Der Schutz kritischer Infrastruktur in einer globalisierten Welt am Beispiel der Kommunikationstechnik

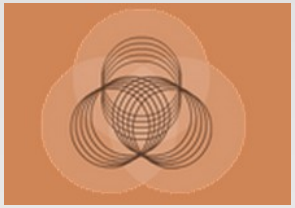
Thomas Reinhold,
IFSH - Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Gliederung des Vortrags

- Über das IFSH / Persönliche Vorstellung
- ICT Infrastrukturen in Deutschland und Weltweit
  ICT - information and communication technology
- ICT als kritische Infrastrukturen, Abhängig- und Verwundbarkeiten
- Bedrohungen der ICT
- Militärische Nutzung von ICT und sicherheitspolitische Fragen
- Schutzmöglichkeiten für ICT
- Ein Ausblick auf den Cyberspace

About

- Über das IFSH
  - Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg
  - Stiftung der Stadt Hamburg 1971, Wolf Graf Baudissin erster Leiter
  - Wissenschaftliche Forschung und Politikberatung
  - Sicherheitspolitische und Naturwissenschaftliche Arbeitsbereiche



- Über mich
  - Diplom Informatiker, Nebenfachstudium der Psychologie
  - Seit 2009 Fellow des IFSH, seit 2013 Promovend
  - Mitglied im Forschungsverbund Naturwissenschaft, Abrüstung und internationale Sicherheit (FONAS)
  - Freiberuflicher Software-Entwickler

Exkurs – Zum Begriff „Cyberspace“

- EU Cybercrime Convention (2001):

  By connecting to communication and information services users create a kind of common space, called "cyber-space"

- Cyber Security Strategy UK (2011):

  “an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services”

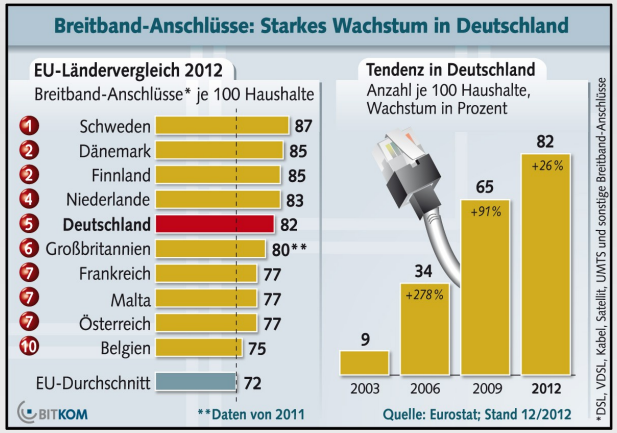
- Alle vernetzungsfähigen Computer & deren Infrastrukturen
- Alle Daten der Systeme, deren Austausch & Nutzeraktionen
- Vom Smartphone über Server bis zum Industrierechner

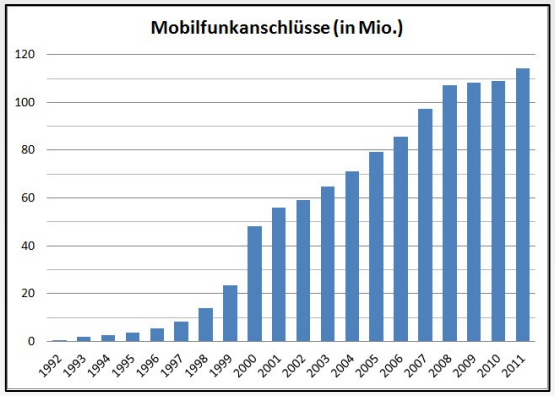
Exkurs – Zum Begriff „ICT“

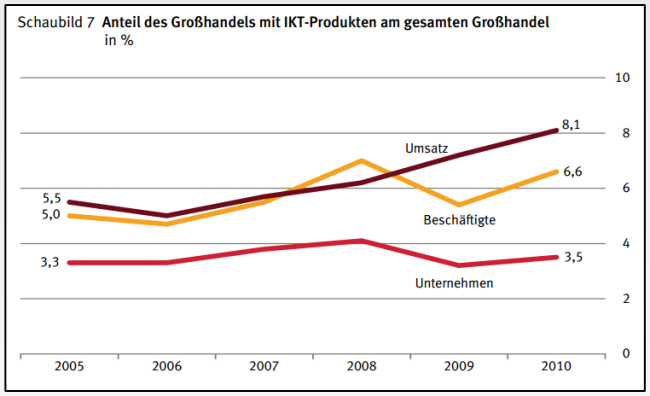
- ICT = *information and communication technology*
- ICT umfasst die Technologie für:
  - die Übermittlung von Informationen durch den Raum („Kommunikation“)
  - die Übermittlung von Informationen durch die Zeit („Speicherung“)
  - Umformung von Informationen in Raum und Zeit ("Computer-Berechnungen")

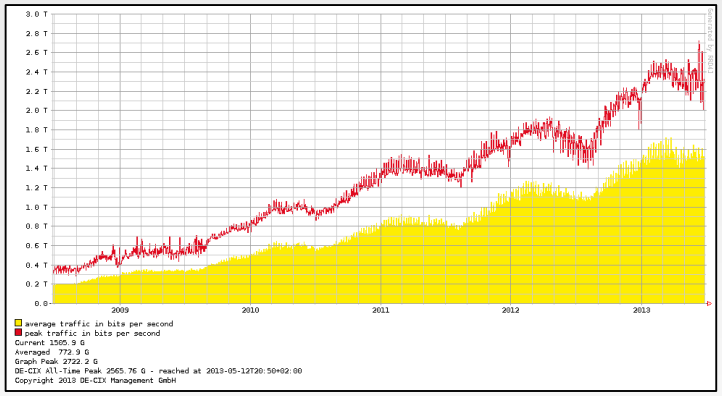
ICT Infrastrukturen - In Deutschland

- Bestandteile
  - Telekommunikationsanbieter (Mobilfunk / Fest)
  - Internet-Serviceprovider, Kabeldienstbetreiber
  - Daten-Carrier, Backbones und Austausch-Knoten
  - Rechenzentren, Server-Farmen, Cloud-Dienste



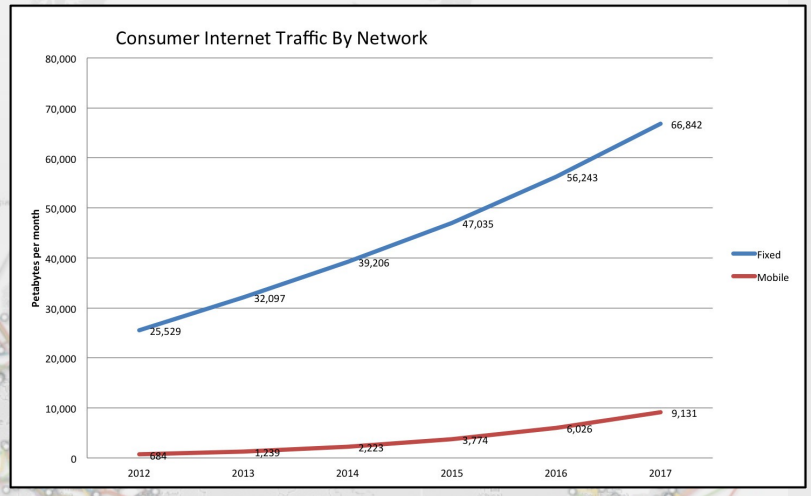






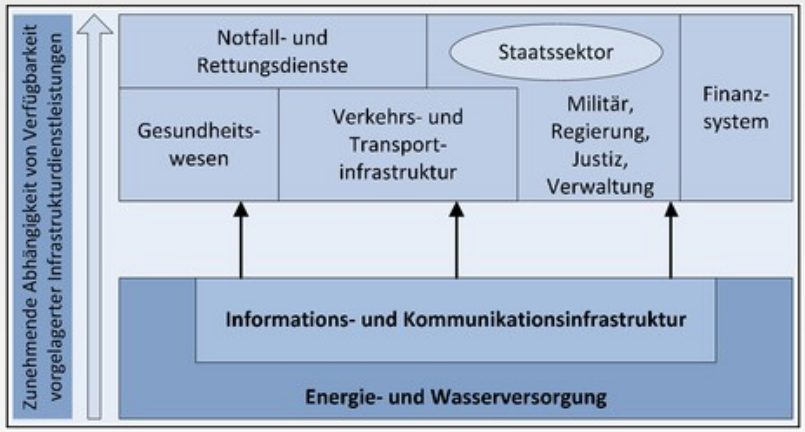
ICT Infrastrukturen – Weltweit

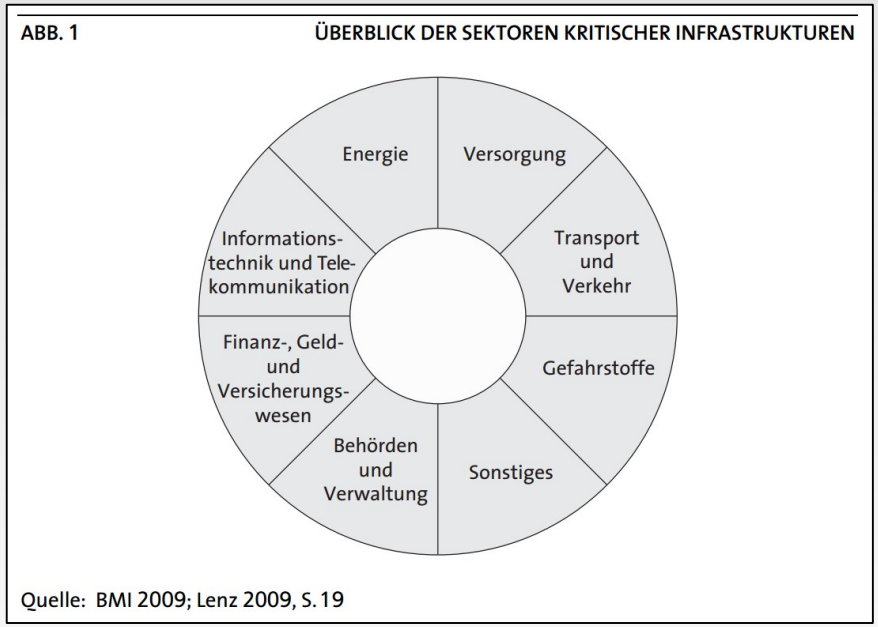
- Bestandteile
  - Glasfaser Backbones
  - Exchange Points (~ 340 IXPs weltweit, 165 Europa, 80 Nordamerika)
  - Datenaufkommen/Tag: ~ 1.800 Petabyte
  - TLD-DNS-Dienste (Root Nameserver)



Kritische Infrastrukturen

- Kritische Infrastrukturen
  - *„sind Institutionen 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.“*
  - Unterteilung in 9 interdependente Sektoren
  - Verschieden starke Abhängigkeiten





Kritische Infrastrukturen II

- Dimension der „Kritikalität“
  - *„Die Kritikalität einer Kritischen Infrastruktur bezeichnet ihre Bedeutsamkeit bezüglich der Konsequenzen, die Störungen, Ausfälle von Funktionen oder Zerstörungen für die (Versorgungs-)Sicherheit der Gesellschaft mit wichtigen Gütern & Dienstleistungen haben“*
  - Studie des Schweizer Bundesamts für Bevölkerungsschutz 2009:

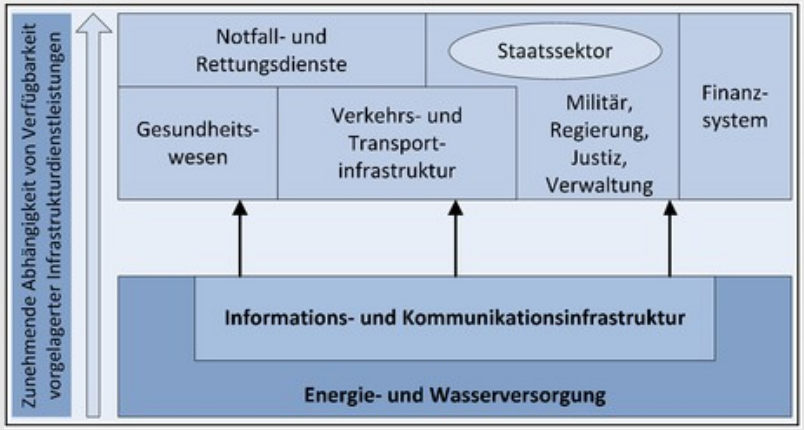
    - Telekommunikation 9/9 Punkten
    - Informationssysteme und -netze 7/9
    - Internet jeweils den Wert 7/9
  - Nur vier weitere Sektoren ähnliche hohe Bewertungen: Stromversorgung (9/9), Straßen/Schienenverkehr (8/9) und Banken (7/9)

Sektoren	Teilsektoren
Behörden	Parlament, Regierung, Justiz, Verwaltung
	Forschungseinrichtungen
	Nationale Kulturgüter
	Ausländische Vertretungen und Sitze internationaler Organisationen
Chemische Industrie	Produktion, Transport, Lagerung und Verarbeitung chemischer Stoffe
Energie	Stromversorgung
	Erdölversorgung
	Erdgasversorgung
Entsorgung	Abwasser
	Industrie- und Hausabfälle
	Kontrollpflichtige Abfälle
Finanzen	Banken
	Versicherungen
Gesundheit	Ärztliche Betreuung und Spitäler
	Arzneimittel
	Labors
Informations- und Kommunikationstechnologien (IKT)	Telekommunikation
	Informationssysteme und -netze
	Internet
	Instrumentations-, Automations- und Überwachungssysteme
	Rundfunk und Medien
Nahrung	Versorgung mit Lebensmitteln und Gewährleistung der Lebensmittelsicherheit
	Trinkwasserversorgung
Öffentliche Sicherheit, Rettungs- und Notfallwesen	Blaulichtorganisationen (Polizei, Feuerwehr, sanitätsdienstliches Rettungswesen)
	Zivilschutz
	Armee
Verkehr	Strassenverkehr
	Schienenverkehr
	Luftverkehr
	Schifffahrt
	Postwesen und Logistik

	Sehr grosse Kritikalität*
	Grosse Kritikalität*
	Reguläre Kritikalität*

ICT als Bestandteil kritischer Infrastrukturen

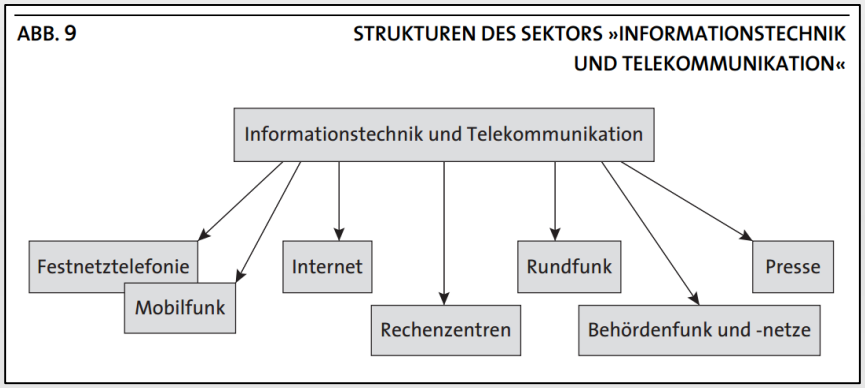
- Besonderheiten des Sektors ICT
  - weitreichende Abhängigkeiten
  - hohe Kritikalität
  - (fast) 100%ige Stromabhängigkeit



- Kritikalität
  - Unterschiedlichste ICT-Dienste auf Basis geteilter Infrastrukturen (Fernsehen, (Mobil)Telefonie, Internet, Behördenfunk, Behördennetze, Finanzen)
  - größeren Komplexität, mehr beteiligte Betreiber, höhere Störungsanfälligkeit
  - Zusammenbruch eines Teildienstes => erhöhte Beanspruchung von Ausweichdiensten

ICT als Bestandteil kritischer Infrastrukturen II

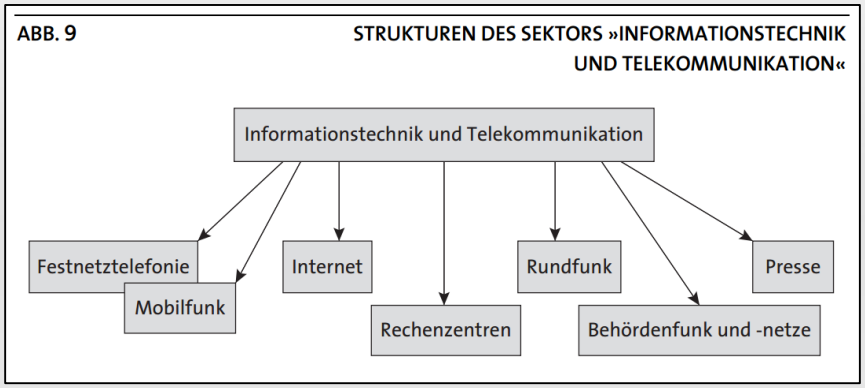
- Kritische Bestandteile der ICT
  - Telekommunikations-Sicherstellungs-Verordnung TKSiV §2 definiert das Mindestangebot an Dienstleistungen bei Auftreten einer Krise/Katastrophe



  - 1. Telefon-Wählverbindungen einschließlich Funktelefondienst
  - 2. Wählverbindungen bei ISDN
  - 3. Einrichtung von Telefon-, Funktelefon- und ISDN-Anschlüssen
  - 4. Einrichtung von Übertragungswegen für Ton- und Fernsehsignale
  - 5. Entstörung der genannten TK-Dienstleistungen

ICT als Bestandteil kritischer Infrastrukturen III

- ABER:
  - Keine explizite Regelung für Schutz vor IT-spezifischen Gefahren (Cyberangriffen)
  - Fehlende gesetzliche Betreiberpflichten im Bereich der IT-Dienste
  - Insbesondere keine explizite Regelung für das Domain Name System



- Ausfallsicherheit und Gewährleistung von Notbetrieb der TK-Infrastruktur ist Aufgabe der Bundesnetzagentur, aber:

  „Eine politisch-strategische Befassung der Bundesnetzagentur mit dem Thema Kritischer IT-Infrastrukturen ist nicht zu erkennen“ (TAB-Studie 2011)

ICT: Verwundbarkeiten

- TAB-Studie 2011: fast keine systematischen Untersuchungen der einzelnen Bedrohungen und ihrer Auswirkungen
- Schadenshöhe bei Blackout > 6,50 Euro/kWh (Interview Rösler, 2011)
- Studie TU Berlin (2011) > 8,50 EUR/kWh

Naturereignisse	Technisches / menschliches Versagen	Terrorismus, Kriminalität, Krieg
Extremwetterereignisse u.a. Stürme, Starkniederschläge, Temperaturstürze, Hochwasser, Hitzewellen, Dürren	Systemversagen u.a. Unter- und Überkomplexität in der Planung, Hardware-, Softwarefehler	Terrorismus
Wald- und Heidebrände	Fahrlässigkeit	Sabotage
Seismische Ereignisse	Unfälle und Havarien	sonstige Kriminalität
Epidemien und Pandemien bei Mensch, Tier und Pflanzen	Organisatorisches Versagen u.a. Defizite im Risiko- und Krisen-management, unzureichende Koordi-nation und Kooperation	Bürgerkriege und Kriege
Kosmische Ereignisse u. a. kosmische Energiestürme, Meteoriten und Kometen		

ICT: Verwundbarkeiten – Exemplarische Beispiele

- Struktur des ICT-Versorgungsnetzes
  - ICT durch hierarchisch gegliederte Vermittlungsstellen strukturiert
  - Fernvermittlungsstellen, per Notstromaggregate (NSA) 8h bis 48h gepuffert
  - Ortsvermittlungsstellen versorgen 10.000 bis 100.000 Kunden, haben USV (Unterbrechungsfreie Stromversorgung) mit Puffer für 15min bis 8h
  - Basisstationen im Mobilfunknetz per USV 15min bis 8h gepuffert
  - Blackout beträfe auch DSL/Kabelmodems, Anschlusstechnik i.a.R. ohne Puffer

    => Blackout beträfe zuerst Zugänge zu den ICT-Diensten, selbst wenn deren Kern-Infrastruktur noch funktionsfähig ist

  - Rechenzentren & Serverfarmen i.a.R. durch USV/NSA für mehrere Tage abgesichert (oft redundant) aber Datenleitungen zwischen Knoten ggf. betroffen

ICT: Verwundbarkeiten – Exemplarische Beispiele II

- Behördenfunk (Polizei, FFW, Rettungsdiensten, THW, Zoll)
  - Wechsel von analogem zu digitalem TETRA-System
  - Neue Antennenstandorte und Vermittlungsstellen nur 2h Batteriepuffer (früher 4-8h)
- Kommunikation der Regierung und Bundesverwaltung
  - Informationsverbund der Bundesverwaltung (IVBV), Informationsverbund Berlin-Bonn (IVBB), Bundesverwaltungsnetz (BVN)
  - Zukünftig zusammengefasst zu gemeinsamer Infrastruktur „Netze des Bundes“ (NdB)
  - Maximal 72h Puffer für zentrale Netzbestandteile über NSA
- Weitere nicht-öffentliche Netze
  - Zahlungsverkehrsnetz der Banken (EC/ATM/Transfer und Handel) haben hohe Systemstandort-Redundanz, eigene Transfer-Netze und Puffer von ca. 1 Woche
  - DFN, ...

ICT: Verwundbarkeiten – Exemplarische Beispiele III

TAB. 3 ZEITLICH GESTUFTE AUSFÄLLE IM SEKTOR »INFORMATIONSTECHNIK UND TELEKOMMUNIKATION«

	Endgeräte	Vermittlungstechnik	Backbonenetze
Festnetz (mit analogem Endgerät)	**	**	****
Festnetz (DSL-Anschluss, VoIP)	*	**	****
Mobiltelefon	***	**	****
Satellitenfunk	***	****	****
BOS	***	**	**
Internet	*	**	****
Behördennetze	***	***	***
Fernsehen	*	***	***
Hörfunk (batteriebetriebenes Radio, Autoradio)	****	****	****

* sofort; ** binnen Stunden; *** binnen Tagen; **** binnen Wochen

Lesehinweis: Hinsichtlich des Anfalls der jeweiligen Ebene ist zu beachten, dass jeweils das schwächste Glied über die Funktionsdauer entscheidet. Dieses ist unterlegt.

ICT: Beispiele signifikanter Vorfälle

- ENISA - Europäische Agentur für Netz- und Informationssicherheit
  - Förderung der Informationssicherheit innerhalb der EU fördern, Analyse von Risiken, Entwicklung von Standards, Incident-Beratung
  - Art. 13a der EU-Framework Directive (2009/140/EC) als Harmonisierungs-Ansatz für die Meldung von signifikanten ICT Vorfällen und deren Vermeidung
- ENISA Anual Incidents Reports 2012
  - 80 signifikante Vorfälle
  - Umstellung auf VoIP: Ausfall 400.000 Anschlüsse für 14h
  - Internet-Routing-Fehlkonfiguration: 17h Internet-Ausfall, 1.3 Mio. Nutzer, inkl. „112“
  - DDoS-Attacke gegen Provider-DNS: 2.5 Mio. Nutzer, 2h Internetausfall
  - Sturm/Unwetter: 1.0 Mio. Nutzer für 24h bis 2 Wochen ohne mobiles Telefonnetz

ICT: Beispiele signifikanter Vorfälle II

- ENISA Anual Incidents Reports 2012

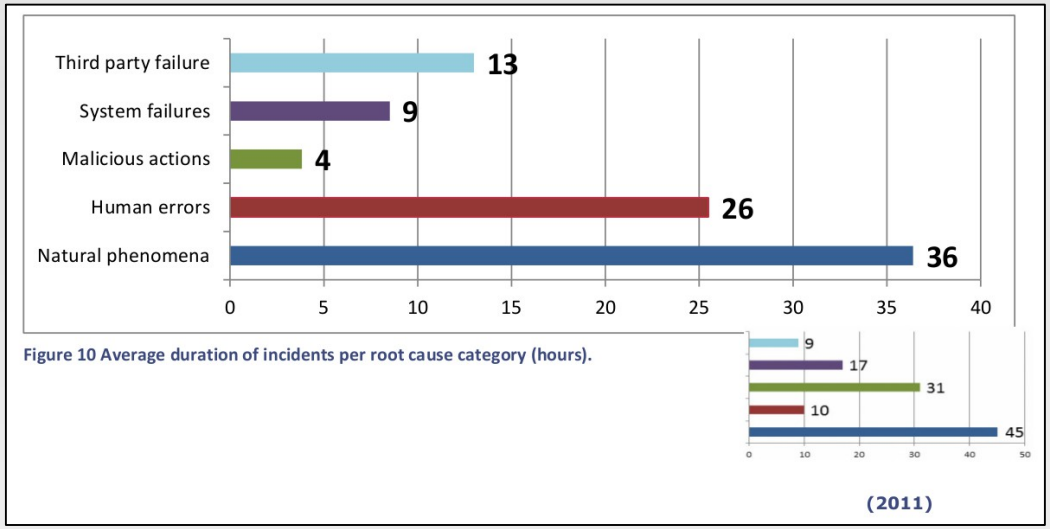


Figure 10 Average duration of incidents per root cause category (hours).

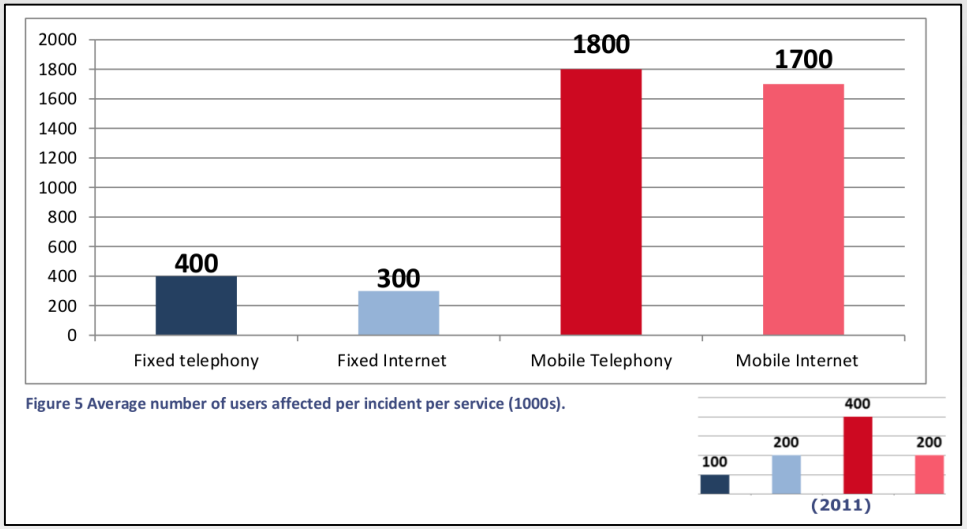


Figure 5 Average number of users affected per incident per service (1000s).

=> Mobilfunk am meisten betroffen

=> Internet-Ausfälle betrafen im Schnitt die meisten Nutzer

=> die meisten Vorfälle betrafen Mobilfunk und Mobiles Internet

=> in 37% alle Vorfälle war auch die Verfügbarkeit von Notrufen (112) betroffen

Bedrohungen der ICT: Cybercrime vs. Cyberwar

- Aspekte bei der Bewertung
  - Ziel des Angriffs: Spionage, Sabotage oder Angriff mit Störwirkung
  - Identität und Motivation des Angreifers
  - Politische Rahmenbedingungen des Angegriffenen
- Abgrenzung Krieg vs. Kriminalität
  - Cybercrime → Fragen nach Regelungen der internat. Strafverfolgung
  - Cyberwar → Fragen nach den politischen Motivationen und Ziele der Akteure

Bedrohungen der ICT: Klassifikation

- Strukturelle Gefahren
  - Agenda-Setting, oder „Wer kontrolliert das Internet“
  - Das Problem der Dominanz weniger nationaler Industrien
  - Überwachungs- und Kontrollmaßnahmen
- Technologische Gefahren
  - Hacker
  - Cybercrime
  - Schadsoftware

Bedrohungen der ICT: Strukturelle Gefahren I

- Agenda-Setting
  - Selbst-Regulation vs. Steuerung durch internationale Gremien (ITU)
  - Standarisierung der Funktionsweise durch US-amerikanische Gremien
    IRTF - Internet Research Task Force
    IETF - Internet Engineering Task Force
    ICANN - Internet Corporation for Assigned Names and Numbers
    IANA - Internet Assigned Numbers Authority
- Industrie- & Infrastrukturdominanz
  - IT-Infrastruktur auf Basis weniger US-amerikanischer Firmen
  - Geheimdienstenkooperationen für den Datenzugriff, Key-Escrow, Hintertüren in Hard- und Software, Insider-Wissen
  - Bsp: Cisco, IBM, Microsoft, Huawei, ZTE, ...

Bedrohungen der ICT: Strukturelle Gefahren II

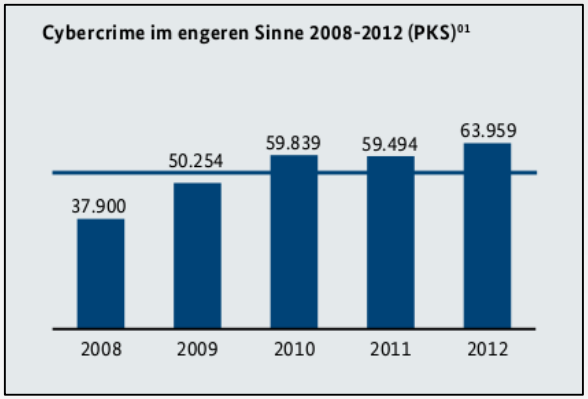
- Überwachung und Kontrollmaßnahmen
  - Enthüllungen E. Snowden
  - Erfassen von Daten (PRISM, Upstream, ...)
  - Auswertung und Analyse (Xkeyscore)
  - Speicherung (Stellar Wind, ShellTrumpet)

"You're not waiting for someone to decide to turn information into electrons and photons and send it (..) You're commuting to where the information is stored and extracting the information from the adversaries' network. We are the best at doing it. Period."

Michael Hayden, ehemaliger Leiter der NSA/CIA unter G.W. Bush

Bedrohungen der ICT: Technologische Gefahren I

- Hacker
  - White-Hat-Hacker (Idealisten, Datenschützer, Netz-Aktivisten)
  - Black-Hat-Hacker (Gruppen, Betreiber von Schadsoftware-Infrastrukturen)
  - Nationalisten (DDoS-Attacke Estland 2007, Syrian Electronic Army 2013)
- Cybercrime
  - Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten
  - Fälschung im Rechtsverkehr bei Datenverarbeitung
  - Datenveränderung, Computersabotage
  - Ausspähen von Daten, Phishing bei Onlinebanking
  - DDoS (Distributed Denial of Service)
  - Wirtschaftlicher Schaden 2012: 71,2 Mio. Euro



Bedrohungen der ICT: Technologische Gefahren II

- Malware
  - Malware: Software mit unerwünschter, ggf. schädlicher Funktion
  - Klassifikation nach Verbreitung, Schaden, Absicht, Zielsystem, Kontrollmöglichkeiten
    - Viren — Reproduktion durch Einschleusen in Software
    - Würmer — Aktive Selbstverbreitung über Netzwerkdienste
    - Trojaner — Schadcode verborgen in scheinbar nützlicher Software
    - Botnetze — Verborgene Software auf Rechnern, über zentrale Server ferngesteuert
  - Zero-Day-Exploits als „heiliger Gral“
  - Schwarzmarkt, Firmen und Dienstleister für Sicherheitslücken und Malware
  - Bsp: NSA 2013 mit 25 Mio. $ Budget für Aufkauf von Sicherheitslücken

Militärische Nutzung von ICT

- 33 Staaten, militärische Cyber-Programmen in Sicherheits- und Militärdoktrinen (J. Lewis 2011: Preliminary Assessment of National Doctrine and Organization)
  - USA: Department of Defence Cyber strategy (2011)
    handling the cyberspace as warfare domain (..) allows (DoD) to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests
    - Plan X (DARPA) 1.54 Mrd. $ von 2013 bis 2017 für „cyber-offense“
    - US Cyber command: bis zu 5000 Mitarbeiter in den nächsten Jahren
  - Russland: Erneuerte Militärdoktrin (2010)
    (equipping includes) “the development of the forces and means of information warfare”
  - China: White Paper on National Defence (2004)
    (the Army takes) „informationalization as its orientation and strategic focus”
  - Deutschland: Bericht des BMVg an Verteidigungsauschuß vom 5.6.2012
    "Eine Anfangsbefähigung zum Wirken in gegnerischen Netzwerken wurde erreicht"
    - Abteilung Computernetzwerkoperationen des Kommando Strategische Aufklärung seit 5 Jahren im Aufbau

Militärische Nutzung von ICT II

- Mindestens zwei bestätigte Cyberattacken
  - Stuxnet, Teil des Programms „Olympic Games“, gestartet 2006 von G.W.Bush
  - Flame, Kooperation US/Israelisches Militär zur Überwachung iranischer Netze
- Technische Offensiv-Möglichkeiten der NSA
  - Hacker-Einheit „Tailored Access Operations“ (600 Personen, Field Unit)
    „we hack backbones“
  - Eigenentwicklung von Malware, Betrieb eines Botnetzes, Glasfaser-Zugriffe
  - Zugriff auf alle großen mobilen Betriebssysteme (iOS, Android, Blackberry)
  - 2011: 231 gezielte Cyberangriffe (~3/4 gegen Ziele mit höchster Priorität)
  - Programm "Genie" für Kontrolle ausländischer Netzwerke, 652 Mio $ Budget (Ende 2013: auf 85.000 strategisch ausgewählten Computern zu platzieren)
- China (APT1 / PLA 61389), Nordkorea …

Militärische Nutzung von ICT III

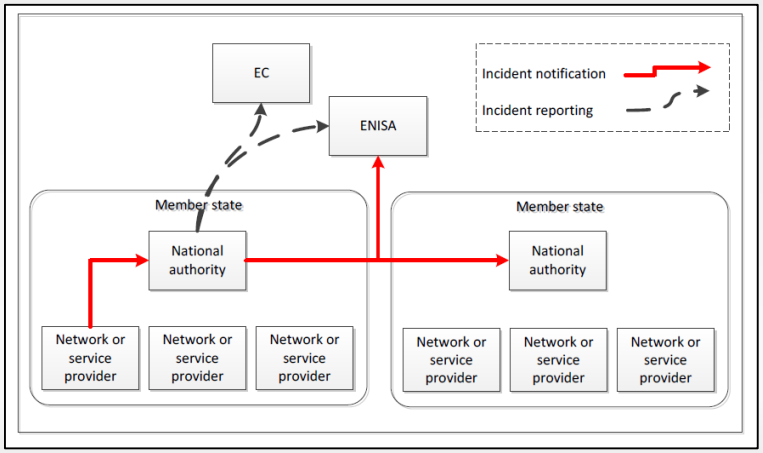
- Sicherheitspolitische Fragen
  - Abschreckung und Auslösen einer neue Rüstungsdynamik
  - Unklares Drohpotential, unklare Gefährdungssituation
  - Politische Instabilität durch geheime Cyberwar-Programme
  - Das Attributions-Problem und das Selbstverteidungsrecht nach dem „ius ad bellum“
  - Rüstungskontrolle und Non-Proliferation von (Dual Use)-IT Gütern
  - Cyberattacken zwischenstaatlicher Akteure
  - Freiheit vs. Kontrolle

Schutzmöglichkeiten für ICT

- Technische Möglichkeiten
  - Technische Konzepte als für Schutz für „normale“ Angriffe suffizient
  - Integration bestehender Sicherheitstechnik in Industrie-Prozesse
  - Aber: theoretischer Zugriff der NSA auf beliebige Daten unabhängig von Schutz
  - Einzige Schwellen für staatliche Cyberoperationen bleiben der Grad der notwendigen Geheimhaltung und die verfügbare Vorbereitungszeit
  - Starke Kryptographie „by design“ als einziger Ausweg für Datenintegrität
  - 100% sichere, zertifizierte Zuliefer- und Produktionsketten
  - Entnetzung als Ansatz bietet zweifelhaften Schutz

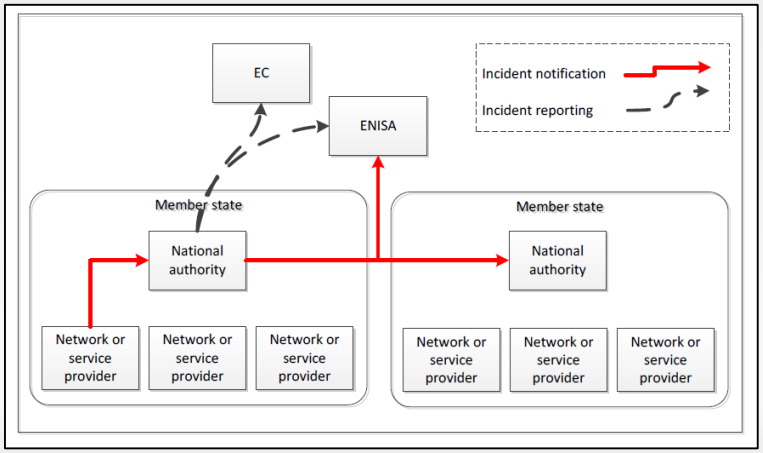
Schutzmöglichkeiten für ICT II

- Politische Möglichkeiten
  - Internationale Vernetzung zur Behandlung von Cybersicherheits-Vorfällen
  - CERTs (Computer Emergency Response Team): Gruppe von IT-Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfällen als Koordinator mitwirkt bzw. sich ganz allgemein mit Computersicherheit befasst
  - Aufbau klarer hierarchischer Informationsstrukturen von Bürger-Industrie-Staat-EU
  - ENISA - Europäische Agentur für Netz- und Informationssicherheit, Art. 13a der EU-Framework Directive (2009/140/EC)



Schutzmöglichkeiten für ICT III

- Krisenübungen (ENISA, Cyber Europe 2010/2012)
  - Übungsszenarios: starke Netzstörungen durch fiktiven Cyberangriff auf Europa auf öffentliche elektronische Dienste (E-Gouvernement/Finanzdienste)
  - Erkenntnisse:
    - Zusammenarbeit Informationsaustausch auf internationaler Ebene
    - Hierarchisierung von Vorfällen und deren Grad
    - Hierarchisierung von Meldesystemen, Klare Kommunikationsrichtlinien und Kanäle
    - Klare Grundladen (rechtliche) für öffentlich-private Kooperationen
    - Skalierbarkeit der Strukturen im Augen behalten



	1h<...<2h	2h<...<4h	4h<...<6h	6h<...<8h	>8h
1%<...< 2% of users					
2% < ...< 5% of users					
5% <...< 10% of users					
10% <...<15% of users					
> 15% of users					

Table 1 Combination of thresholds

Schutzmöglichkeiten für ICT IV

- C(S)BM - Confidence (and security) building measures
  - Konzept in den 70'er Jahren im Rahmen der KSZE entwickelt
  - Glaubhaft die Abwesenheit von Bedrohungen demonstrieren
  - Unsicherheiten über Absichten der gegnerischen Seite verringern
  - Die Möglichkeiten eingrenzen, in Krisensituationen militärischen Druck auszuüben
  - Kommunikation in Krisenzeiten verbessern
  - Transparenz zu Aufgaben, Strategien, Stärke & Doktrinen der Streitkräfte herstellen

*"to **reduce** and even **eliminate** the causes of **mistrust, fear, misunderstanding and miscalculations** with regard to relevant military activities and intentions of other States" (..) to help to **prevent military confrontation** as well as covert preparations for the commencement of a war, to reduce the **risk of surprise attacks and of the outbreak of war by accident**."*

General Assembly, Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament, UN document A/S-15/3, 28 May 1988, pp. 28–33.

Schutzmöglichkeiten für ICT V

- C(S)BM - Maßnahmen
  - Deklaratorische Ansätze: NATO CCDCOE Tallinn Manual
  - Politische Seminare zu internationalen Cyberspace-Doktrinen
  - Bilaterale militärische Übungen (China-US-Wargames 2012)
  - Verzicht auf den „First-Use“ von Cyberwaffen
  - Entwicklung von einheitlichen Standards und Bewertungsmaßstäben
  - UN-Cyberkonventionen und Verifikations-Maßnahmen
  - Cyberspace als „man made domain“ strukturell und funktionell gestaltbar

*“to **reduce** and even **eliminate** the causes of **mistrust, fear, misunderstanding and miscalculations** with regard to relevant military activities and intentions of other States” (..) to help to **prevent military confrontation** as well as covert preparations for the commencement of a war, to reduce the **risk of surprise attacks and of the outbreak of war by accident**.”*

General Assembly, Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament, UN document A/S-15/3, 28 May 1988, pp. 28–33.

Ein Ausblick auf den Cyberspace

- Konsequenzen die NSA-Enthüllungen
- Realität und konkrete Verfügbarkeit von Cyberwaffen
- Debatte über Datenschutz und Privatsphäre vs. Kontrolle
- Weiter wachsende Abhängigkeit von IT und IT-Infrastruktur
- Weiterer Trends zur Autonomisierung (Smart Grid)
- Stärkeres Sicherheitsbewusstsein bei Planern und Entscheidern
- Stärkere internationale Kooperation beim Kampf gegen Cybercrime

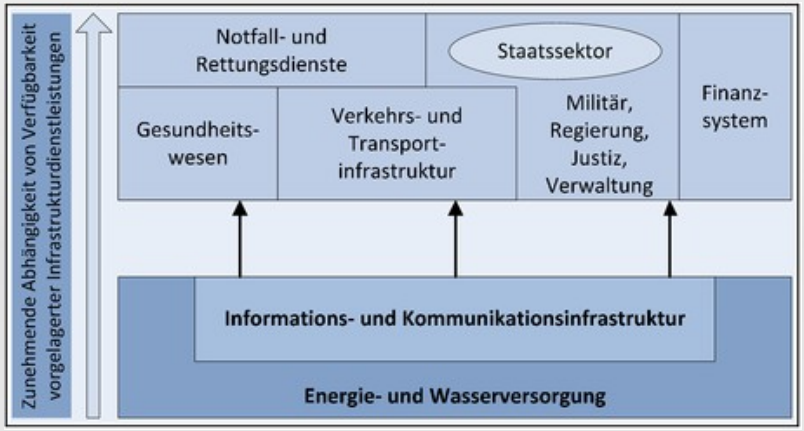
- Bald erste offizielle Verwendung von „Cyberwaffen“
- Reiner „Cyberkrieg“ sehr unwahrscheinlich

Quellen

- „Ein großräumiger und langandauernder Stromausfall: eine nationale Katastrophe“ TAB-Studie 2011: http://www.tab-beim-bundestag.de/de/aktuelles/20110512.html
- Publikationen zum Thema Schutz Kritischer Infrastrukturen des BASB (Schweiz) http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.html
- Datenbank der „Cyberwar“-Vorfälle und News: http://cyber-peace.org
- Glossar zu PRISM & Co.: http://goo.gl/oislVL
- Kryptographie Blog Bruce Schneier: www.schneier.com/blog
- „The NSA-Files“: http://www.theguardian.com/world/the-nsa-files
- Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg http://ifsh.de
- Cyber-Sicherheitsstrategie für Deutschland (BMI) http://goo.gl/o2YIWZ
- Internetplattform zum Schutz Kritischer Infrastrukturen http://www.kritis.bund.de/ und die dort verlinkte KRITIS-Strategie für Deutschland

Anhang: Abhängigkeiten der KRITIS von ICT

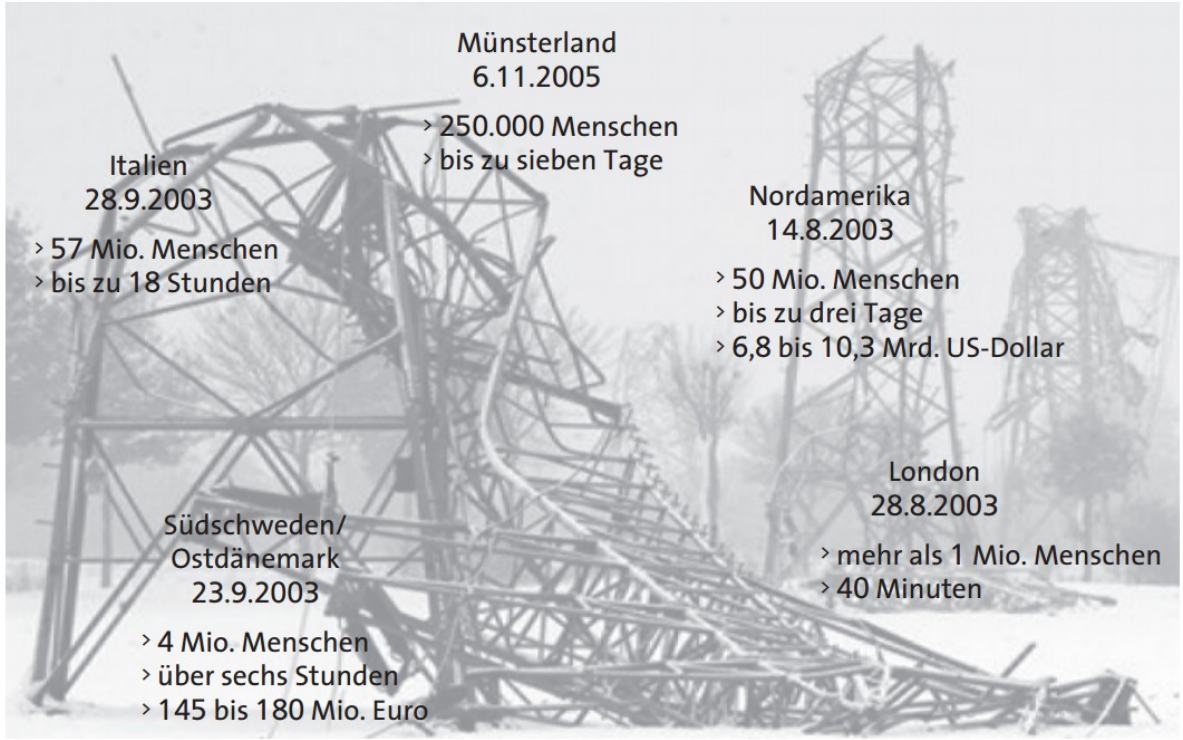
Sektoren	Teilsektoren
Behörden	Parlament, Regierung, Justiz, Verwaltung
	Forschungseinrichtungen
	Nationale Kulturgüter
	Ausländische Vertretungen und Sitze internationaler Organisationen
Chemische Industrie	Produktion, Transport, Lagerung und Verarbeitung chemischer Stoffe
Energie	Stromversorgung
	Erdölversorgung
	Erdgasversorgung
Entsorgung	Abwasser
	Industrie- und Hausabfälle
	Kontrollpflichtige Abfälle
Finanzen	Banken
	Versicherungen
Gesundheit	Ärztliche Betreuung und Spitäler
	Arzneimittel
	Labors
Informations- und Kommunikationstechnologien (IKT)	Telekommunikation
	Informationssysteme und -netze
	Internet
	Instrumentations-, Automations- und Überwachungssysteme
	Rundfunk und Medien
Nahrung	Versorgung mit Lebensmitteln und Gewährleistung der Lebensmittelsicherheit
	Trinkwasserversorgung
Öffentliche Sicherheit, Rettungs- und Notfallwesen	Blaulichtorganisationen (Polizei, Feuerwehr, sanitätsdienstliches Rettungswesen)
	Zivilschutz
	Armee
Verkehr	Strassenverkehr
	Schienenverkehr
	Luftverkehr
	Schifffahrt
	Postwesen und Logistik



- Smart Grid
- Gesundheitskarte
- TOLLCollect
- AIS
- Offshore-Fernsteuerung
- Luftleitsysteme
- ...

Anhang: Beispiele großer Stromausfälle

ABB. 2 BEISPIELE FÜR GROSSE STROMAUSFÄLLE



Quelle: eigene Darstellung

14. - 22. August 2003 Norden USA/Kanada

Wartungsfehler der Netze, verbunden mit Marktaufsplittung und Deregulierung

62 GW elektrische Leistung sowie
50 Mio. Personen betroffen

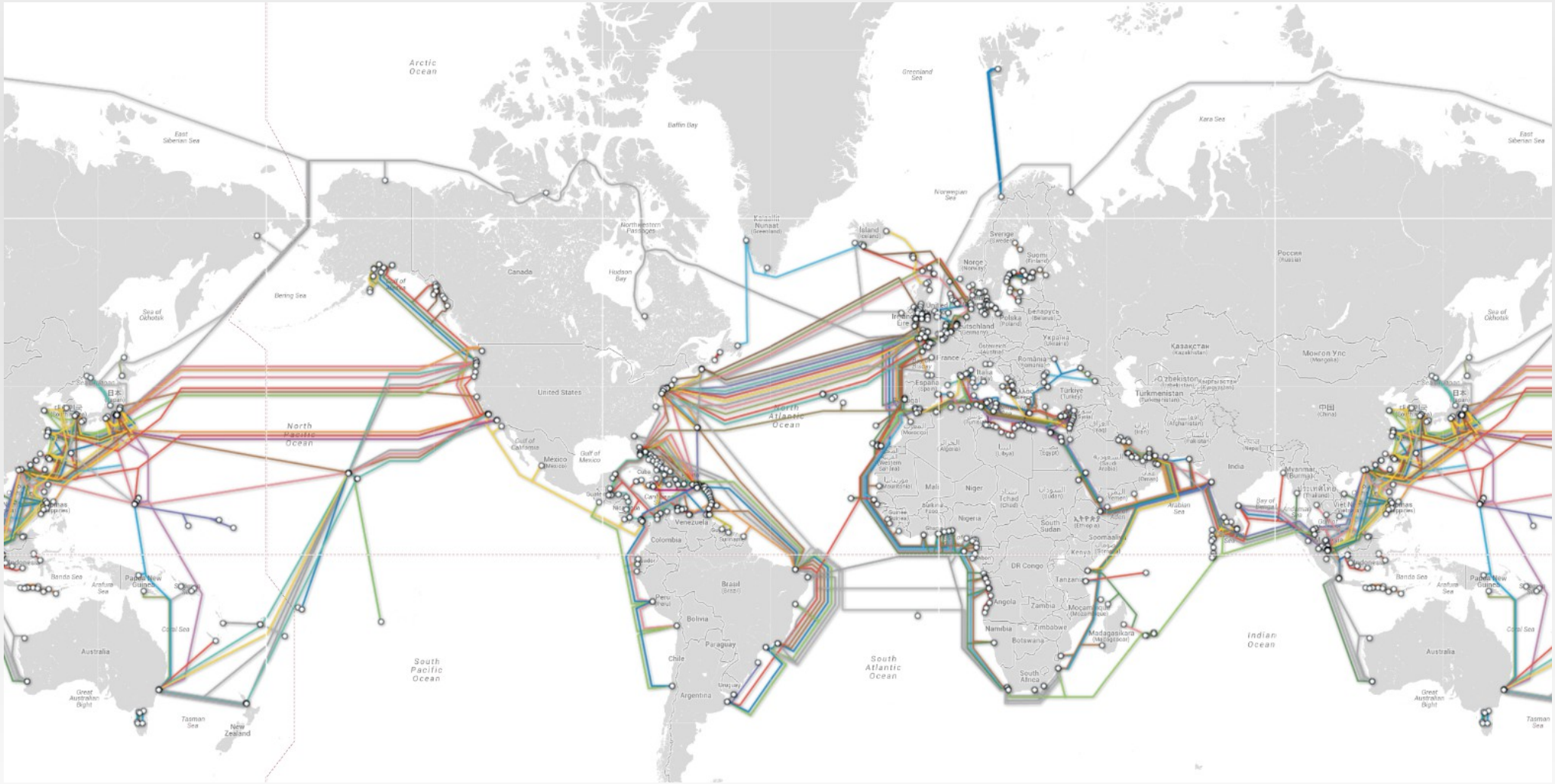
Telefonfestnetz mit Notstrom-Generatoren stabilisiert

IT-Netzwerke Ausfall von 4h (2000 St.) bis 2 Tage, Backbones stabil

Schaden für Wirtschaft Ontarios
~ 1 bis 2 Mrd. Kanadische Dollar

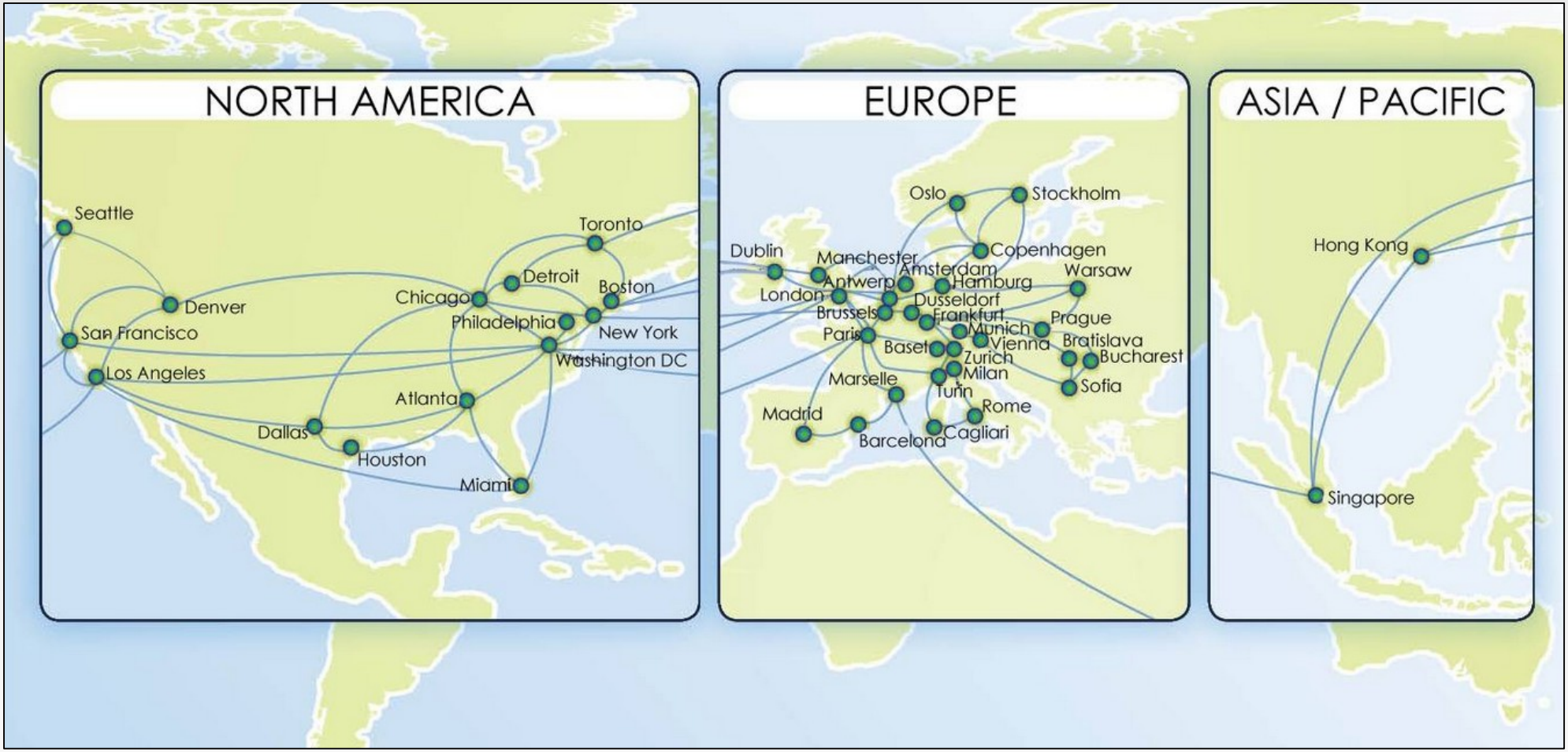
25. November 2005 Münsterland
Heftige Schneefälle, eingeknickte Strommasten und gerissene Hochspannungsleitungen
Ortschaften bis zu 5 Tage komplett ohne Strom, Schaden etwa 100 Millionen Euro

Anhang: Weltweite Untersee-Glasfaser-Backbones



http://www.submarinecablemap.com

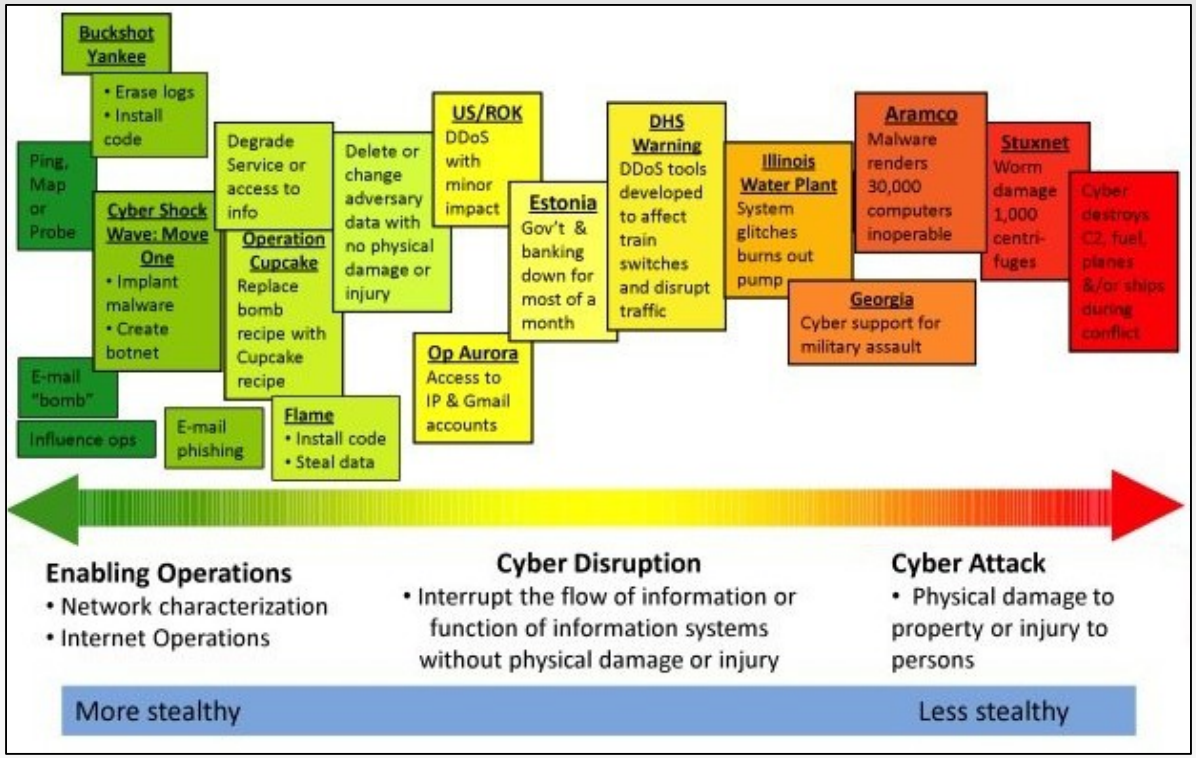
Anhang: Internet-Exchange-Points 2010



http://www.jaymiescotto.com

Anhang: Klassifikation von Cybervorfällen

- Kontinuums-Klassifikation
  - Gary D. Brown & Owen W. Tullos
  - (a) Access/Enabling Operations
  - (b) Cyber Disruption
  - (c) Cyber Attack



Anhang: Aufwand einer militärischen Cyberoperation

- Anforderungen für einen erfolgreiche Cyberattacke
  - Sehr klares und genaues Missionsziel und nötige Befugnisse
  - Spezifische Zielinformationen, i.a.R. Vorfeldaufklärung nötig
  - Unbekannte Sicherheitslücken (Zero day exploits)
  - Hochgradig professionelles Entwicklungs/Test/Angriffs-Team
  - Beständigkeit des Angriffes in Qualität und Dauer
- Zeitpunkt des 1. Angriffs → Vorteil wandert zum Verteidiger
- ~ Lebensspanne einer entdeckten Lücke: 500 Stunden
- Entwicklungsaufwand eines militärischen Angriffs: ca. 2 bis 5 Jahre

Anhang: APT – Advanced persistant threat

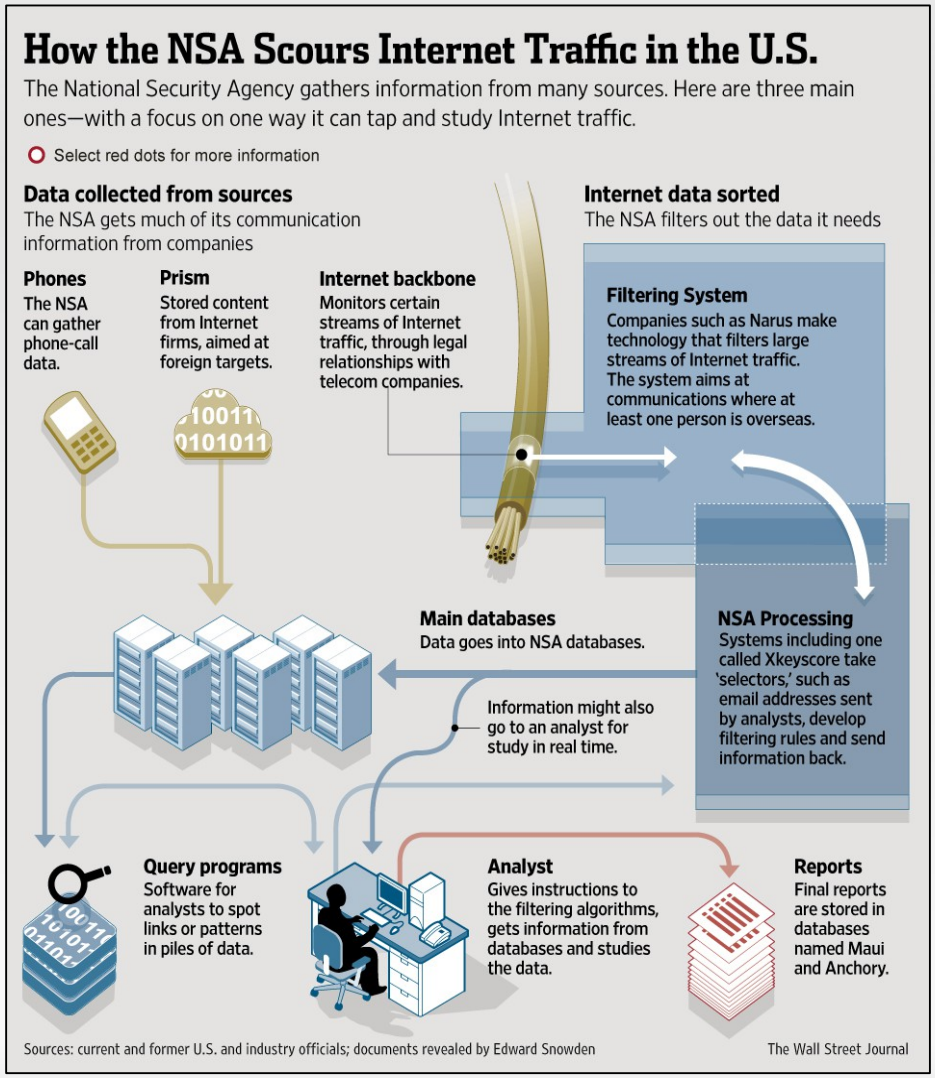
- Begriff für komplexen, zielgerichteten längeren Angriff auf kritische IT-Infrastrukturen und kritische vertrauliche Daten
  - **Advanced** (deutsch: fortgeschritten) Abgrenzung zu herkömmlichen Angriffen mit Schadsoftware auf unbestimmte, nicht spezifische Opferzahlen. Ein APT hingegen erfolgt auf selektierte Opfer, Personen mit erweiterter Technik
  - **Persistent** (deutsch: andauernd) Abgrenzung zu herkömmlichen Angriffen mit Beschränkung auf einschleusen der Schadsoftware auf nur einen Rechner. APT hingegen nutz den ersten infizierten Rechner nur als Sprungbrett in das lokale Netz der betroffenen IT Struktur bis das Hauptziel
- Beispiele
  - Stuxnet (2005 – 2010; Iranische Atomanlage
  - Operation Aurora (2009-2010; Google, Adobe Systems, Yahoo und Symantec)
  - Shady RAT (2006-2011; mehrheitlich US-Behörden, Unternehmen, UN, IOC)

Anhang: NSA Programme - Erfassen

- PRISM & Upstream
  - Bezahlte Dienstleistung für den Direktzugriff auf Daten von Google, Microsoft, Apple, Yahoo, Youtube, Facebook, AOL, Skype und Paltalk
  - Kooperationen mit großen Traffic-Carriern (Level 3, Verizon, AT&T)
- Tailored Access Operations
  - 600 Personen-Hacker-Einheit inkl. „Field-Unit“ für Vor-Ort-Zugriff
  - > 60.000 Zugriffe weltweit (viele chinesische Systeme, DE-CIX)
- Bullrun
  - Schwächung und Knacken von Kryptographie-Systemen
- Tempora (UK Government Communications HQ)
  - Abhören und Mitschneiden von Datenübertragungen (Atlantik, naher Osten)

Anhang: NSA Programme - Auswerten

- Xkeyscore
  - Analyse-Tool für Zugriff auf Datenbestände
  - Zusammenführung von Daten
  - Zugriff auf *„fast alles, was ein typischer Nutzer im Internet macht“*
  - z.T. auch vom BND genutzt
- Boundless Informant
  - Frontend für Überblick über Datenbestände und Überwachungsmaßnahmen



Anhang: NSA Programme - Speichern

- NSA-eigene Rechenzentren
  - Utah, Vollbetrieb Ende 2013
  - Fort Meade, Washington, Vollbetrieb 2015
- Datenaufkommen
  - Weltweit 1.826 Petabyte pro Tag (1.826.000 TB)
  - 29 Petabyte täglich durch NSA „touched“
  - 0.007 PB (7TB) täglich ausgewertet == 270 Mio. Seiten Fließtext
- Speicherung von Inhalten, Verbindungs- und Meta-Daten
  - Einige Tage bis teilweise mehrere Jahre
  - EvilOlive und ShellTrumpet, Stellar Wind
- Zusätzliche weitere, primär militärische Datenquellen