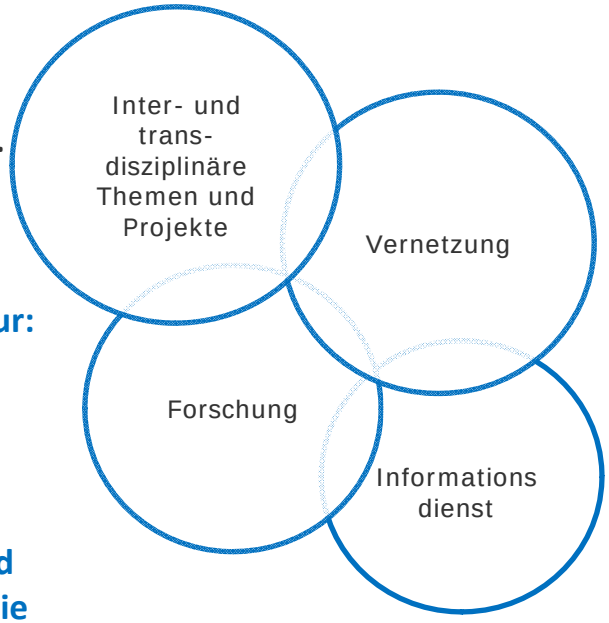
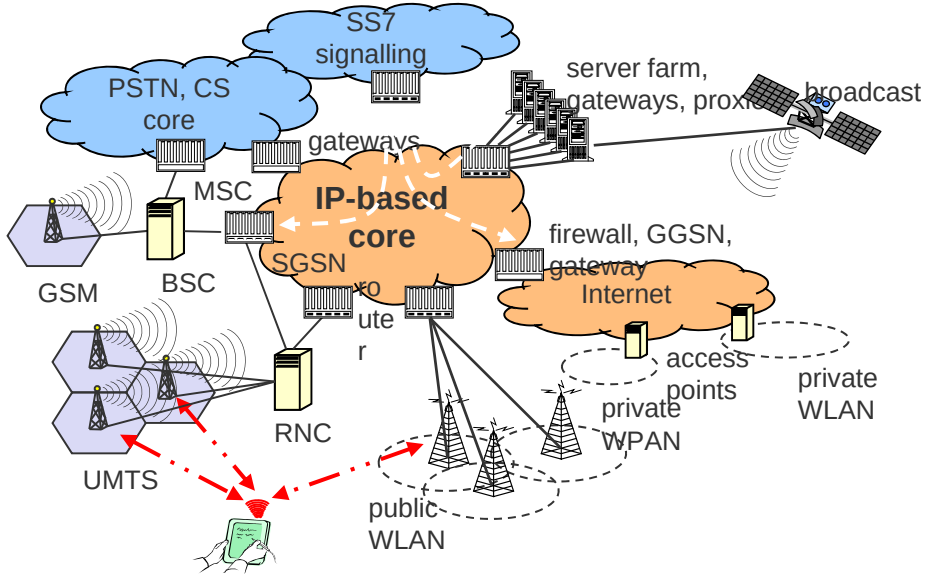
Forschungsforum: forschen, koordinieren, vernetzen, kommunizieren

- Inter- und transdisziplinär.
- 4 Workshops, mit über 240 Teilnehmern, 7 Publikationen.
- 2 Workshops zum Thema:
  1. **Kritische Infrastrukturen: „Konzept Kritische Infrastruktur: Vulnerabilitäten moderner Stromnetze und wie wir damit umgehen“**
  2. **Kriminalität und Cyberkriminalität: „Kriminalität – alte und neue Herausforderungen für die Sicherheit“**
- Fachkongress „Risikokommunikation“ mit dem Bundesministerium des Innern
- Vernetzung mit dem Zukunftsforum



Risikoidentifikation: Kommunikationsnetze heute

- Überwiegend digitale Netze; kaum mehr analoge Netze
  - immer mehr Telefonie über das Internet
- Funknetze - Mobilfunk dominiert
  - über 5,3 Milliarden Mobilfunknutzer, ca. 1 Milliarde angeschlossene Festnetzrechner



Auch ein Funknetz basiert auf einer Infrastruktur!

- Internet der Dinge - „embedded systems“
- Abhängig von direkter Stromversorgung
- **„Alles hängt mit allem zusammen.“**

Risikoidentifikation: Kritische Infrastruktur

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Kritische Infrastruktur

- *„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.“* [www.bmi.bund.de]
- Beispiele: Energieversorgung, IKT, Transport- und Verkehr, Wasserver-/-entsorgung, Gesundheitswesen, Ernährung, Notfall-/Rettungswesen, Katastrophenschutz, Parlament, Regierung, Verwaltung, Justiz, Finanz-/Versicherungswesen, Medien/Kulturgüter

Vulnerabilität

- Unter Vulnerabilität versteht man „physische, soziale, ökonomische und ökologische Faktoren und Prozesse, die die Anfälligkeit einer Gesellschaft gegenüber Gefahren (hazards) erhöhen.“
  [UN International Strategy for Disaster Reduction]

f (Vulnerabilität) = Exposition (*hazard*), Anfälligkeit, Bewältigungskapazität

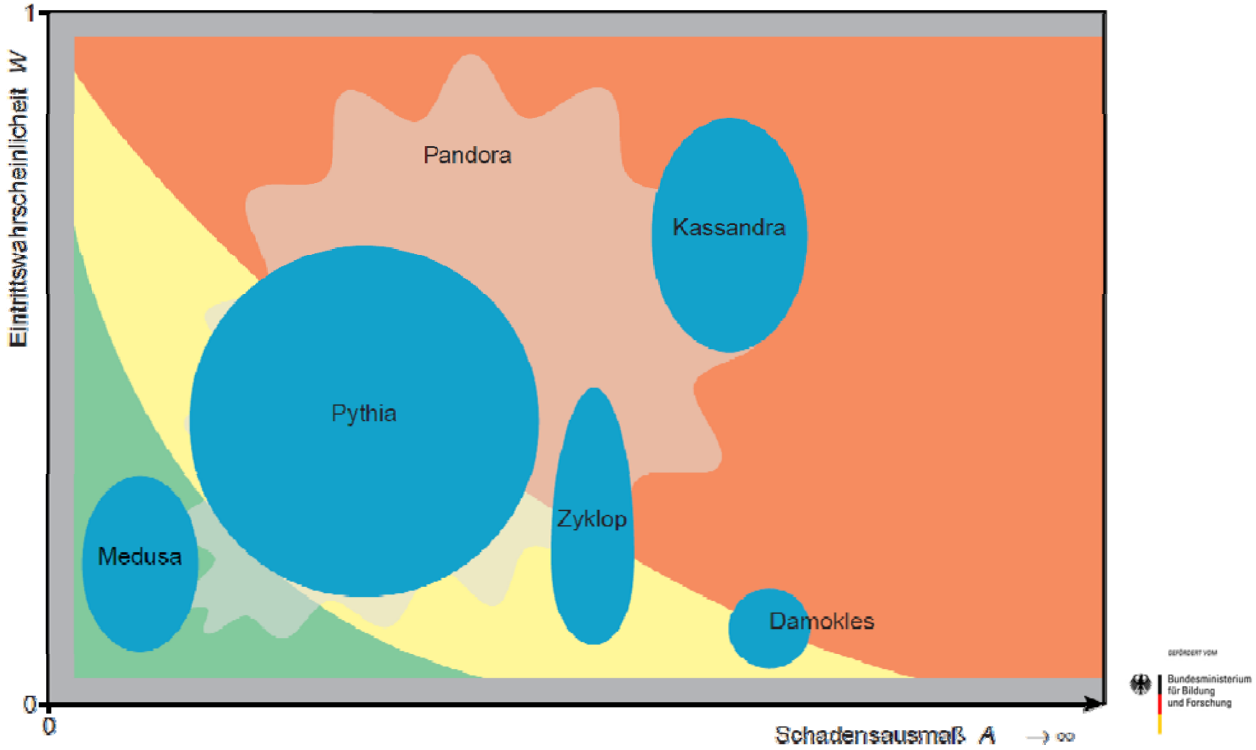
Gefördert vom Bundesministerium für Bildung und Forschung

Risikoklassifikation

Klassischer Risikobegriff = Eintrittswahrscheinlichkeit x Schadensausmaß

Klassifikation in Abhängigkeit von Eintrittswahrscheinlichkeit x Schadensausmaß
* (Nach WBGU 1998, Renn 2007)

- Damokles
- Zyklop
- Pythia
- Pandora
- Kassandra
- Medusa



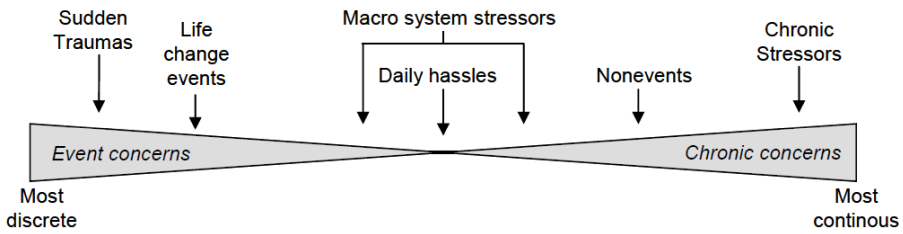
*= Erweiterte Bewertungskriterien

Risikoklassifikation

- Klassifikation in Abhängigkeit der Unsicherheit der Vorhersage
  (Rumsfeld 2002, Daase 2007, Taleb 2008)

	Known	**Unknown**
Known	Bekannte Risiken	Neue, aufkommende Risiken
Unknown	Vorenthaltene, ignorierte Risiken	Nicht kalkulierbare Risiken

- Klassifikation in Abhängigkeit weiterer Charakteristika
  - Entgrenzung in Zeit, Raum und Schaden
  - Hohe Komplexität
  - Hohe Unsicherheit / Ungewissheit
  - Hohe Ambiguität



➔ Systemische Risiken (vgl. OECD 2003, Renn 2007)

Beispiel: Kritische Infrastruktur Energieversorgung

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Trends: mehr Technik, mehr Player, größere Räume

- Technisch:
  - enge Kopplung der Stromversorgung an IKT-Steuerungstechnik
- Politisch /gesellschaftlich:
  - Liberalisierung der Strom- und Gasmärkte in der EU seit 1998
  - Regulierung, Privatisierung
  - Unbundling der Netze
  - Integration von Erneuerbaren Energien

Folgen: mehr IKT

- Koordination- / Kommunikationsaufwand nimmt zu
- Störanfälligkeit nimmt zu
- **smart grids:** bidirektionale Steuerung, Dezentralisierung, …
- smart metering

bisher nur Pilotprojekte

Gefördert vom Bundesministerium für Bildung und Forschung

Beispiel: Infrastruktur Energieversorgung

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Anforderungen aus der Perspektive des Rechts §

(Prof. Dr. Johann-Christian Pielow, Ruhr-Universität Bochum)

- Energiewirtschaftsgesetz (EnWG): nur Aspekte von *safety*, Aspekte von *security* fehlen bislang.
- Anreizregulierung (BNetzA) – „Qualitätsregulierung“ fehlt
- Gesetzliche Regelungen zur Abwehr von „energieuntypischen“ Störungen (Angriffe von außen) und für Hilfsmaßnahmen bei Versorgungsunterbrechungen fehlen.
  - Wird bisher dem allgemeinen Polizei- und Ordnungs- bzw. KatastrophenschutzR überlassen
- *smart energy – smart grids – smart metering*
  - Vervielfältigung der Rechtsbeziehungen durch neue Akteuere oder „Rollen“ (Messstellenbetreiber, -dienstleister, Prosumer, Betreiber virtueller Kraftwerke, IKT-Anbieter, Internet-Marktplatzbetreiber, …)
  - Regelungsdefizite im Bereich der „Systemverantwortung“ der Netzbetreiber
  - Vorgaben zur „Entflechtung“ (*Unbundling*) der Energienetze
  - künftige (Koordinatoren-) Rolle der Regulierungsbehörden noch unklar

Gefördert vom Bundesministerium für Bildung und Forschung

Risikomanagement: Nutzerperspektive

Der Nutzer ist Opfer und ggf. Akteur, da er Ressourcen zur Verfügung stellt

- Nutzersensibilisierung ist wichtig, aber …
  - kognitive Ressourcen sind begrenzt und die Komplexität hoch.
  - Wahrnehmung und Bewertung von Risiken ist subjektiv.
  - Bevölkerung differenziert zwischen personaler und sozialer Betroffenheit
  - es können unerwünschte Thematisierungseffekte auftreten.
  - darf nicht zur Externalisierung von Sicherheitsaufgaben führen.
- Selbstschutz und Selbsthilfefähigkeit verbessern
  - Förderung von Medienkompetenz: Grundregeln der Mediennutzung
  - Förderung von Systemvertrauen, Ambiguitätstoleranz & Orientierungswissen
  - kein Internetführerschein / Internet-TÜV .
- (Sozialwissenschaftliche) Forschung zu
  - Wahrnehmung systemischer Risiken / Ausfall kritischer Infrastrukturen
  - Resilienz & Vorsorge in der Bevölkerung hinsichtlich IT bezogener Systemrisiken

Risikomanagement: Gesamtgesellschaftliche Aufgabe

- Risikomanagement durch Kommunikation sollte …
  - offen und transparent erfolgen.
  - das Ausmaß an Unsicherheit offen legen.
  - zielgruppenorientiert erfolgen.
  - dialogisch und nicht aufklärerisch erfolgen.
  - frühzeitig erfolgen, um eine Kommunikationsbeziehung aufzubauen.
  - den Medienwandel einbeziehen (Online-Medien).
- „Neue“ Risikokultur
  - Offene Risikokommunikation zwischen Staat, Unternehmen und Bürgern
  - Diskussion zur Diskrepanz zwischen Sicherheit und Freiheit
  - Strategien für den Umgang mit dem Unerwarteten entwickeln (Unknown unknowns, Pythias)
  - Dialogische Entwicklung kollektiven Risikobewusstseins
- (Sozialwissenschaftliche) Forschung zu dialogischer Risikokommunikation und Wissenstransfer im Bereich systemischer Risiken

Risikomanagement: Technische Anforderungen

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Strategie: Wissen verbessern – Überraschungen vorbeugen – Wirkungen begrenzen

- Erkenntnisprobleme reduzieren
  - Z. B. Entwicklung von dynamischen Modellen, die Wechselwirkungen modellieren können
  - Erforschung von intersektoriellen Abhängigkeiten (Kaskadeneffekten)
- Erforschung des Dunkelfeldes Cybercrime
  - Z. B. Forensik („Auch Cyberkriminelle machen Fehler und hinterlassen Spuren.“)
- Erforschung der Möglichkeiten der Verwundbarkeitsreduktion
  - Entnetzung? Komplexitätsreduktion?
- Anforderungskatalog an eine sichere IKT-Architektur definieren
- Qualitätsanreize f. mehr Sicherheit
- Selbstschutz- und Selbsthilfefähigkeit von Systemen verbessern
  - Self-x-Fähigkeiten integrieren

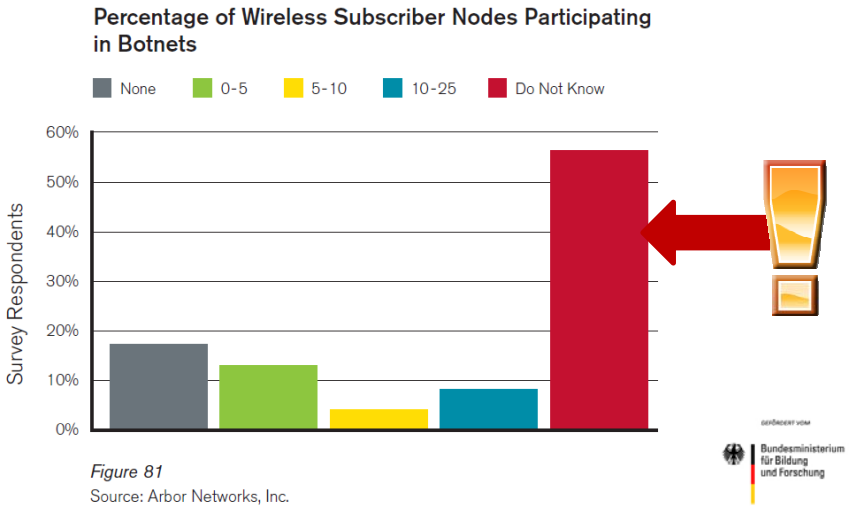


Figure 81
Source: Arbor Networks, Inc.

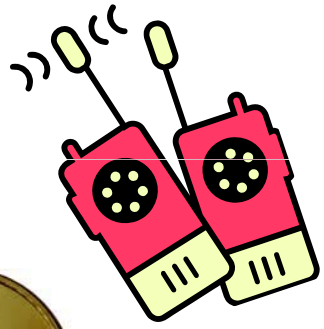
Risikomanagement: Bewältigungspotenziale stärken

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Strategie: Krisenmanagement stärken – Schadwirkungen reduzieren

- Vollzugsprobleme abbauen
  - Forensik ausbauen (Auch Cyberkriminelle machen Fehler und hinterlassen Spuren …)
  - Ressourcen und Manpower der Strafverfolgungsbehörden
- Krisenmanagement ausbauen
  - International
  - Staat und Betreiber
- Recovery: Kernfunktionalitäten prioritär instand setzen
- Kommunikationstechniken für Notfälle
  - Spontane Kommunikation, unabhängig von Infrastruktur
  - Autarke Systeme mit Möglichkeit zur Ankopplung an klassische Strukturen
  - Nicht nur high-tech, sondern auch **low-tech** Lösungsmöglichkeiten
  - Integration simpler, (analoger) walkie-talkie-Funktionalität in Handys – damit einfache Sprachkommunikation im Notfall



Gefördert vom Bundesministerium für Bildung und Forschung

Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Vielen Dank für Ihre Aufmerksamkeit !

jochen.schiller@fu-berlin.de
lars.gerhold@fu-berlin.de
marie-luise.beck@fu-berlin.de

www.sicherheit-forschung.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung