Die Waffen des Cyberwar

Über die Technik der digitalen Aufrüstung und begriffliche Schwierigkeiten

Thomas Reinhold

reinhold@ifsh.de

Gliederung des Vortrags

- Glossar
- Typen und Klassifikationen von Schadsoftware
- Vorkommnisse seit 2010
- Zusammenhänge und Akteure hinter der Software
- Trends in der digitalen Aufrüstung
- Zum Aufwand einer Cyberattacke
- Abgrenzungs- und Definitionsprobleme
- Quellen

Glossar – Zum Begriff Cyberspace

- *EU Cybercrime Convention (2001):*

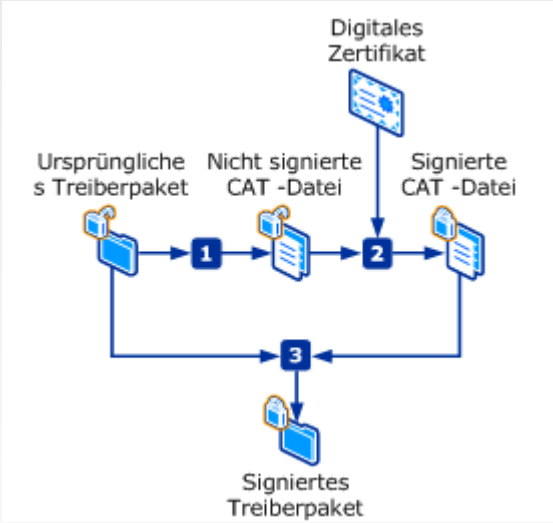
  By connecting to communication and information services users create a kind of common space, called "cyber-space"

- *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”

Glossar - Technische Begriffe

- Command & Control Server (C&C-Server)
- Zero-day-exploit
  - unbekannte Sicherheitslücke
  - Ungeschütze Angriffsmöglichkeit
- Digitale Zertifikate
  - eindeutige digitale Unterschrift
  - Sicherheitsprüfung vor Installation system-kritischer Software
  - betrieblich gut geschützte Information



Typen und Klassifikationen von Schadsoftware

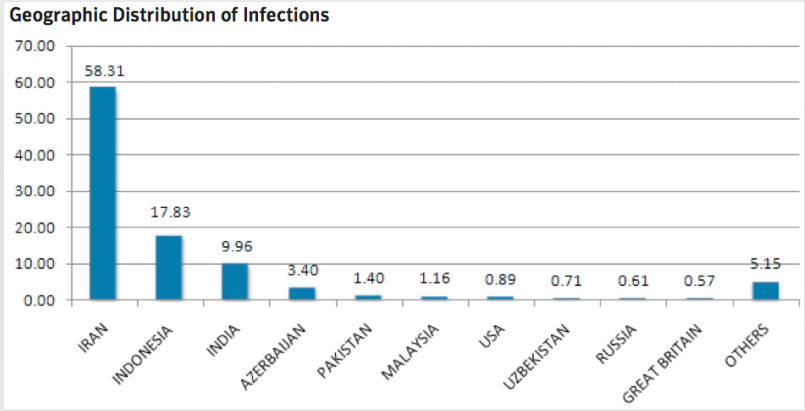
- Malware: Software mit unerwünschter, ggf. schädlicher Funktion
- Klassifikation nach Verbreitungsart, Schaden, Absicht, Zielsystem, Kontrollmöglichkeiten …
  - Viren — Reproduktion durch Einschleusen in Software
  - Würmer — Aktive Selbstverbreitung über Netzwerkdienste
  - Trojaner — Schadcode verborgen in scheinbar nützlicher Software
  - Botnetze — Verborgene Software auf Rechnern, die über Command-&-Control-Server ferngesteuert wird

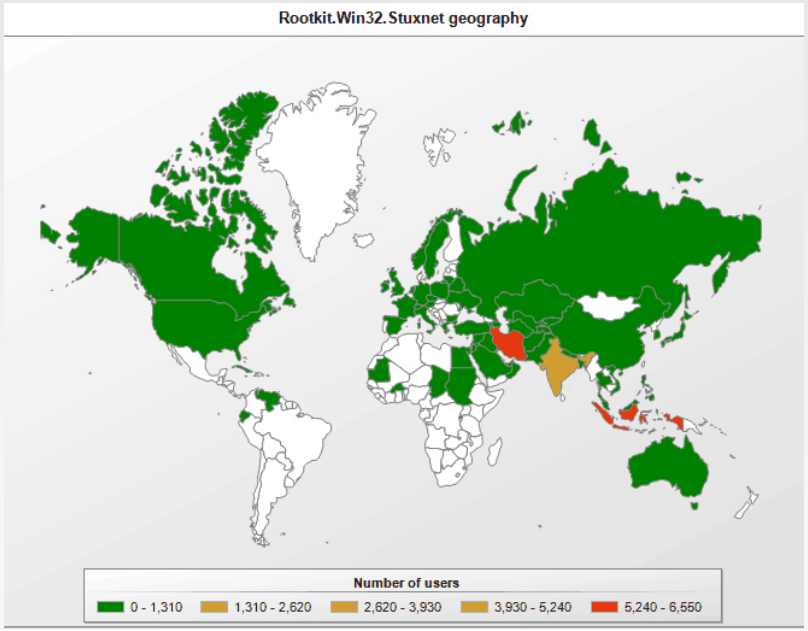
Vorkommnisse seit 2010 – Übersicht

Malware	Entdeckt	Sicher aktiv seit
Stuxnet	Juni 2010	Juni 2009
Duqu	September 2011	November 2010
Flame	Mai 2012	März 2010
Gauss	Juni 2012	September 2011
Mahdi	Juli 2012	September 2011
Rocra	Oktober 2012	Mai 2007

Stuxnet - Keyfacts

- entdeckt: Juni 2010
- sicher aktiv seit: Juni 2009
- Verbreitung: Industrieanlagen im Iran, Indonesien, Indien
- Infektion und Replikation
  - modifizierter USB-Stick
  - Windows-Netzwerkumgebung
- Hauptziel:
  - Schadwirkung
  - Zerstören von Uran-Zentrifugen





Stuxnet - Details

- Targeted Attack
  - für spezifische Hardware entwickelt (Siemens Step 7 SCADA)
  - für spezifische Anlage(n) entwickelt
- Überwindung des ”Air gap”
- Verwendung digitaler Zertifikate & vier Zero-day-exploits
- Millionen-Dollar-Projekt für Technologie, Entwicklung und SCADA-Testanlage
- Mehrjähriger Aufwand

Duqu – Keyfacts

- entdeckt: September 2011
- sicher aktiv seit: November 2010
- Verbreitung: 5 Technologie- und Forschungsorganisationen mit Sitz in Frankreich, Niederlande, Schweiz, Ukraine, Indien, Iran, Sudan, Vietnam
- Infektion und Replikation
  - modifiziertes WORD-Dokument
  - Windows-Netzwerkumgebung
- Hauptziel: gezielte SigINT und Spionage

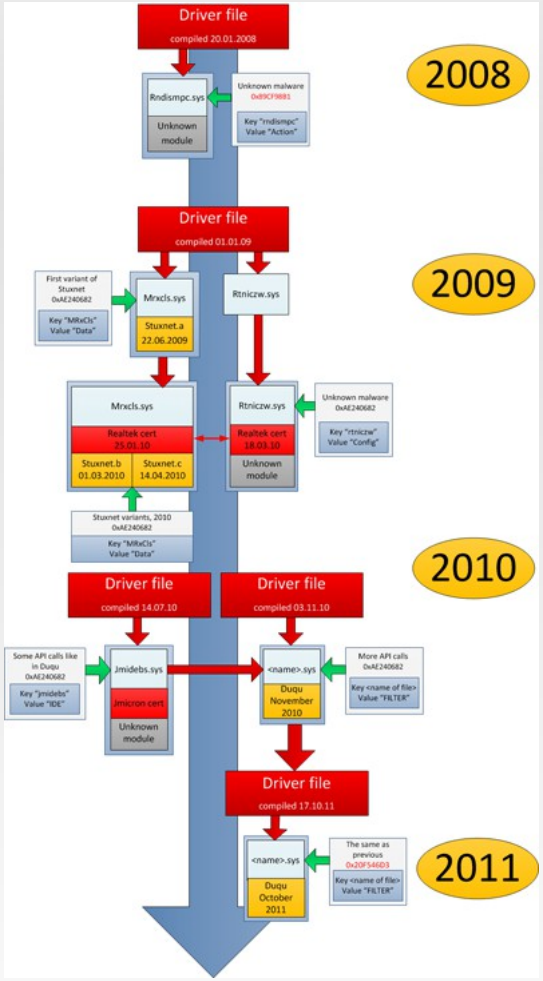
Duqu – Details

- Payload:
  - Aufnahme von Screenshots & Tastatureingaben
  - Sammlung von Netzwerk-Informationen
  - Suchen & Kopieren bestimmter Dateien
  - Eindeutige Identifikation jedes infizierten Systems
- Direkt über C&C-Server gesteuert
- Geringe Streubreite
  - 30-Tage Selbstabschaltung
  - Killswitch, im Oktober 2011 ausgelöst

Duqu – im Vergleich

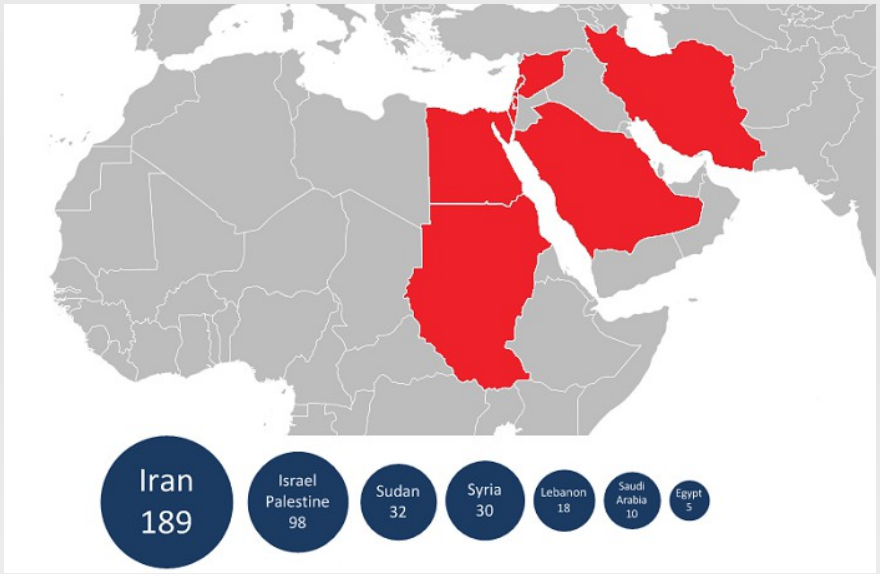
- Gesamtarchitektur zu Stuxent identisch
- Gleiches digitales Zertifikat wie bei Stuxnet

- Plattform „Tilded“ als Basis v. Duqu & Stuxnet
- „Tilded“ seit Ende 2007/08 entwickelt
- Wahrscheinlich weitere Projekte mit Tilded zwischen 2007 und 2011 realisiert



Flame – Keyfacts

- entdeckt: Mai 2012
- sicher aktiv seit: März 2010
- Verbreitung: Iran, Israel/Palästina, Libanon, Saudi-Arabien
- Infektion und Replikation
  - modifizierte USB-Sticks
  - Netzwerkumgebung und lokaler Windows-Update-Mechanismus
- Hauptziel: ”breite” SigINT und Spionage



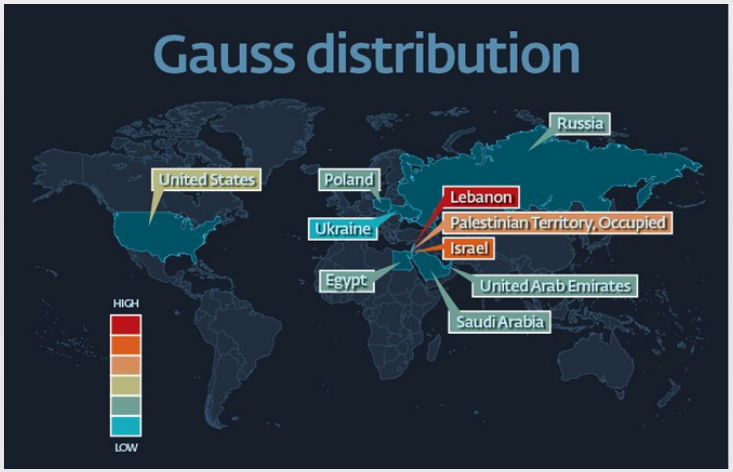
Flame – Details

- Payload ähnlich Duqu viele komplexe, nachladbare Module für Verschlüsselung, Datenbankzugriffe, Datenkompression
- Bluetooth-Geräte ausgelesen
- Killswitch im Juni 2012 ausgelöst
- C&C-Server noch aktiv und in Weiterentwicklung
- Teile von Flame bereits 2007 in Malware „Skywyper“ verwendet

Flame – im Vergleich

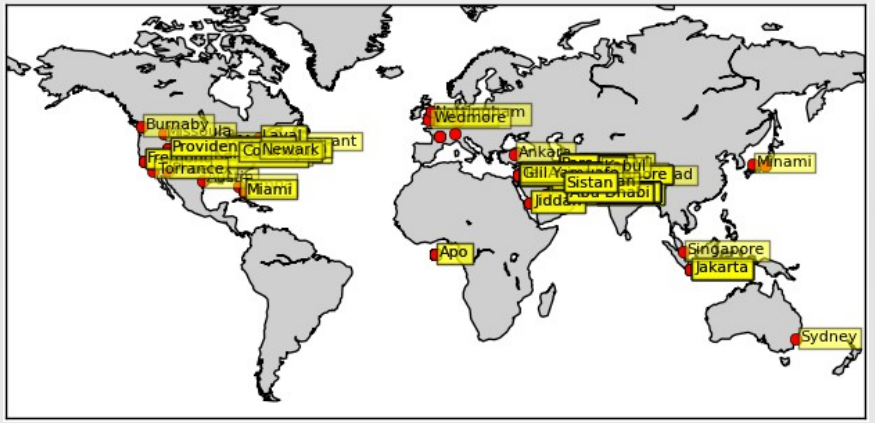
- Sehr viel komplexere Architektur & Code
- Verwendung zweier Zero-day-exploits wie bei Stuxnet
- Code-Verwandtschaft zwischen Stuxnet-Modulen und Flame
- Vermutlich parallel zu Tilded-Plattform entwickelt
- Gemeinsamer Ressourcenpool der Entwickler

Gauss



- entdeckt: Juni 2012
- sicher aktiv seit: Sept. 2011
- Verbreitung: Libanon, Israel, Palästina
- keine Replikation
- Hauptziel: gezielte SigINT von Individuen
  - Spionage von E-Mail & Social Media Zugängen
  - Onlinebanking (regionale Banken, CitiBank, PayPal)
  - Browser-Verlauf, Cookies
- Nicht gelöscht, aber seit Juli 2012 im Schlafmodus
- Vermutlich auf Basis von Flame entstanden

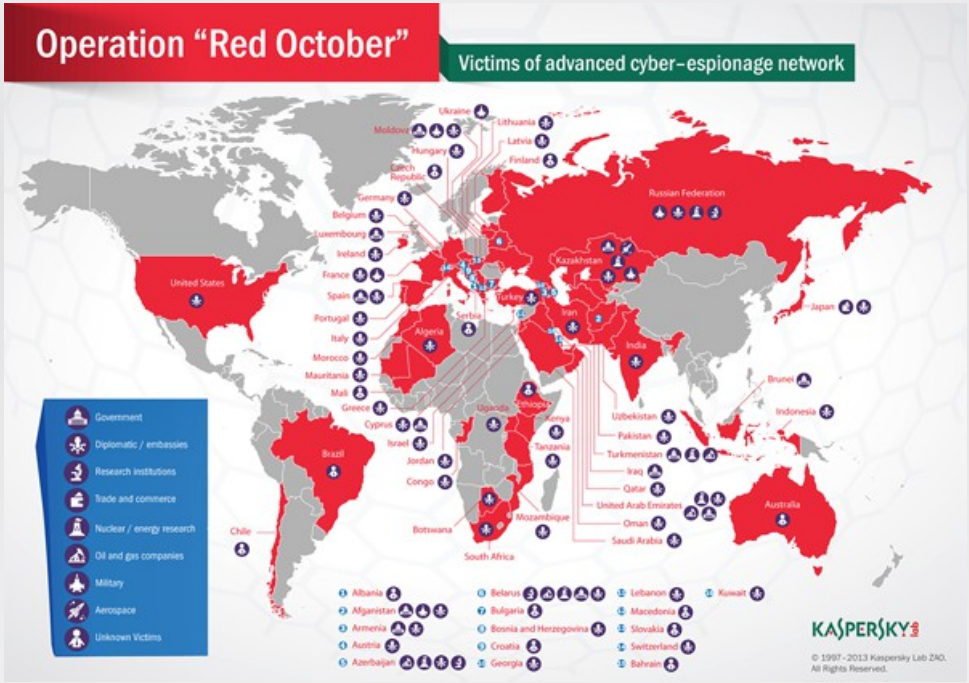
Mahdi



- entdeckt: Juli 2012
- sicher aktiv seit: September 2011
- Verbreitung: Iran, Pakistan, USA
  Finanzen, Wissenschafts & Verwaltung
- Infektion und Replikation
  - Modifizierte Powerpoint & Bilddateien mit religiösen/politischen Bezügen
- Hauptziel: Spionage und Datendiebstahl
- Keine Verwandschaft zu Stuxnet & Co, keine Zero-Day-Exploits
- Simpel aber effektiv
- Viele persische Bezeichnungen im Code

Rocra – Keyfacts

- entdeckt: Oktober 2012
- sicher aktiv seit: Mai 2007
- Verbreitung: Spitzeneinrichtungen und diplomatische Vertretungen, insb. Osteuropa und Zentralasien
- Infektion und Replikation
  - gezielt thematische E-Mails
  - lokale Ausbreitung unter Ausnutzung gesammelter Informationen
- Hauptziel: Spionage von Daten höchster Vertraulichkeit
  - u.a. Daten eines populären Verschlüsselungsprogramm der EU/NATO



Rocra – Details

- Payload
  - Komplex und universell wie Flame
  - Daten auch von mobilen Datenträgern & angeschlossenen Telefonen
- Haupt-C&C-Server über Proxies verborgen
- Gesammelte Daten kontinuierlich weiter verwendet
- C&C-Server vor wenigen Tagen deaktiviert
- Chinesische und russische Bezeichnungen im Code

Zusammenhänge und Akteure hinter der Software

- Mindestens zwei professionelle, komplexe Entwicklungen mit gemeinsamen Ressourcen-Pool
  - Tilded (Stuxnet, Duqu)
  - Flame-Plattform (Flame, Gauss)
- Weitere unabhängige Akteure (Mahdi, Rocra)
- staatliche Kooperationen (Stuxnet, Rocra)

Zusammenhänge und Akteure hinter der Software II

- Urheberschaft von Stuxnet
  - NY Times 1.6.2012, (David E. Sanger)
  - Teil des Programms „Olympic Games“, gestartet 2006 von G.W.Bush
  - US-Gemeinschaftsentwicklung mit israelischem Militär
- Urheberschaft Flame
  - Washington Post 19.6.2012 (E. Nakashima, G. Miller , J. Tate)
  - Entwicklung des US-Militär mit israelischem Militär für kontinuierliches Erforschen & Überwachen der Iranischen Netzwerke

Trends in der digitalen Aufrüstung

- Ausschreibung Cyberwar-Zentrale der US Air Force 08/2012
- Cyberwarfare integraler Bestandteil militärischer Operationen
- Ziele der Ausschreibung
  - Attack: Stören, Unterbrechen, Manipulation, Zerstören fremder Systeme
  - Support: Schwächen finden, Ziele identifizieren, Informationssammlung für die Planung von Operationen, eigene Systeme schützen
  - Development: Möglichkeiten für aktive und defensive Cyberwarfare-Operationen entwickeln

Trends in der digitalen Aufrüstung II

- Bericht des BMVg an Verteidigungsauschuß vom 5.6.2012
  - Abteilung Computernetzwerkoperationen des Kommando Strategische Aufklärung seit 5 Jahren im Aufbau
  - *"Eine Anfangsbefähigung zum Wirken in gegnerischen Netzwerken wurde erreicht"*
  - *"Simulationen [würden] in einer abgeschlossenen Laborumgebung durchgeführt"*

Zum Aufwand einer Cyberattacke

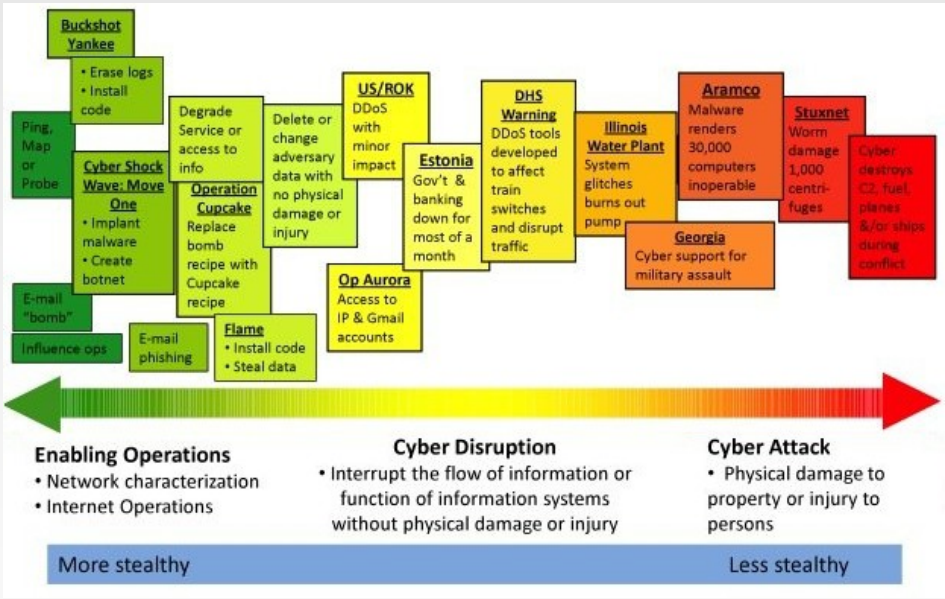
- Anforderungen für einen erfolgreichen Cyberkrieg
  - Sehr klares und genaues Missionsziel und nötige Befugnisse
  - Spezifische Zielinformationen, i.a.R. Vorfeldaufklärung nötig
  - Unbekannte Sicherheitslücken (Zero day exploits)
  - Hochgradig professionelles Entwicklungs/Test/Angriffs-Team
  - Beständkeit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

Abgrenzungs- und Definitionsprobleme

- Abgrenzung Krieg vs. Kriminalität
  - Cybercrime → Fragen nach Regelungen der internat. Strafverfolgung
  - Cyberwar → Fragen nach den politischen Motivationen der Akteure
  - Zentrales Problem: Welches Ausmaß einer nationalen Beeinträchtigung durch externe Cyberzugriffe entspricht einem kriegerischen Akt
- Kritische Infrastrukturen als maßgebliche Schwelle
  - BMI: Energieversorgung, ITK, Transport, Gesundheit, Wasser, Ernährung, Finanzwesen, Staat und Verwaltung, Medien
- Bisherige Vorkommnisse eher explorativ als invasiv
- Frage bleibt: „Was sind Cyberattacken?“

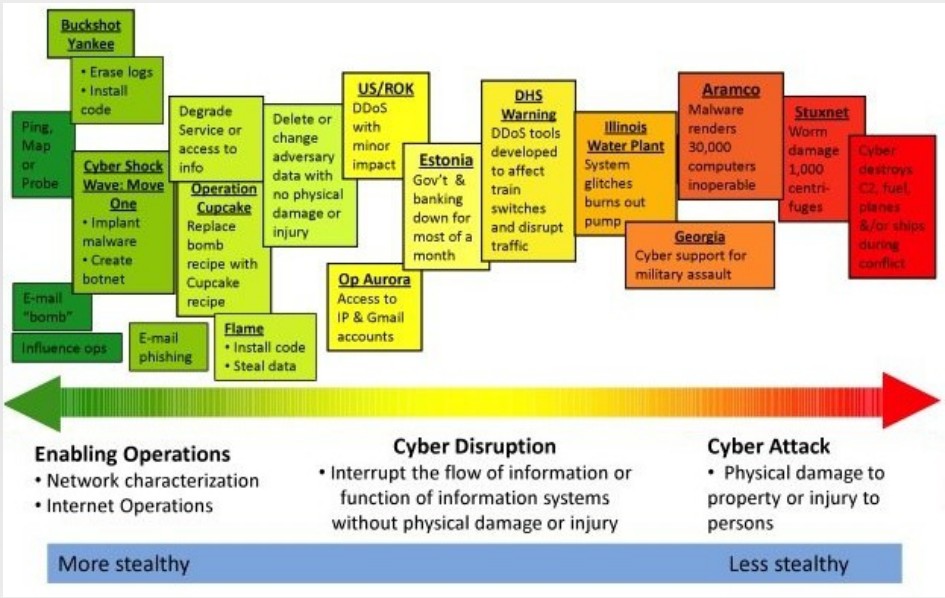
Abgrenzungs- und Definitionsprobleme II

- Aspekte bei der Bewertung
  - Ziel des Angriffs: Spionage, Sabotage oder Angriff mit Störwirkung
  - Identität und vermutliche Absicht des Angreifers
  - Politische Rahmenbedingungen des Angegriffenen (IW)
- Kontinuums-Klassifikation
  - Gary D. Brown & Owen W. Tullos
  - (a) Access/Enabling Operations
  - (b) Cyber Disruption
  - (c) Cyber Attack



Abgrenzungs- und Definitionsprobleme III

- Kontinuums-Klassifikation
  - (a) Access/Enabling Operations
  - (b) Cyber Disruption
  - (c) Cyber Attack
- Weitere Bewertungsmaßstäbe
  - Michael N. Schmitt, Vorsitzender der Abteilung für internationales Recht am US Naval War College
  - Strenge/Härte, Unmittelbarkeit/Direktheit, Grad und Messbarkeit der Zerstörung und Rechtmäßigkeit



- Quellen
  - blogs.mcafee.com
  - searchsecurity.techtarget.com
  - securelist.com
  - heise.de/security
  - kaspersky.com
  - symantec.com/connect
  - „On the Spectrum of Cyberspace Operations“
    (Gary D. Brown and Owen W. Tullos)
    http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations
  - reinhold@ifsh.de

Additional - Das Attributions-Problem

- ”Cyberattacken sind nicht ausreichend gezielt zuordbar und damit für Angreifer ohne negative Konsequenzen”
- Zuordnung wäre unmöglich wenn
  - verwendete Techniken einmalig und unbekannt
  - Angreifer komplett abgeschottet und anonym arbeiten
  - Motivation nicht durch politische Lage Rücksschlüsse zuläßt
  - Angreifer sehr zeitnah und schnell agiert