Der Schutz Kritischer Infrastrukturen als Element der Cybersicherheit

Präsentation von Präsident Christoph Unger

im Rahmen der Carl Friedrich von Weizsäcker Friedensvorlesung
am 20.11.2013 an der Universität Hamburg

Gliederung

- KRITIS - Teil des Bevölkerungsschutzes in Deutschland
- das BBK (Geschichte, Organisation, Aufgabenschwerpunkte)
- KRITIS – Definition
- KRITIS – Gefährdungen / Bedrohungen
- KRITIS – Strategie
- KRITIS – Cybersicherheit
- KRITIS – Produkte

Was so alles passieren kann …

Hochwasser

Stromausfall

Schiffshavarie

Dürre

Wintereinbruch

Gefahrenspektrum

Naturereignisse	Technisches/ menschliches Versagen	Terrorismus, Kriminalität, Krieg
Extremwetterereignisse, u.a. Stürme, Starkniederschläge, Temperaturstürze, Hochwasser, Hitzewellen, Dürren **Wald- und Heidebrände** **Seismische Ereignisse** **Epidemien und Pandemien** bei Menschen, Tieren und Pflanzen **Kosmische Ereignisse**, u.a. Energie- und Partikelstürme, Meteoriten	**Systemversagen**, u.a. Unter- und Überkomplexität in der Planung, Hardware- oder Softwarefehler **Fahrlässigkeit** **Unfälle und Havarien** **Organisatorisches Versagen**, u.a. Defizite im Risiko- und Krisenmanagement, unzureichende Koordination und Kooperation	**Terrorismus** **Sabotage** **Sonstige Kriminalität** **Bürgerkriege und Kriege**

aktuelle Herausforderungen

neue Gefahren (z. B.)

- Zunahme extremer Wetterphänomene aufgrund des Klimawandels
- Cyber-Angriffe auf Kritische Infrastrukturen
- Terrorismus („schmutzige Bombe“)
- technische Havarien

veränderte Rahmenbedingungen (u. a.)

- demographische Entwicklung
- Auswirkungen der Wehrstrukturreform
- Änderung rechtlicher Rahmenbedingungen national (Stichwort Feuerwehrführerschein) und auf EU-Ebene (Einführung des Mehrheitsprinzips durch den Lissabon-Vertrag)
- Haushaltskonsolidierung mit hohen Einsparauflagen

überflutetes Feuerwehrhaus
Quelle: Stadt Buchen im Odenwald

Mögliche Konsequenzen

Mit welchen Schadwirkungen müssen wir rechnen?

- **Physische Schäden**
  (Zerstörungen, Emissionen, …)
- **Personenschäden**
  (Tote, Verletzte, Erkrankte)
- **Kaskadierende Schäden**
  (Schadwirkungen auf andere Bereiche)
- **Volkswirtschaftliche Schäden**
  (unmittelbar und mittelbar)
- **Psychologische Schäden**
  (Verunsicherung, Hysterie, Panik)
- **Politische Schäden (Vertrauensverlust, Krise)**

Grundlagen nach GG

Bevölkerungsschutz
im Verteidigungsfall
(Art. 73 Abs. 1 Nr. 1 Grundgesetz)

Katastrophenschutz
(Art. 30, 70 Grundgesetz)

der Bund

Katastrophenhilfe
(Art. 35 Grundgesetz)

die Länder

BUNDESPOLIZEI

Technisches Hilfswerk

Bundeswehr

ASB Arbeiter-Samariter-Bund

DLRG

Johanniter Unfall-Hilfe

Malteser

Integriertes Hilfeleistungssystem im föderalen Bundesstaat

- **Schadenslagen von nationaler Bedeutung, kriegerische Konflikte**
- **Amts- und Katastrophenhilfe des Bundes (Inland- / Ausland)**

BBK · BUNDESPOLIZEI · Technisches Hilfswerk · Bundeswehr

Bund

Länder

Ggf. Bezirksregierungen

(soweit vorhanden)

Kommunen

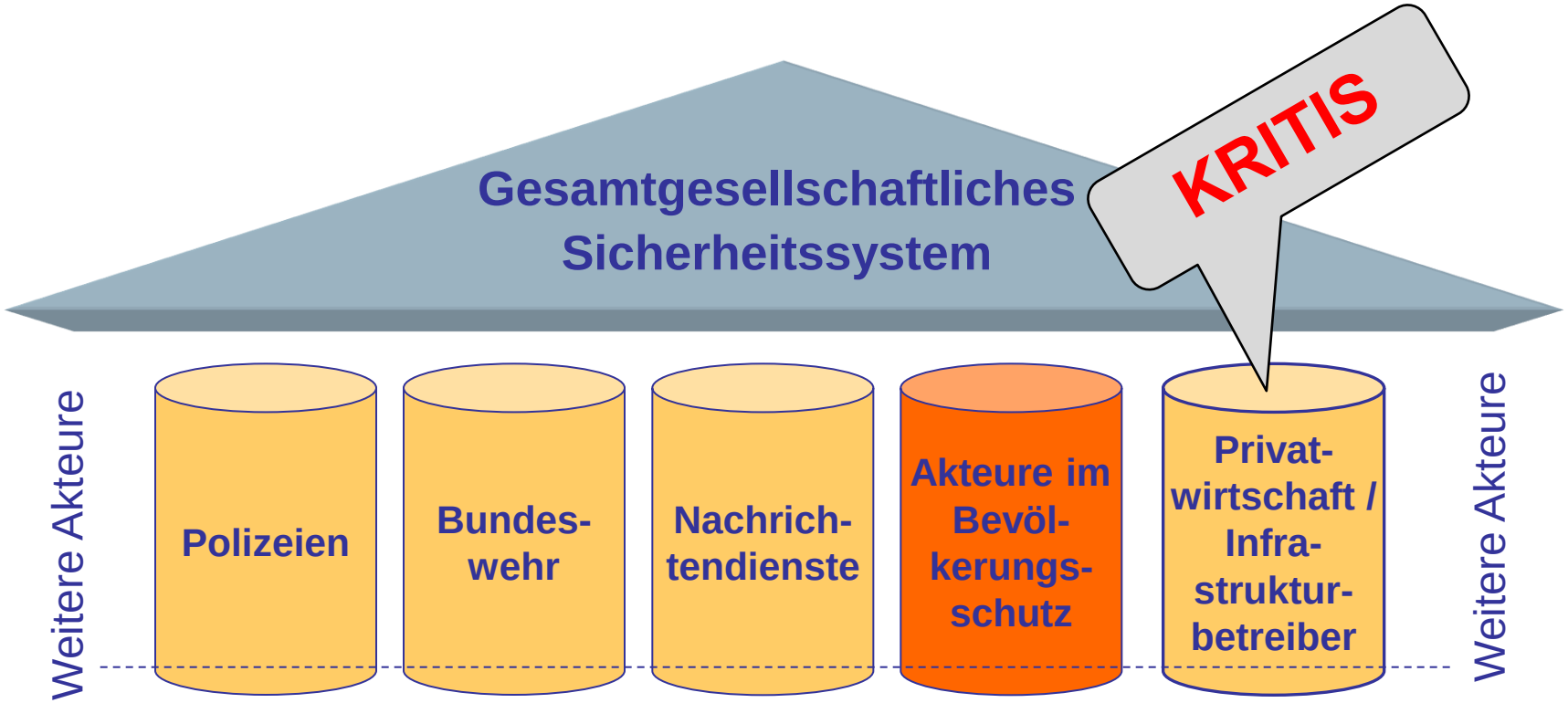
(Landkreise, kreisfreie Städte)

lokale / regionale Großschadens- und Katastrophenlagen

Alltagsereignisse / Rettungsdienst, Brandschutz, Technische Hilfe

ASB Arbeiter-Samariter-Bund · Deutsches Rotes Kreuz · DIE JOHANNITER · Malteser ...weil Nähe zählt. · DLRG · DFV DEUTSCHER FEUERWEHR VERBAND

Gesamtgesellschaftlicher Ansatz



Risiko- und Krisenmanagement zur gesamtgesellschaftlichen Sicherheitsvorsorge

Partner im Bevölkerungsschutz

Bundesministerium des Innern

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

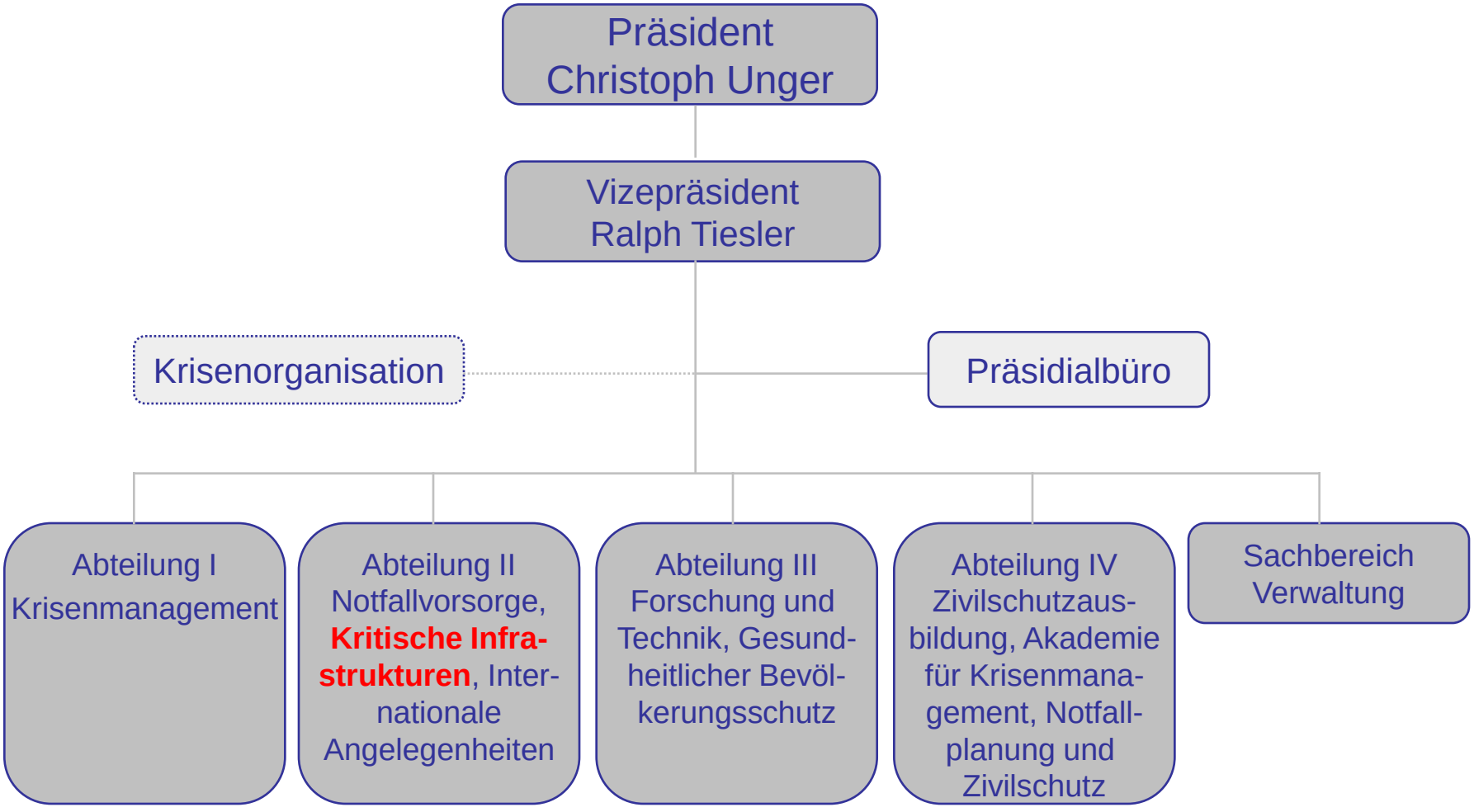
Geschichte des BBK

- 1957:
  Bundesdienststelle
  für zivilen Bevölkerungsschutz
- 1958 - 1974:
  Bundesamt für zivilen
  Bevölkerungsschutz **(BzB)**
- 1974 – 1999:
  Bundesamt für Zivilschutz **(BZS)**
- 2001 – 2004
  Zentralstelle für Zivilschutz
  im BVA

2002

- **seit 1. Mai 2004 BBK**

Das BBK - Organigramm



Anzahl der Beschäftigten: ~ 350

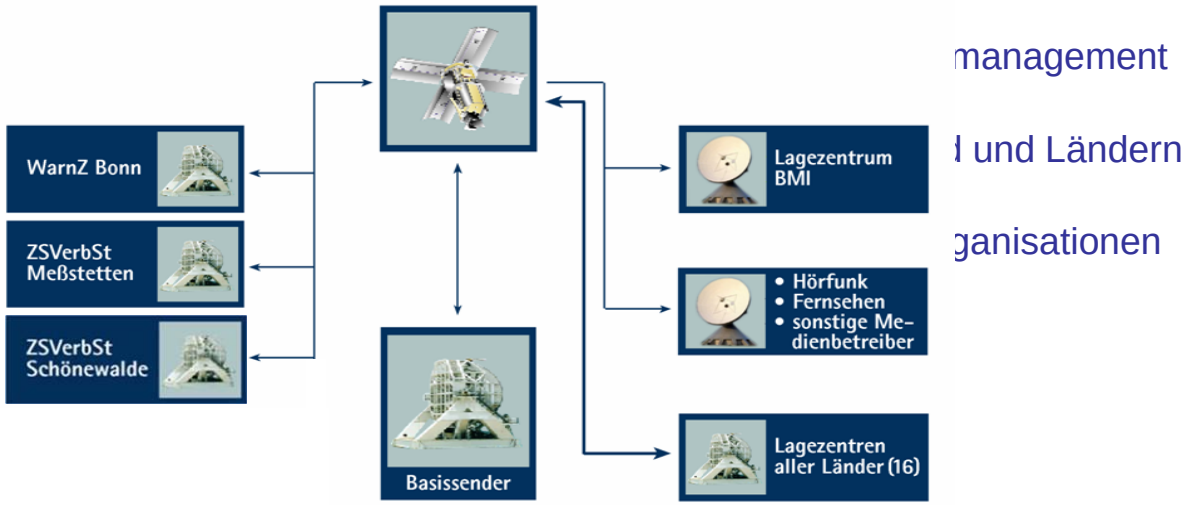
Haushaltsvolumen 2013: ~ 100 Mio. €

Das BBK – Aufgaben (*animierte Folie*)

Um der potenziellen Gefahr durch neue Bedrohungslagen besser begegnen und ein verbreitertes Aufgabenspektrum wahrnehmen zu können, wurde in Bonn das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) errichtet.

Aufgaben des BBK sind u.a.:

- Wahrnehmung von Aufgaben des Bundes im Zivilschutz



- management
- l und Ländern
- ganisationen

BBK – die Informations-, Wissens- und Dienstleistungsplattform des Bundes im Bevölkerungsschutz

KRITIS als eine Schwerpunktaufgabe

KRITIS-Definition

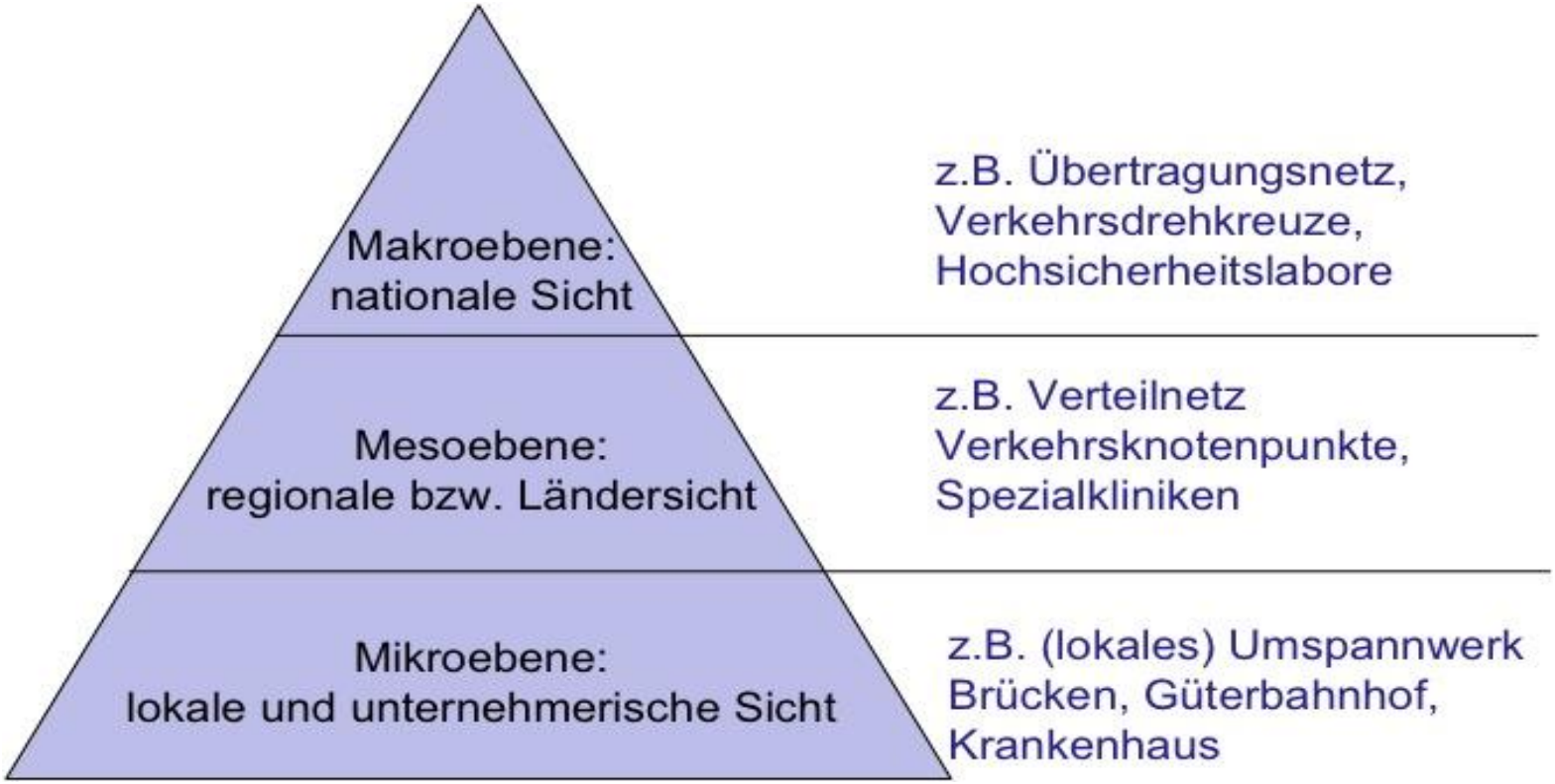
"Kritische Infrastrukturen sind
Organisationen und Einrichtungen
mit wichtiger Bedeutung
für das staatliche Gemeinwesen,
bei deren Ausfall oder Beeinträchtigung
nachhaltig wirkende Versorgungsengpässe,
erhebliche Störungen der öffentlichen Sicherheit oder
andere dramatische Folgen eintreten würden."

Definition der Bundesregierung in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (2009)

KRITIS-Sektoren

Ebenen-Modell KRITIS

- Unterschiedliche Bedeutung KRITIS auf den verschiedenen Ebenen



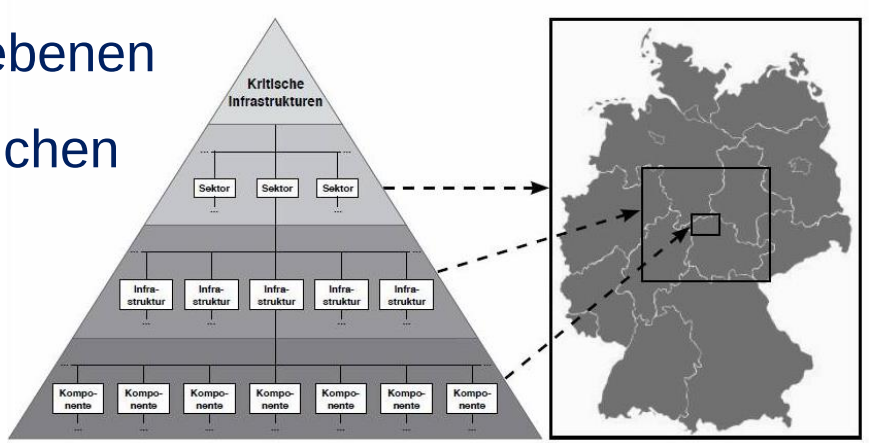
Was ist kritisch?

Herausforderung 1: Festlegung von Kriterien

- Über alle Verwaltungsebenen und Sektoren
- handhabbar und gerichtsfest

Herausforderung 2: Festlegung von Schwellenwerten

- durch die einzelnen Verwaltungsebenen
- Für die einzelnen Sektoren / Branchen
- handhabbar, gerichtsfest, „kommunizierbar“



➢ derzeit in der Erarbeitung und Diskussion

Gefahren/Bedrohungen für Infrastrukturen

Ölkrise
Ein externer Preisschock wie im Lehrbuch: Die Opec verteuert das Öl, und in **Deutschland** ruht der Autoverkehr.

11. September
Terroristen steuern Verkehrsflugzeuge ins **World Trade Center** und das Pentagon. Die Weltwirtschaft steht still.

Wintereinbruch
Im **Münsterland** knickt ein Schneesturm Strommasten und lässt 250 000 Menschen tagelang ohne Elektrizität.

Computerkrieg
Hacker, vermutlich aus Russland, attackieren das IT-System **Estlands** und legen dort Server sowie Internet-Zugänge lahm.

Aschewolke
Der Ausbruch des Vulkans **Eyjafjallajökull** blockiert Europas Luftverkehr. Das trifft auch Tourismus und Industrie empfindlich.

„Wir glaubten, gerüstet zu sein, wurden aber eines Besseren belehrt“

(Alfred Meinerzhagen, Geschäftsführer der Gemeinsamen Kommunale Datenverarbeitung anlässlich eines Stromausfalls in Siegburg, 2003)

Nationale KRITIS-Strategie

Kabinettsbeschluss im Juni 2009

Ziele

- Stärkung des Risiko- und Krisenmanagements
- Best mögliche Erhaltung der Funktionsfähigkeit Kritischer Infrastrukturen

Ansatz

- Kooperativ
- All-Gefahren
- Interdisziplinär
- Sektorübergreifend
- Risiko basiert

Nationale KRITIS-Strategie

Schutz KRITIS als gemeinsame Aufgabe von Staat und Wirtschaft

Staatliche Gewährleistungsverantwortung für KRITIS

Betreiberverantwortung der Unternehmen

- KRITIS überwiegend in privater Hand
- Abhängigkeit von anderen Sektoren
- Eigensicherung i.S.v. BCM

Gemeinsame Verantwortung Schutz KRITIS

Umsetzung der KRITIS-Strategie

Sicherheitspartnerschaft

- **Branchengespräche unter Beteiligung von:**
  - Verbänden
  - Betreibern Kritischer Infrastrukturen
  - verantwortlichen Ressorts
- **Kooperationen auf Arbeitsebene**
- **Beteiligung an Übungen (z.B. LÜKEX)**
- **Forschungsprojekte**
- **Schutzkonzepte**

in 2012:

7 Gesprächsrunden des BMI mit der Wirtschaft zur IT-Sicherheit von KRITIS in verschiedenen Sektoren/Branchen

Besondere Risiken: Cyberangriffe

Leon Panetta, Direktor CIA: „Das nächste Pearl Habor wird ziemlich sicher eine Cyberattacke auf unser Stromnetz sein.“

Die Welt, Dienstag 18. Mai 2010

Bild: Pepsprog, Pixelio

Besondere Risiken: Cyberangriffe

„Hacker aus China spähen Ölkonzerne aus“

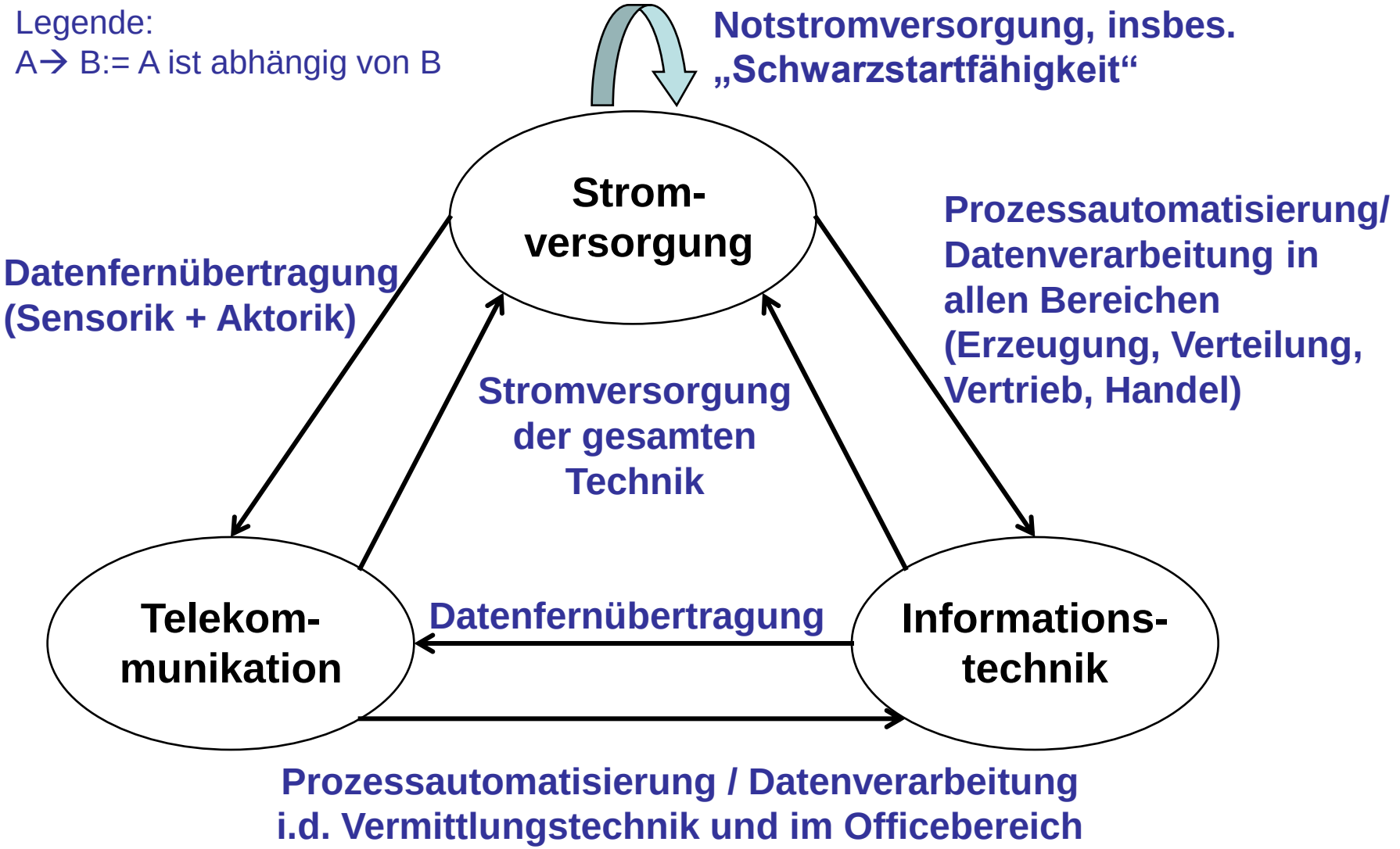
„Computervirus legt Notruf in Australien lahm“

„Hacker greifen französischen Atomkonzern an“

„Stuxnet-Wurm befällt iranisches Atomkraftwerk“

Interdependenzen

Legende:
A→ B:= A ist abhängig von B



Cybersicherheitsstrategie

NPSI → Cybersicherheitsstrategie

UP Bund (Bundesbehörden)

Cyber-AZ

UP KRITIS (Unternehmen)

- Cyber-Sicherheitsrat
- Nationales Cyber-Abwehrzentrum
- Kritische IT-Infrastrukturen
- IT der Bürger
- IT des Staates
- Einsatz verlässlicher Informationstechnologie
- Internationale Zusammenarbeit
- Abwehr von Cyber-Angriffen
- Wirksame Kriminalitätsbekämpfung
- Personalentwicklung der Bundesbehörden

- AG Krisenmanagement
- AG Übungen
- AG ….
- Einrichtung SPOC

Quelle: BMI. IT 3 – Dr. Günther Welsch

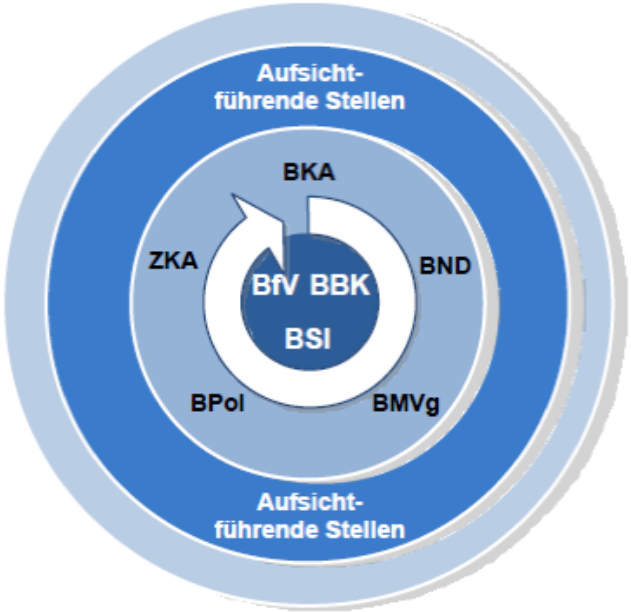
IT-Sicherheit – Nationales Cyber-Abwehrzentrum

Akteure

- „enger Kreis“: BSI, BBK, BfV (ca. 10 Personen)
- erweiterter Kreis: u.a. BKA, BND, Aufsichtsbehörden, …

Ziele

- Informationsdrehscheibe; verbesserter Informationsstand
- gemeinsame Lageeinschätzung und -bewertungen
- Erstellung von Handlungsempfehlungen
  - für den Cyber-Sicherheitsrat
  - für Betreiber Kritischer Infrastrukturen
- Verbesserte Reaktionszeiten



IT-Sicherheit - Nationales Cyber-Abwehrzentrum

Fachlicher Beitrag des BBK

- Analyse der Auswirkungen eines IT-Ausfalls auf KRITIS, Prognosen Versorgungssicherheit
- Analyse Hilfeleistungspotentiale/Redundanzen
- Kontakte zu KRITIS-Unternehmen, Informationsübermittlung
- Themen u.a. in GMLZ-Lageberichte, deNIS II+, BBK-Publikationen
- Einbindung Cyber-AZ in LÜKEX 2011

Perspektiven

- Auf- und Ausbau eines behördenübergreifenden Beobachtungs-, Analyse- und Beratungsnetzwerkes (Bund und Länder)
- Auf- und Ausbau eines (gegenseitigen) Informationsmechanismus
- Aufbau neuer und Nutzung bewährter Informationswege zw. Behörden und Unternehmen

LÜKEX 2011- Angriff auf IT-Infrastrukturen

Ziele

- Verdeutlichung der IT-Gefährdungen und -Abhängigkeiten
- Sensibilisierung für Folgewirkungen
- Überprüfung / Optimierung des Zusammenwirkens der Bundesressorts im gesamtsstaatlichen KM im Rahmen einer IT-Krise (gem. NPSI)
- Verbesserung der länder- und bereichsübergreifenden Zusammenarbeit
- Integration von IT-KM-Strukturen in das bereichsübergreifende Krisenmanagement
- Aufrechterhaltung der Schlüsselbereiche des öffentlichen und nicht-öffentlichen Lebens (kritische Geschäftsprozesse)
- Koordinierung vom Maßnahmen zwischen öffentlichen Stellen und Betreibern Kritischer Infrastrukturen (KRITIS)
- Optimierung der bereichsübergreifenden Medien- und Öffentlichkeitsarbeit

LÜKEX 2011- Angriff auf IT-Infrastrukturen

Beteiligte:

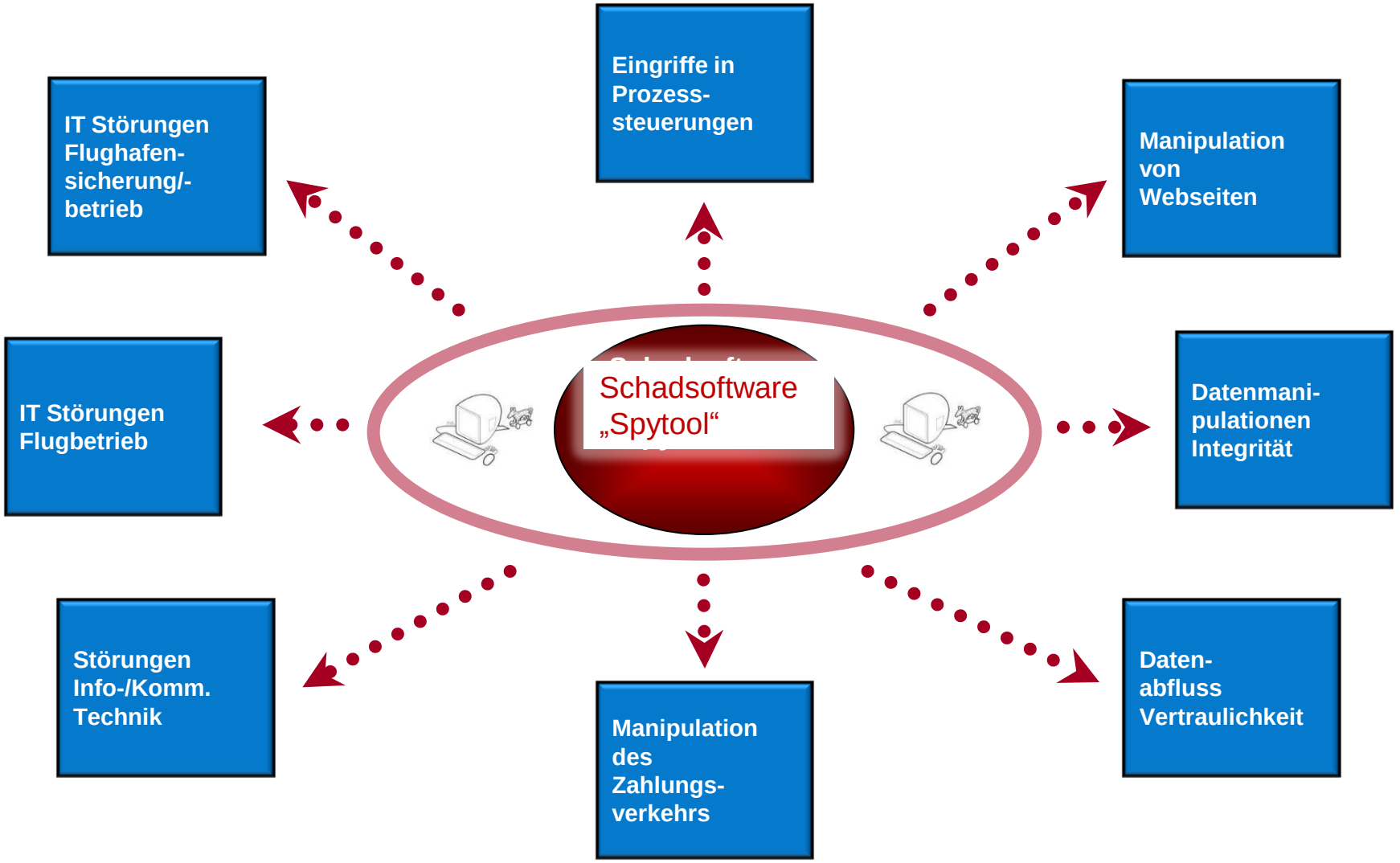
- 11 Bundesressorts und -behörden (BMI, BBK, BSI, …)
- 37 Länderressorts und -behörden
- 33 KRITIS-Einrichtungen (TK, Finanzwesen, Verkehr, Energie)
- International: EZB und Eurocontrol

Insgesamt während der Übungstage ca. 3.000 Personen

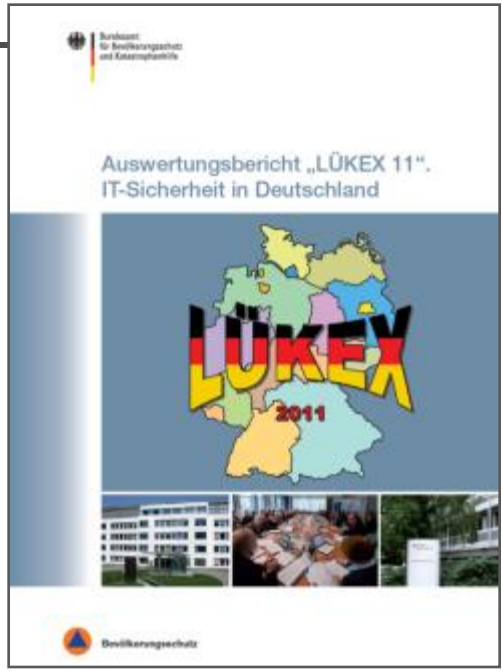
Zeitplan:

- Übungsdurchführung: 30.November/ 1. Dezember 2011
- Vorbereitung:
  - 5 Workshops der AG LÜKEX von 07/2010 bis 09/2011
  - 3 Themenworkshops (IT-Lagebild, Bund-Länder-Zusammenarbeit, Zusammenarbeit mit Unternehmen)

LÜKEX 2011- Szenariogestaltung



LÜKEX 2011- Erfahrungen



- Übung hat einen entscheidenden Beitrag zur (Weiter-) Entwicklung und Integration des IT-KM geleistet, schon bestehende Strukturen (IT-Abt. im BMI, BSI, IT-KM in Hessen) hatten Modellcharakter
- Übung hat Schnittstellenprobleme zwischen allg. und IT-KM offen gelegt, die weitergehende Regelungen erfordern (besonders wenn verschiedene Ressorts zuständig sind)
- „IT-Fachberater" für Krisenstäbe; Einbeziehung (zumindest zeitweise) von Beratern aus KRITIS-Bereichen in Krisenstäbe notwendig
- Im Vorgriff auf „VerwaltungsCERT-Verbund" wurde Zusammenarbeit Bund-Länder im IT-KM vorangebracht (Meldeverfahren BSI-Länder)
- Verfahren der Zusammenarbeit mit KRITIS-Betreibern (UP KRITIS) konnte weiter entwickelt werden
- Meldeverfahren über GMLZ stellt eine sinnvolle Ergänzung dar, sollte jedoch um eine (Gesamt-) Lagebeurteilung mit prognostischer Komponente ergänzt werden

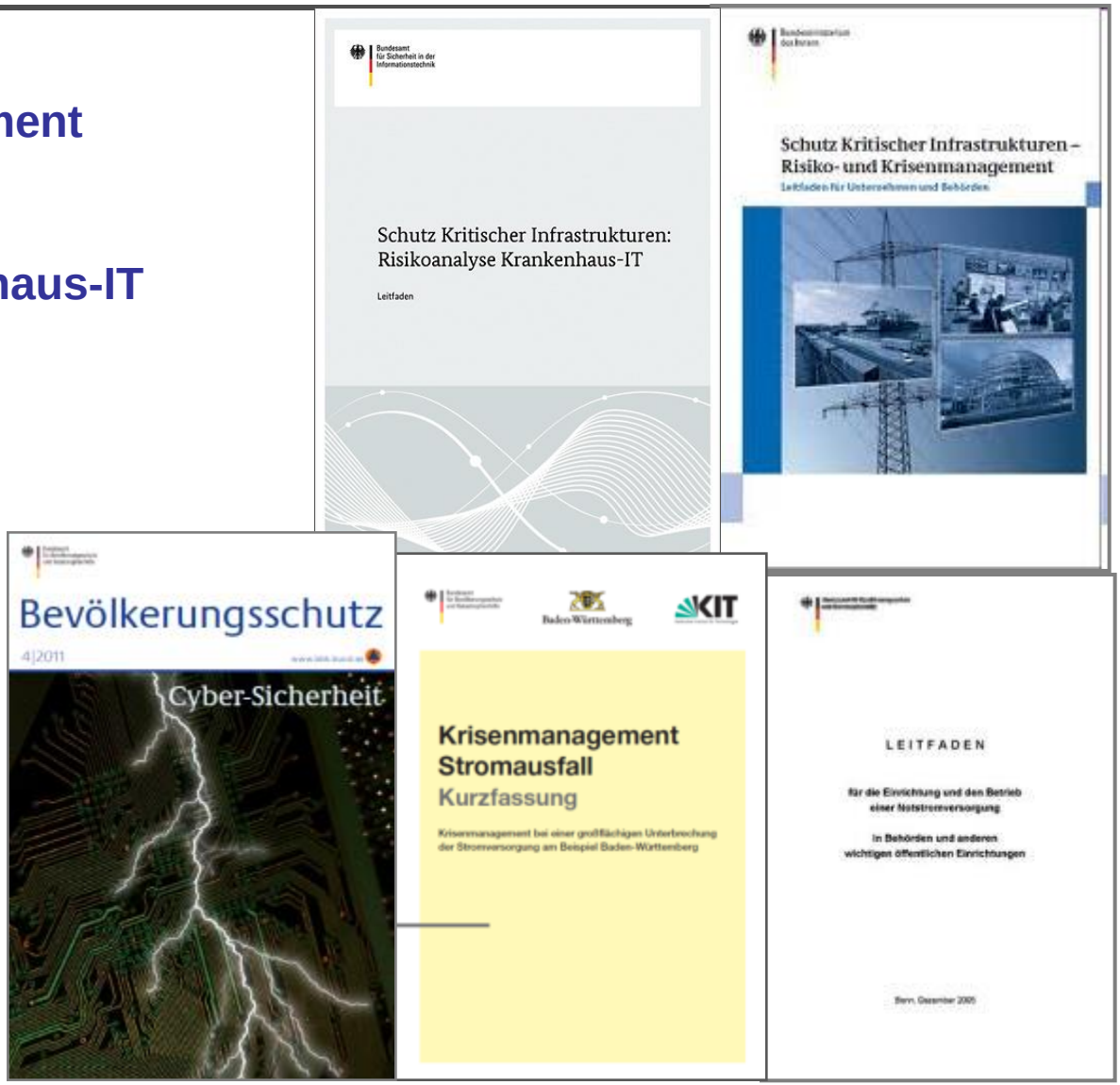
LÜKEX 2011- Erfahrungen

- LÜKEX als ein zeitgemäßer Governance-Ansatz im Bereich des strategischen Krisenmanagements bewährt
- Strategische Übungen als eine Form des Umgangs mit Ungewissheit; durch interdisziplinäre Diskurse können hyperkomplexe Zusammenhänge kritisch reflektiert und transparent gemacht werden.
- Der LÜKEX-Prozess repräsentiert eine neue gesamtgesellschaftliche Verständigungsform mit dem Ziel der Ausbildung von Resilienz für extreme Krisenlagen

Unterstützung durch Produkte des BBK

u. a.:

- **Risiko-/ Krisenmanagement für Betreiber KRITIS**
- **Risikoanalyse Krankenhaus-IT**
- **Notstromleitfaden**
- **Krisenmanagement Stromausfall**
- **Bevölkerungsschutz-Magazin (Sonderheft Cyber-Sicherheit)**



Fazit

- IT-Bedrohungen sind eine besondere Herausforderung für den Schutz kritischer Infrastrukturen.
- IT-Bedrohungen können nur im Dialog zwischen Behörden und der Wirtschaft wirksam bekämpft werden.
- Der Bevölkerungsschutz ist nicht unvorbereitet, weil IT-Infrastrukturen schon seit 2004 Teil der Nationalen Strategie zum Schutz kritischer Infrastrukturen sind.
- Eine Frage wird uns aber immer mehr herausfordern: Welches Maß an Sicherheit ist in einer zunehmend vernetzten Welt, in der IT-Anwendungen und elektronische Dienste das Leben bestimmen, realisierbar, um einerseits den möglichen (und notwendigen) Schutz umzusetzen, andererseits aber die Segnungen“ der Technik nicht vollständig zu blockieren?
- Mit der Cyber-Sicherheitsstrategie und der Einrichtung des Cyber-Abwehrzentrums hat der Bund die aktuelle Herausforderung angenommen.

Christoph Unger

Vielen Dank für Ihre Aufmerksamkeit!

Präsident BBK
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
Provinzialstraße 93
53127 Bonn - Lengsdorf
Tel.: 022899/550-0
Url.: www.bbk.bund.de