Cyber-War – Was verbirgt sich hinter dieser Chiffre?

Götz Neuneck (neuneck@ifsh.de)
Institut für Friedensforschung und Sicherheitspolitik
an der Universität Hamburg

1. Die Dynamik des Internet
2. Cyberangriffe: Hype oder Bedrohung?
3. Reaktionen und Strategien
4. Mögliche weitere Schritte

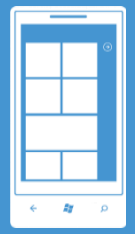
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

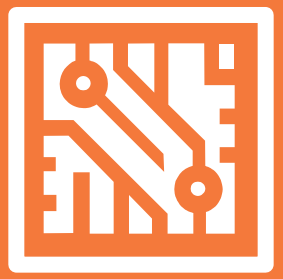
- Welche Dynamiken gehen vom Internet aus und was bedeuten diese für Staaten und IO ?
- Wodurch bzw. durch wen genau im Netz wird die Macht von Staaten in Frage gestellt?
- Worauf zielen Virenattacken wie z.B. STUXNET?
- Wird das Internet zu einem neuen Mittel der militärischen Kriegsführung?

Anpassung → Abhängigkeit

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Internet Nutzer	Mobile Nutzer	Weltbevölkerung	RFID Tags
2 Milliarden	5 Milliarden	7 Milliarden	10 Billionen





Milliarden Nutzer, verbunden mit Billionen Geräten unterstützen vitale gesellschaftliche Funktionen.

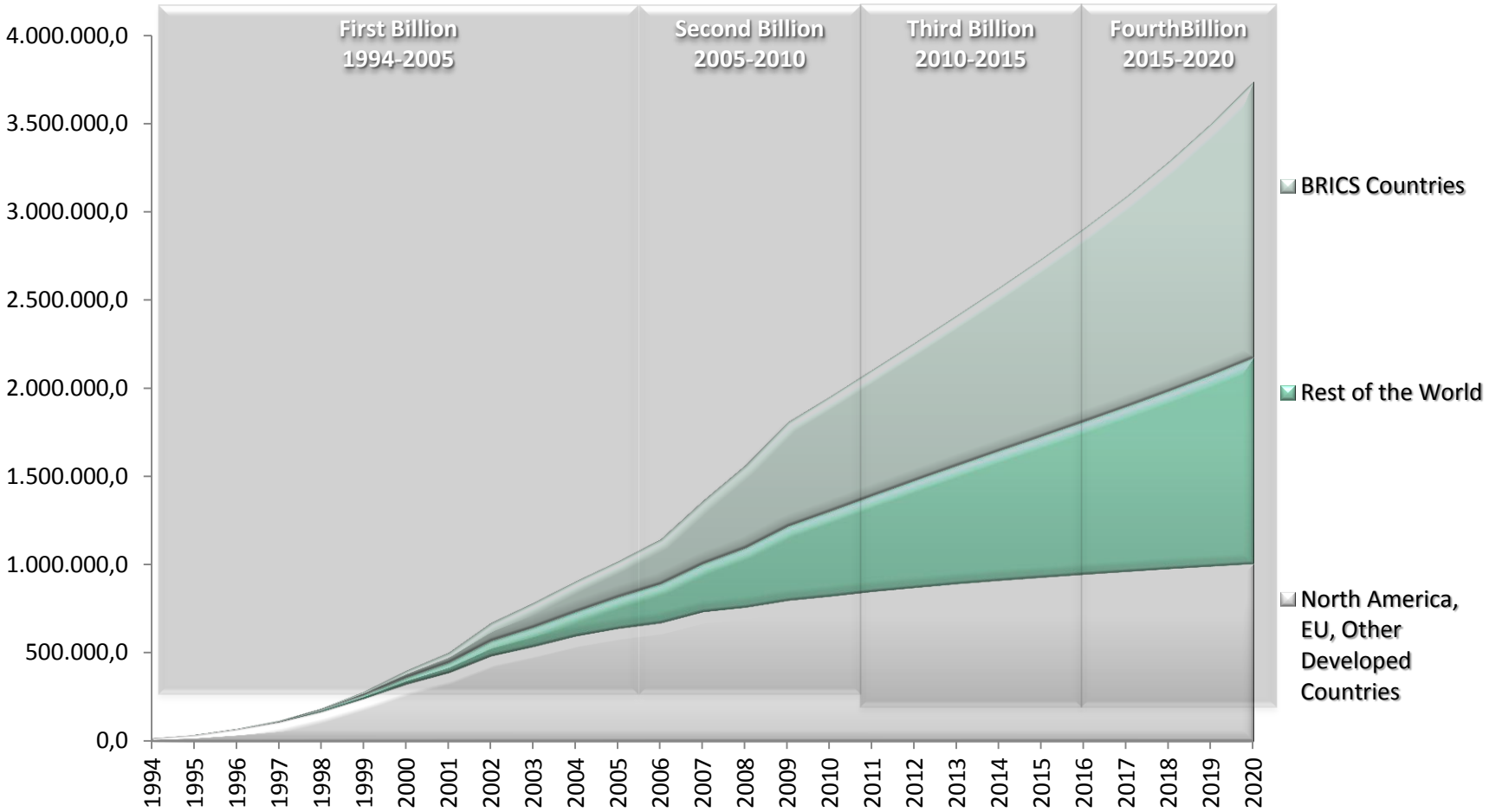
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Internet = Die Globalisierung bestimmende Entwicklung

- Computerleistung verdoppelt sich alle 18 Monate („Mooresches Gesetz“)
- Speicherleistung: 16 MB entspricht Text der Bibel
- 1993 gab es ca. 50 Web-Seiten; 2011 sind es 555 Mio.
- Datenverkehr wächst bis 2016 um das Achtzehnfache
- Monatlich werden 10,8 Exabyte (18 Nullen) übertragen

Nutzung:

- email, Bankabbuchung, Shopping, Social Networks
- Firmen, Industrieunternehmen, Regierungen, Presse


First Billion
1994-2005
Second Billion
2005-2010
Third Billion
2010-2015
FourthBillion
2015-2020
4.000.000,0
3.500.000,0
3.000.000,0
2.500.000,0
2.000.000,0
1.500.000,0
1.000.000,0
500.000,0
0,0
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
BRICS Countries
Rest of the World
North America, EU, Other Developed Countries

Cyberspace ist „Schlüsseldimension des 21. Jahrhunderts“

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Joseph Nye: Aufsatz: „Cyberpower“ [1]

- „Machtzugewinn“ von Internet-Nutzern und NRO: „softpower“

  Beispiele: Wikileaks, Arabischer Frühling: Twitter-Revolte
- Gründe: " „…der niedrige Eintrittspreis, Anonymität und Asymmetrien bei der Verwundbarkeit geben kleineren Akteuren mehr Fähigkeiten, ‚hard‘ und ‚soft power‘ im Cyberspace auszuüben als in stärker traditionellen Gebieten der Weltpolitik“
- Machtdiffusion ist Charakteristikum der Weltpolitik
- „Große Mächte“ werden die „Cybersphäre“ nicht dominieren können
- Machtverschiebungen, kein Machtwechsel

[1] Joseph Nye: Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge/Mass., Mai 2010

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Chancen:

- Weltweite Kommunikation und Datenaustausch
- Digitale Wirtschaft: hoher wirtschaftlicher Nutzen
- Immer mehr Dienste: Bank, Steuerung, Wahlen,.....

Gefahren:

- Cyberkriminalität (z.B. Phishing) →Organisierte Kriminalität
- Cybermobbing
- Cyberpropaganda
- Sabotage
- Cyberwar?

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Ebenen:

- Technisch: Bedrohung, Verbreitung, Schaden
- Sicherheitspolitisch: Nutzen, Wahrnehmung
- Rechtlich: Souveränität, Nachweis, Anwendbarkeit

- national; lokal, regional , international

Akteure:

- individuell
- I&K-Industrie
- Regierungen
- Organisationen: UN, NATO, EU, OSZE, OECD, ITU

Abgrenzung zu: CyberCrime, Cyber Spionage, Cyber Vandalismus etc.

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Was sind Cyber Angriffe ?

- Schon der Eindringversuch in einen PC wird als Angriff gewertet
- Symantec: 2010: „3 Milliarden Angriffe“ (47% As, 30% Eu, 20 Am.)
- Bundesamt für Sicherheit in der Informationstechnik: alle 2 Sekunden tritt neue Malware auf
- Wirkung: Verunstaltung von Webseiten, Datendiebstahl
- Die Angriffsroutinen werden zunehmend komplexer
- Der ökonomische Schaden ist nicht gering: „I love you“ (2000) 10 Mio. USD
- Motive: Protestaktionen, OK
- Hauptproblem Attribution d.h. Zurückverfolgung des Angreifers

Verschiedene Grade von Cyberangriffen

Bedrohungsgrad	1	2	3
Expertise	unerfahren	hoch	Sehr anspruchsvoll
Finanzierung	gering	gut	Extrem gut
Motivation	opportunistisch	gezielt	Schaden im Land
Instrument	Viren, Würmer, Trojaner, Bots	Dto.	Dto. Geheime Präsenz im Netz
Unterstützung	privat	Gruppe	Auslandsgeheimdienst
Detektion	leicht	mittel	schwer

Quelle: US Homeland Security

Historische Cyber Zwischenfälle:

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- 1982: UdSSR Pipeline: 3 kT-Explosion (CIA?)
- Golfkrieg:* 1999/2003 Störung elektronischer Kommunikation des Irak
- 1998: Serbien: Störung der Luftverteidigung durch NATO und Blockade des NATO-Email Verkehrs und von NATO-Websites
- April/Mai 2007 Estland: 22 Tage DDOS
- 2007:* Al Kibar-Angriff Israels auf Syrien
- 2008: Variante des Wurms „SillyFDC“ agent.btz befällt viele US--Militärrechner
- August 2008* Georgien: Cyber Attack und Bombardierung von IT-Einrichtungen durch Russland
- 2007-2009 USA: Spionage F-35 Baupläne Lockheed
- 4. Juli 2009: Stromausfälle 14 US- und 12 südkoreanische Einrichtungen

Cyber War is Coming?

„Die Cyber-Bedrohung ist für unsere Nation eine der schwersten vor uns liegenden Herausforderungen in Bezug auf die wirtschaftliche und nationale Sicherheit“

B. Obama, REMARKS ON SECURING OUR NATION'S CYBER INFRASTRUCTURE, 5/29, 2009

„Angriffe auf Computernetze geschehen immer häufiger, sind besser organisiert und kostspieliger, was den Schaden angeht, den sie staatlichen Verwaltungen, Unternehmen, Volkswirtschaften und potenziell auch Transport- und Versorgungsnetzen und anderer kritischer Infrastruktur zufügen; sie können eine Schwelle erreichen, die den Wohlstand, die Sicherheit und die Stabilität von Staaten und des euro-atlantischen Raums bedroht.“

NATOs New Strategic Concept, November 2011, Nr.12

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Reale Gefahr oder gelenkte Wahrnehmung ?

- Abhängigkeit vom Cyberspace steigt
- Transformiert Grenzen, Hierarchien, Autorität
- Bsp.:E-mail, Handys, Bank, Facebook, Google, Wikileaks
- Vorfälle in verschiedenen Bereichen nehmen zu
- Stuxnet – neue Dimension ? („digitaler Bunkerbuster“)
- Duqu – Proliferation ?
- EU, NATO, Bundesregierung etc.
- Pentagon Direktive: Grund für konventionellen „Gegenschlag“ ?

- Digital Pearl Harbour, 9/11 of the Cyber World
- Digital First Strike, Cyber Weapon of Mass Destruction

→Bewertung der Vorfälle, Grad und Schaden nötig

Welche Cyber Waffen sind denkbar?

Bewusste „logische“ Angriffe (WEB-basiert):

Malware:
- Logische Bomben; Trojaner; Keylogger, Virus
- Root-Kit
- Webbasierte Malware

Angriffsszenarien:
-Distributed Denial of Service (DDoS) Attack
-BotNets
-Zero-Day Exploits
-Embedded Malware

Bewusste „physische“ Angriffe (EM-Strahlen):
- Bomben
- EMP-Waffen, HERF-Guns
- Jammer

Gefahren im Netz:

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Viren:

- den PC infizierende Programme**: Daten löschen !**
- verbreiten sich über **USB-Stick, CD-ROM oder Internet**
- können sich in **ausführbaren Dateien** verstecken**: .exe .xls**
- 3 Typen**: Boot-Viren, Datei-Viren, Makro-Viren**

Würmer:

- schnelle Verbreitung (oft email), infizieren keinen fremden Code

Trojaner:

- nützliches Programm hat ein Schadprogramm „im Bauch“,
- verbreitet sich nicht selber, Datenverlust unbemerkt

Spyware:

- Programme zum Ausspionieren des Surfverhaltens (z.B. Keylogger)

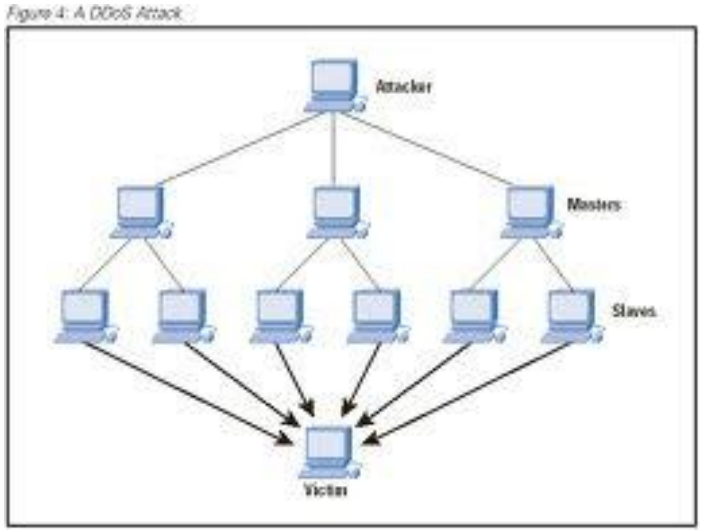
https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/Viren/viren_node.html

Angriffsarten:

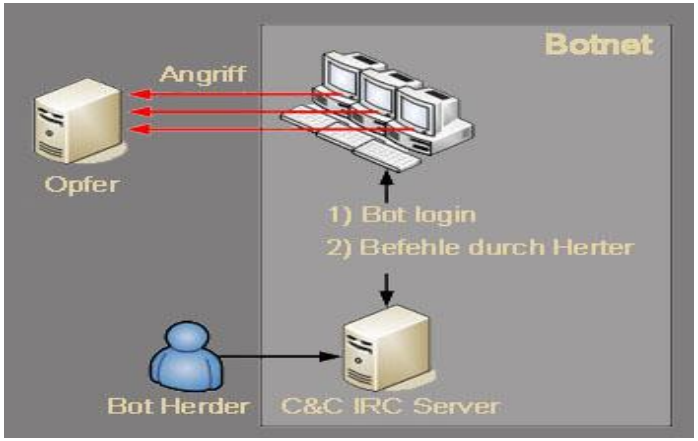
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Phishing:

Denial-of-Service-Attacken (DOS)



Bot-Netz Angriffe:



Animationsfilm (6 Min):
https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/BotNetze/botnetze_node.html

Akteure

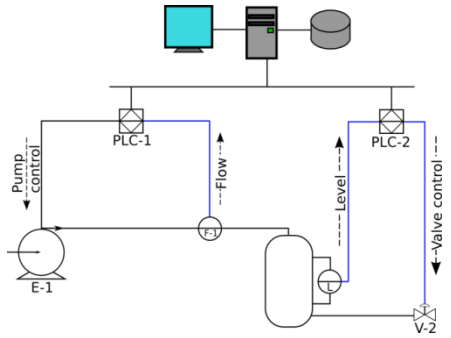
- **Recreational Hacking**: Morris (1988), Melissa (1999)
- **Umfassende kriminelle Angriffe**: EC-Karten PW-Diebstahl
- **Hactivism**: Websites, Defacing
- **Industriespionage:** Data Mining, Cyberspionage
- **koordinierte Angriffe** gegen Regierungen, DDOS
- **Infiltration von Netzwerken**

 erfolgen täglich, verdeckt, Schutz möglich, schwierig:

Detektion der Verursacher

Stuxnet

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg



- **komplexer Wurm-Angriff** auf Industrieanlagen mit Prozesstechnik
- liefert Informationen an externen „Operateur“ und ermöglicht die

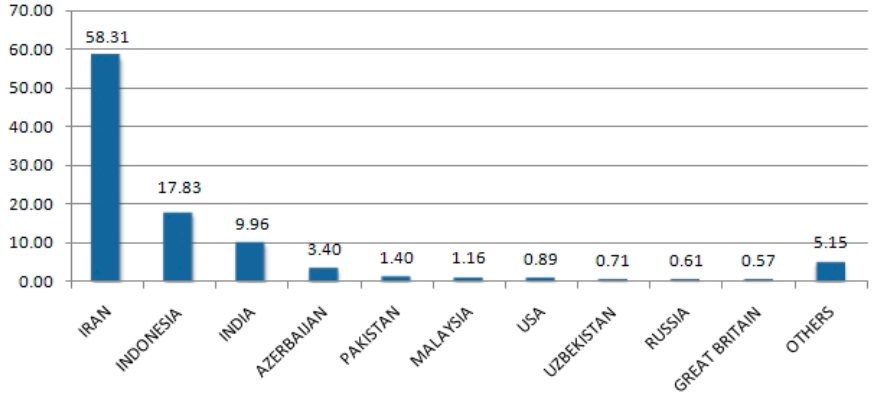
Manipulation von Industrieanlagen

- 30.000 Industrieanlagen im Iran, 45.000 weltweit betroffen
- gelangt über die **Steuerungssoftware WinCC, SIMatic in Netze**
- Notwendig: fundiertes Wissen über **SCADA**-Technologie (Supervisory Control and Data Acquisition) und Ausnutzung von Windows-Sicherheitslücken („Zero-Day-Exploits“)

Stuxnet

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Infektionen weltweit
  - 3 Infektionswellen ausgehend von 5 iranischen Einrichtungen
  - Insgesamt 100.000 infizierte Systeme (Symantec Dossier)
  - 24 Siemensanlagen (Mitteilung Siemens 11.03.2011)
- Schäden
  - laut Siemens keine an ihren Anlagen
  - Iranische Uranzentrifugen (2009 Natanz, Bushehr)
  - Iranische Ölindustrie



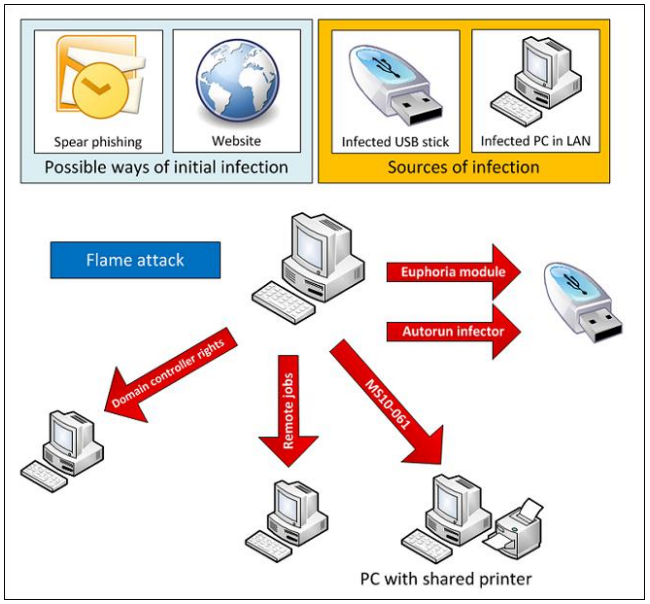
„Olympic Games“

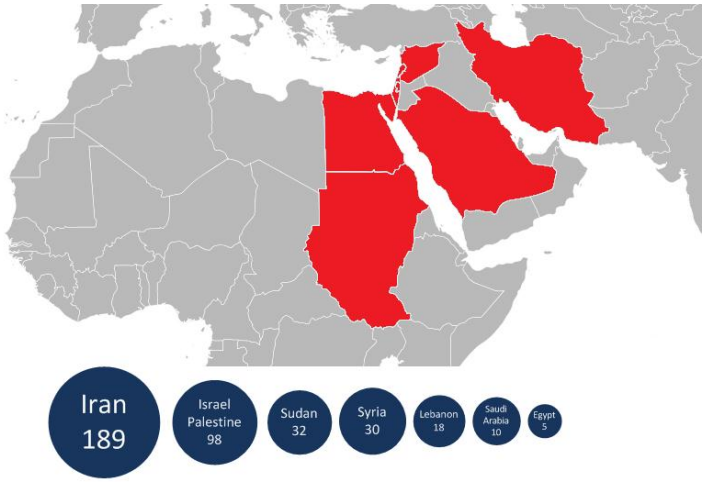
IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- 2006 Iran nimmt UA wieder auf
- 2007 NSA und Israel beginnen das Programm. Teile der Anlage werden aufgebaut
- 2008 Erste Zerstörungen in Natanz
- 2009 Bush informiert Obama über das Programm

Supertrojaner Flame

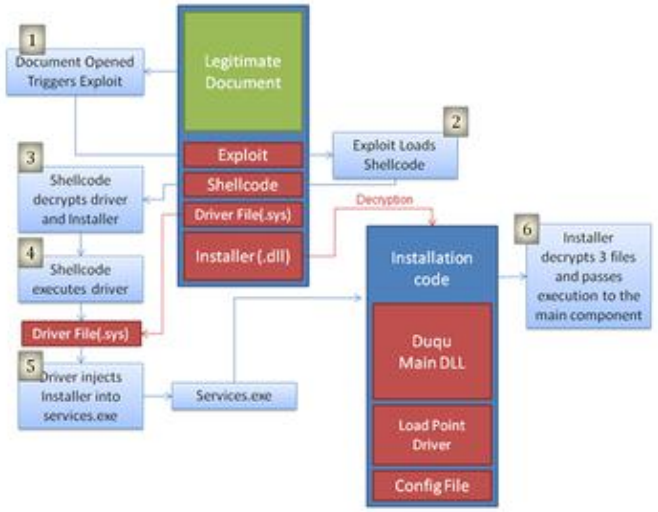
- Verändert Einstellung im befallenen Computer und überwacht Datenverkehr im LAN
- Mikro on/off, Screenshots,
- Wenig Mühe der Verschleierung
- Mehrere Module
- Seit August 2010 im Einsatz
- Derselbe Urheber wie STUXNET
- Ca. 5000 PC vor allem im Mittleren Osten befallen: Iran, Israel, Palästina, Sudan, Syrien

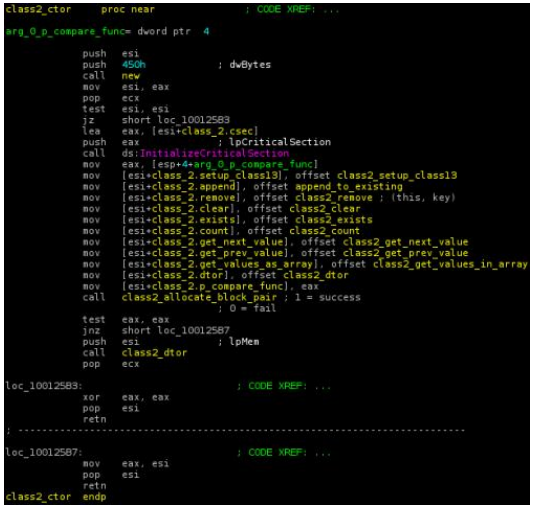




Überwachungstool DUQU

- Duqu-Bot verbreitet sich über Zero-Day-Lücke im Windows Kernel
- Verwandtschaft zu STUXNET ?
- 2011 entdeckt
- Nur gezielte Angriffe, da nur 8 Tage aktiv
- Überwachungstool bei Unternehmen zur Herstellung von Industriesteueranlagen eingeschleust
- F, NL,CH,UKR, IND, IRN



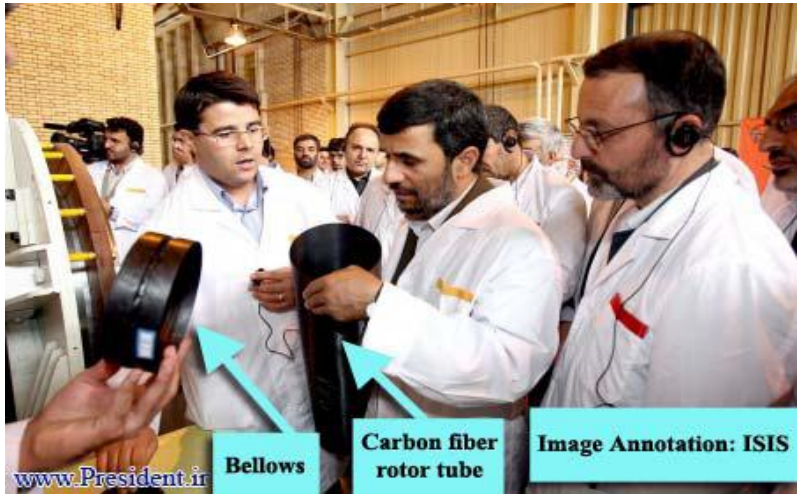


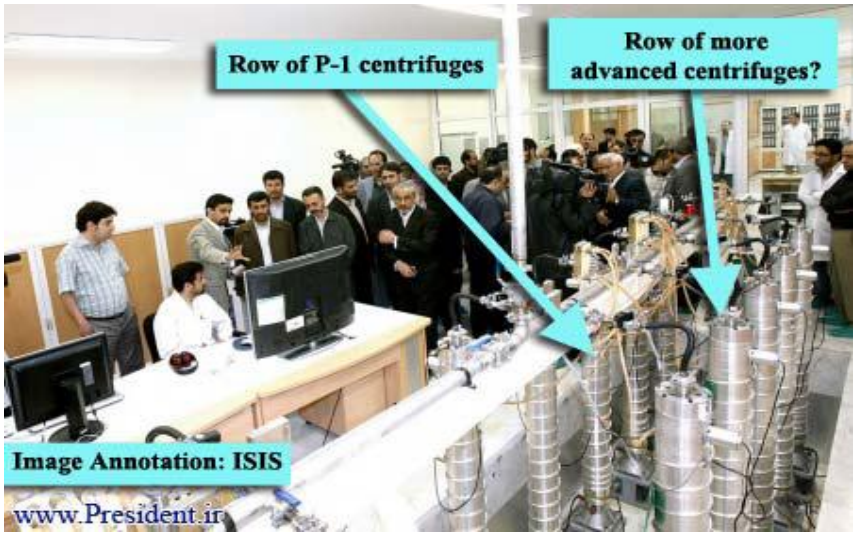
Supervirus

Name	Code	Wirkung	aktiv	entdeckt
Stuxnet		Zerstörung von ca. 500 GZ	2009/2010	2010
Duqu	500 kB,C++ OOC, nutzt Lücke bei Windows	Ausspionieren von Herstellern von Industriesteueranlagen, nur 8 Tage aktiv		2011
Flame	20 x Code als STUXNET; 100 x Code normaler Virus	Überwachungstool	Mind. Seit 8/2010	5/2012

Aurora Experiment 2007

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg



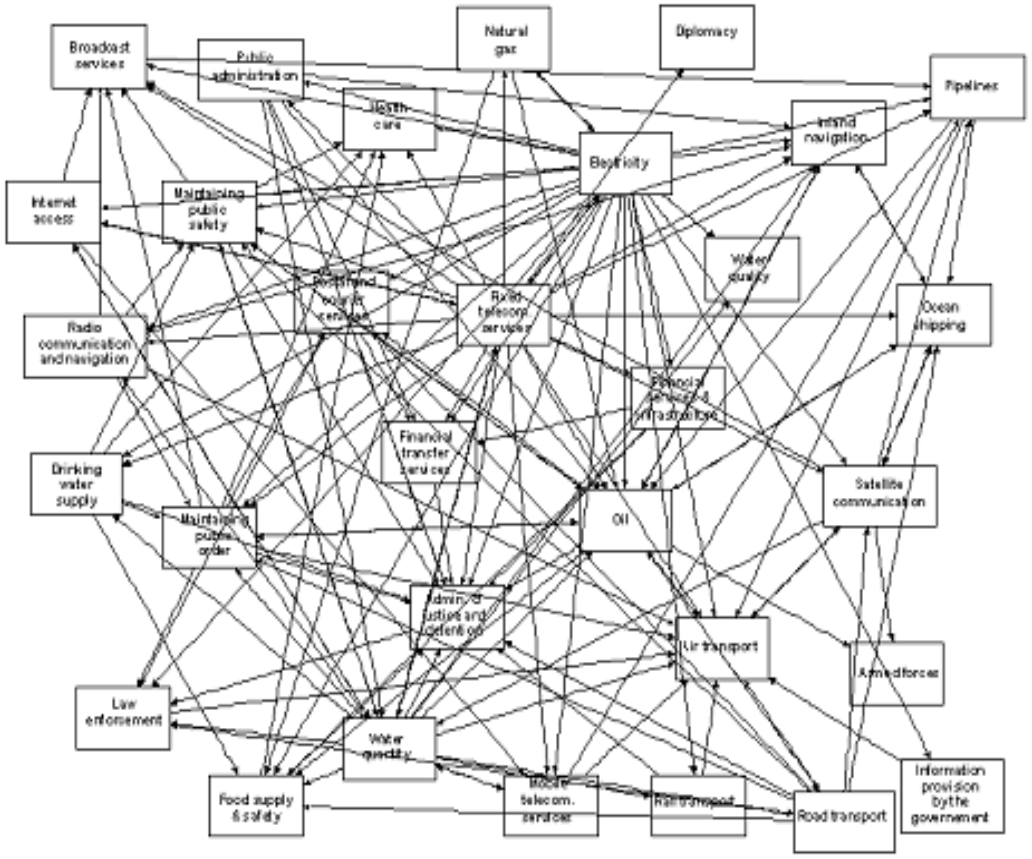


http://solar-photon.com/images/IranCentrifuge.png

Kritische Infrastrukturen

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Figure 4. Critical Infrastructure Inter-Dependencies



Vergleich: Waffen / Cyber Weapons

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Waffe	Nutzer	Speed	Medium	Ziel	Begrenzungen	
Physical	Military	~Km/s	Luft/Boden/ See	physical	Verträge	
Logical	User/PC	c	Cyberspace	Cyber-domain, Dual Use	Selbstbe-schränkung/ Verhaltens-regeln	

- Die Unterscheidung von militärischen und nicht-militärischen Zielen ist im Cyberspace schwierig
- Cyber Weapons haben andere Eigenschaften als traditionelle militärische Waffen
- Ein Cyberangriff kann erfolgen, ohne den Angriff oder den Angreifer zu identifizieren (unsichtbarer Gegner)

3. Reaktionen von Staaten:

USA:

- Pentagon: US Cyber Command seit 2010, „volles Spektrum“, Plan X
- DARPA: 2013-2017: 1.54 Milliarden USD „Cyberbudget“
- State Department: „Intern. Zusammenarbeit“ aber „sich und Partner verteidigen“
- Department of Homeland Defense: Schutz kritischer Infrastrukturen

Russland und China:

- „Information Operations“, Militär-Doktrin, asymmetrisch, **wenig bekannt**
- Vorschlag für einen Vertrag in den VN

Deutschland:

- Nationale Cyber-Sicherheitsstrategie (23. Februar 2011)
- Cyber-Abwehrzentrum und nationaler Cyber-Sicherheitsrat
- Cyber-Außenpolitik: Konferenz Dezember 2012
- Bundesamt für die Sicherheit in der Informationstechnik (BSI)

Internationale Organisationen:

Vereinte Nationen

- Erster Hauptausschuss der General assembly
- Group of Governmental Experts: 1. Bericht 2. Weitere Gruppe

OSZE:

- Konferenz, Vertrauensbildende Maßnahmen

NATO

- Kein Artikel V. Mechanismus
- Co-operative Cyber Def. Centre of Excellence (CCDCOE) Tallin 2008
- Diverse Einheiten, Boards: CDMA, NCSA
- Training, Übungen, Seminare

Europäische Union:

- ENISA: European Network and Information Security Agency NISA

Andere: ITU, OECD etc.

Cyber Armeen ?

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- U.S. Cyber Command: 40.000 auch fähig für Angriffe?
- China-Hacker: 150.000 ?
- Nordkorea ?
- Russland: 50.000?
- andere Staaten? Frankreich, Deutschland
- 120 Staaten wird Web-Spionage nachgesagt (McAfee 2007)

Zukünftige Konflikte können von Cyber-Angriffen begleitet werden. Die Frage ist, welchen Schaden (insbesondere ökonomischen) sie anrichten sollen? Abschreckung?

Untersuchung von 133 Staaten (CSIS)

- **36 Staaten ohne eine Debatte über militärische Rolle**
- **33 beziehen Cyberwarfare in ihre militärische Planung und Organisation mit ein:**

  Erwähnung in der Militärdoktrin für

  - Aufklärung
  - Informationsoperationen
  - Unterbrechung von kritischen Netzen/Diensten
  - Cyberangriffe komplementär zu elektronischer Kriegsführung

- **12** Staaten haben (USA) bzw. wollen demnächst Cybercommands einrichten: Argentinien, Brasilien, China, Dänemark, Deutschland, Indien, Iran, Kanada, Schweiz, Südkorea
- **Cyber Defense ist eine Sorge für viele Staaten**

Reaktionen und Administration der BW

- Seit 1992 **präventive** Cyberabwehr in IT-Sicherheitsstrategie
- Speziell ausgebildete IT-Sicherheitsbeauftraggte in allen Dienststellen
- Bundesamt für Informationsmanagement und Informationstechnik in der Bw (IT-AmtBw)
- 2002 CERTBW eingerichtet (IT-AmtBw)

Krisenmanagement, Angriffserkennung, Schadensbegrenzung

- Risiko-Management Board
- Kommando: Strategische Aufklärung: Abt. CNO
- Erste Fähigkeiten zum Wirken in gegnerischen Netzen“ ???

4. Welche Beschränkungsmaßnahmen sind im Cyberspace machbar?

Individuell: AntiViren-Programme, Firewall, Awareness, Authentification, Malware Scanners, Cryptography

Lokale Netze: Intrusion Detection Systems

Industrie: Bessere Produkte. Höhere Sicherheitsstandards, Koordination

National: Frühwarnung, CERT-Team Zusammenarbeit, Attribution/Forensik, militärischer Einsatz, Abschreckung

International: Nutzung des HVRs, Vertrauensbildung, Internationale Konventionen, Markierung von humanitärer Kritischer Infrastruktur?

Rechtliche Regelungen:

- **VN-Charta: Art. 2.4**

„*Alle Mitglieder unterlassen in ihren internationalen Beziehungen jede gegen die territoriale Unversehrtheit oder die politische Unabhängigkeit eines Staates gerichtete oder sonst mit den Zielen der VN unvereinbare Androhung oder Anwendung von Gewalt*“

Wenn angegriffen, haben sie Selbstverteidigungsrecht Art. 51

- **Genfer Konventionen (1949, 1977, 2005):**

Regeln zur Kriegsführung: Schutz von Personen, Hospitälern etc.

- **Budapester-CyberCrime Konvention (2001)**

„gemeinsame Politik zur Verbrechensbekämpfung zum Schutz der Gesellschaft gegen Cyberverbrechen“

Kontrovers ist, ob „Cyberwar“ als irreguläre Kriegsführung angesehen wird oder nicht. Definitionen /Rechtsstatus nicht klar

Internationales Recht

Jus ad bellum:

1. Wann können Cyberangriffe zu einer **internationalen Bedrohung** werden und zu Gewalteinsatz führen? (Staaten/UN)
2. Wann kann ein „bewaffneter Konflikt“ den Einsatz nötiger und proportionaler Selbstverteidigung rechtfertigen?
3. Sind Rüstungskontrollregelungen auf den Cyber Space anwendbar und welche Einschränkungen bringen sie mit sich?

Jus in Bello (Humanitäres Völkerrecht)

1. Können die Regeln und Prinzipien, die für die klassische Kriegsführung gelten, auf “Cyberwarfare” übertragen werden?
2. Was folgt daraus für den Schutz der Zivilbevölkerung bzw. des Militärs im Kriegsfalle?
3. Welche Gegenmaßnahmen sind erlaubt?

Was ist ein Cyber-War ??

Cyber-Krieg: umfassender Angriff auf IT-Netze eines oder mehrerer Länder im Cyberspace

Cyberkriegsführung sind „*Aktionen eines Staates, um die Computer oder Netzwerke eines anderen Staates zu durchdringen, um Schaden oder Unterbrechung zu verursachen***“** [1]

[1] Richard Clarke; R. Knake: Cyber War: The Next Threat to National Security and what to do about it?, New York 2010, S.12

Regeln im Cyberspace

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

1. **Territorial-Regel:** Die I&K-Infrastrukturen auf dem nationalen Territorium sind Bestandteil der jeweiligen staatlichen Souveränität.
2. **Verantwortungs-Regel:** Die Tatsache, dass ein Angriff von dem Staatsterritorium ausgeht, ist ein Beweis, dass der Akt diesem Staat zugerechnet wird.
3. **Kooperations-Regel:** Daraus ergibt sich, dass der Verursacherstaat mit dem betroffenen Staat kooperiert.
4. Jeder Staat hat das Recht sich **selbst zu verteidigen.**
5. **Persönlicher Daten-Schutz** gewährleistet**?**
6. Pflicht zu **Selbstschutz** und **eigener Sicherheitsvorsorge**
7. **Frühwarnregeln** für potenzielle Zielstaaten
8. Pflicht zur **Information der Öffentlichkeit** vor/bei Bedrohungen
9. Einbeziehung von CyberCrime in **nationale Gesetze**
10. **Aktion/Regulierung** fußen auf dem Mandat einer Organisation

Quelle: E Tikk, Survival 3/2011

Vertrauensbildung:

Sicherheits-/Friedenspolitische Maßnahmen

- (Un-)verbindliche Erklärungen bis hin zum Vertrag
- Arbeitsgruppen (Frühwarnung)
- Informationsaustausch bzgl. Angriffen
- Basis-Standards Internet-Regeln, best Practices
- Cybercenter

Rechtliche und technische Massnahmen

- Auslegung der Regeln des HVRs: Markierung geschützter Bereiche
- Awareness (Industry, User)
- Early Warning
- International CERT-Coordination
- Attribution Scanning

Vorschläge:

- **VN und OSCE arbeiten an:**
  - „Vertrauensbildenden Maßnahmen“ (GGE)
- **Russland und China:**
  - „International Code of Conduct for Information Security“
- **World Federation of Scientists**
- **Einige Staaten:**
  - bilaterale Konsultationen
- **International Telecommunication Union**
- **Clarke: „Cyber Treaty“:**
  - verbietet Angriffe auf zivile Ziele