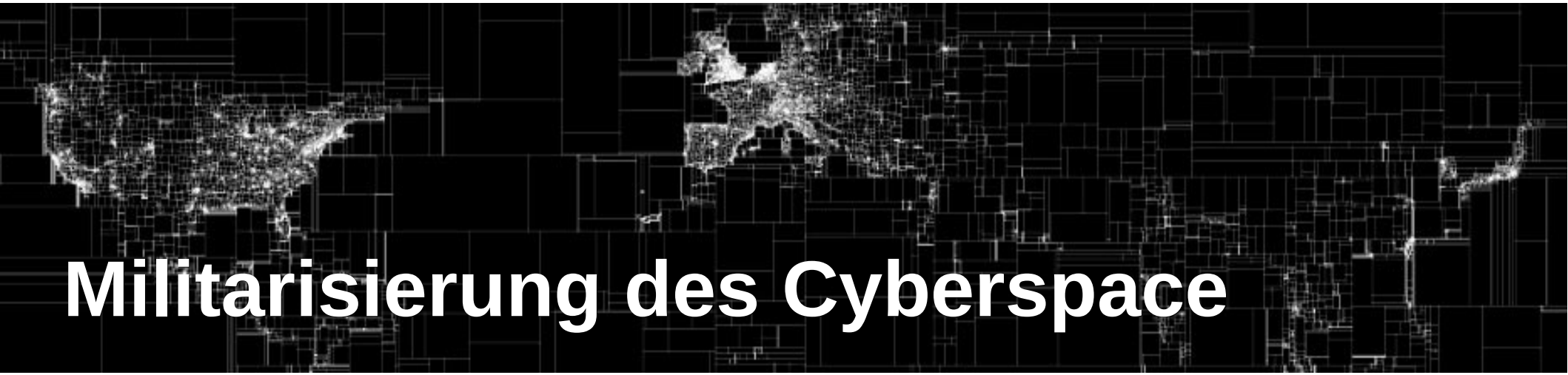


Militarisierung des Cyberspace

Folgen für die internationale Sicherheit,
Probleme, Trends und Lösungsansätze

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

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

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

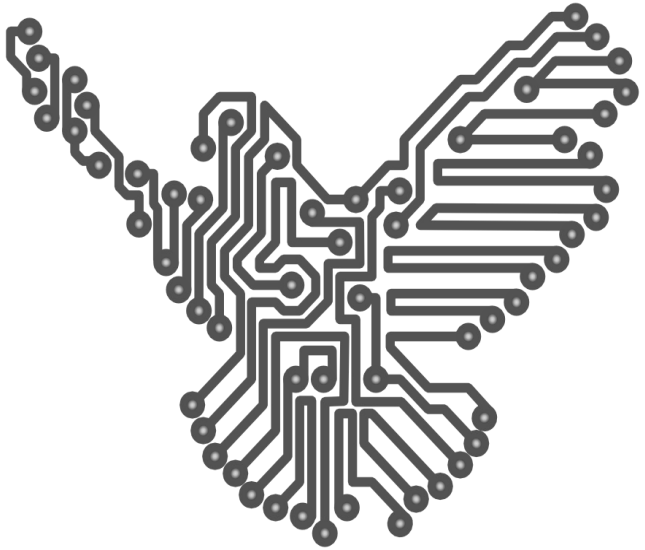
ifsh.de

Das IFSH /2

- Mitarbeiter Arbeitsgruppe IFAR²

  “Interdisziplinäre Forschungsgruppe Abrüstung, Rüstungskontrolle und Risikotechnologien”

- Dipl. Informatiker, Vertiefung Künstliche Intelligenz und Psychologie
- Datenbank/Blog cyber-peace.org
- 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
  - Abschreckung
  - Rüstungswettläufe

* 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*) 40 Staaten mit offensiven militärischen Cyberprogrammen
- Tallinn Manual zur Anwendung des Völkerrechts im Cyberspace
- MADIANT Bericht zur chinesischen Militär-Hackereinheit PLA 61398

* 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*) 40 Staaten mit offensiven militärischen Cyberprogrammen
- Tallinn Manual zur Anwendung des Völkerrechts im Cyberspace
- MADIANT Bericht zur chinesischen Militär-Hackereinheit PLA 61398
- 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

? Anwendbarkeit etablierter Normen des Völkerrechts

- Was ist der „Cyberspace”
  - Informationssicherheit (Proposal Russland/China an die UN 2013)
  - Cybersicherheit (USA/Europa)
- 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

Völkerrecht & Cyberspace /2

- „Tallinn Manual“
  - NATO Exzellenz-Zentrum CCDCOE
    (NATO Cooperative Cyber Defence Centre of Excellence)
  - Nicht-bindende Analyse von Völkerrechtlern, Militärwissenschaftlern und militärischen Mitarbeiten
  - „Armed attack“ und “use of force” im Cyberspace
  - Analogien zu “kinetischen Wirkmitteln”
  - *Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force*
  - *Civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate.*

Völkerrecht & Cyberspace /3

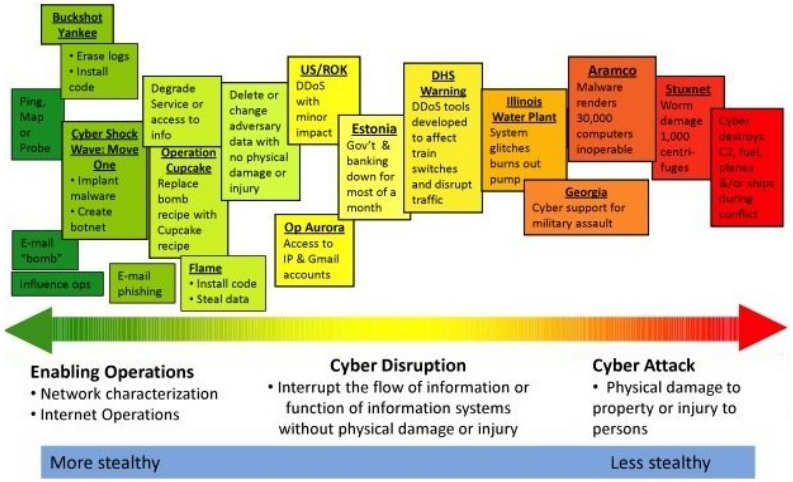
- Zur Definition von Cyberwaffen
  - OECD Studie “Reducing Systemic Cybersecurity Risk” (2010)

    “A weapon is - directed force - its release can be controlled, there is a reasonable forecast of the [actual] effects it will have, and it will not damage the user, his friends or innocent third parties”

    > Situationsbezogener Ansatz als Ausschlußkriterium was keine Cyberattacken sind

  - Kontinuums-Klassifikation nach Brown & Tullos:

    > Einordnen von Vorfällen in ein Schadens-Spektrum
    > Ebenfalls situationsbezogene Bewertung
    > “Schwelle” bei Schädigung von Objekten oder Personen



Völkerrecht & Cyberspace /4

- Zur Definition von Cyberwaffen
  - “Cyber-weapons: legal and strategic aspects”, Stefano Mele, 2013

    „*a weapon can be also an abstract concept thereby not necessarily a material one, as international and domestic legislation have considered it up to now*”

    > Bewertung anhand juristischer und strategischer Dimensionen:
    > Anwendungs-Kontext und vermeintlicher Zweck
    > Beabsichtigter Schaden
    > Konkrete absichtsvolle Auswahl eines strategisch relevanten Ziels

Rüstungskontrolle und Non-Proliferation

- Ausbreitung militärischer Rüstungsgüter / kritischer Bestandteile
  - regulieren
  - kontrollieren
  - unterbinden
- Schwierigkeiten durch spezifische Eigenschaften
  - Virtualität & Immaterialität der Güter
  - Problem der Quantifizierbarkeit oder “wie zählt man Malware”
  - Dual-Use-Problematik
  - Fehlende Verifikationsmöglichkeiten

Rüstungskontrolle und Non-Proliferation /2

- Wassenaar-Abkommen
  - 1996: Abkommen zur Exportkontrolle von konventionellen Waffen und doppelverwendungsfähigen Güter und Technologien (“Dual use”)
  - Rüstings-Transparenz innerhalb der Gruppe von Mitgliedsstaaten
  - Ergänzung von 2013:

    “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.
  - Konkrete Umsetzung liegt im Ermessen des einzelnen Mitgliedstaates
  - Aber: Meldeangaben erst nach Export, keine Rechenschaftspflichten zu einzelnen Entscheidungen, keine einheitliche Bewertungsgrundlage

Technische Schwierigkeiten

- Das “Payload”-Problem
  - Abgrenzung zwischen Kriminalität, Spionage und Sabotage eher eine Frage der Motivation des Akteurs als der angewandten technischen Mittel
- Abgrenzung von Offensive und Defensive
- Attribution im Cyberspace
  - Maßgebliche Voraussetzung für Selbstverteidung UN Charta Ar.t 51
- Territoriale Souveränität und Grenzen im Cyberspace
- IT kritischer Infrastrukturen mit besonderem Schutzbedarf

… und weitere Probleme

- Verbindungen Geheimdienste und Militär
  - NSA-Direktor auch Direktor des US Cyber Command mit explizit offensiver Ausrichtung und weiterer militärischer Einrichtungen
  - US Presidential Policy Directive PPD-20, Oktober 2012
- Cyberattacken zwischenstaatlicher Akteure
- Internet Governance
  - Selbstregulation vs. Steuerung durch internationale Gremien (ITU*)
  - Weiterentwicklung und Standarisierung technischer Konzepte (IETF**)
  - Nationale Souveränitäten
- Freiheit vs. Kontrolle

* 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

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 zukünftig integraler Bestandteil aller “Combat missions”

Aktuelle internationale Situation /2

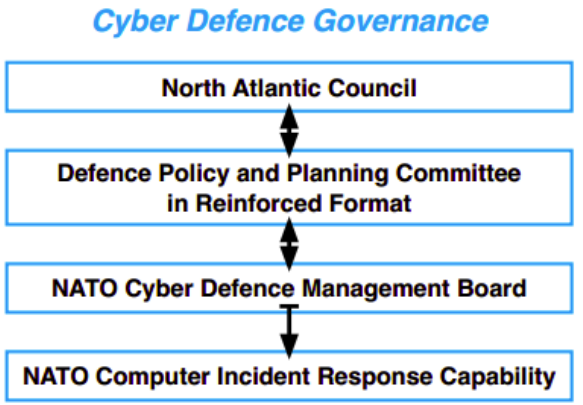
- Russland
  - *„The task of equipping the armed forces and other troops includes the development of the forces and means of information warfare, and the creation of new types of precision weapons and the development of their information security”*
  - Aufbau einer Cyber-Einheit für die Verteidigung 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 Treffen der NATO-Verteidigungsminister: Cyberwar ständiger Tagesordnungspunkt und Teil der Verteidigungsplanung
  - Seit 2011 Cyber Defence Management Board im Rahmen der NATO Policy on Cyber Defence
  - 2014 NATO Gipfel Wales:
    „Nato leaders are expected to accept that there is no distinction between cyber attack and physical attack"



- Deutschland
  - Kommando Strategische Aufklärung mit Computer Networks Operation-Einheit (seit 2006) die auch für offensive Operationen ausgebildet wird (60-75 Personen)
  - Aufbau eigener Bereich neben Marine, Luftwaffe & Heer
  - Bisher keine Rechtsgrundlage für offensive Operationen aber eine *"Eine Anfangsbefähigung zum Wirken in gegnerischen Netzwerken wurde erreicht"*

Politische und technische Lösungsansätze

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

!

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**

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

    > USA: Framework for Improving Critical Infrastructure Cybersecurity

    > EU: Vorbereitung einer Meldepflicht bei „kritischen Vorfällen signifikanter Größe" *

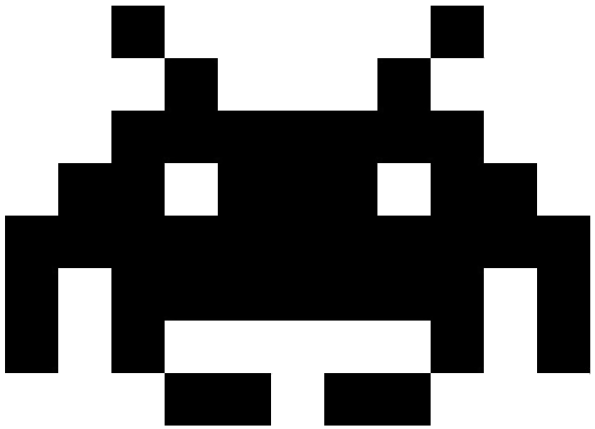
    > Deutschland: Cyber-Sicherheitsgesetz **
  - Regulierung des Handels mit Schadsoftware

    > 12.2013: „intrusion software" als Bestandteil des 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

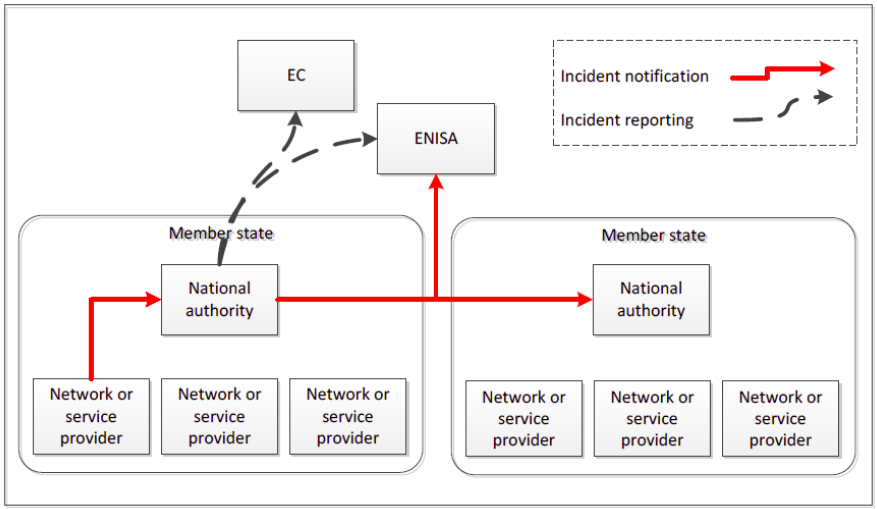
Ansätze für den Cyberspace – Praxis

- 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

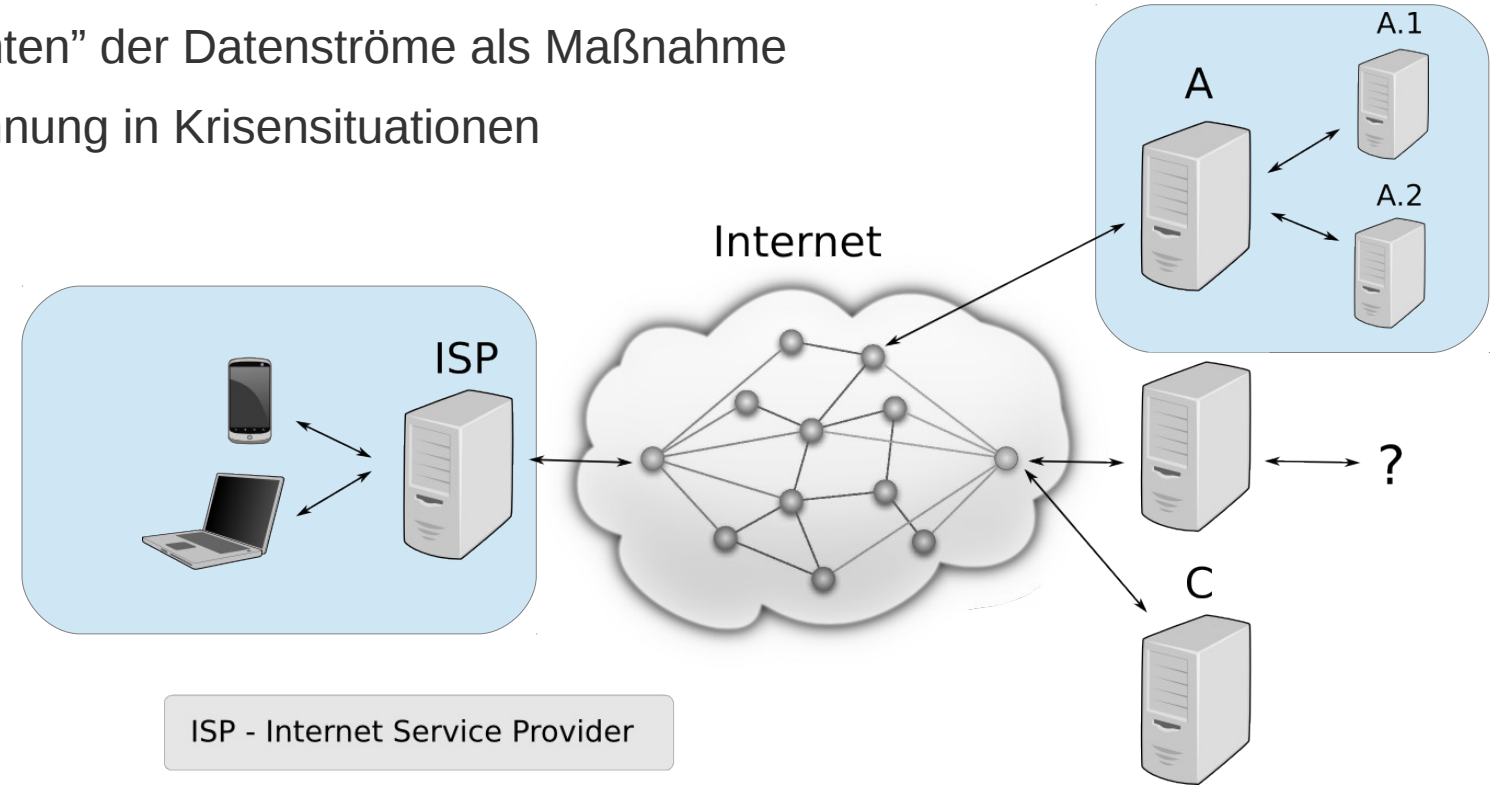
- Mögliche weitere praktische Ansätze
  - Speicherung / Austausch / Sichtung von Verbindungsdaten

    > Unilaterale Selbstverpflichtung zur Transparenz

    > Überwachung der defensiven Orientierung von Cyberprogrammen

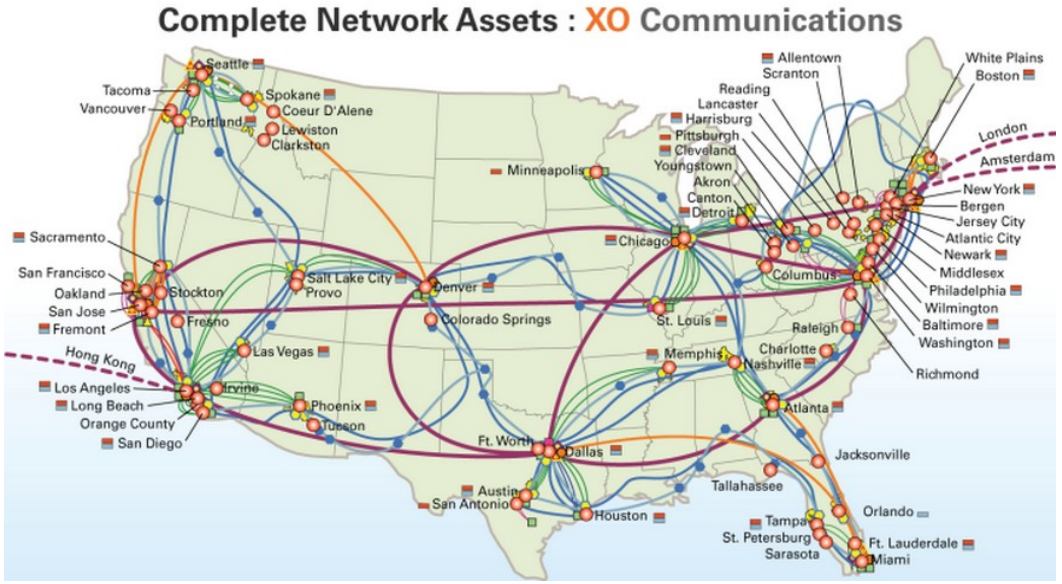
    > Rückverfolgung ungewöhnlicher Aktivitäten

    > “Durchleuchten” der Datenströme als Maßnahme für Entspannung in Krisensituationen



Ansätze für den Cyberspace – Fiktion

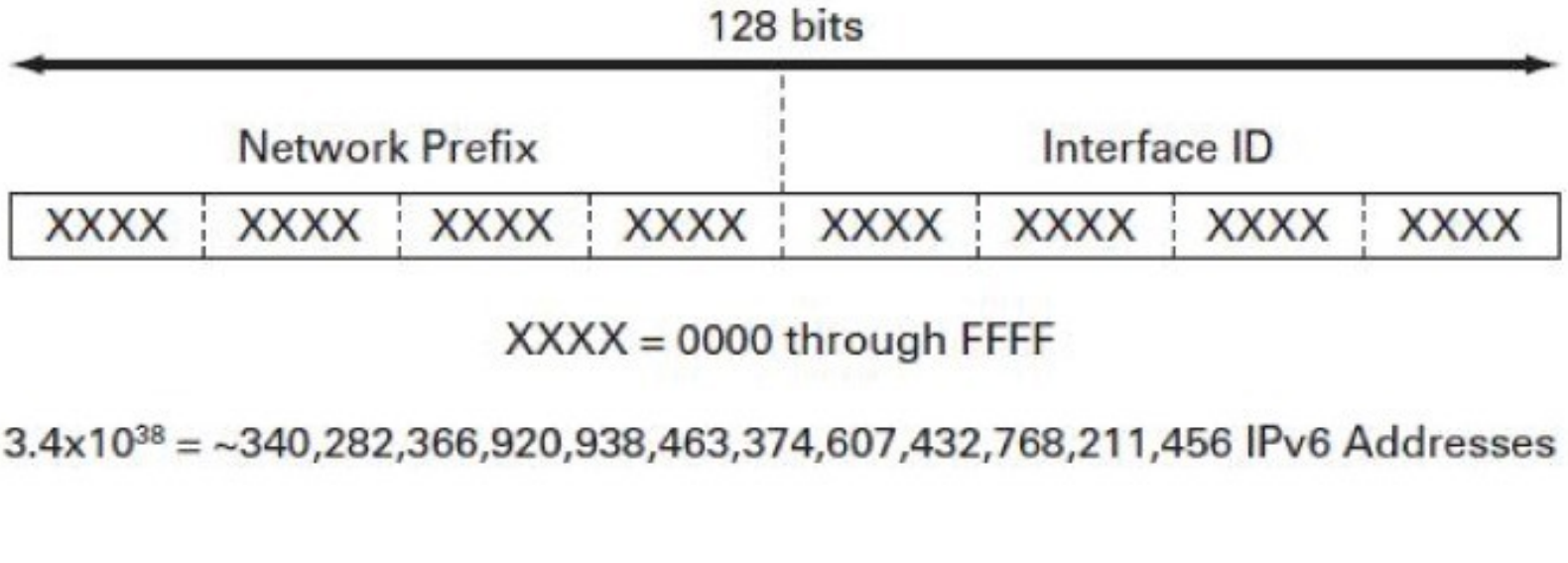
- Ideen für weitere technische Ansätze
  - der Cyberspace als einzigartige “man made domain”
  - Grenzen im Cyberspace
    > Staatliche Souveränität
    > Verlässlichkeit für andere Staaten
    > BGP – Border Gateway Protocol *



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

Ansätze für den Cyberspace – Fiktion /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

Stuxnet & Co.

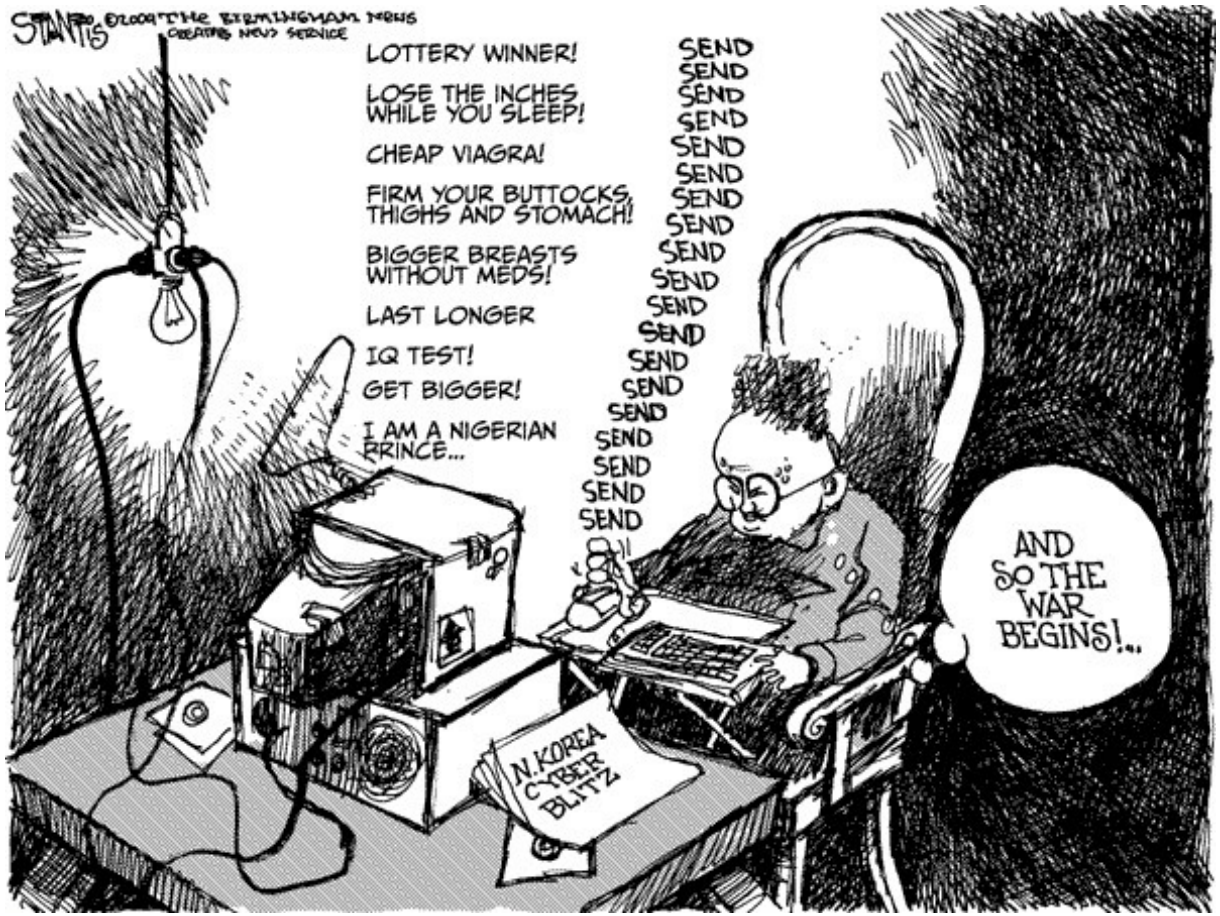
Stuxnet – ein finaler Rückblick

- „To Kill a Centrifuge“ - A Technical Analysis of What Stuxnet’s Creators Tried to Achieve, R. Langner, Nov. 2013
- Zwei Sabotage-Versionen von Stuxnet
  - *„Both attacks aim at damaging centrifuge rotors, but use different tactics. The first (and more complex) attack attempts to over-pressurize centrifuges, the second attack tries to over-speed centrifuge rotors and to take them through their critical (resonance) speeds*
  - Spätere (aufgedeckte) Version „much simpler and much less stealthy“
  - Erste Version eher Produkt einer *„limited (..) in-group of top notch industrial control system security experts“*, zweite Version eher Planungsbestandteil einer höherrangigen Abteilung *„where the original crew is taken out of command by a casual 'we’ll take it from here' by people with higher pay grades“*
- *„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

- Server und Arbeitsplatzrechner von 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

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



Anhang: Fähigkeiten der NSA, eine Auswahl

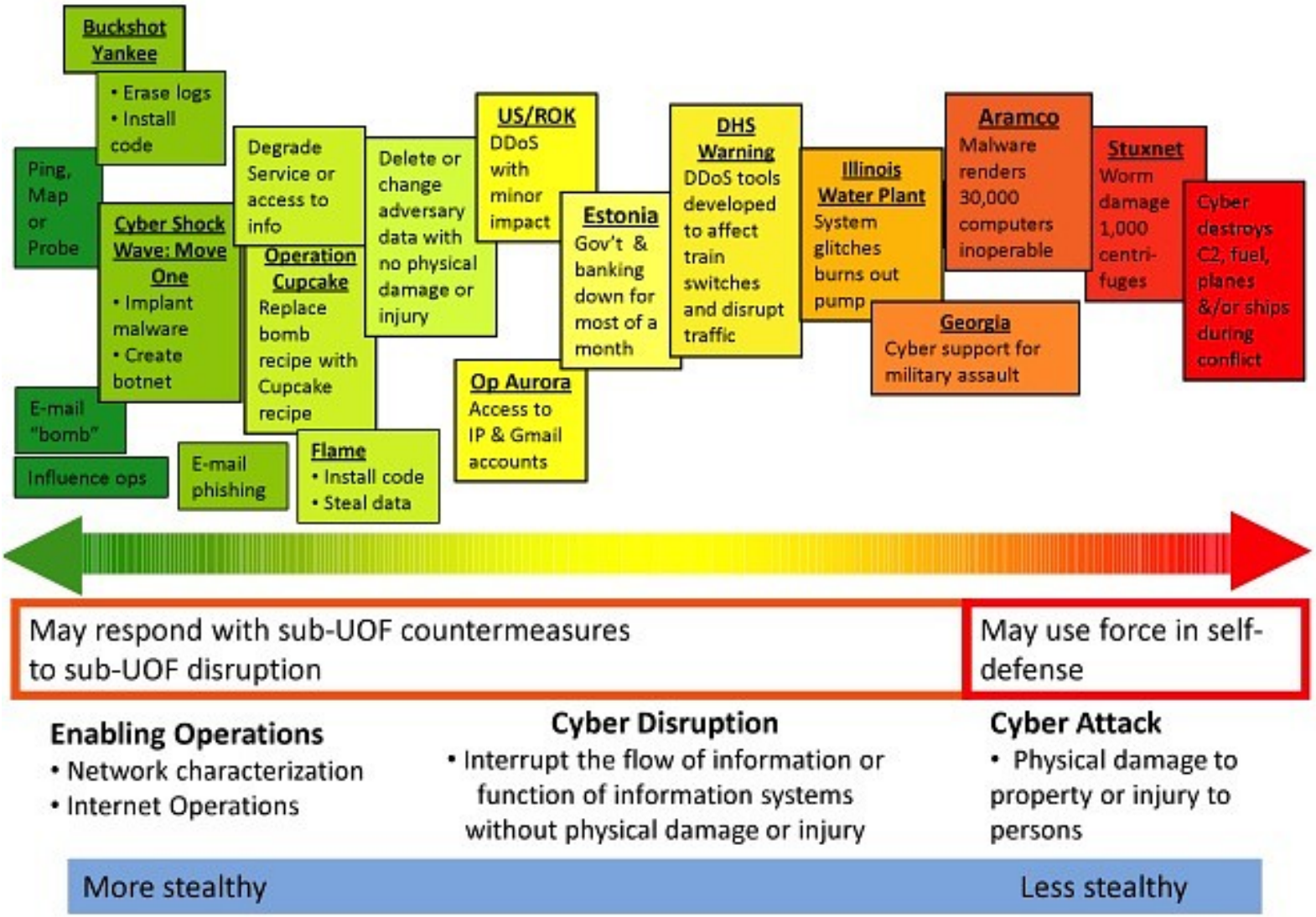
- Fähigkeiten der NSA (eine Auswahl)
  - Zugriff auf wichtige Datenschnittstellen bei IT-Anbietern und IT-Infrastrukturen (PRISM, UPStream, Stormbrew)
  - Zugriff auf wichtige Sicherheits-, Handels- und Telekommunikationsdaten (VISA, Swift, Fluggastdaten)
  - Eigene parallele Server-Infrastrukturen im 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

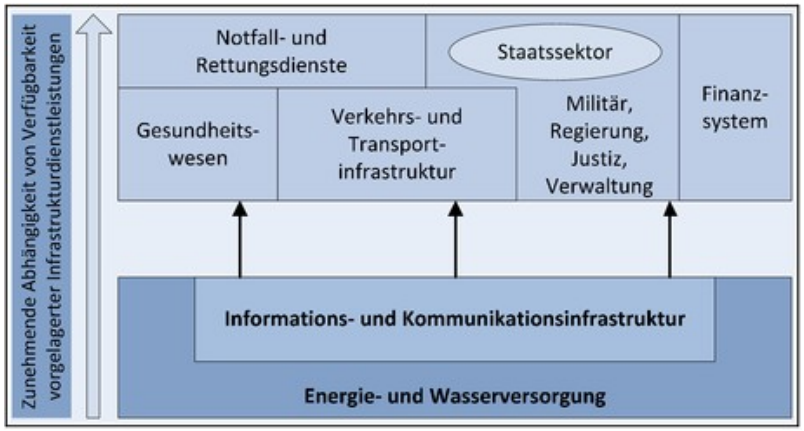
Anhang: Cyberwaffen nach Brown/Tullos

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 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