IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Cyber War Revisited - Die internationale Dimension der Cyberdebatte

Götz Neuneck (neuneck@ifsh.de)

1. „Is Cyberwar Coming?“
2. Cyberattacks: Hype oder reale Bedrohung?
3. Reaktionen von Staaten
4. Regulationen und Beschränkungen

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.

Chancen und Gefahren

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, Freizeit, …..

Gefahren:

- Cyberkriminalität (z.B. Phishing) → Organisierte Kriminalität
- Cyberterrorismus?/ Cyberpropaganda?
- Cyberspionage/Sabotage
- Cyberwar/cyber warfare? „Virtual Arms Race“

Cyber War is Coming?

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

„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

„Ich habe oft gesagt, dass es eine große Wahrscheinlich-keit gibt dass das nächste **Pearl Harbour** mit dem wir konfrontiert sind, ein Cyber Angriff sein kann“

CIA Director Leon Panetta bei der Nominierung zum Verteidigungsminister, 9. Juni 2011

Cyber War is Coming?

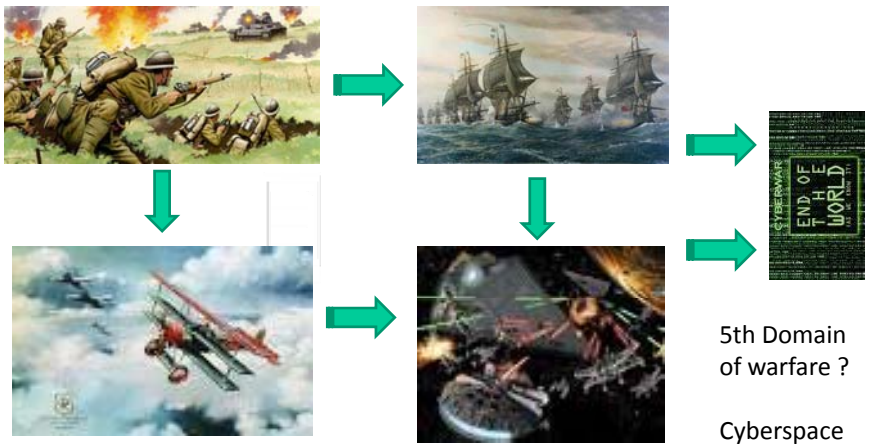
IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Cyber attacks have been „escalated from an issue of moderate concern to one of the most serious threats to our national security. We now live in a world of weaponized bits and bytes, where **an entire country can be disrupted by the click of a mouse**“ **General Martin Dempsey, Chairman JCS**

„Let‘ s say you take an action. **We depend on this stuff more than anyone else**. We`re more vulnerable than anybody else in the world. …Most of the communications in the world flow through the United States and we are the biggest user and beneficiary. So there‘s a great hesitancy to use anything in a cyber context because **it‘s relatively easy** to punch in a pretty aggressive way.“ **Mike McConnell, Booz Allen Hamilton**

“Armed Conflict will migrate form land to cyberspace”

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg



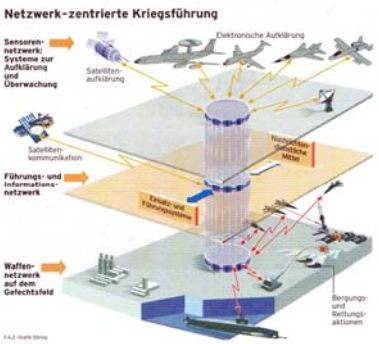
5th Domain of warfare ?

Cyberspace

Revolution in Military Affairs: Using Cybertechnologies

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- **Drone Warfare**
- **Net-centric Warfare**
- **Precision-guided weapons**
- **Integration of Technologies**
- **Asymmetric Situations**
- **Effects and Concerns:**
  - Uses space capabilities
  - Netted weapons/soldiers
  - Attacks on infrastructure



War and Warfare

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

War is direct, somatic violence between (non)-state actors

Wars occur when states in a situation of social conflict and opposition find that the pursuit of incompatible or exclusive goals cannot be confined to non-violent modes

The Penguin Dictionary of Int´l Relations 1998

"War is thus an act of force to compel our enemy to do our will"

Carl von Clausewitz

Many types: inter-state, civil, conventional, WMD, ……

Warfare: Set of techniques used by a group to carry out war

2002-2011: 4 inter-state wars, 73 state-based (37 in 2011)

22.500 war casualties in 2011 SIPRI Yearbook 2012

More effects: failed states, poverty, disorder etc.

$1.756 billion **global military expenditures** (2,5% BIP)

Einführung: Offene Fragen

- Ist ein Cyberkrieg möglich?
- Wird an Cyberwaffen geforscht?
- Findet ein digitales Wettrüsten statt?
- Wird das „Internet“ zu einem neuen Medium oder Mittel der militärischen Kriegsführung?
- Welche Anstrengungen unternehmen Staaten für den Cyberangriff und die Verteidigung?
- Welche internationale Maßnahmen können längerfristig eingeführt werden, um eine „Bewaffnung des Cyberspace“ zu verhindern?

Was ist der Cyberspace ? „ man-made and expanding“

Internet, WWW, kritische Infrastrukturen…….

„Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infra-structures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security“

White House: The National Strategy to Secure Cyberspace, 2003

4 layer model:

- Physical: PCs, Server, Router, satellites, sea cabel
- Logical: Software, „code“
- Content: Information and Data
- Social: governments, civil society

Was ist ein Cyber-War ?

Heute:

- **Cyber Spionage (Diebstahl von Daten → Datenschutzregeln**
- **Cyber Sabotage (Unterbrechen von Diensten (Estland 2007))**
- **Cyber Exploitation (Heimliches Stehlen und Unterbrechen)**
- **Bombardierung von IT-Installationen**

Cyber-Krieg: umfassender Angriff auf IT-Netze eines oder mehrerer Länder im Cyberspace, der zum Verlust von Menschenleben führt.

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

Cyber war: Different Phases and Preparations

In peacetime:

- Espionage, sabotage as preparation of cyber war?
- „pre-crime“ prevention by surveillance
- → Ambiguity, suspicion and escalation possible

In a crisis:

- Cyberattacks on military communication ?
- Escalation to a war?

In a war situation:

- Preventive cyber attacks?
- Preventive conventional attacks on cyberspace components?
- Is strategic cyber war possible?

Mehrere Debatten

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Verschiedene Diskurse überlagern sich:

- **Internet Governance: Macht und Organisation**
  - Zugang, Kontrolle, Abschalten, Zensur
  - ITU or ICANN: Vereinte Nationen oder Selbstregulation
- **Kritische Infrastrukturen:**
  - Disruptive Unterbrechung oder Zerstörung von Krit. Infrastrukt.
- **Militarisierung des Internet**
  - Spionage, Sabotage, Psy Ops etc.
- **Kriegsführung mit oder gegen das Internet:**
  - Internet als Teil oder Ziel der Kriegsführung

2. Cyberangriffe:

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Was sind Cyber Angriffe ? Spachgebrauch ?

- 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

Akteure

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- **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

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

Verschiedene Grade von Cyberangriffen

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

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

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

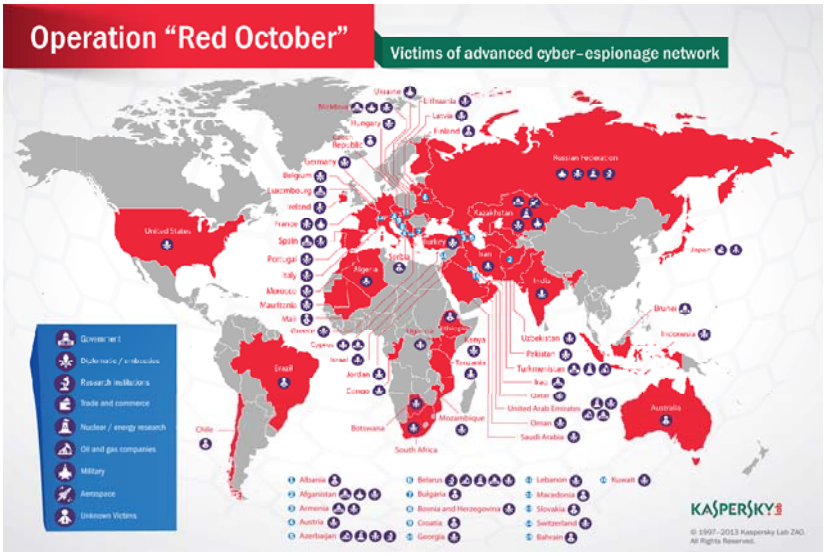
Trojaner:
- nützliches Programm hat ein Schadprogramm „im Bauch“,
- verbreitet sich nicht selber, Datenverlust unbemerkt

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

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

Operation Red October in Russia

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg



National Security Agency and GCHQ (UK)

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- 13 Agencies
- 2013$ 53 billion (1998: $26,6 bill)
- 200 cables tapped 2010
- 29 Petabyte „touched" (1,6%) of data traffic 1,826 Pb
- 7 Tb analyzed daily (.0004%)

Intelligence Cycle:

- 6,3 bio. for Data Processing/ Exploitation
- Build-in Backdoors
- Influence on Standards/Cryptography

Welche Cyber Waffen sind denkbar?

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

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

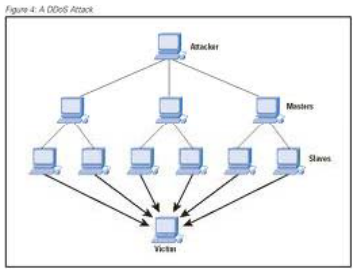
Bewusste „physische“ Angriffe (EM-Strahlen):
- Bomben
- EMP-Waffen, HERF-Guns
- Störsender (Jammer)

Angriffsarten:

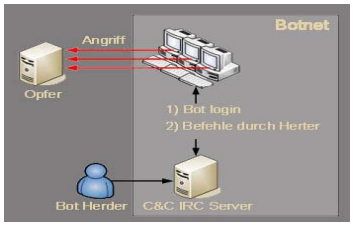
IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Phishing:

Denial-of-Service-Attacken (DOS)



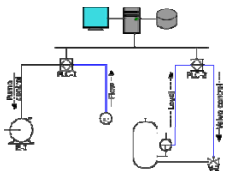
Bot-Netz Angriffe:

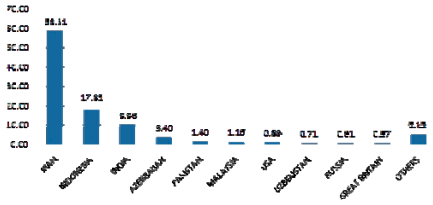


Animationsfilm (6 Min):
https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/BotNetze/botnetze_node.html

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 von WIN-Sicherheitslücken („0-Day-Expl“)
- 3 Infektionswellen ausgehend von 5 iranischen Einrichtungen
- 24 Siemensanlagen (Mitteilung Siemens 11.03.2011)

„Olympic Games“

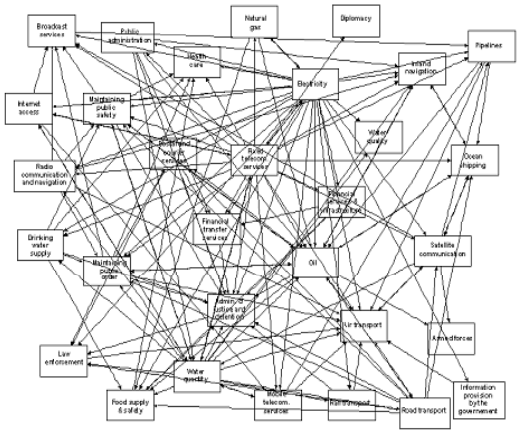
IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- 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

Kritische Infrastrukturen

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Figure 4. Critical Infrastructure Inter-Dependencies



UHH 4. Dezember 2013 19

Charakteristika von Cyberwar:

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- Potential von Cyberwaffen ? (Aufwand, Dauer, Ziel und Effizienz)
- Offensive Dominanz ?
- Detektion und Attribution
- Technologische Volatilität (Proliferation)
- Selbstabschreckung?

UHH 4. Dezember 2013 Seite 26

3. Reaktionen von Staaten - Überblick -

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

USA:

- Pentagon: US Cyber Command seit 2010, „volles Spektrum“, DARPA 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. Code of Conduct

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)

Vereinigte Staaten

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- *WH: International Strategy for Cyberspace, Mai 211*

  „open, interoperable, secure, reliable information“ (S.8)
- *Pentagon: Strategy for Operating in Cyberspace, Juli 2011*

  “DoD will fully integrate a complete spectrum of cyberspace scenarios into exercises and training” (S. 6)
- Verantwortung: DHS, FBI, Cyber Command, 13 agencies
- DARPA Forschung: „Foundational Cyberwarfare“ Plan X 2013-2017: 1.54 Milliarden USD „Cyberbudget“
- *Presidential Decision Directive* PDD-20 (Top Secret)
  - Definitionen: Cyberspace , Defensive /Offensive Cyber Effects Operations (D/OCE) und Verantwortungsbereiche

Vereinigte Staaten

PPD-20: 20/10/12 (secret): „A new Tool of Warfare?“

- Developing „Offensive Cyber Effects Operations“ OCEO
- Developing a target list
- Approval by POTUS for cyberops if „significant consequences“
- USG has mature capabilities for cyber collection

Tailored Access Operations (TAO) of NSA

- 600 person unit operational since 1998
- Sophisticated hacking software, 60.000 attacks worldwide
- Penetrated Chinese ICT systems for 15 years

Defense Science Board Study 2013 recommends

- To develop world class cyber offense capabilities,
- an expanded legion of „cyber warriors“ and
- ensuring a nuclear strike capability in the face of an „existential cyber attack“?

Bundeswehr

Reaktionen und Administration der BW

- Seit 1992 **präventive** Cyberabwehr in IT-Sicherheitsstrategie
- Speziell ausgebildete **IT-Sicherheitsbeauftragte** 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“ ???

Bundeswehr „Strategische Aufklärung“

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Kommando Strategische Aufklärung in Gelsdorf

- Fernmeldetruppe EloKa seit 2002
- 5.500 Soldaten und 500 Zivilbeschäftigte
- „Abteilung sat-gestützte Aufklärung“
- Der Kernauftrag des Kommandos ist die Unterstützung der Informations-bedarfsdeckung der BW und Aufklärung
- 2009: **Abt. für Information/CNO**
- 76 Personen
- Übungen und Entwicklung für offensive Cyberfähigkeiten

Untersuchung von 193 Staaten (UNIDIR/CSIS/IFSH)

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- **114 (68) Staaten haben nationale Cybersecurity Programme**
- **67 Staaten haben zivile und 47 Staaten militärische Programme**
- **41 Staaten 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

UNIDIR: The Cyber Index; Genf 2012

- **27 (12)** Staaten haben bzw. wollen demnächst Cybercommands einrichten: z.B. Argentinien, Brasilien, China, Dänemark, Deutschland, Indien, Iran, Kanada, Schweiz, Südkorea etc
- **6** Staatenveröffentlichten militärische **Cyberstrategiedokumente**
- **17** entwickeln **offensive** Cyberaktivitäten

Cyber Armeen ? Pressezahlen

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)

4. Welche Beschränkungen sind möglich ?

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

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?

Regulations, Limitations, Preventio

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- Raising user awareness (Knowledge? Industry?)
- Capacity Building (Less developed Countries)
- Prevention and Early Warning (Surveillance?)
- „Defense“ (Resilience, Firewalls, Encryption)
- „Offense“ (Cyberweapons, Cyberdeterrence)
- Crisis Managment and Damage Limitation

Prevention:

- Code of Conduct (Which norms? Definitions)
- Arms Control Regulation (No First Use)
- Strengthening International Humanitarian Law

35

Internationale Organisationen:

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

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.

Vorschläge:

- **VN und OSCE arbeiten an:**
  - „Vertrauensbildenden Maßnahmen“
- **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

UN Group of Gov`l Experts 2013

- 15 experts: P5 + ARG, AUS, EGY, EST, GER, IDO, IND, JPN,
- *“to study possible cooperative measures in addressing existing and potential threats”*
- *“to elaborate CBMs and norms, rules or principles of responsible behaviour of States”*
- agreed on 4 categories to promote a “*peaceful, secure, open and cooperative ICT environment*”
  - Universal Legal Framework: (IHL, Art. 51 UNCh etc.)
  - Building Transparency and Trust (CBMs, Comm. Links)
  - Exchange views and information (incl. private sector)
  - Support international capacity building

UN General Assembly, Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security” A/68/98, June 24, 2013.

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?

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 im Cyberspace...

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- Schaffung und Implementierung von **praktikablen Normen und verantwortungsvollem Verhalten** von Akteuren (Staaten)
- Verhinderung eines **Kriegsausbruchs** und **Kriseneskalation**
- Steigerung gegenseitigen Vertrauens durch Berechenbarkeit und **Frühwarnung**
- Längerfristig : Erarbeitung von verbindlichen R**üstungskontroll-maßnahmen** im und für den Cyberspace
- Erarbeitung von gemeinsamen Grundlagen/Sprache in Bezug auf neue Cybergefahren (Capacity building, gemeinsame Definitionen)
- Hilfe beim Schutz von nationalen /internationalen Krit. Infrastrukturen

Vertrauensbildung:

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Sicherheits-/Friedenspolitische Maßnahmen

- (Un-)verbindliche Erklärungen bis hin zu einem 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

Transpareny and Confidence Building Measures

IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Schaffung von politischen, rechtlichen und militärischen Begrenzungen für die „Stationierung“ und den Einsatz von militärischen offensiven Cybermitteln

- **„Best practices“:**
  - OSCE Cyber Doktrin Seminar könnte diskutieren:
  - Gemeinsame Definition für gemeinsames Verständnis
  - Besuche von Militärs und gemeinsame Übungen
- **Risk Reduction Maßnahmen:**
  - Aufbau von Risk Reduction Centern (Datenaustausch)
  - Aufbau von regionalen/globalen Frühwarnmechanismen
- **Capacity Building:**
  - Gemeinsame Übungen von CERTs, Weitergabe von Wissen
- **Cyber Convention ?**

Einige Schlussfolgerungen

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

1. Es besteht die Befürchtung, dass Konflikte auch verstärkt im Cyberspace (bewaffnet?) ausgetragen werden.
2. Vorbereitungen für „offensive Cyberoperationen“ von Staaten werden unternommen. Ihr Einsatz bricht ein Tabu.
3. Es fehlen klar definierte Normen und Regeln sowie erprobte Konfliktlösungsmechanismen.
4. Ein Normbildungsprozess und die Diskussion von VBM regional wie global ist dringend nötig
5. Dialog, Erziehung, Kooperation müssen verstärkt werden.
6. Ein digitales Wettrüsten muss verhindert werden
7. Die internationale Staatengemeinschaft muss verstärkt Anstrengungen unternehmen, den Cyberspace „friedlich, zuverlässig und sicher“ zu organisieren

Letzte Worte …….

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

„The potential misuse of this power is terrifying high, to say nothing of the dangers introduced by human error, data-driven false positives and simple curiosity.“

„Fighting for Privacy is going to be a long, important struggle. We may won some battles, but the war is far from over“ Eric Schmidt, the New Digital Age