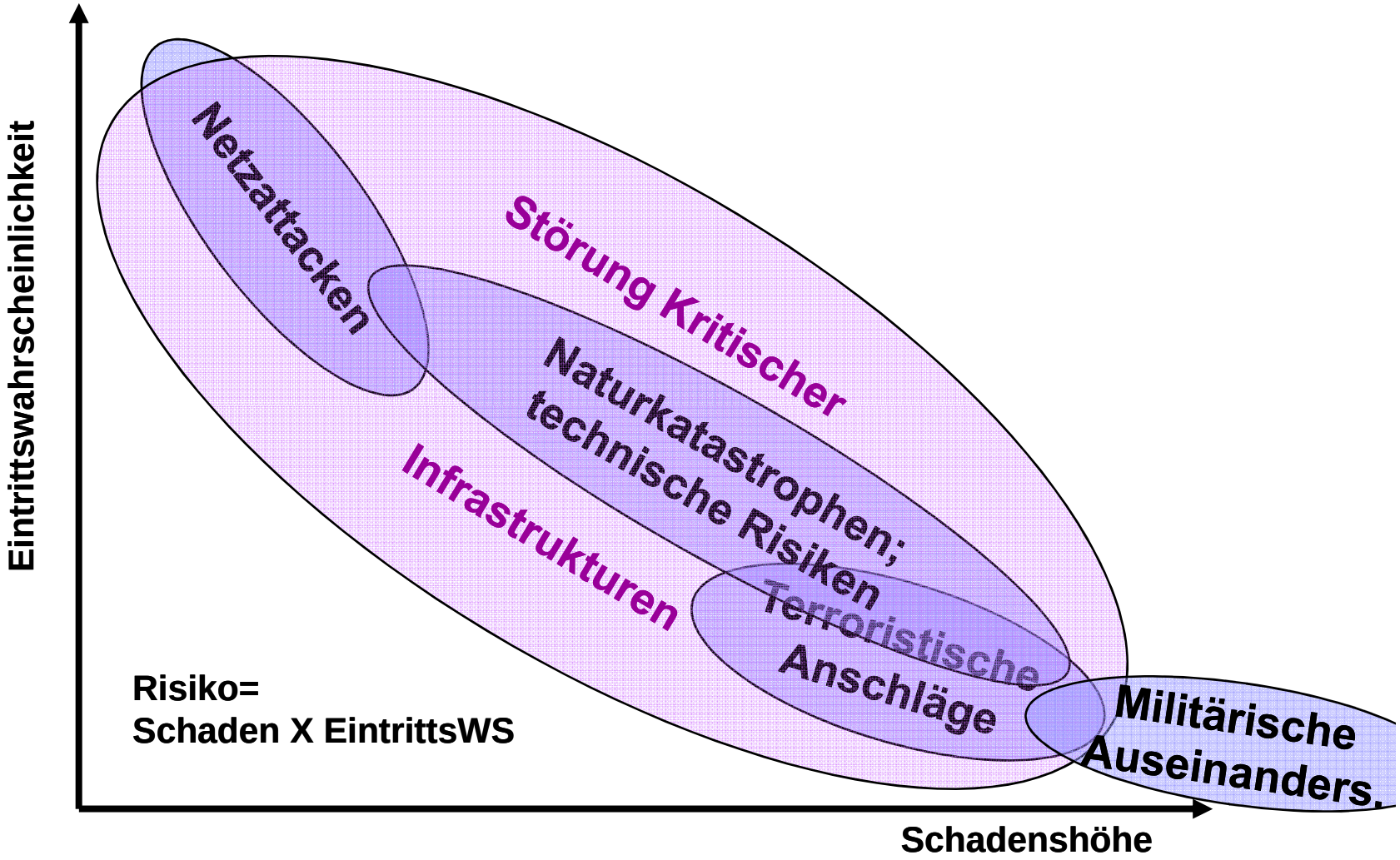
Vernetzte Systeme, deren Ausfall oder Beeinträchtigung erhebliche Auswirkungen haben auf

- **Gesundheit und Leben der Bevölkerung**
- **Die Wirtschaft**
- **Die Funktionsfähigkeit von Staat und Gesellschaft**

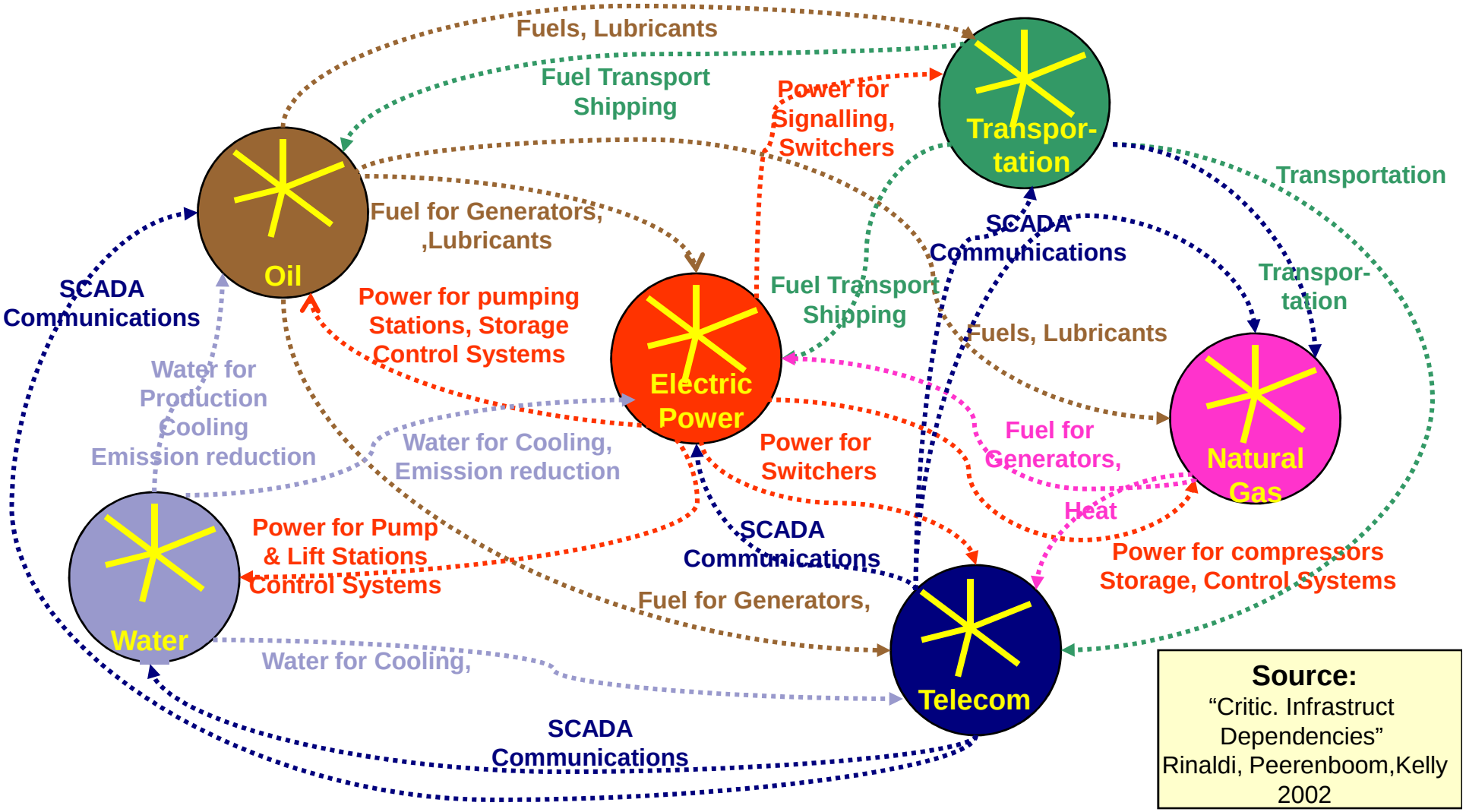
Kritische Infrastrukturen

Herausforderungen für die vernetzte Gesellschaft

Risikobetrachtung



The Risk Factor Interdependencies



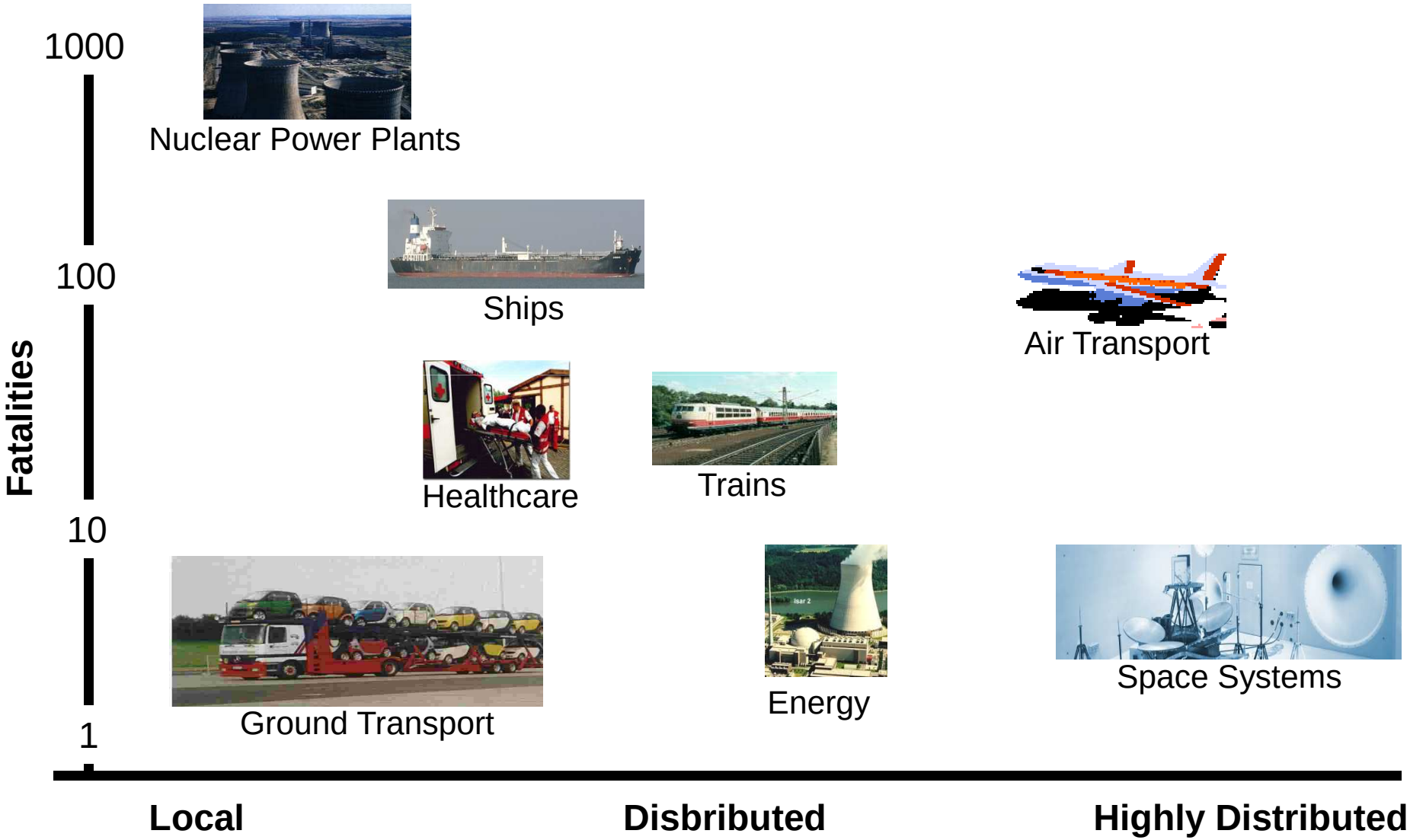
Source:
"Critic. Infrastruct Dependencies"
Rinaldi, Peerenboom,Kelly
2002

Infrastrukturen: Schadenskategorien

	Angriffe		Schadenskategorien											
Kritische Infrastrukturen	Wahrscheinl.	Möglichkeit	Personen	Finanzen	Infrastrukturen	Material	Produktion	Markt/ Produkte	Umwelt	Administration	Politik	Gesellschaft	Wissen	Ethische Werte
1 Telekommunikation	hoch	hoch	gering	hoch	hoch	gering	hoch	mittel	gering	mittel	gering	hoch	gering	gering
2 Energie	hoch	hoch	hoch	hoch	hoch	mittel	hoch	gering	hoch	mittel	gering	hoch	gering	gering
3 Wasser/Lebensmittel	mittel	mittel	hoch	gering	mittel	hoch	mittel	gering	hoch	gering	hoch	hoch	gering	gering
4 Transport/Verkehr	hoch	mittel	hoch	mittel	hoch	mittel	hoch	mittel	gering	gering	gering	mittel	gering	gering
5 Finanzwesen	hoch	hoch	gering	hoch	gering	gering	mittel	mittel	gering	mittel	mittel	hoch	gering	mittel
6 Sensitive Industrien	mittel	mittel	gering	mittel	gering	mittel	hoch	mittel	mittel	gering	mittel	gering	mittel	gering
7 Sicherheitsdienste/Bw	mittel	mittel	hoch	gering	mittel	gering	gering	gering	gering	mittel	hoch	hoch	gering	mittel
8 Gesundheitswesen	hoch	gering	hoch	gering	gering	gering	gering	gering	gering	mittel	mittel	hoch	gering	mittel
9 Kulturelle Einrichtungen	mittel	gering	gering	gering	gering	gering	gering	gering	gering	gering	gering	gering	gering	mittel
10 Regierung/Verwaltung	hoch	mittel	gering	mittel	mittel	gering	gering	gering	gering	hoch	hoch	mittel	mittel	mittel
11 Medien	hoch	mittel	gering	gering	gering	gering	gering	gering	gering	gering	mittel	hoch	mittel	mittel
12 Erziehung/Ausbildung	hoch	gering	gering	gering	gering	gering	gering	gering	gering	gering	gering	mittel	mittel	mittel

hoch mittel gering

Cyber Terrorism and Critical Infrastructures




AKSIS
www.aksis.de
Ziele
Programm
Ausblick
Kontakte
Veröffentlichungen
Quellen
Arbeits-
Kreis
Schutz von
Infra-
Strukturen
Ausbildung & Erziehung
Tele-kommuni-kation
Energie
Medien
Wasser & Lebens-mittel
Politik & Verwaltung
Transport & Verkehr
Kulturelle & Soziale Einricht-ungen
Finanz-wesen
Gesund-heits-wesen
Bundes-wehr & Sicherheits-dienste
Sensitive Industrien

Das Beispiel Elektrizitätsversorgung

▪Komplexität	▪Netze/ Technik ▪Betrieb
▪Interdependenzen	▪Fast alle Sektoren abhängig ▪Bsp.: TK; Gesundheitsw.; Verkehr
▪Worst Case Scenarios	▪Simultane Störung von E- und I-Netz ▪Störfälle ≥ (N-1)
▪Markt/ Liberalisierung	▪Investitionen in Scherheit ? ▪Netze arbeiten näher am „limit“
▪Internationalität	▪Abhängigkeit von anderen ▪Controlsyst. nicht durchgängig
▪Besondere Merkmale	▪Offenheit-Verwundbarkeit ▪Technik z.T. veraltet ▪Analyse und Steuerungs-Methoden nicht adäquat

Challenges for Analysis and Methodologies

From Cold War to CIP

System View:	from Components	to Networks
	from Single Sector	to Multidisciplinary
	from Bounded	to Unbounded
MOE/Metrology:	from Few	to Manyfold
Knowledge:	from Comprehensive	to Inkomplete
Concepts:	from Known	to Emergent
Stakeholders:	from One or Few	to Many
Ownership:	from Clear	to Diffuse
Threat:	from „Classical“	to Asymmetric
Methodology:	from Familiar	to Novel
Legal&Regulatory:	from Stable	to Uneasy
Parties:	from Two	to Many

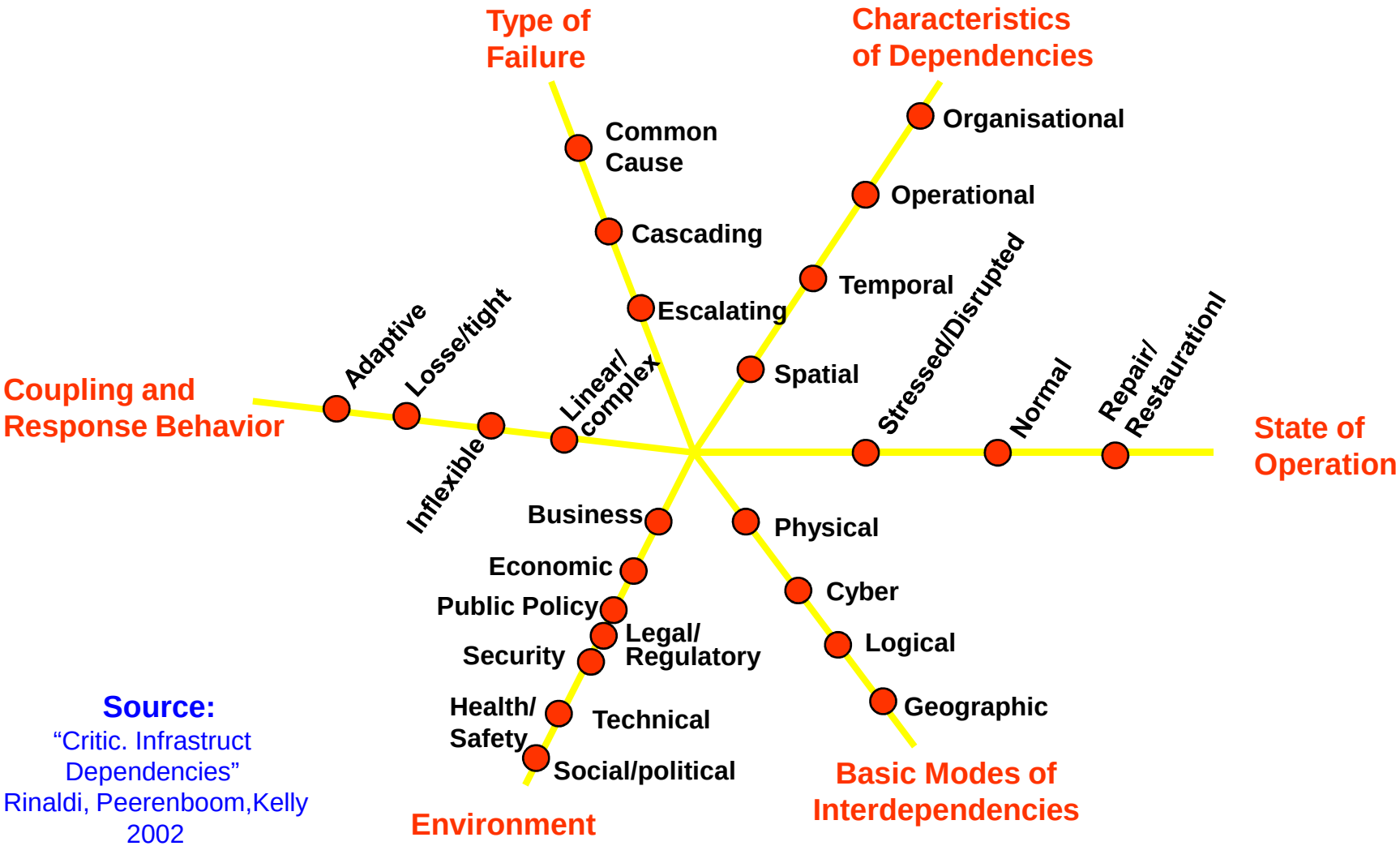
Merkmale kritischer Infrastrukturen

Beispiel Auswirkungen des Angriffes auf das WTC.....

- **Primärwirkung**
  - 3000 Todesopfer
  - Milliarden Dollar Sachschaden
- **Folgewirkungen**
  - Umsatzrückgänge aller Fluggesellschaften
  - Konkurs einiger Versicherungen und Fluggesellschaften
- **Kaskadenartige Ausbreitung der Folgewirkung**
  - weltweite Kursstürze an den Börsen
  - Auswirkung auf die weltweite Konjunkturentwicklung

Einflussfaktoren Kritische Infrastrukturen:

Herausforderungen für die vernetzte Gesellschaft



Source:
"Critic. Infrastruct Dependencies"
Rinaldi, Peerenboom,Kelly 2002

Herausforderungen Kritischer Infrastrukturen

- Vergleich CIIP – CIP -

	IT-Infrastrukturen	Kritische Infrastrukturen
Bedrohung	Primär aus dem „Netz“	Alle Bedrohungsarten möglich
Wirkung	Störungen/ Ausfälle von Netzen und Computern	Folgewirkungen größerer Dimension in andere Systeme
Verantw.	IT-Provider/ -Betreiber	Zusammenwirken mehrer Betreiber, BOS, ….PPP‘s
Vorbeu-gung	IT- Sicherheitskonzept	Ganzheitliche Sicherheitsstrategie und Umsetzungsplan
Reaktion/ Abwehr	CIO-/ CSO- Organisation; CERTs u. CERT-Verb‘de	Nationale u. internationales Krisenmanagement

Möglichkeiten der Problembehandlung

Bedrohungsmodell

Angriff

Übungsangriff

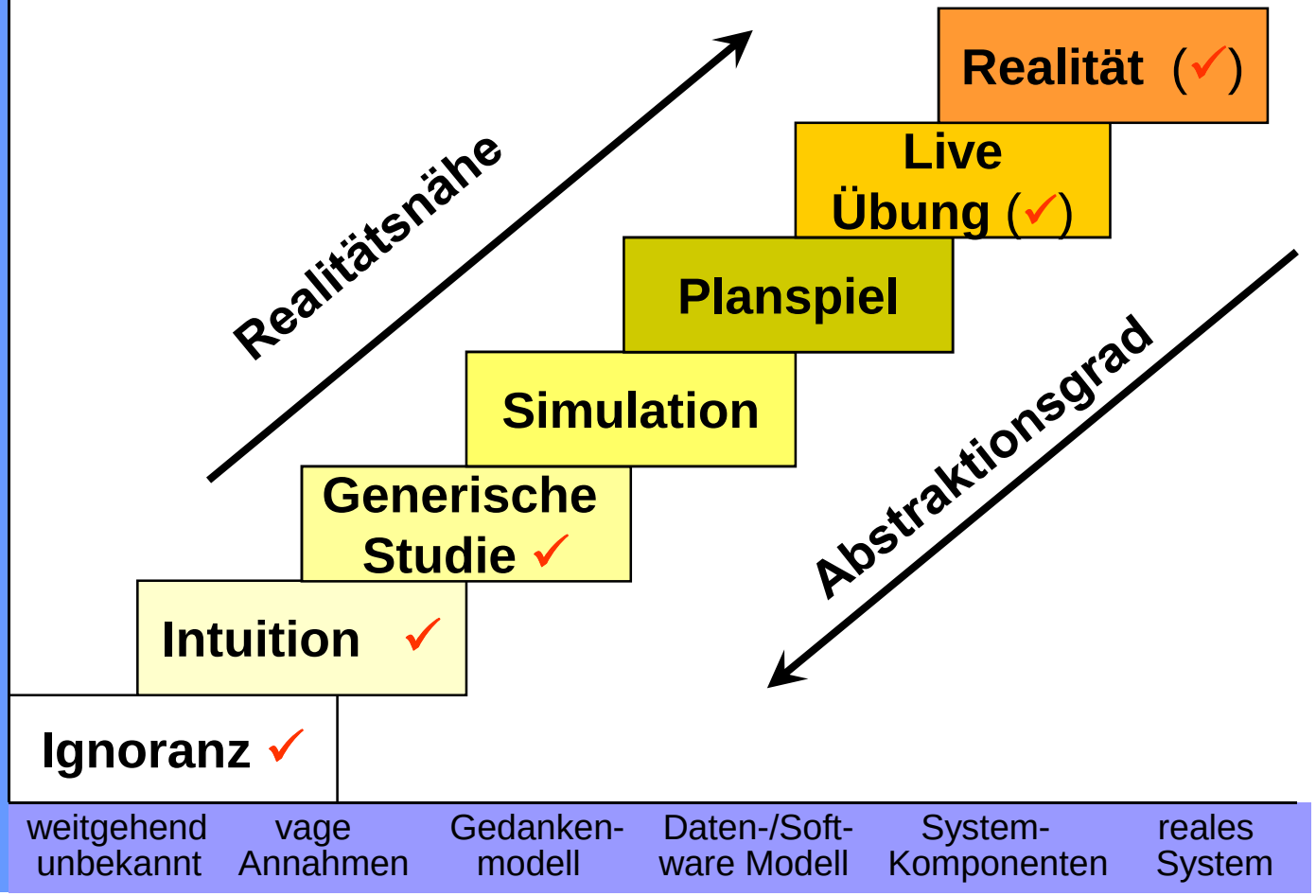
Simulierter Angriff

Computer basiertes Szenario

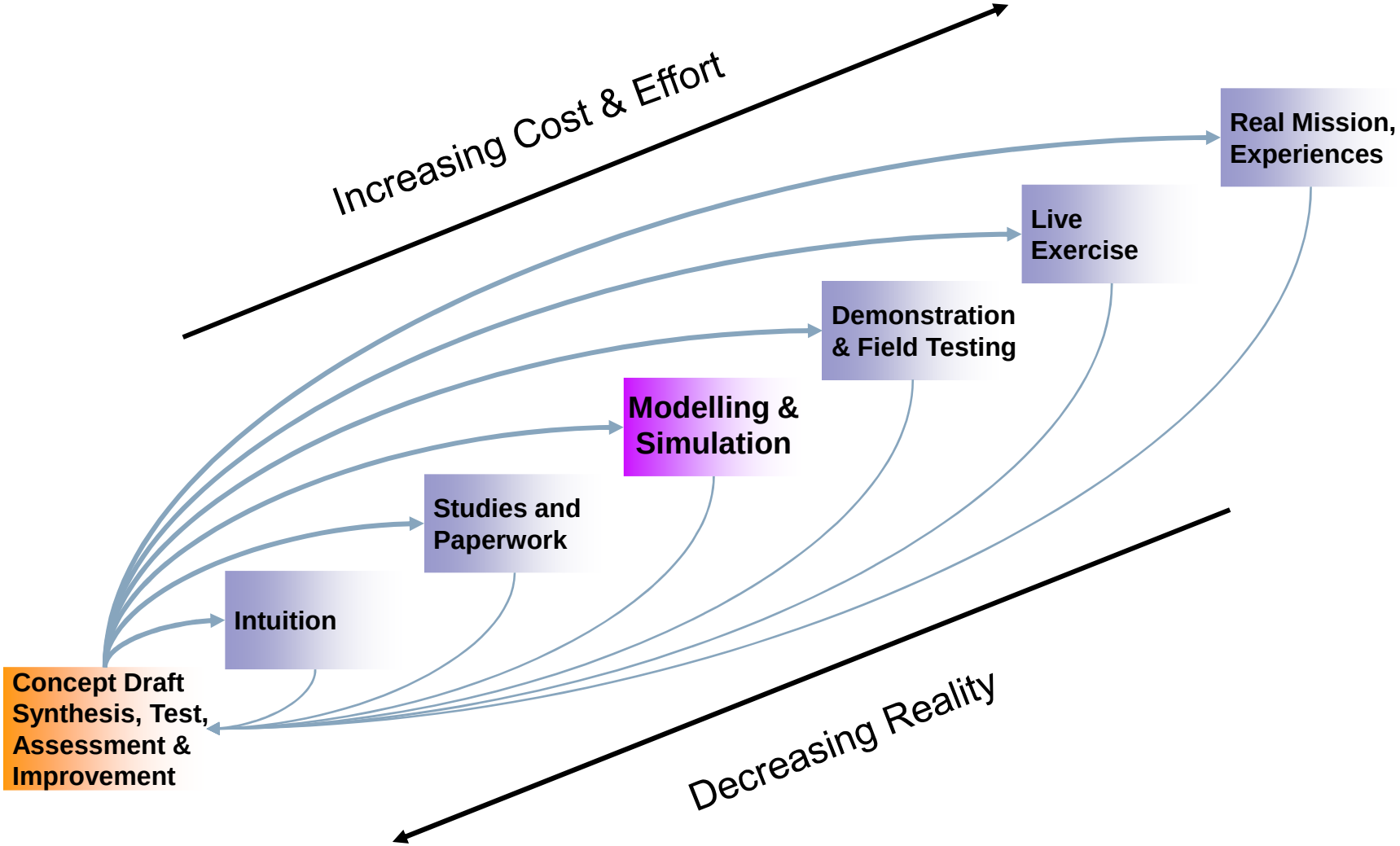
Gedachtes Szenario

Vorstellungen

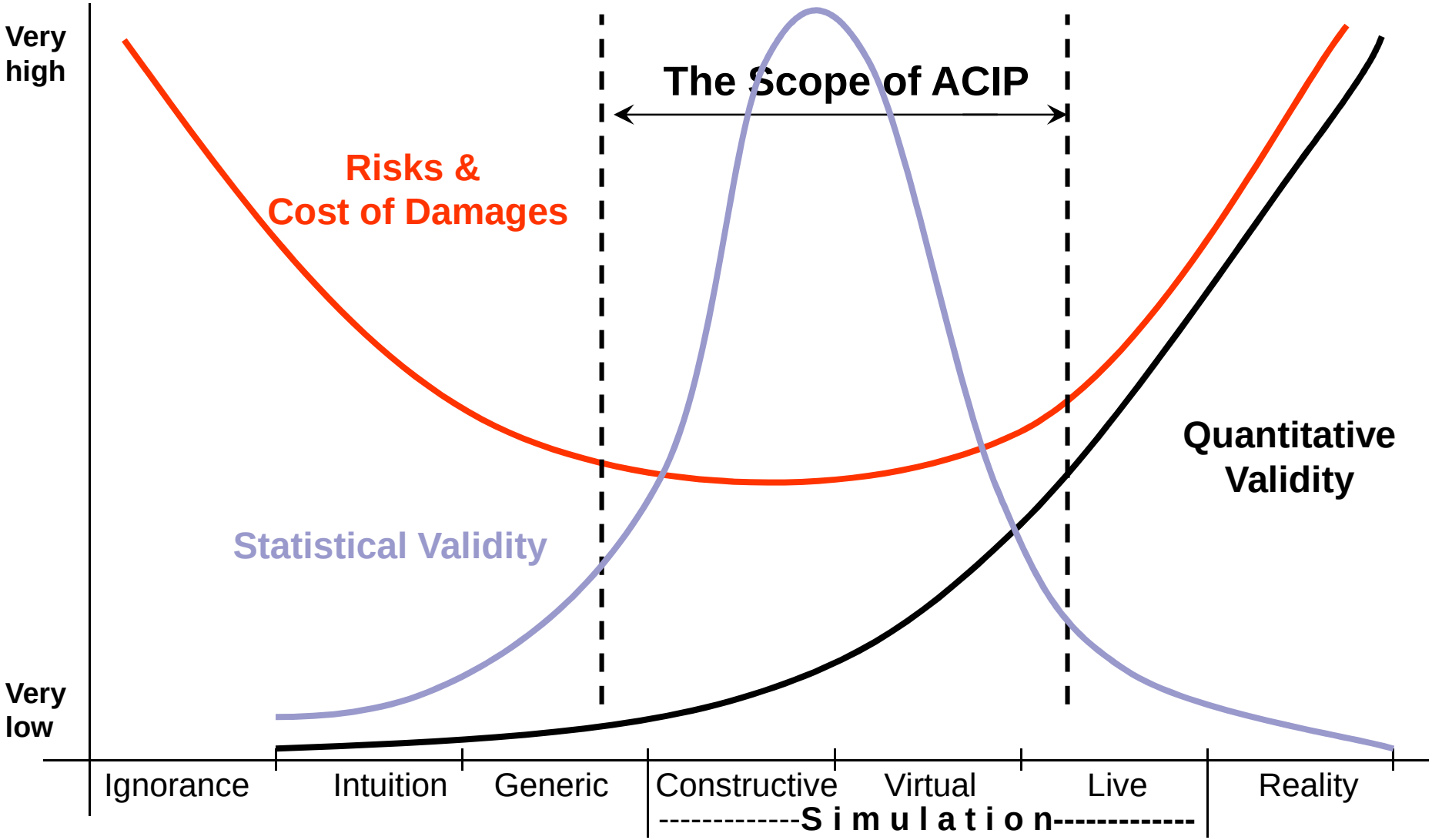
Wer weiss?



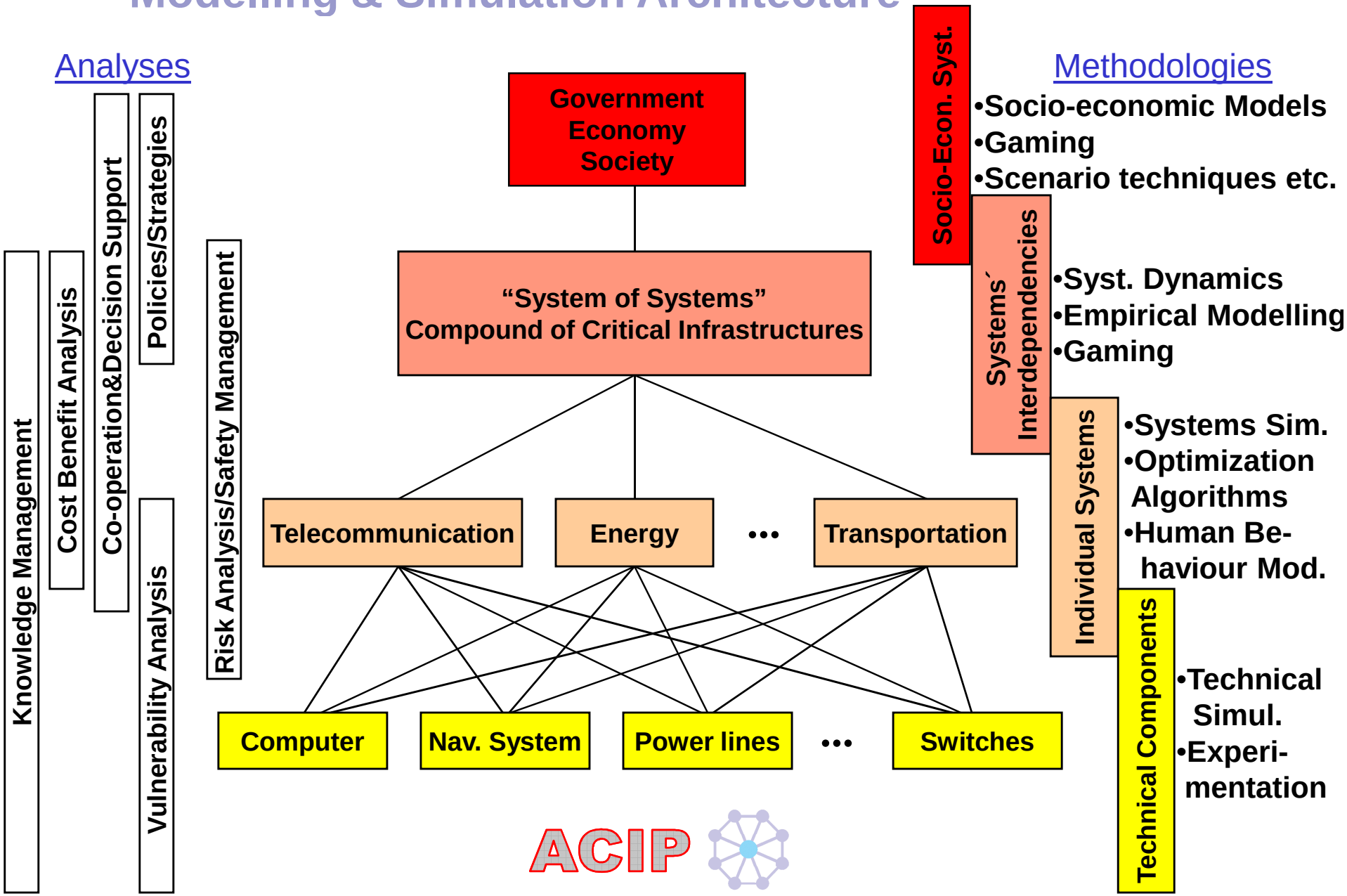
Modellind and Simulation for Problem Solving



The Benefits of Approaches



Modelling & Simulation Architecture



Inhaltsübersicht

1. Das Problem
2. Besonderheiten der Kritischen Infrastrukturen
3. Programme und Maßnahmen
4. Beispiele
5. Resumé und Ausblick

Schutzkonzepte und Maßnahmen anderer Staaten

- Beispiele -

- **Promising Efforts**

EU	EDA;ENISA;ESRP
UK	IAAC; NISCC
Swizerland	InfoSurance; Melanie
Sweden	SEMA
NE	The NE CIP Project
Australia	DoD; Att.Gen
USA	PCCIP….DHS

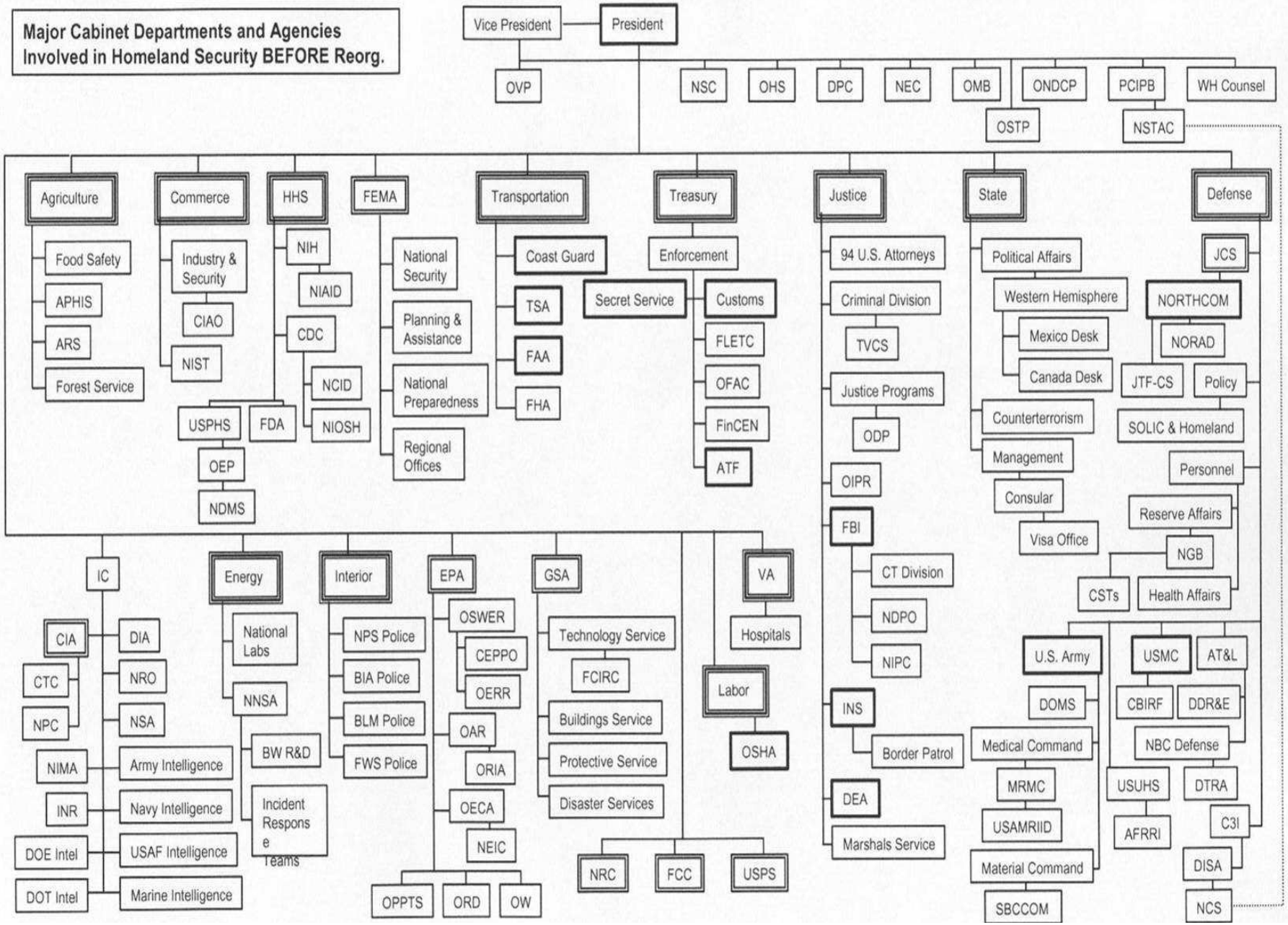
- Emerging Problem **Awareness**
- **Co-operative** Programs and Organisations developing
- Lack of **Harmonization** and **Implementation**

Cyber Terrorism and Critical Infrastructures

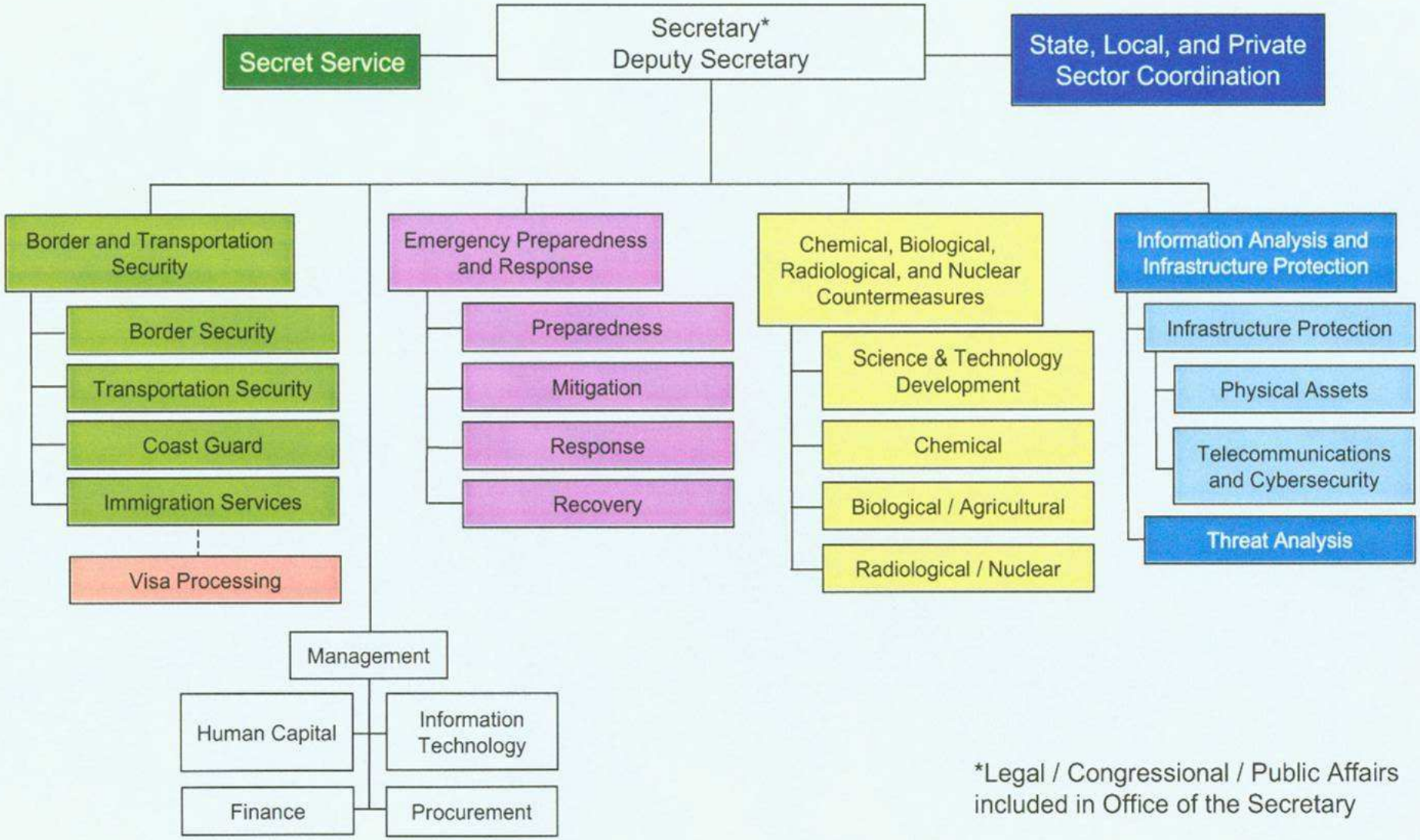
Efforts in the USA

- JV2010/2020 and Information Warfare
- From the PCCIP to the National Plan …
- ⇨ **Post 9/11/2001:**
- National Strategy for Homeland Security
- The Department for Homeland Security
- The National Stretegy to Secure Cyberspace
- Several Organisations and Cooperations
- The National Security Presidential Directives
- The Role of Science and Technology (NSF; NISAC; …)
- The international View

Major Cabinet Departments … before DHS



Organization of the Department of Homeland Security



*Legal / Congressional / Public Affairs included in Office of the Secretary

CIP-“Players“ in the USA

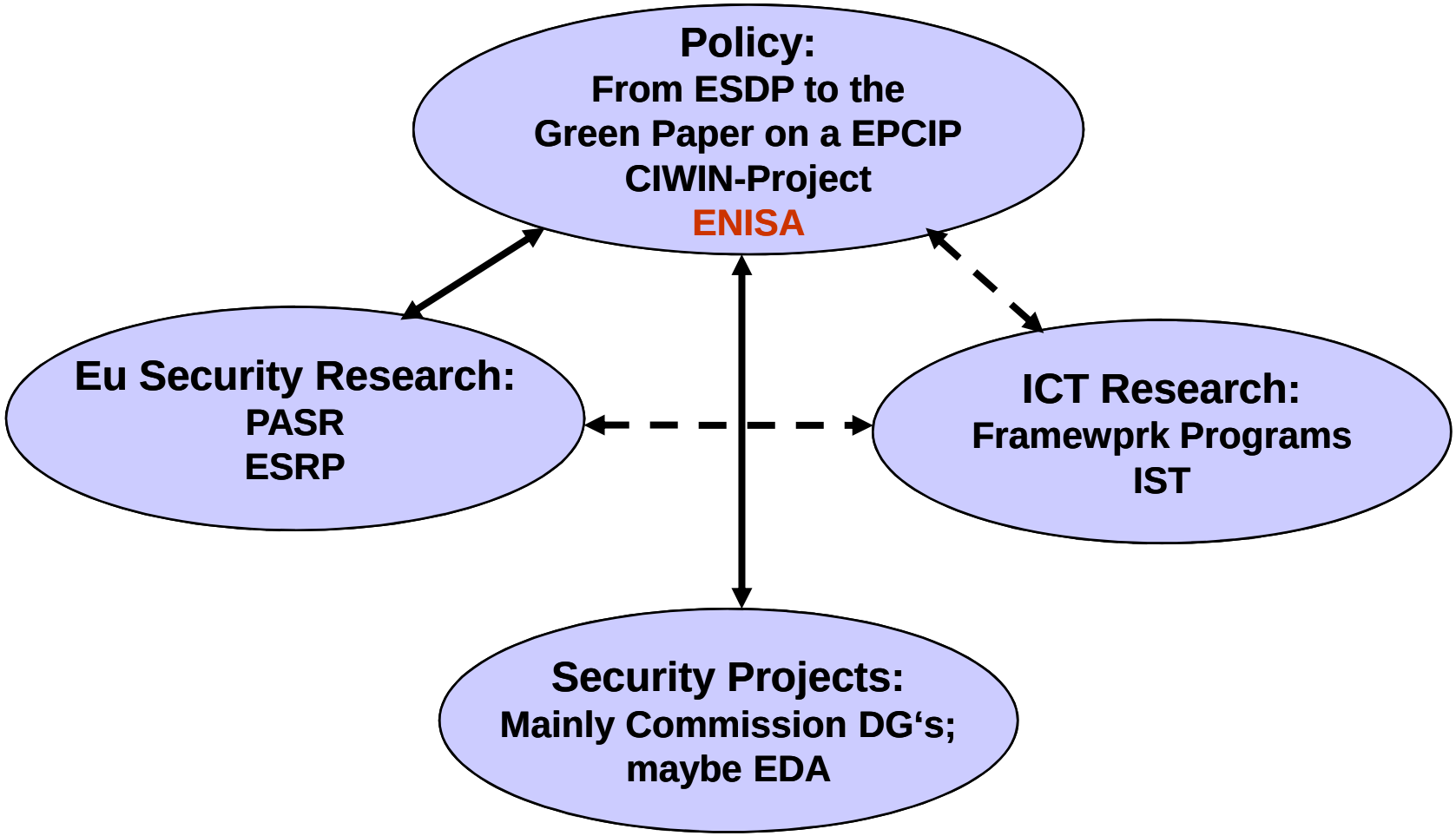
- PCCIP
- EPRI
- SRI
- IDA
- CSC
- CIAO
- National Coordination Center for Telecommunication
- NIPC
- INOGATE
- InfraGard
- ISACs
- Harvard University
- University of Wosconsin
- Carnegy Mellon University – CERT Coordination Center
- Argonne National Laboratory – Infrastructure Assurance Center
- Sandia National Laboratories / NISAC
- Lawrence Livermoore

Maßnahmen in Deutschland
- Einige Beispiele -

- Erste KRITIS-Initiative 1997
- AKSIS – Arbeitskreis Schutz von Infrastrukturen
- Die Anti-Terror-Pakete der Bundesregierung 2002
- Gründung BBK 2004
- Die neue Strategie zum Schutz der Bevölkerung in Deutschland 2003
- KRITIS: Uhtersuchungen, Kooperationen und der „Nationale Plan“ (IIS) 2004/2005
- Der CERT– Verbund; Bürger CERT
- Lagebericht IT- Sicheheit; Vorgehensmodell; Basisschutzkonzept
- LÜKEX 2004, 2005
- Intetrnationale Aktivitäten – IWWN

Fazit: Zu IT: 0.k.; zu Krit.IS: wenig; Posit. Beisp. Bankenverband

The EU Approach to CIP



Schutzkonzepte und Maßnahmen der Europäischen Union

ESDP:	**E**uropean **S**ecurity and **D**efence **P**olicy
PASR:	**P**reparatory **A**ctioon in….. **S**ecurity **R**esearch
ESRP:	**E**uropean **S**ecurity **R**esearch **P**rogram
EDA:	**E**uropean **D**efence **A**gency
ENISA:	**E**uropean **N**etwork and **I**nformation **S**ecurity **A**gency
EPCIP:	**E**uropean **P**rogram for **C**ritical **I**nfrastructure **P**rotection / Green Paper…
MIC:	**M**onitoring and **I**nformation **C**entre

EU: Hope and Vision

- High and Growing Attention in the EU
- Growing Attention at Member State´s Governments
- Promising Local Efforts, Programs and Organizations
- Improving Regional and Global Exchange and Information Sharing
- R&D Programs and Approaches at Many Places
- Building of Communities
- Harmonization of Terminology, Approaches, Standards
- Establishing of Joint R&D Projects
- Establishing of Joint Administrative and Operational Efforts

Green Paper on a European Program for Critical Infrastructure Protection

- Background, Scope, Objectives
- Key Principles
- A Common EPCIP Framework
- National Critical Infrastructures
- EU CI‘s: Definition; Interdependencies; Implementation
- Role of CI- Owners, Operators and Users
- EPCIP Suggested Supporting Measures:
  - CIWIN
  - Common Methodologies
  - Funding
  - Evaluation and Monitoring

Inhaltsübersicht

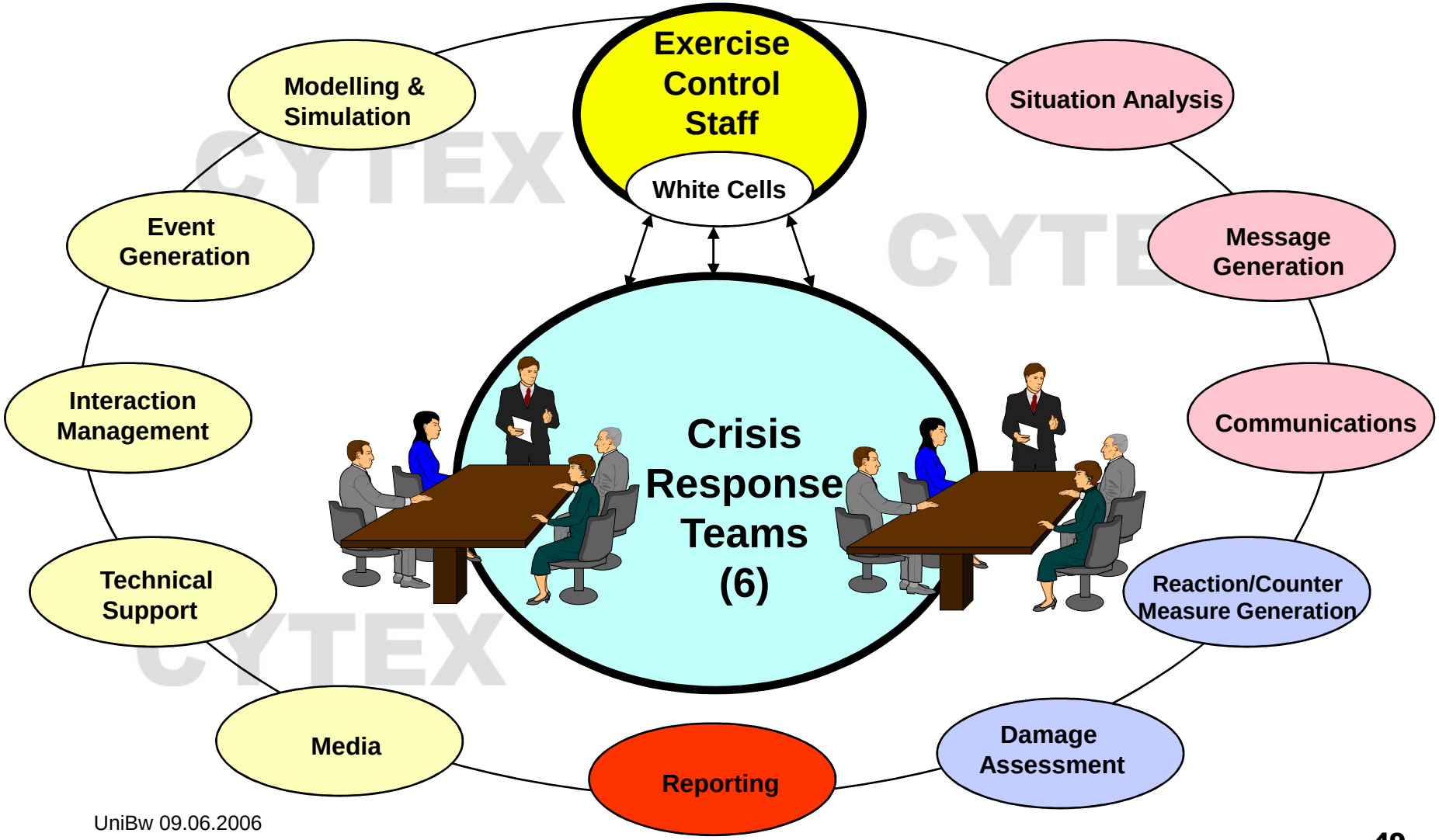
1. Das Problem
2. Besonderheiten der Kritischen Infrastrukturen
3. Programme und Maßnahmen
4. Beispiele
5. Resumé und Ausblick

Szenarien-basierte Planspiele
– ein geeignetes Mittel und Werkzeug für:

- Sensibilisierung
- Analyse von Szenarien/ Bedrohungen/ Verwundbarkeiten
- Bewertung von Konzepten und Alternativen
- Erarbeiten von Handlungsempfehlungen
- Erprobung und Optimierung von Strategien
- Übung und Ausbildung
- Verbesserung der Kooperation und Verständigung (Der sog. „Stakeholder“)

The Cyber Terror Exercise

Game Elements and Organisations



Untersuchung von Szenarien

- Analyse des Bedrohungspotentials Auswirkungen, Folgewirkungen
- Analyse des (Handlungs-) Bedarfs
- Bewertung der Wirksamkeit und Robustheit von Maßnahmen
- Erfordernisse für Prävention, Management und Angriffsfolgen
- Maßnahmen der Wirkungsminderung
- Grundlagen für die sicherheits-politische Bewertung

Keine Erzeugung neuer Schreckensbilder, sondern Untersuchung wie und mit welchen Auswirkungen das Unmögliche erscheinende Realität werden kann!

- **Training** von Krisenstäben und Sicherheitsbeauftragten durch simulierten Ausfall von Betriebsabläufen mit Folgewirkungen auf andere Abläufe
- Geübt werden:
  - die Lageermittlung
  - die Identifikation der Schadensursache und deren Behebung
  - das Ereignismanagement
  - Maßnahmen zur Beherrschung der Schäden und der Abmilderung der Schadensfolgen
  - Maßnahmen zur Herstellung des bestimmungsgemäßen Betriebes
  - Pressearbeit
- Training im Rahmen eines Spieles und gemeinsame Gruppenarbeit

Ziele

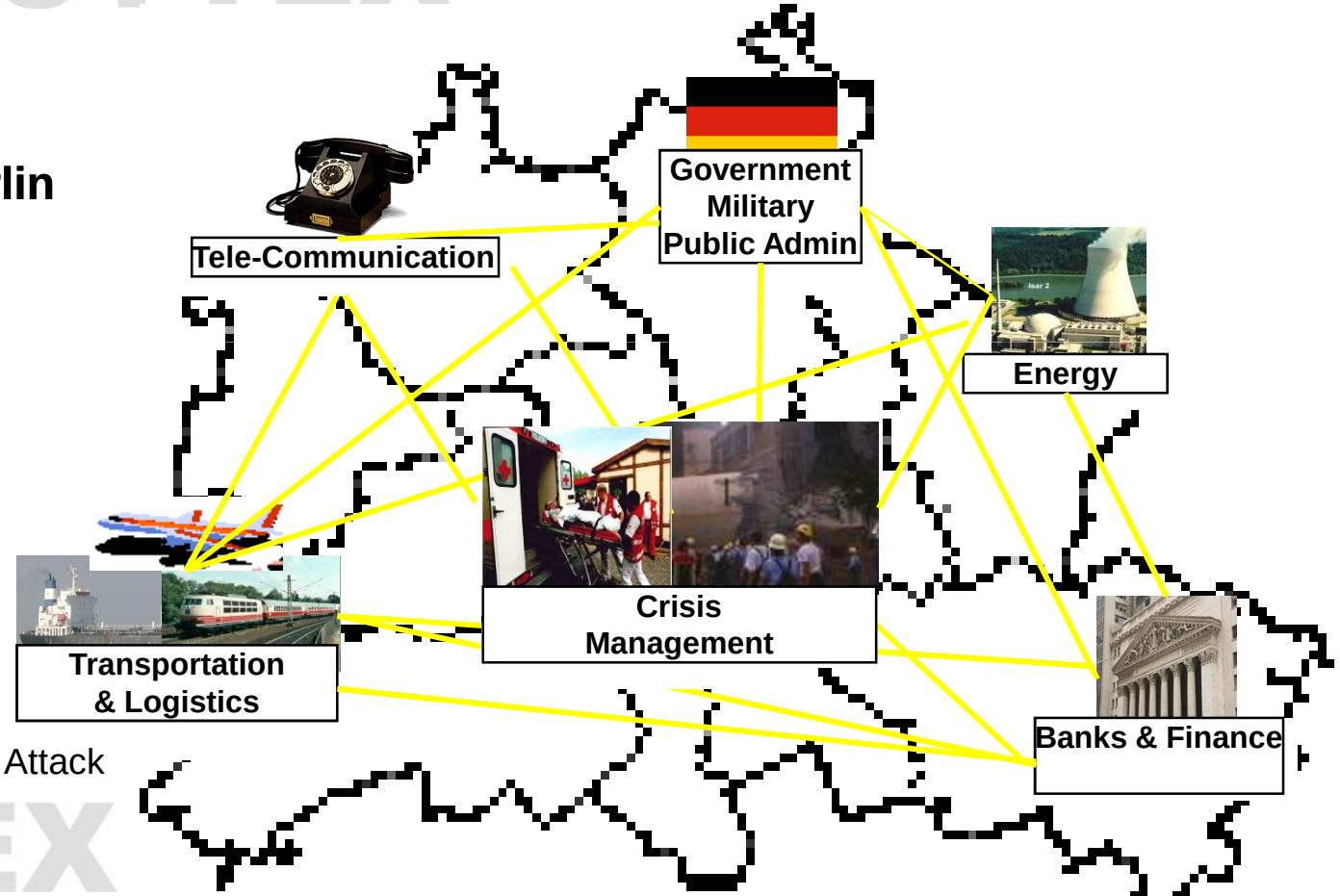
- Szenarien entwickeln, erproben
- Risiken identifizieren
- Information austauschen
- Meldewege erproben
- Komplexität beherrschen,- zumindest verstehen
- Wechselwirkungen ermitteln
- Rollen/Aufgaben definieren, üben
- Maßnahmen testen
- Empfehlungen ableiten
- Öffentlichkeitsarbeit vorbereiten
- Methodik und Werkzeuge demonstrieren und erproben

Cyber Terror Exercise

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

Rahmenbedingungen

- Wirtschaftspolitische Situation in 200x
- Militante Anti-Globalisierungsorganisation
- Gut vorbereitete und konzertierte Serie von Angriffen im Großraum Berlin auf alle wichtigen Infrastrukturen
- Absichten der Angreifer
  - Zusammenbruch des öffentlichen Lebens
  - Erpressung der Bundesregierung
  - Freilassung gefangengehaltener Kollegen
  - Veröffentlichung eines politischen Manifests
  - Minimierung der eigenen Risiken

Das CYTEX - Szenario

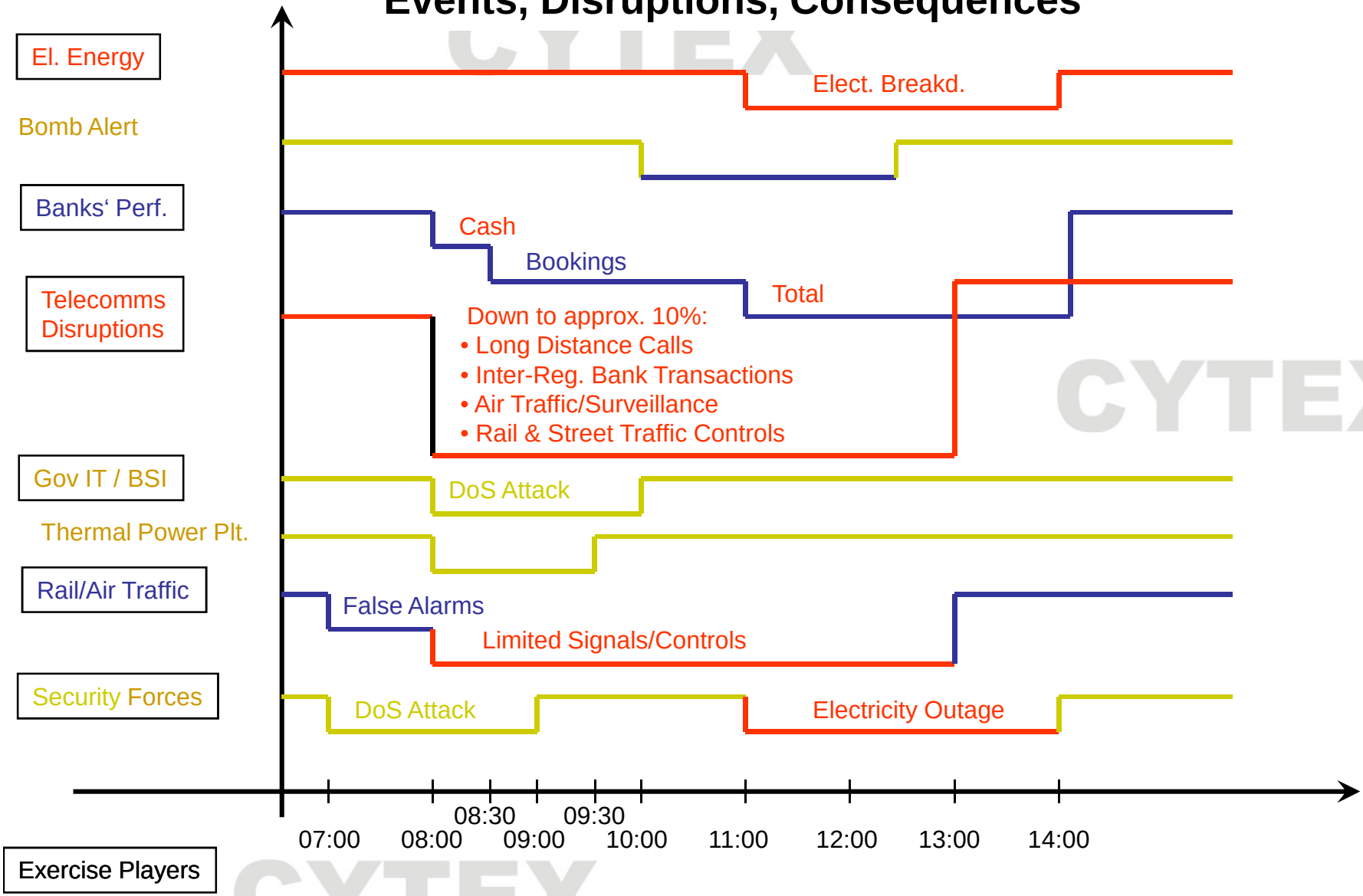
Die Planung für den Tag X :

- **Hauptangriff gegen die Leitzentrale der Energieversorgung**

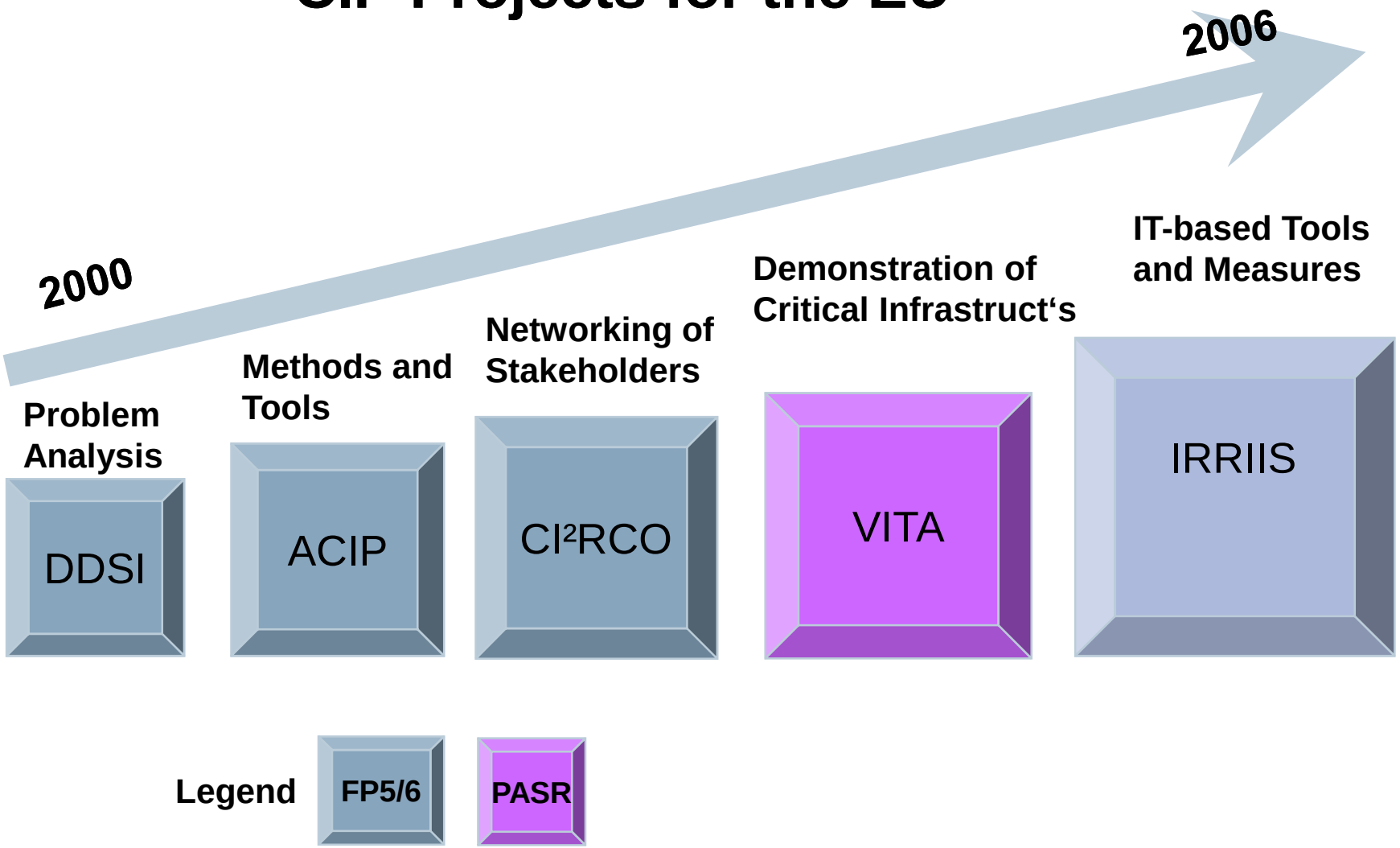
Flankieren des Hauptstoßes durch

- **Einen Angriff auf die Flugsicherung in Tegel**
- **Einen Angriff auf die Leitzentrale der deutschen Eisenbahn AG**
- **Einen Virusangriff auf die überregionalen Vermittlungs-systeme der Telekommunikation**
- **DOS-Angriffe auf die Einsatz-zentralen von Polizei und Feuerwehr**

Events, Disruptions, Consequences



CIP Projects for the EU

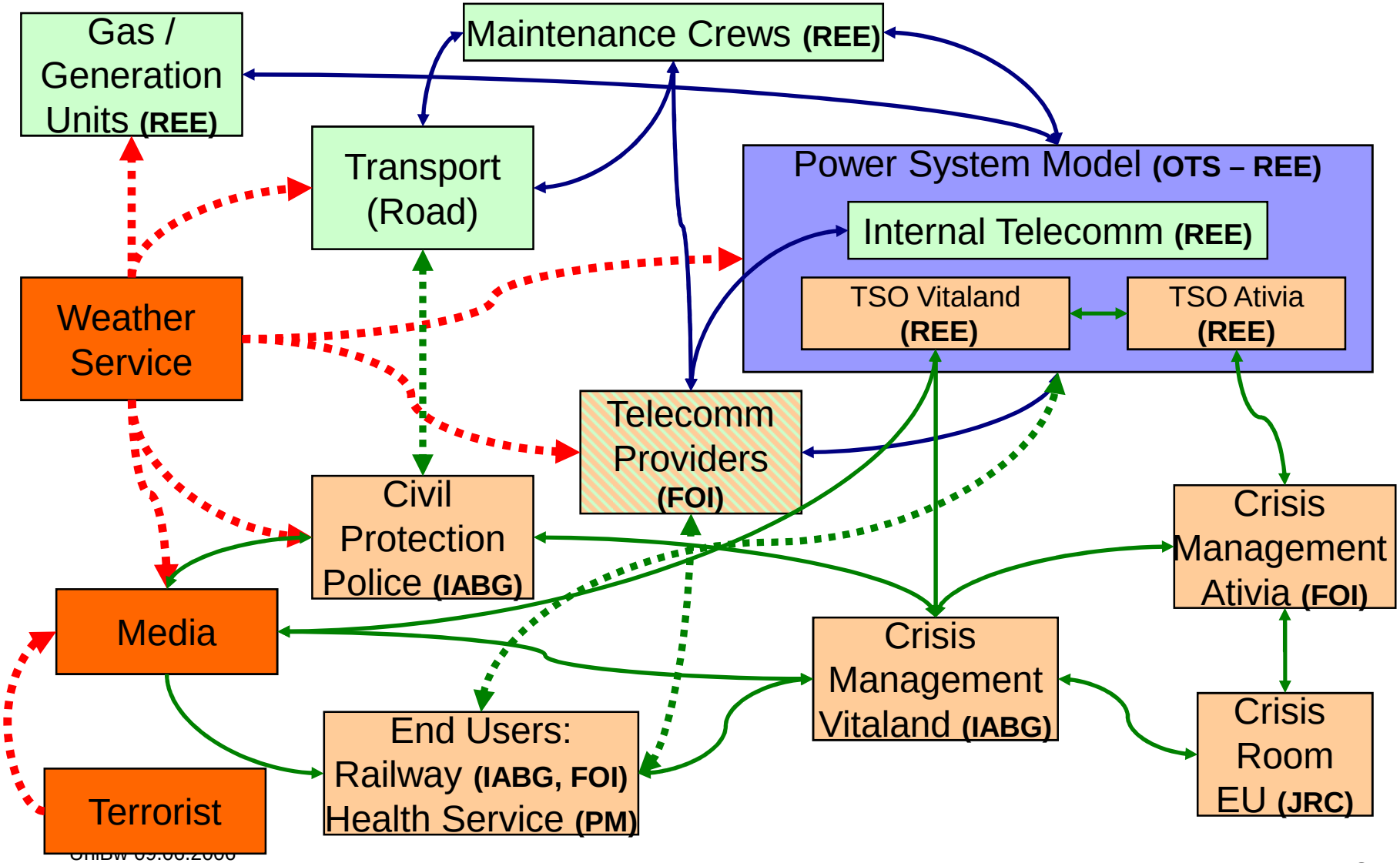


Objectives of the VITA project

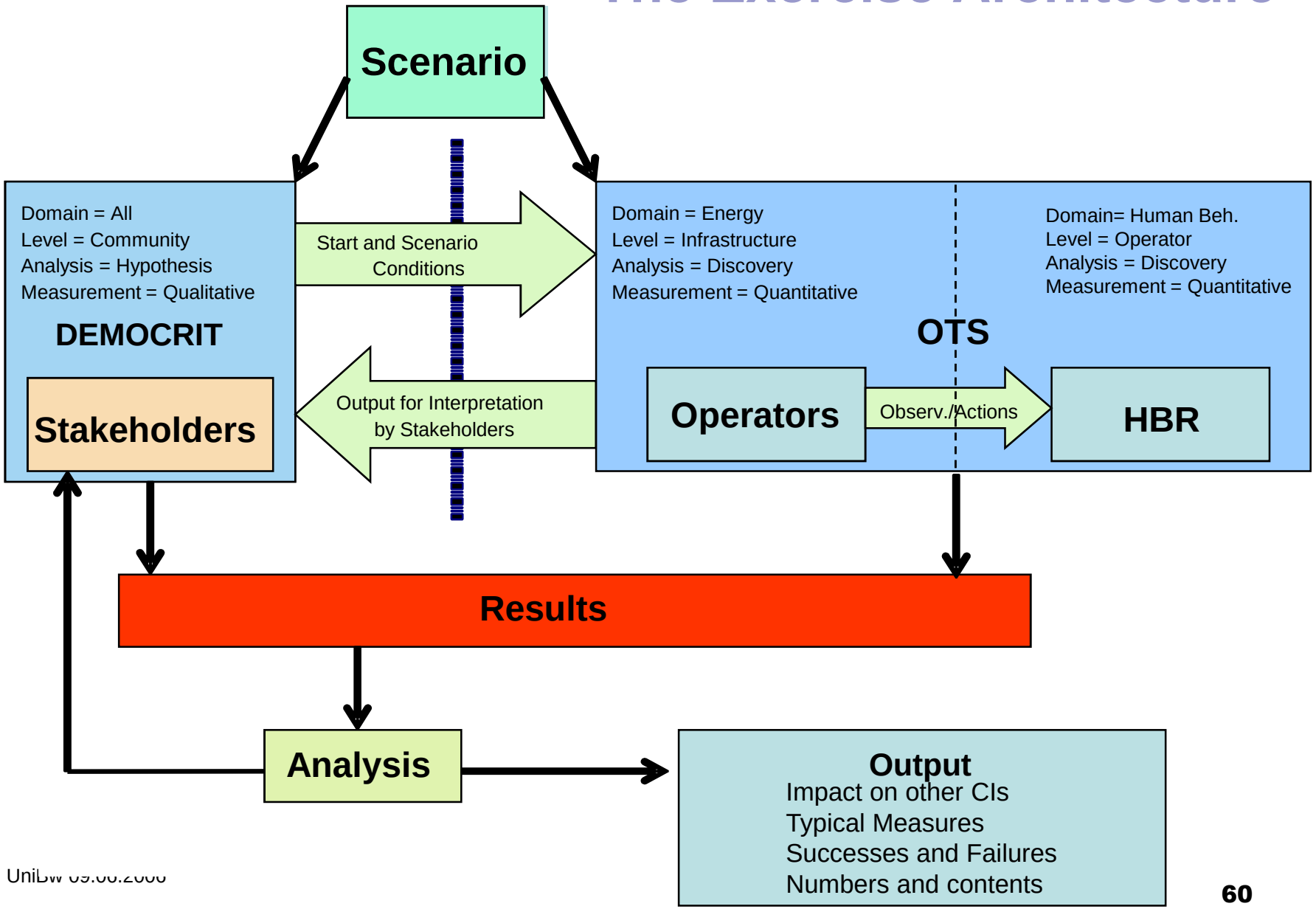
- Vital Infrastructures Threats and Assurance -

- Demonstrate Scenario Impacts of EU Relevance
- Odentify Operational EU Requirements
- Motivate CI Stakeholders
- Show Interdependencies and Cascading Effects
- Explore the Need for New Countermeasures
- Analyse Human Behaviour under Stress
- Demonstrate and Validate Methodology and Tools
- Facilitate Interdisciplinary Views and Discussions

VITA Exercise Generic Model



The Exercise Architecture



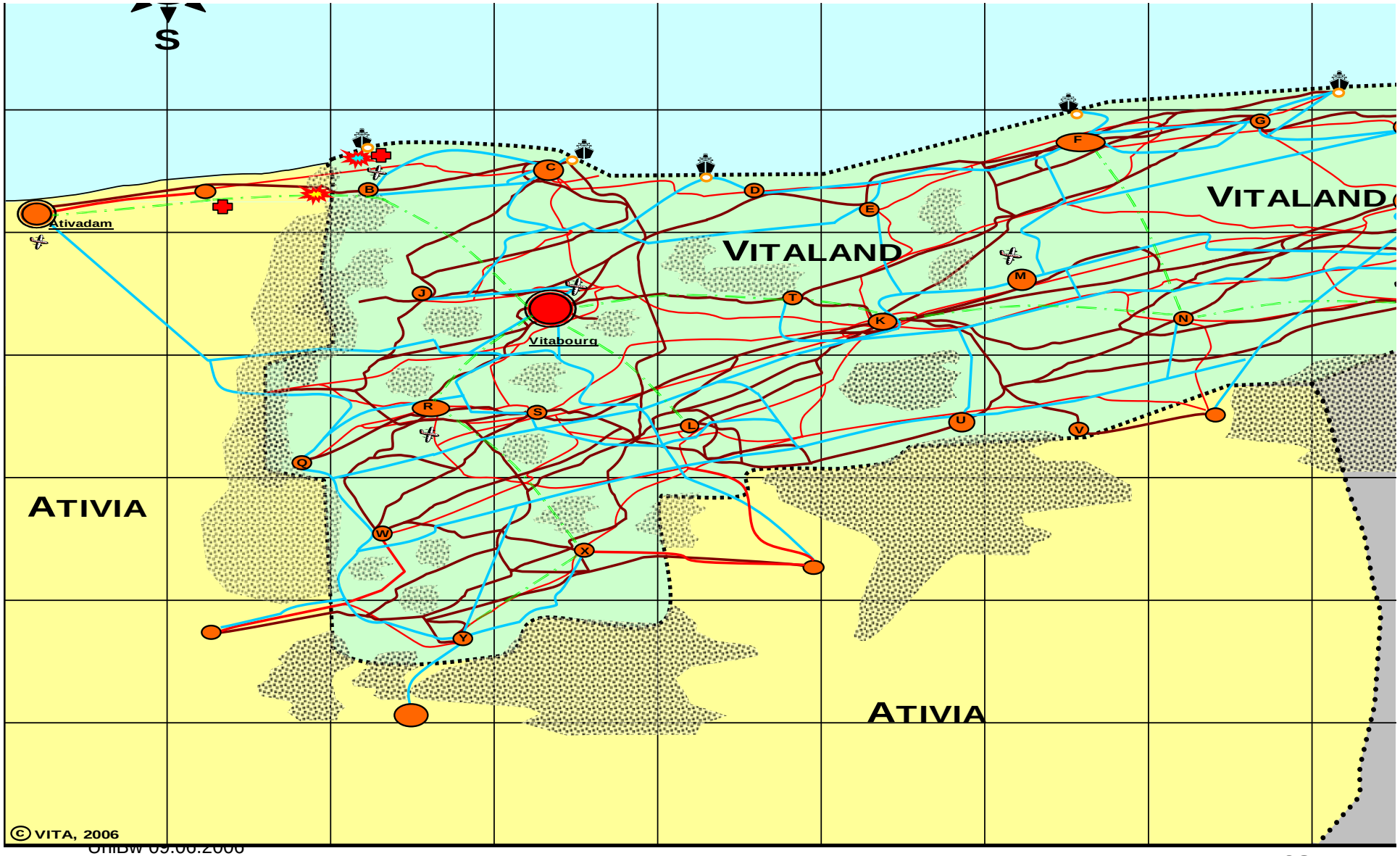
The Course of the Exercise

- **Pre-Phase**: Setting of initial conditions (asynchronous)
- **Session 1**: Initial deterioration (real-time)
- **Session 2**: Crisis escalation (real time)
- **Session 3**: Recovery/ Restoration (asynchr.; no OTS)

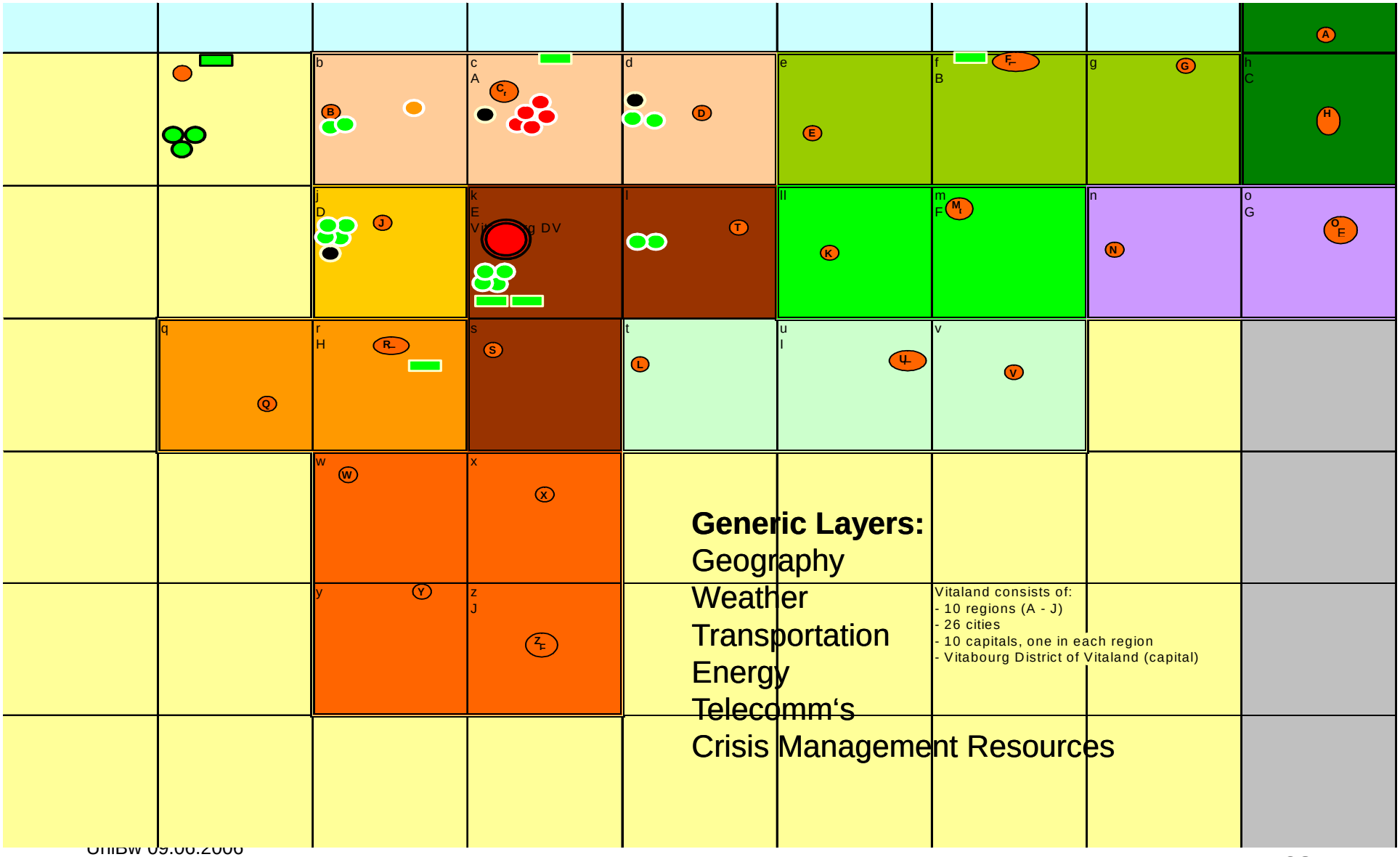
- Short **discussion**/ exchange after each session
- **Joint** structured **assessment** session

Pre-condiTions	Session 1	Discussion	Session 2	Debrief/ Discussion	Lunch	Session 3 (no OTS)	Debrief/ Discussions	Assessment
	Arising Crisis		Escalation			Recovery		

VITA Exercise Map



VITA Generic Map Layers



Generic Layers:
Geography
Weather
Transportation
Energy
Telecomm's
Crisis Management Resources

Vitaland consists of:
- 10 regions (A - J)
- 26 cities
- 10 capitals, one in each region
- Vitabourg District of Vitaland (capital)

VITA Experiment

-Typical events-

- Adverse weather
- Christmas time
- Storm and snowfall strike the electricity system
- Lack of gas supply
- From local to country wide electricity blackout
- Terrorist claims
- Traffic Breakdown and serious accidents
- Industry Crises
- Telecomm‘s breakdown
- Healthcare system in big trouble
- Security services seriously overloaded/ immobile
- Cross-border coordination required

VITA Experiment

-Major Findings-

- The **scenario** was rather dramatic, however realistic
- The **interdependencies** between CIs led to severe unexpected consequential damages and cascading effects
- The challenges and **workload** for managing the crisis at the different levels was extremely high
- There is a need for well prepared **coordination** between the various crisis management and civil protection organisations and resources, within the countries, and at international level
- The **human factors** influencing the quality of operators in critical situations were recorded. They can be related to the scenario and are qualified to being used as feedback for prompting the acting individual and for selecting high quality personnel
- The **methodologies and tools** chosen and adapted by the VITA team were the most effective way to approach this complex security domain of critical infrastructure protection

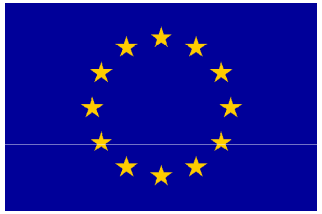
Inhaltsübersicht

1. Das Problem
2. Besonderheiten der Kritischen Infrastrukturen
3. Programme und Maßnahmen
4. Beispiele
5. Resumé und Ausblick

StrategieÜberlegungen

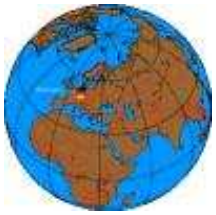
- lokal

- regional



- national

- global



Randbedingungen für eine Strategie

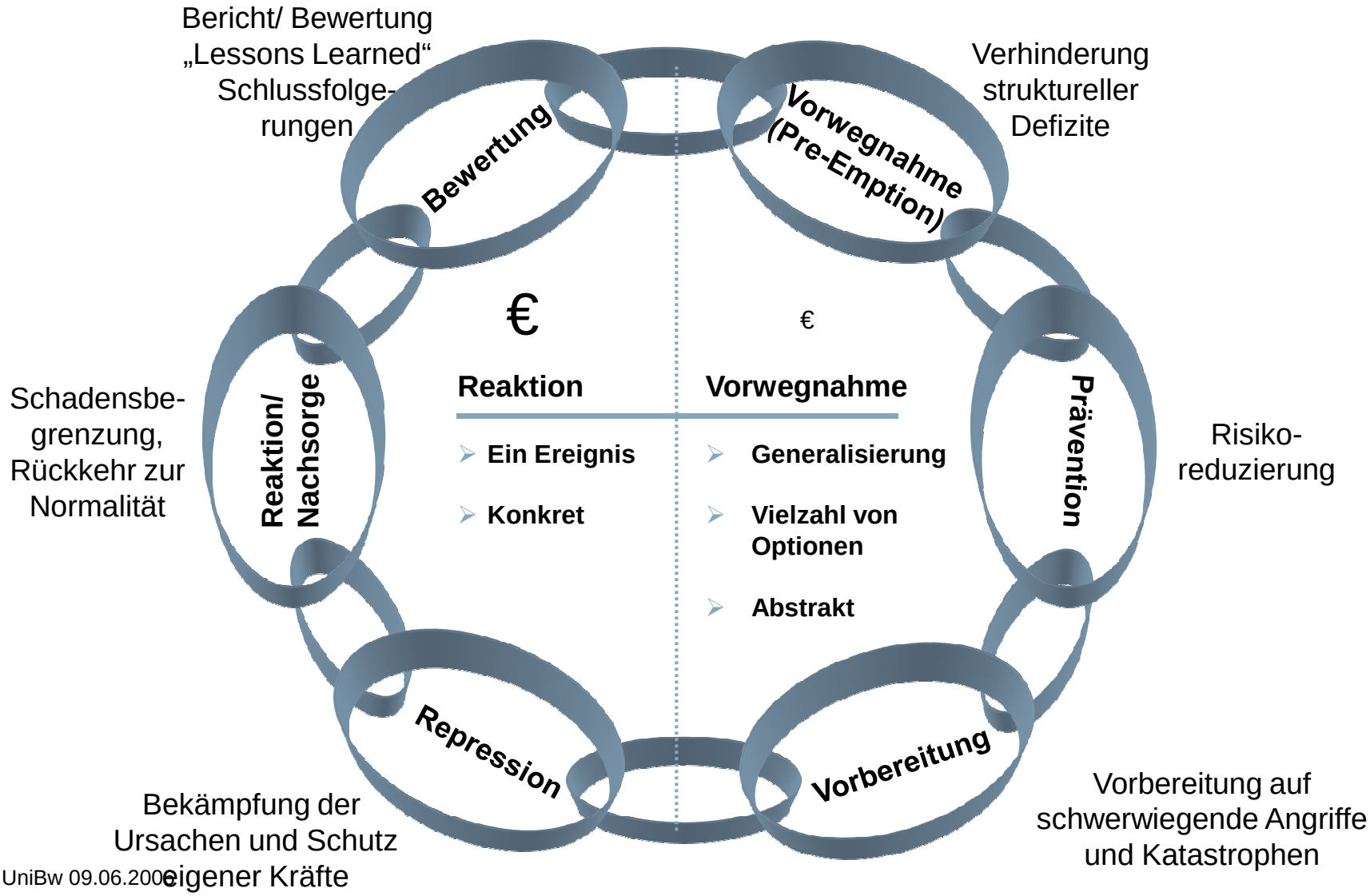
- Risikoeinschätzungen haben im öffentlich-politischen Raum eine kurze Halbwertszeit - das verstärkt den Spielraum für strategische Überraschungen

- Absoluter Schutz gegen alle denkbaren Bedrohungen ist unmöglich

- Staat, Wirtschaft und Gesellschaft stehen deshalb ständig vor dem Problem, welches Restrisiko trotz aller getroffenen Maßnahmen noch tolerierbar erscheint

- Eine Risikoanalyse und Schutzstrategie müssen Medienwirkung und öffentliche Reaktion berücksichtigen

Die Sicherheitskette



Quelle: TNO/IABG

Die „KEY PLAYERS“ und ihre Sichtweisen

„PPP“

Staat

- Politik
- Gesetzlicher Rahmen
- Sicherheitskräfte

➡ *Handlungsfähigkeit*

Forschung

Medien

Personen
Infrastrukturen
Bedrohungen
Risiken

Wirtschaft

- Erfolg
- Wachstum

➡ *Kontinuität*

Gesellschaft

- Bewusstsein
- Verhalten

➡ *Schutzbedürfnis*

Sicherheit als Public-Private-Partnerships (PPP)

- Sicherheitspolitische Gesamtbewertung/“**Nutzen**“ von Sicherheit
- Staatliche **Anreize** für Schutzkonzepte in & von Unternehmen
- Wirtschafts-, Standort- & Industrie**politik** zugunsten ganzheitlicher Sicherheit
- **Ausrüstung** überprüfen (BOS und Wirtschaft)
- **Üben von Szenarien**
- Gegenseitiges **Fordern & Fördern** aller Partner in Politik und Wirtschaft (Dialog)
- **Gemeinsam** führen und **handeln** im Ernstfall

Herausforderungen der Kritischen Infrastrukturen

- Die Entwicklung der **Sicherheitsstrategien** für kritische Infrastrukturen verlangt die **präventive** Auseinandersetzung mit möglichen Szenaren, *auch* für den „worst case“
- Das setzt einen **politischen Willen** und einen neuen, *langfristig* angelegten nach vorne gerichteten Denkansatz voraus
- Es werden **organisatorische, rechtliche** und **finanzielle** Rahmenbedingungen für die notwendige **Kooperation** zwischen Staat, Wirtschaft und Gesellschaft benötigt
- Eine Sicherheitsstrategie kann nur **ressortübergreifend** angelegt sein (u.a. Stärkung BSR)
- Dieser „ **Top Down**“ Prozess muß durch eine Vielzahl von **Einzelmaßnahmen** bei Ausbildung, Ausrüstung, Verfahren, Prozeduren in der Wirtschaft, der öffentlichen Verwaltung und der Gesetzgebung unterfüttert werden
- Notwendigkeit **internationaler** Abstimmung und Kooperation
- **Prävention** vor Reaktion
- **Interoperabilität** auf allen Ebenen

Interoperabilität für den Einsatz
- Der Schlüssel für Zusammenarbeit und Erfolg -

- **Strategie**: Verständigung und Harmonisierung im politischen Denken und Handeln
- **Operation**: Abgleich von Verfahren und Regeln
- **Technik**: Vereinheitlichung von Ausrüstung und Schnittstellen

Die Hindernisse sind weniger technischer sondern organisatorischer und politischer Natur !

Interoperabilität von Schutzsystemen in Kritischen Infrastrukturen
- Das Beispiel Energieversorgung -

- Mehrere Tausend Versorger in Europa
- Veraltete Kontroll- und Steuerungstechnik
- Veraltete Verfahren („N-1“)
- Keine gemeinsamen Standards
- Keine überregionale Zusammenarebeitsfähigkeit
- Liberalisierung: Zwang zum Betrieb an den Systemgrenzen
- Kein Kosten-Nutzen-Modell für Sicherheitsinvestitionen
- Energienetz und Kontrolle/Steuerung/Sicherheit sind immer noch getrennte Disziplinen
- Die Abhängigkeit anderer Infrastrukturen und QoS !

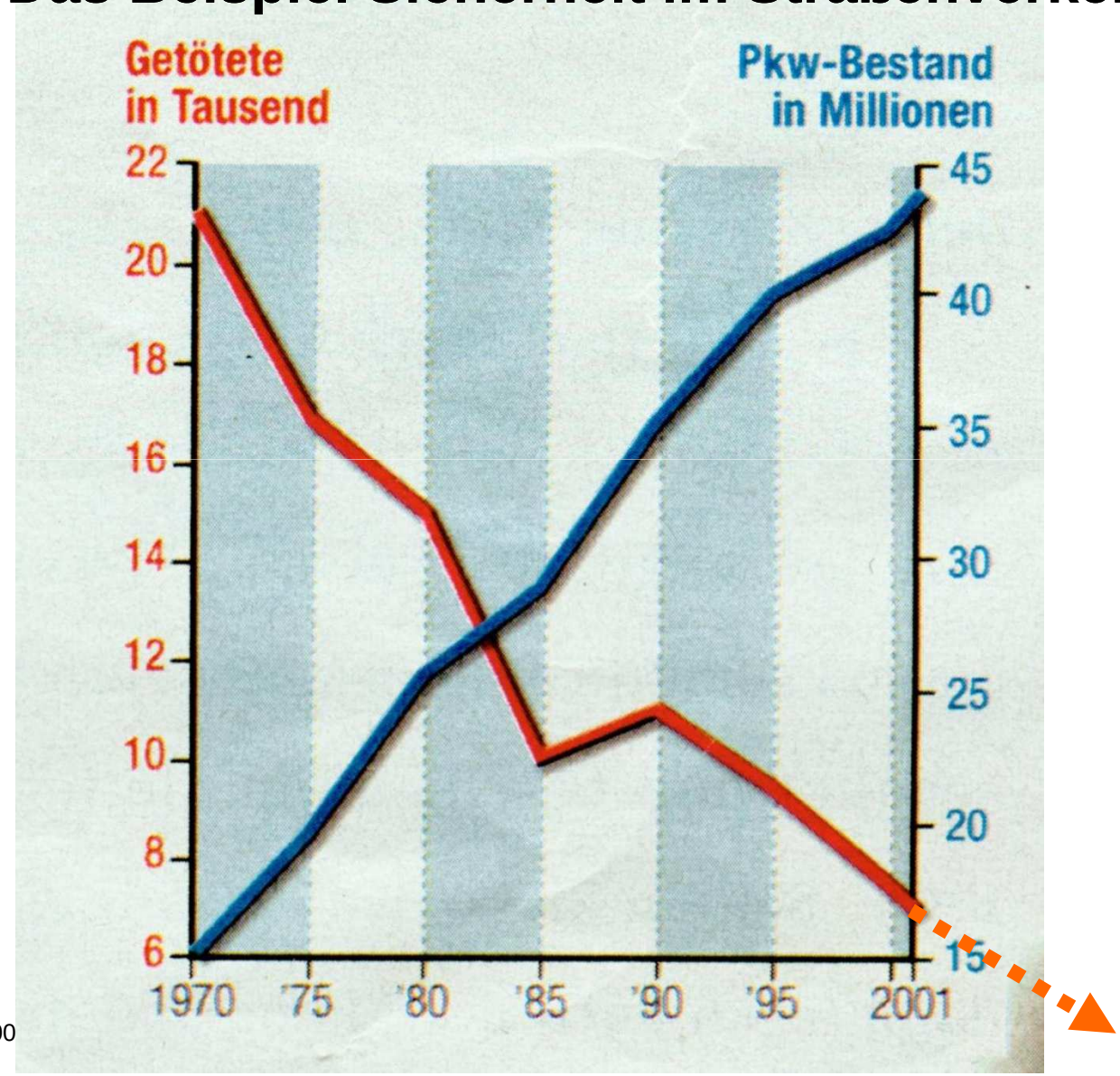
Internationale Zusammenarbeit

- Definitionen (Außenpolitik – Weltinnenpolitik)
- Bündnisrollen, Bündnispolitik (Wer kann was leisten?)
- Internationale Kooperationen / Koalitionen
  - Information sharing
  - Melde- und Alarmierungssysteme
  - Abgestimmte Rules of Engagements (RoE)
  - Vorabdefinition von Koalitionsfällen
  - Gemeinsames Üben von Szenarien
  - Gegenseitige Unterstützung im Ernstfall
- Verhinderung von Monopolisierung (z.B. ECHELON, GPS, Microsoft)
- Entwickeln eines “Code of Conduct” (z.B. Internet)

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
- **Langfristig** und zuverlässig Planen und umsetzen:
  die Beispiele Anti-Terror-Paket, Luftsicherheitsgesetz, Tsunami
- **Transnationale** Effekte

Das Beispiel Sicherheit im Straßenverkehr



Resümé

- **Die Informationsgesellschaft:**
  - **Birgt zunehmende neue Risiken**
  - **Ist neuen Bedrohungen ausgesetzt**
  - **Mit z.T. unbekannten Folgen**
  - **IT ist überall kritischer Faktor**
- **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**
  - **Langfristig und international denken und handeln**

Kritische Infrastrukturen

- Eine neue Herausforderung -

WimEsA
Universität der Bw München
9. Juni 2006

Reinhard W. Hutter
Sicherheitsberater
hutter@iabg.de
reinhard.hutter@gmx.de

Ich danke Ihnen für Ihre Aufmerksamkeit