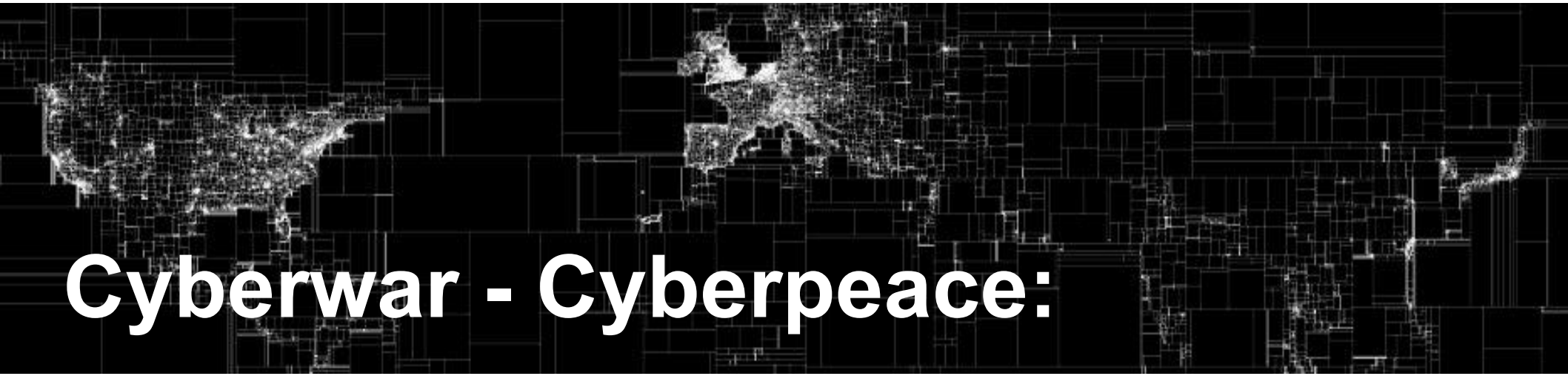


Cyberwar - Cyberpeace:

Die Bundeswehr zieht ins Cyberfeld

Thomas Reinhold – reinhold@ifsh.de – cyber-peace.org

Das IFSH
Ein Blick zurück
Alte Konzept, neue Probleme
Stand der Dinge und Akteure
Politische, technische und gesellschaftliche Lösungsansätze
Stuxnet und Co.

Das IFSH

Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg
Wurzeln in nuklearer Abrüstung
Sicherheitspolitische und naturwissenschaftliche Arbeitsbereiche
Wissenschaftliche Forschung und Politikberatung

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

ifsh.de

Das IFSH /2

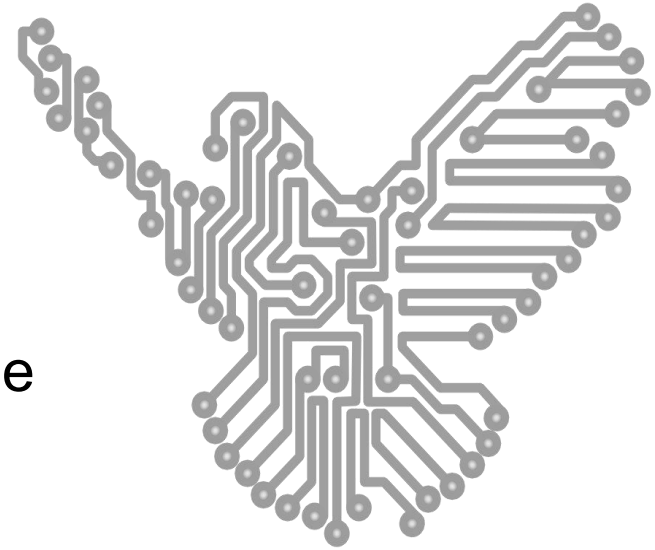
Mitarbeiter Arbeitsgruppe IFAR²

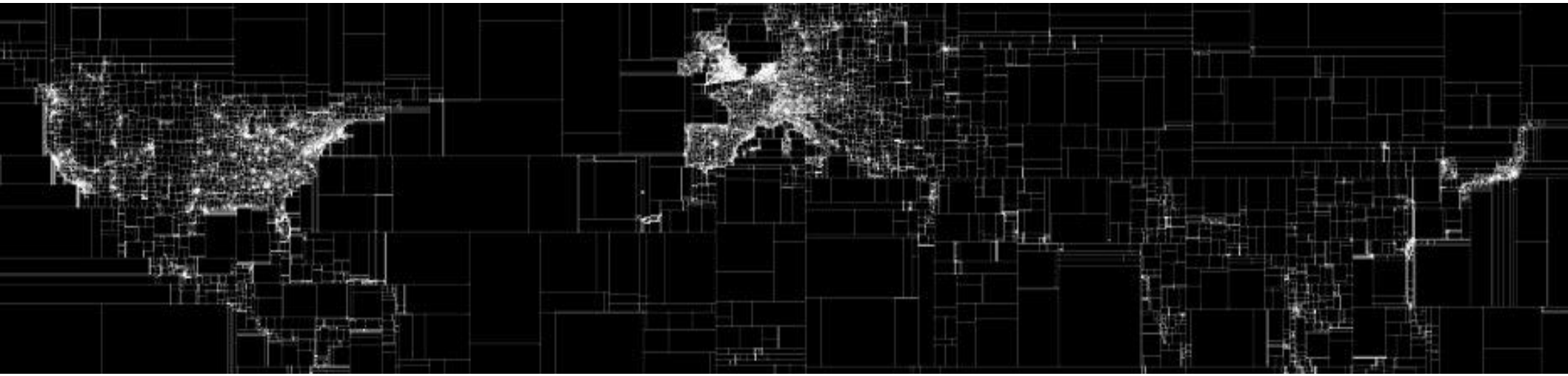
“Interdisziplinäre Forschungsgruppe Abrüstung, Rüstungskontrolle und Risikotechnologien”

Dipl. Informatiker, Künstliche Intelligenz und Psychologie

Datenbank/Blog cyber-peace.org

2015: Campaigner der Cyberpeace-Kampagne des FIfF e.V. *





Ein Blick zurück

Stuxnet

Stuxnet 2010

Politisches Nachspiel

- Was kommt als nächstes
- Gibt es Cyberwaffen
- Eigene Verwundbarkeit
- Konsequenzen für die internationale Sicherheit

Urheber: Israel und USA*

Belastung zwischen-staatlicher Beziehungen

* New York Times, 1.6.2012 „Obama Order Sped Up Wave of Cyberattacks Against Iran“

Was seit damals geschah

UN-Bericht zur Militarisierung des
Cyberspace (UNIDIR* / CSIS*)
47 Staaten mit militärischen Programmen

Tallinn Manual zur Anwendung
des Völkerrechts im Cyberspace

* UNIDIR - United Nations Institute for Disarmament Research
* CSIS - Center for Strategic and International Studies

Was seit damals geschah

UN-Bericht zur Militarisierung des Cyberspace (UNIDIR* / CSIS*)
47 Staaten mit militärischen Programmen

Tallinn Manual zur Anwendung des Völkerrechts im Cyberspace

Veröffentlichungen von E. Snowden zu den FIVE-Eyes und ihren Ressourcen

Obamas Presidential Policy Directive PPD 20/2012

* UNIDIR - United Nations Institute for Disarmament Research
* CSIS - Center for Strategic and International Studies

Erkenntnisse gewonnen aber
auch neue Probleme aufgeworfen

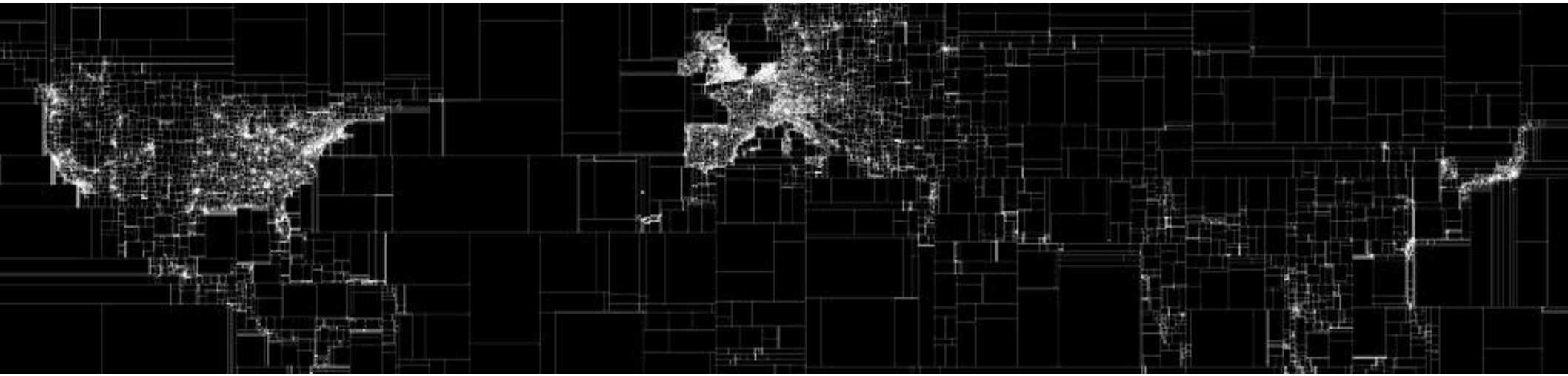
?

- Offensive invasive Schadsoftware (“Cyberwaffen”)
- Cyberspace als zusätzliche militärische Domäne
- Eigene Verwundbarkeiten
- Konsequenzen für die internationale Sicherheit

Erkenntnisse gewonnen aber auch neue Probleme aufgeworfen

?

- Offensive invasive Schadsoftware (“Cyberwaffen”)
- Cyberspace als zusätzliche militärische Domäne
- Eigene Verwundbarkeiten
- Konsequenzen für die internationale Sicherheit



Alte Konzepte – Neue Probleme

Cybercrime vs. Cyberwar

Cybercrime

→ Fragen nach Regelungen der internat. Strafverfolgung

Cyberwar

→ Fragen nach den politischen Motivationen der Akteure

→ Fragen nach der Bewertung von Vorfällen

Zentrales Problem:

Welches Ausmaß einer Beeinträchtigung durch externe Cyberzugriffe entspricht einer Bedrohung des Staates ?

Völkerrecht & Cyberspace

Was ist der "Cyberspace" und was bedeutet "Cybersicherheit"

- Informationssicherheit (Proposal Russland/China an die UN 2013)
- IT-Security (USA/Europa)

Was ist eine "Cyberwaffe"

- Einordnen in ein Schadens-Spektrum
  - “Schwelle” bei Schädigung von Objekten oder Personen
- Kontext-Ansatz:
  - Anwendungs-Kontext
  - vermeintlicher Zweck
  - Beabsichtigter Schaden

Anwendbarkeit etablierter Normen des Völkerrechts ?

Völkerrecht & Cyberspace /2

Das Recht zum Krieg (ius ad bellum)

UN Charta Art. 2 (4) → Gewaltverzicht („use of force”)

UN Charta Art. 51 → Recht zur Selbstverteidigung

Das Recht im Krieg (ius in bello)

Genfer Konventionen

Prinzip der Proportionalität

„Tallinn Manual“

NATO Exzellenz-Zentrum CCDCOE in Tallinn

Nicht-bindende Analyse von Völkerrechtlern, Militärwissenschaftlern und militärischen Mitarbeiten

Analogien zu “kinetischen Wirkmitteln”

Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force

Rüstungskontrolle und Non-Proliferation ...

- Ausbreitung militärischer Rüstungsgüter / kritischer Bestandteile
  - regulieren
  - kontrollieren
  - unterbinden
- Wassenaar-Abkommen
  - 1996: Abkommen zur Exportkontrolle von konventionellen Waffen
  - und doppelverwendungsfähigen Güter und Technologien (“Dual use”)
  - Ergänzung von 2013 um "intrusion software"
  - Konkrete Umsetzung liegt im Ermessen des einzelnen Mitgliedstaates

... Schwierigkeiten dabei ...

- Spezifische technische Eigenschaften
  - Virtualität & Immaterialität der Güter
  - Problem der Quantifizierbarkeit oder “wie zählt man Malware”
  - Dual-Use-Problematik
  - Fehlende Verifikationsmöglichkeiten
- Abgrenzung von Offensive und Defensive
- Attribution im Cyberspace
  - Maßgebliche Voraussetzung für Selbstverteidung UN Charta Art. 51
- Territoriale Souveränität und Grenzen im Cyberspace

… und weitere Probleme

Verbindungen Geheimdienste und Militär

- NSA-Direktor auch Direktor des US Cyber Command mit explizit offensiver Ausrichtung und weiterer militärischer Einrichtungen

Cyberattacken nichtstaatlicher Akteure

Internet Governance

- Selbstregulation vs. Steuerung durch internationale Gremien (ITU*)
- Weiterentwicklung und Standarisierung technischer Konzepte (IETF**)

Freiheit vs. Kontrolle

Zivilschutz und Verantwortlichkeiten

Individual- und Selbstdatenschutz

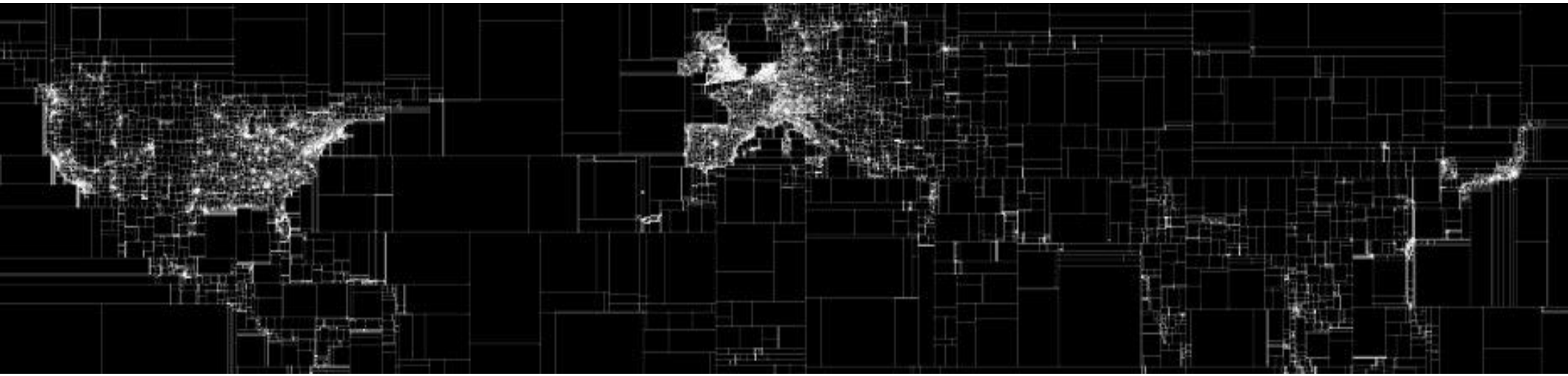
…

* ITU – International telecommunications union
** IETF – Internet engineering task force

Erkenntnisse gewonnen aber auch neue Probleme aufgeworfen

?

- Offensive invasive Schadsoftware (“Cyberwaffen”)
- Cyberspace als zusätzliche militärische Domäne
- Eigene Verwundbarkeiten
- Konsequenzen für die internationale Sicherheit



Stand der Dinge und Akteure

Aktuelle internationale Situation

UN Institute for Disarmament Research „The Cyber Index - International Security Trends and Realities“, 2013

- 47 Staaten mit militärischen Cyberdoktrinen
- 10 Staaten mit explizit offensiven Programmen

USA: aktuelle „Strategie für den Cyberspace” des DoD

- Abschreckung durch Aufbau von wirksamen Mitteln für IT-Gegenschläge
- Verteidigung auch mit konventionellen Mitteln bei Cyberattacken
- *The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack” (..) “We obviously have a capability to do that, not just in cyber but in other ways”*
- (U.S. Defense Secretary Ash Carter)
- Cyber integraler Bestandteil aller “Combat missions”
- Cyberkampf gegen IS

Aktuelle internationale Situation /2

Russland

„The task of equipping the armed forces and other troops includes the development of the forces and means of information warfare, and the creation of new types of precision weapons and the development of their information security"

Aufbau einer Cyber-Einheit für die Verteidigung russischer IT-Systeme bis 2017

China

APT1 / Militäreinheit 61398 in Beijing (Madiant-Bericht)

seit 2006 141 Einbrüche in rund 20 existentielle Industrien, Infrastrukturen (Stromversorgung, RSA) und große US-amerikanische Unternehmen

„We estimate that Unit 61398 is staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure"

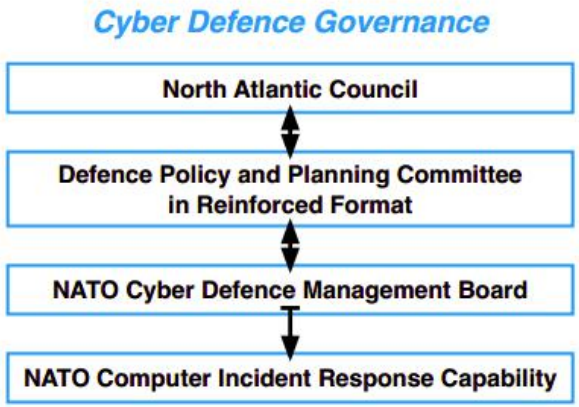
Aktuelle internationale Situation /3

NATO

2013: Cyberwar ständiger Tagesordnungspunkt und Teil der Verteidigungsplanung

2016:

- Cyber Bestandteil der kollektiven Verteidigung
- Cyber-Attacken können Art. 5 auslösen
- Ausbau der militärischen Cyber-Ressourcen



Deutschland

Kommando Strategische Aufklärung mit Computer Networks Operations-Einheit (seit 2006) mit 60-75 Personen

April 2017: Aufbau eigener Bereich neben Marine, Luftwaffe & Heer

- 13.700 Dienstposten (Großteil umverteilt)

BMVg: Eigene Abteilung für Cyberfragen

Fragwürdige Rechtsgrundlage für offensive Operationen

Erster inoffizieller Einsatz der CNO Einheit im Herbst 2015

Aktuelle internationale Situation /4

Wirtschaftliche Akteure

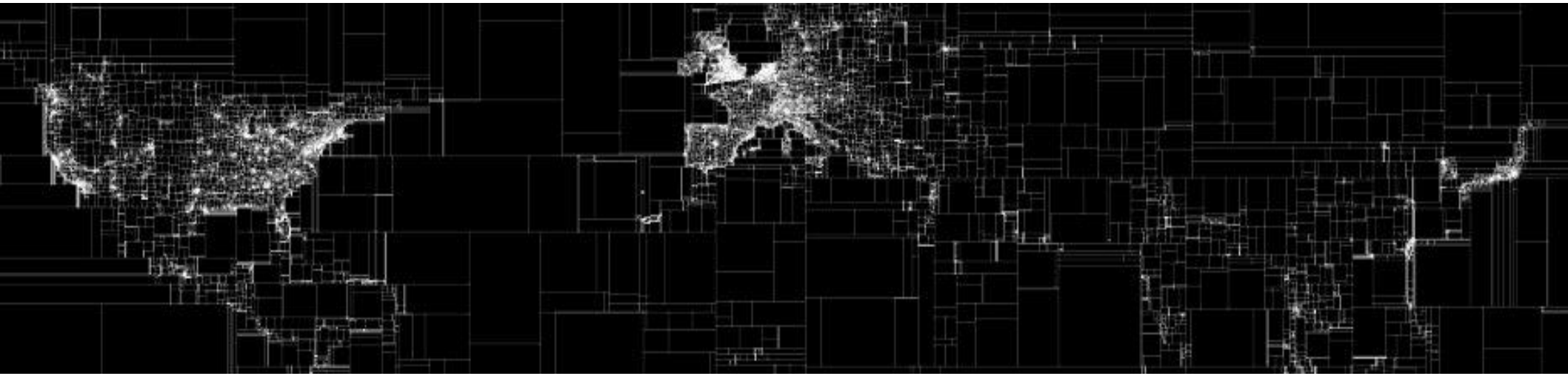
- BWI (IT-Dienstleister der Bundeswehr), seit 2016 100% InHouse des Bundes
  - Siemens
  - IBM
- Sponsoren der PITS 2016 - Deutschlands größter Kongress mit begleitender Ausstellung für IT-Sicherheit bei Behörden

Platinsponsor

Goldsponsoren

Silbersponsoren

Bronzesponsoren



Politische, technische und gesellschaftliche Lösungsansätze

! Es geht um die **Erwartung** und **Bewertung** des Handelns von Staaten durch Staaten und um gemeinsame **Regeln**

! Es geht um die **Erwartung** und **Bewertung** des Handelns von Staaten durch Staaten und um gemeinsame **Regeln**

Vertrauensbildende Maßnahmen

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
- Eingrenzung der eigenen Möglichkeiten, in Krisensituationen Druck durch militärische Aktivitäten auszuüben
- Kommunikation in Krisenzeiten verbessern
- Transparenz über Aufgaben, Stärke und Doktrinen der Streitkräfte herstellen

* KSZE - Konferenz über Sicherheit und Zusammenarbeit in Europa

Vertrauensbildende Maßnahmen /2

Maßnahmen

Seminare zu Doktrinen, Informationsaustausch, Etablierung von Kommunikationskanälen, Konferenzen über thematische Fragen

Defensive Orientierung von Streitkräften, Verzicht auf den „First use“

Demilitarisierte Zonen & gemeinsame militärische Übungen

Monitoring als Signal der Verbindlichkeit & Verifikationsmöglichkeit

Bilaterale Vereinbarungen bis zu internationalen Abkommen

Measures	Elements	Applicable for Cyber Space?
Geographical	• Demilitarized Zones • Thin-out Zones	• Not possible
Structural	• Defensive Orientation of Armed Forces	• Accept defense but prohibit offense?
Operational	• Limits on Maneuvers and Exercises	• Prohibit offensive military exercisies
Declaratory	• No first Use	• Unilateral declarations
Verification	• Air- or space-based sensors	• unlikely

*Neuneck, G, "Confidence Building Measures - Application to the Cyber Domain", Lecture, 2012

Ansätze für den Cyberspace – Politik

Politische Ansätze

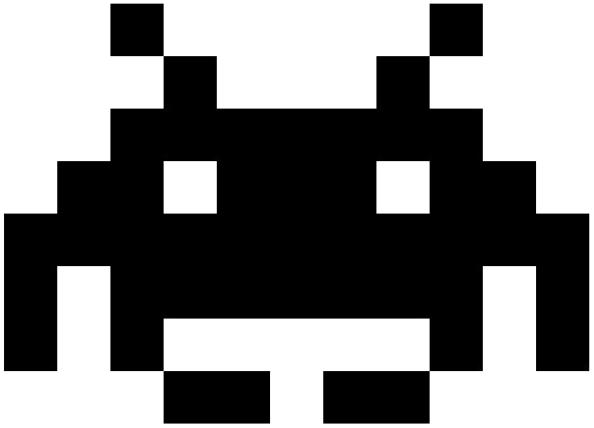
- Verständigung auf gemeinsame Terminologie und Definitionen
  - Cyberspace
  - Cyberwaffen & Cyberattacken und die angemessene Verteidigung
  - Kombattanten
  - Cybersecurity …
- Gemeinsame Arbeitsgruppen
  - USA-Russland im Rahmen der Nuclear Risk Reduction Center (NRRC)
  - USA-China Expertengruppe zu Wirtschaftsspionage
  - China-Russland Cyber-Abkommen
- Gemeinsame Krisenübungen
  - Cyber Europe '10/'12/'14 zwischen EU/USA
  - USA-China “Wargames” zu Cyberangriff 2012

* ENISA - European Union Agency for Network and Information Security

Ansätze für den Cyberspace – Politik /2

Politische Ansätze

- Meldepflichten für Unternehmen bei Cyberattacken
  - EU: Meldepflicht bei „kritischen Vorfällen signifikanter Größe” *
  - Deutschland: Cyber-Sicherheitsgesetz **
- Regulierung des Handels mit Schadsoftware
  - Wassenaar-Abkommens
- Transparenz und Monitoring bei Cyberwaffen
  - Export-Register (UN-COMTRADE***)
  - Höchstgrenzen für Schlüsseltechnologien
  - Inspektionen nach dem Vorbild der IAEA****

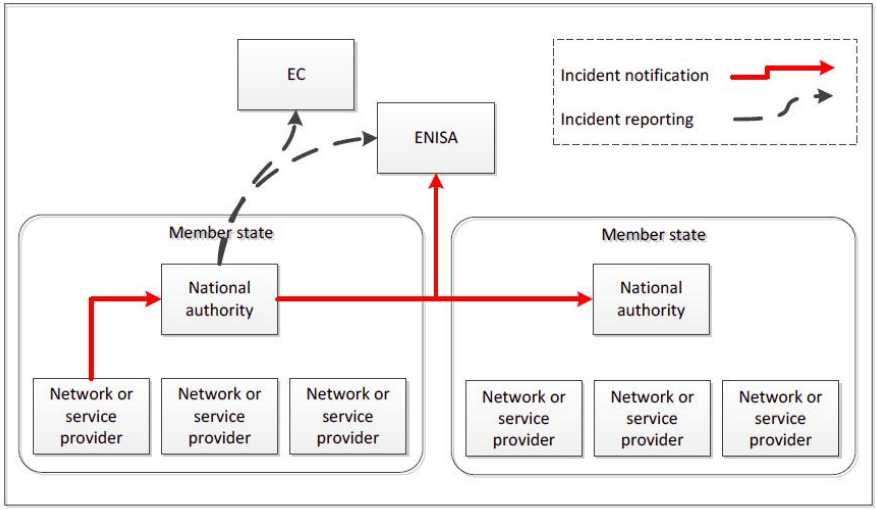


* http://www.europarl.europa.eu/committees/en/imco/all-announcements.html
** http://www.bmi.bund.de/DE/Nachrichten/Dossiers/ITSicherheit/itsicherheit_node.html
*** COMTRADE - United Nations Commodity Trade Statistics Database - comtrade.un.org
**** IAEA - International Atomic Energy Agency

Ansätze für den Cyberspace – Praxis

Praktische Ansätze

- Ausbau von CERTs*
- Nationale Melde- und Eskalationshierarchien
- Internationale Schnittstellen herstellen, bspw. ENISA** als EU-Dienstleister
- Austausch über bekannte Sicherheitslücken und Vorfälle



	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					

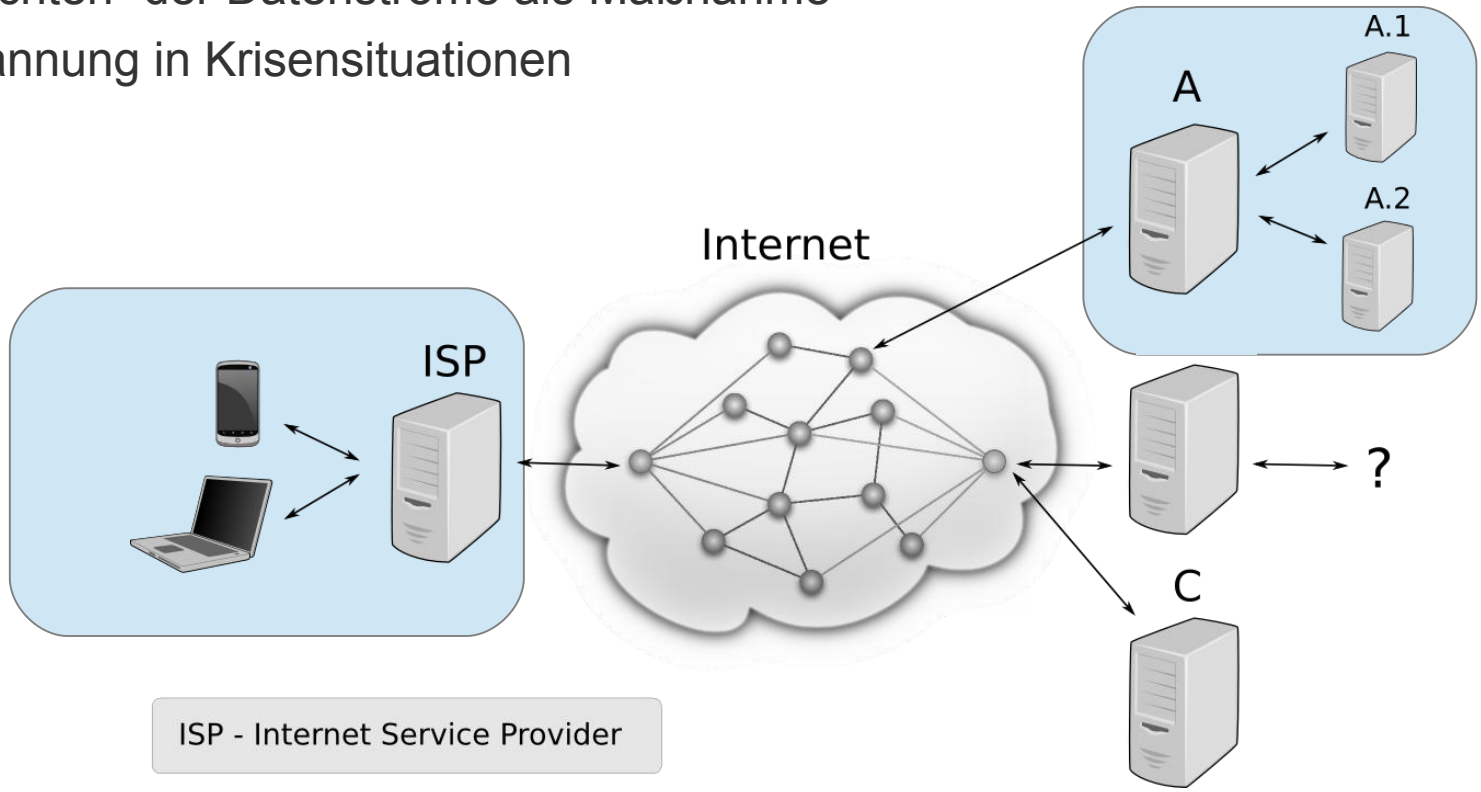
Table 1 Combination of thresholds

* CERT - Computer Emergency Response Team
** ENISA - European Union Agency for Network and Information Security - www.enisa.europa.eu
„Technical Guideline on Incident Reporting“ Oktober 2014

Ansätze für den Cyberspace – Praxis /2

Mögliche weitere praktische Ansätze

- Speicherung / Austausch / Sichtung von Verbindungsdaten
  - Unilaterale Selbstverpflichtung zur Transparenz
  - Überwachung der defensiven Orientierung von Cyberprogrammen
  - Rückverfolgung ungewöhnlicher Aktivitäten
  - “Durchleuchten” der Datenströme als Maßnahme für Entspannung in Krisensituationen



Ansätze für den Cyberspace – Zivilgesellschaft

FIfF e.V. Kampagne Cyberpeace

- Keine Militarisierung des Netzes
- Ächtung von Cyberwaffen

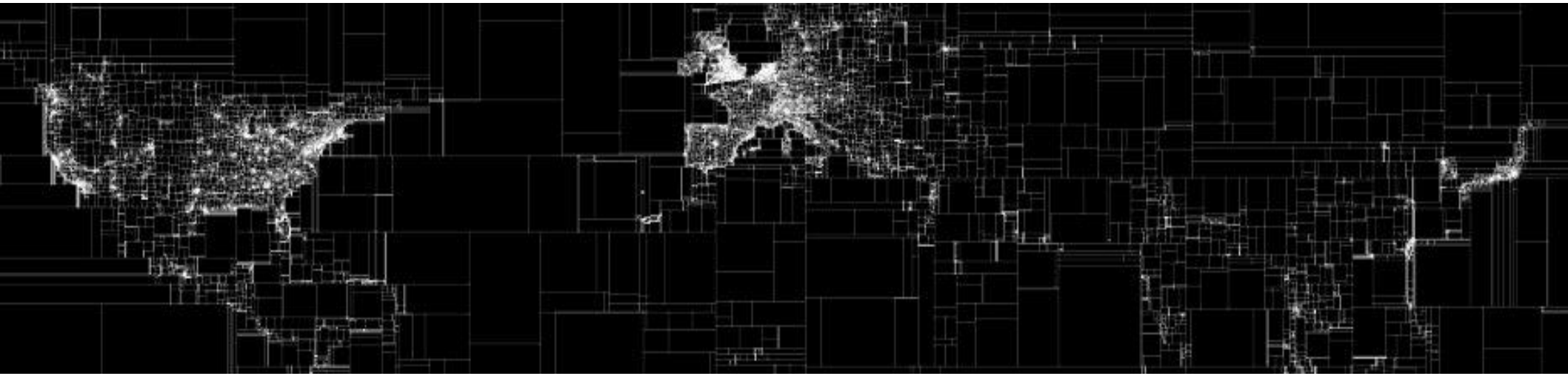
Chaos Computer Club

- Digitale Angriffe sind Streubomben, die große Teile des Internets betreffen" und ein hohes Risiko für weite Bereiche der Zivilbevölkerung darstellen*

ECO (Verband der Internet-Wirtschaft Deutschland)

- Vertrauen ins Netz stärken
- Staatliche Überwachung eingrenzen

https://netzpolitik.org/2015/im-cyber-raum-gibt-es-keine-uniform-bundesregierung-ignoriert-voelkerrechtliche-probleme-zum-cyber-krieg/



Stuxnet & Co.

Stuxnet – ein finaler Rückblick

„To Kill a Centrifuge“ - A Technical Analysis of What Stuxnet’s Creators Tried to Achieve, R. Langner, Nov. 2013

Zwei Sabotage-Versionen von Stuxnet

- Manipulation der Druckverhältnisse
- Manipulation der Zentrifugen-Rotation

„Stuxnet will not be remembered as a significant blow against the Iranian nuclear program. It will be remembered as the opening act of cyber warfare“

Der Sony-Hack

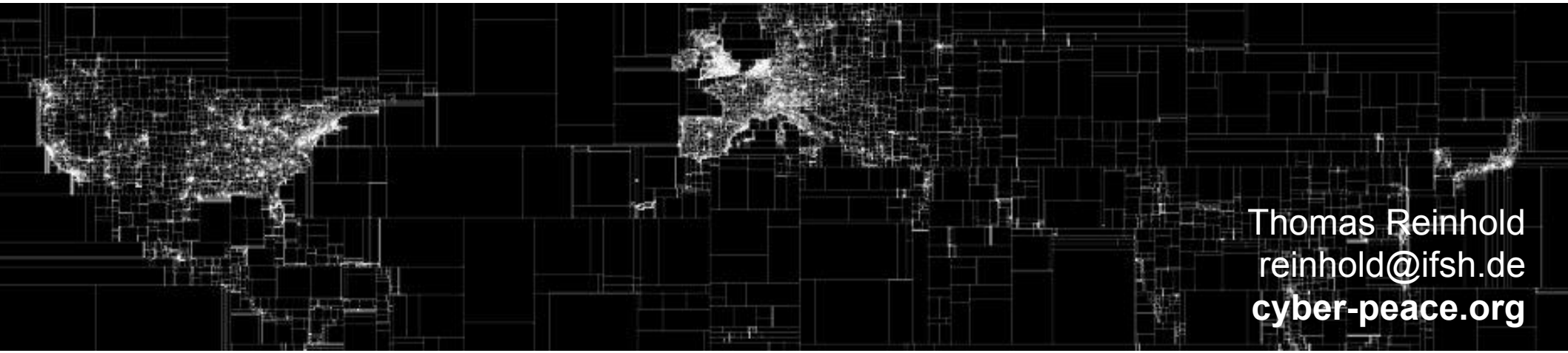
- Sony Pictures Entertainment (SPE) in den USA gehackt
  - Datendiebstahl (Zahlungsdaten, Namen, Adress- und Versicherungsangaben sowie Finanzinformationen von Angestellten und Partnern, private Krypto-Schlüssel)
  - Angeblich 300 Server und 800 Arbeitsplatz-PC “destroyed”
- Herkunft lt. CIA/NSA: Nord-Korea
  - basierend auf IP-Adressen sowie “Erkenntnissen und Ähnlichkeiten zu früheren Vorkommnissen”, später auch lt. NSA-Erkenntnissen
  - *“In general, it’s a situation that rapidly devolves into storytelling, where analysts pick bits and pieces of the “evidence” to suit the narrative they already have worked out in their heads”* (Bruce Schneier)
- Unmittelbare politische Sanktionen durch US-Handelskammer

Der Bundestags-Hack

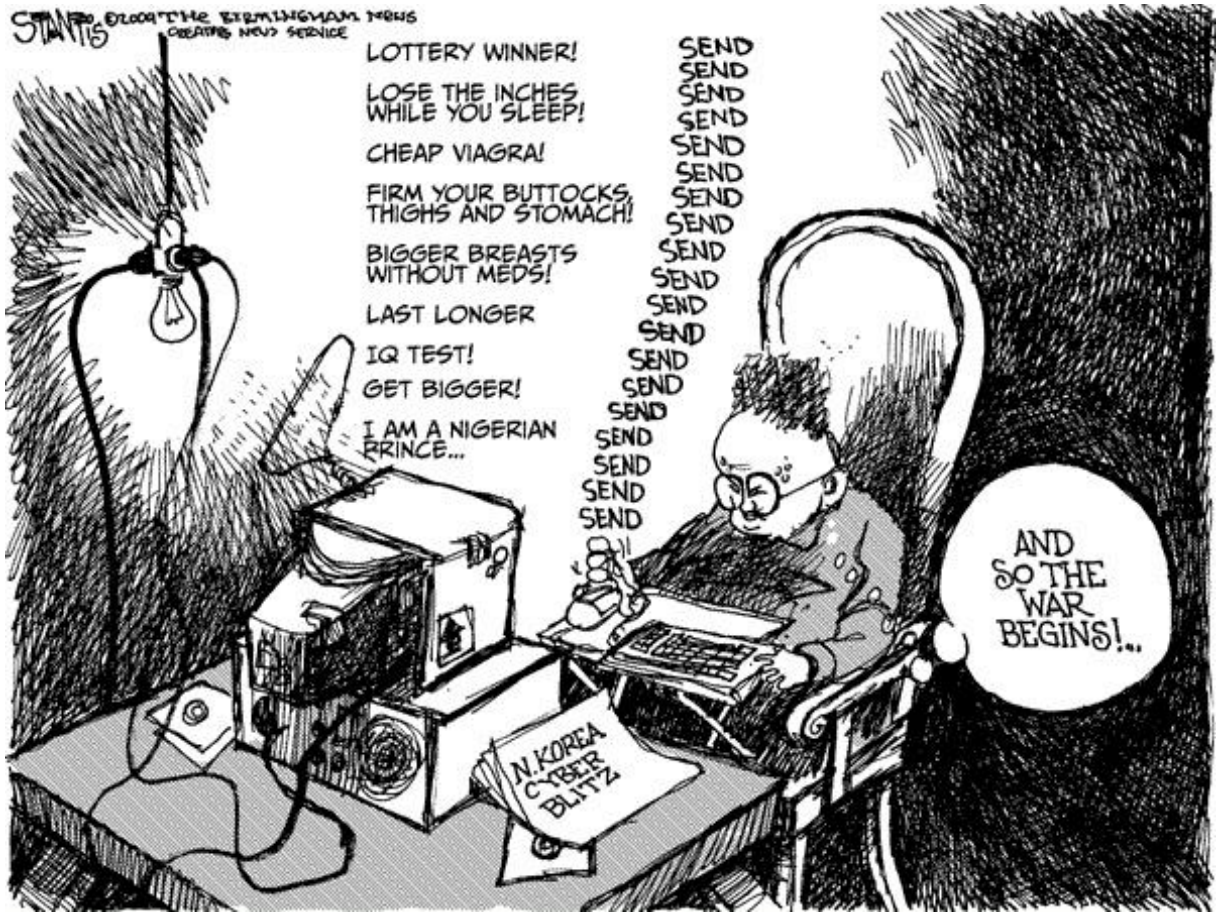
ParlaKom-Hack

- Mai 2015 entdeckt
- Datenabfluß bis mindestens Juni 2015
- Infektion des internen Kommunikationssystem aller Parlaments-Abgeordneten, ihrer Regionalbüros und Mitarbeiter
- E-Mails, Terminkalender-Daten und weitere Kommunikationsinformationen
- Reperatur erst mit kompletter Shutdown während der Sommerpause
- Russische Gruppe APT28 in Verdacht (Gutachten "Die LINKE")*, aber keine offizielle Bestätigung dafür

* "Untersuchungsbericht zu den Angriffen auf die IT der Fraktion DIE LINKE im Bundestag", Claudio Guarnieri



Thomas Reinhold
reinhold@ifsh.de
cyber-peace.org



Anhang: Fähigkeiten der NSA, eine Auswahl

Fähigkeiten der NSA (eine Auswahl)

- Zugriff auf wichtige Datenschnittstellen bei IT-Anbietern und IT-Infrastrukturen (PRISM, UPStream, Stormbrew)
- Zugriff auf wichtige Sicherheits-, Handels- und Telekommunikationsdaten (VISA, Swift, Fluggastdaten)
- Eigene parallele Server-Infrastrukturen im Internet-Backbone für Man-in-the-middle-Attacken und Packet-Injections (FOXACID, Quantum)
- Zugriff auf Glasfaserverbindungen (Tempora) und USS Jimmy Carter
- Automatische Suche nach unsicheren IT-Systemen und Infektion der Rechner (HACIENDA)
- Gezielte Schwächung von IT-Sicherheitsmechanismen (Kryptographie, GSM-Sicherheit)
- Hardware-Modifikation wichtiger weltweiter IT-Hersteller (ANT-Kataloge)

„We Kill People Based on Metadata"

Michael Hayden, ehemaliger Direktor der NSA und der CIA

Anhang: Weitere Cyber-Vorfälle

Belgacom-Hack

- Dienstleister u.a. für das europäische Parlament in Brüssel
- Spear-Phishing gegen Admins
- GCHQ (UK), Spionage

Regin

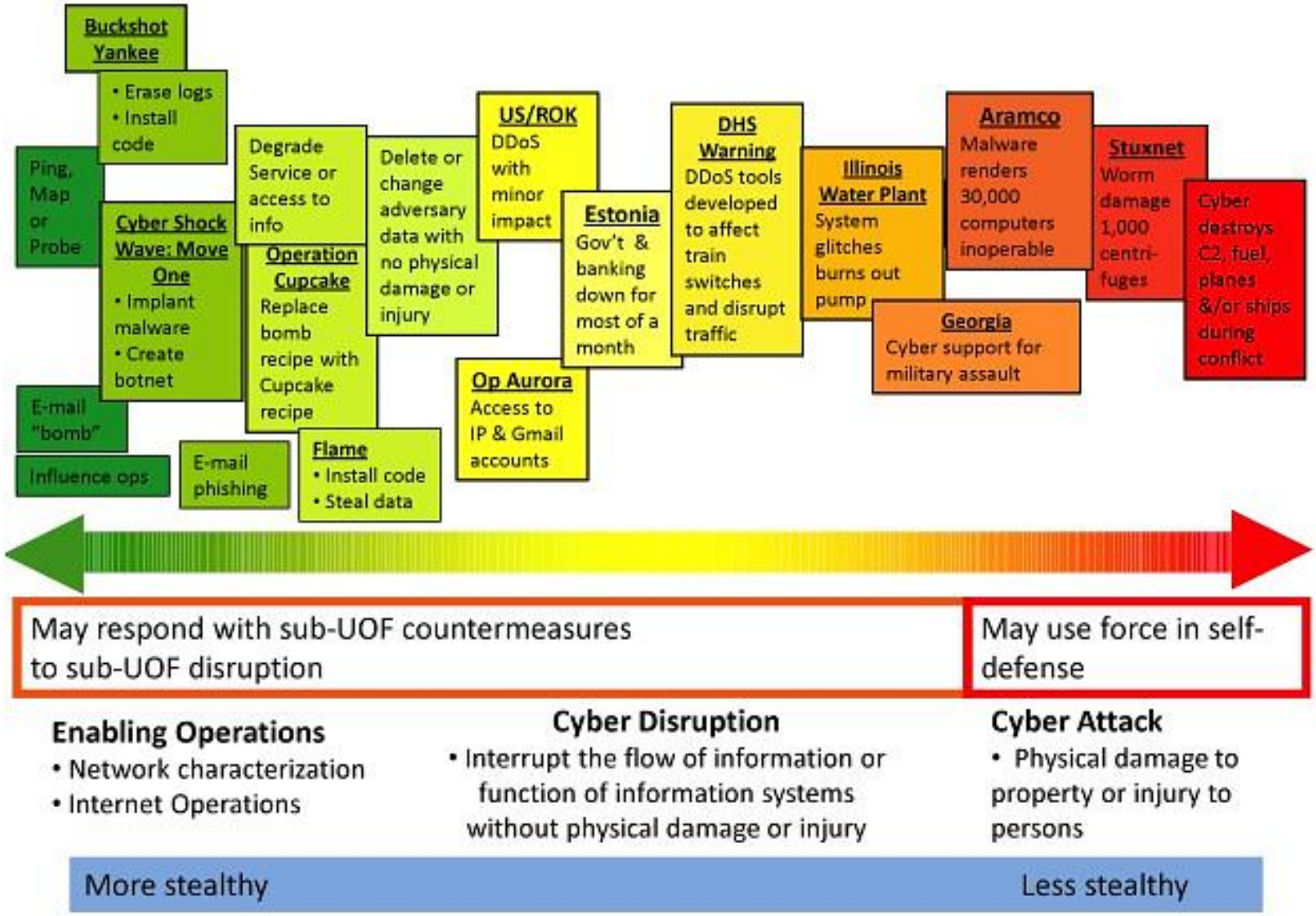
- Computersysteme größtenteils in Russland und Saudi-Arabien
- Unternehmen, staatliche Einrichtungen
- FIVE Eyes (NSA und Co.), Spionage

Uroburos/Turla/Snake

- Spionage, u.a. im Pentagon
- Infektionsvektor bisher unbekannt, Verbreitungsmechanismen sollten auch abgeschottete Systeme erreichen (P2P in lokalen Netzen)
- Russische Bezeichner im Quellcode

Anhang: Cyberwaffen nach Brown/Tullos

Kontinuums-Klassifikation nach Brown und Tullos



Anhang: Kritische Infrastrukturen

Verwundbarkeiten

Unmittelbare und mittelbare Bedrohungen

TAB-Studie 2011: fast keine systematischen Untersuchungen der einzelnen Bedrohungen und ihrer Auswirkungen*

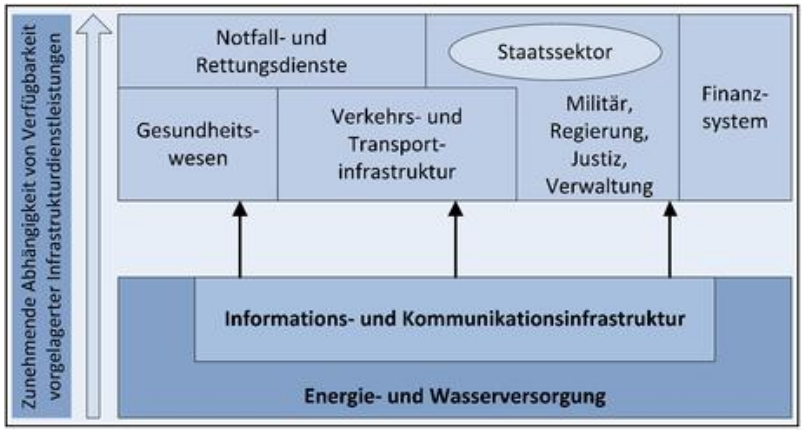
Virtualisierung und De-Zentralisierung von IT-Diensten, alte und bestehende Industrie-Steuerungsanlage (SCADA-Systeme)

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 Sektoren

Starke Abhängigkeiten



* „Ein großräumiger und langandauernder Stromausfall: eine nationale Katastrophe“ Büro für Technikfolgenabschätzung beim deutschen Bundestag (TAB) 2011

Anhang: Wassenaar-Abkommen

“Software” specially designed or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network capable device, and performing any of the following:

a) The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or

b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Anhang: C(S)BM für klassische Technologien

Etablierte Ansätze für bisherige waffenfähige Technologien

- Genehmigungspflichten, Staatshoheit über Produktion, Import und Export gefährlicher Güter
- Exporte/Importe an Partner oder öffentlich Datenbanken melden bspw. UN-COMTRADE*
- Beschränkung auf maximale Mengen bestimmter Güter/Schlüsseltechnologien
- Markierungen von Waffen für Rückverfolgbarkeit
- Sensorik bspw. für geheime unterirdische Atomwaffentests
- Möglichkeit der (unangekündigten) Inspektionen bspw. IAEA**

* COMTRADE - United Nations Commodity Trade Statistics Database - comtrade.un.org
** IAEA - International Atomic Energy Agency

Anhang: CSBM-Ansätze für den Cyberspace

Ideen für weitere technische Ansätze

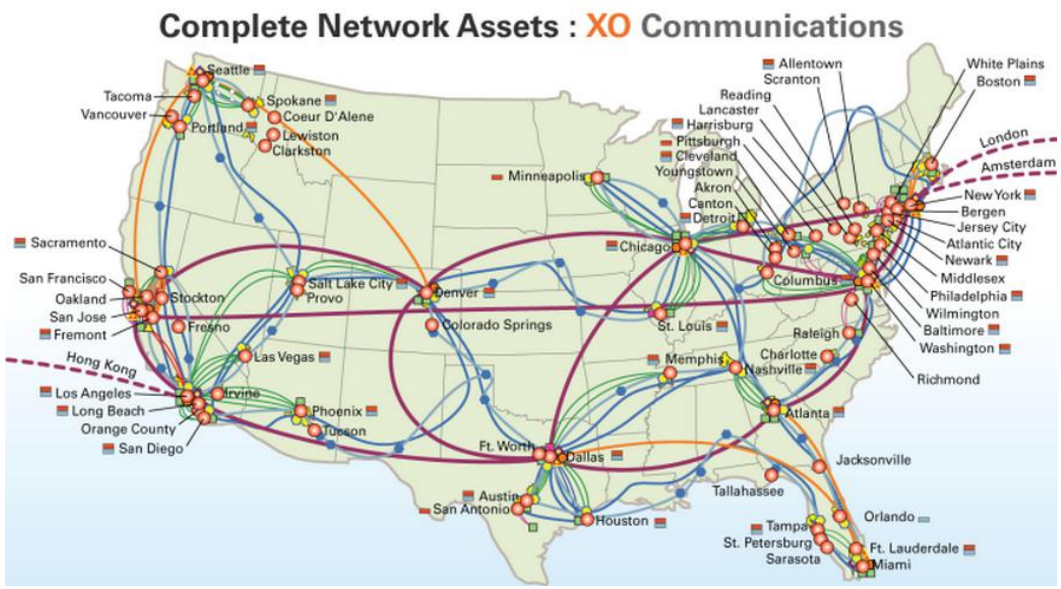
der Cyberspace als einzigartige “man made domain”

Grenzen im Cyberspace

> Staatliche Souveränität

> Verlässlichkeit für andere Staaten

> BGP – Border Gateway Protocol *



* http://de.wikipedia.org/wiki/Border_Gateway_Protocol

Anhang: CSBM-Ansätze für den Cyberspace /2

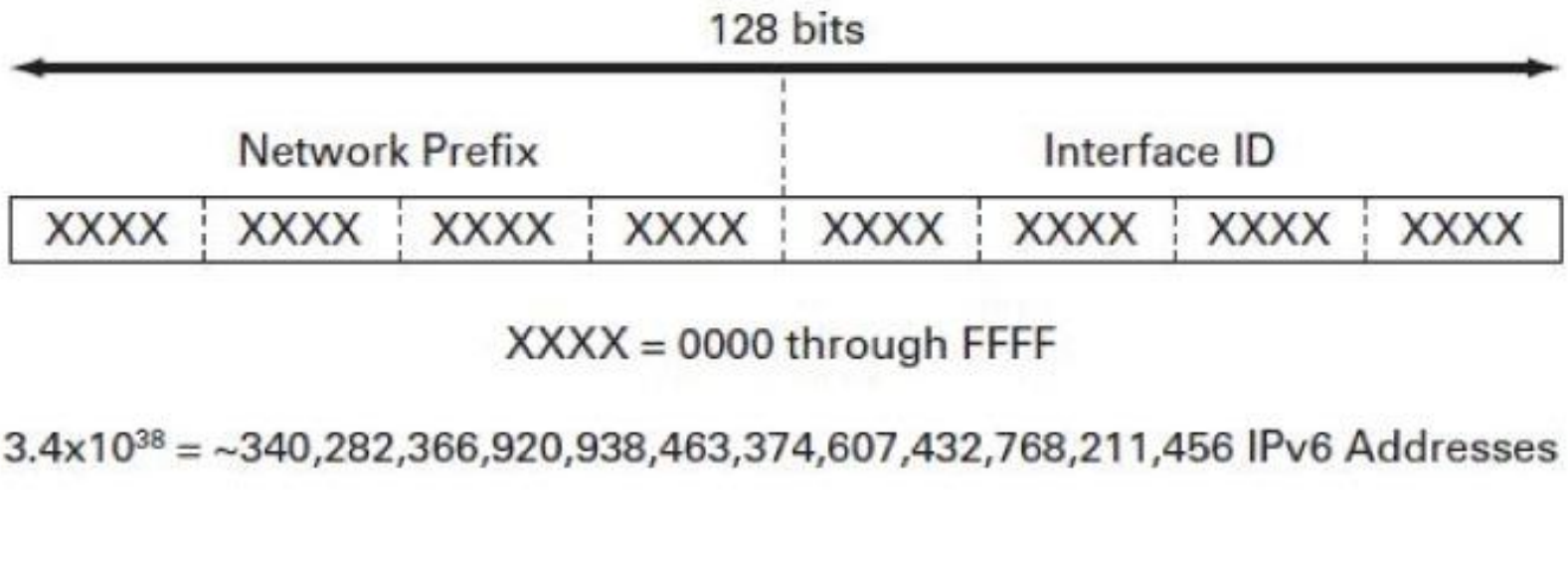
Ideen für weitere technische Ansätze

Eindeutige Identifizierbarkeit von sensiblen Systemen

> Markierung der Datenströme mit ihrem Herkunftssystemen

> Freiwillige Kennzeichen zur Reduktion irrtümlicher Annahmen

> IPv6 – Internet protocol version 6 *



* http://de.wikipedia.org/wiki/IPv6