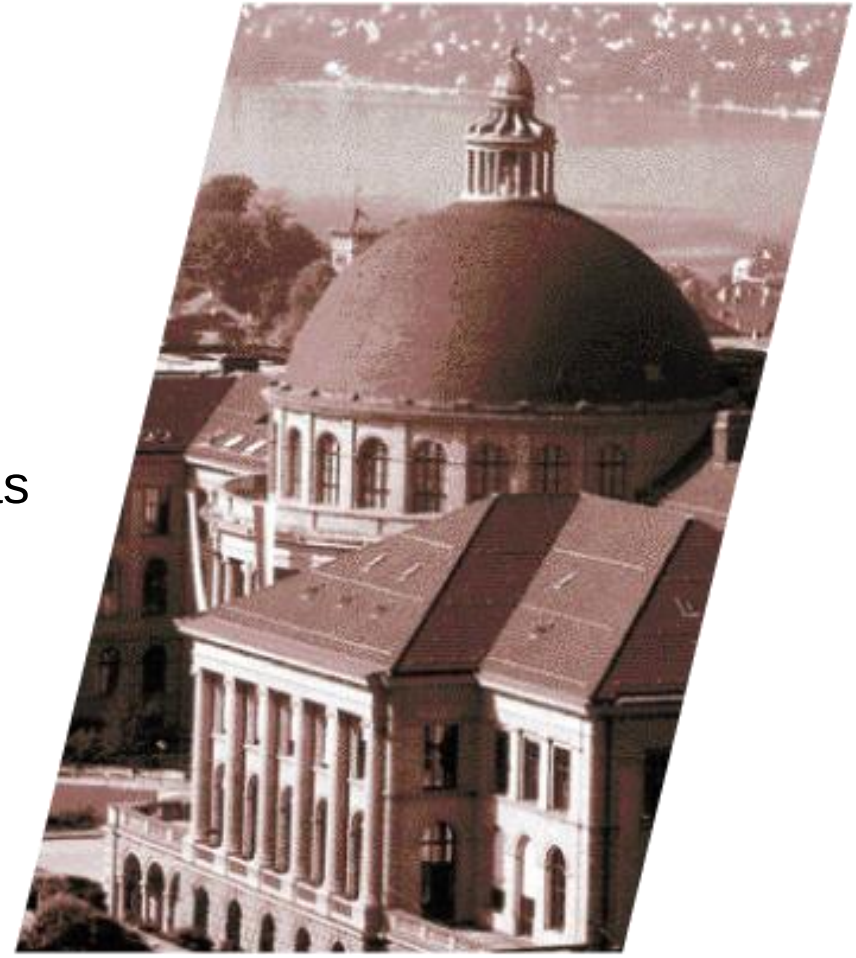
# CENTER FOR SECURITY STUDIES

Swiss Federal Institute of Technology (ETH Zurich)



## Cyberwar: was ist die Gefahr, was ist Hype?

Myriam Dunn Cavelty
25 Oktober 2010

donna informatica

# Struktur

- Stuxnet: der digitale Erstschlag? Ja? Nein? Jein?
- Warum macht der Vorfall so Angst?
  - Geschichte der Cybersecurity und ihr Werdegang hin zu einem sicherheitspolitischem Thema
- Cyber-Eskalationsstufen
- Ein Versuch, die Gefahr einzuschätzen
- Gefahr der Cyberangst (und ihre Gründe)
- Lösungen

# Stuxnet: Der digitale Erstschlag?

- Stuxnet: Computerwurm, entdeckt im Juli 2010
- Sehr komplex, sehr teuer (Schätzung (Symantec): 8-10 Programmierer waren 6 Monate beschäftigt, 7stelliger Dollarbetrag Kosten)
- Untypisches Verhalten für Malware: kein Datendiebstahl, keine Botnet-Funktion, keine möglichst grosse Verbreitung
- Sabotage von Industrieanlagen
- Hoher Befall im Iran / Verzögerungen im Atomprogramm: Ziel Bushehr?

→ Staat steckt dahinter (USA? Israel?)!

→ Cyberwar ist Realität geworden!

# Wirklich?

- Von “hoch spekulativ” (Lagner) zu “es kann sein, dass” (Computerzeitschriften) zu “sicher” in der allgemeinen Presse
- Wir wissen, dass wir nichts wissen (Attribution)
- Es ist wahrscheinlich, dass wir nie wissen werden (Verifikation)

- Aber: Angst vor Cyberwar breitete sich gegenwärtig rasant in Europa aus

- Woher kommt die Tendenz zum Hype im Bereich Cyberwar und damit einhergehend die Tendenz zur Überreaktion im politischen Bereich?

# Informationssicherheit – ein sicherheitspolitisches Problem?

- Sicherheitspolitik beschäftigt sich mit Überlebensfragen bzw. „existentiellen“ Bedrohungen
- Viren und Würmer, SPAM sowie Hackerangriffe sind isoliert betrachtet keine existentielle Bedrohung, auch wenn sie kosten
- Warum wird Informationssicherheit heute trotzdem weltweit als ein **sicherheitspolitisches** Problem betrachtet? Welche Charakteristiken hat die Gefahr?

# Hintergrund

- "We are at risk. Increasingly, America depends on computers. [...] Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (National Academy of Sciences, "Computers at Risk", 1991, p. 7).
- Sowohl die Generierung, die Verwaltung als auch die Verwertung von Information nehmen in unserer Gesellschaft einen immer höheren Stellenwert ein
- Industrienationen stellen hochgradig vernetzte Systeme dar, welche in ihrer Leistungserbringung stark abhängig sind vom reibungslosen Funktionieren der eingesetzten Informations- und Telekommunikationstechnologien



- Ängste um Computersicherheit sind kein Phänomen der 1990er Jahre
  - Viren und Würmer seit Mitte der 80er (Morris)
  - Computerkriminalität (Kevin Mitnick, Captain Crunch)
  - Frühe Hacker-Vorfälle (414s, Operation Sundevil “The Hacker Crackdown” )
  - Film: „War Games“ (1986)
  - Kultur: Cyperpunk
  - Spionage: „Cuckoo‘s Egg“ Vorfall (1988-1989)

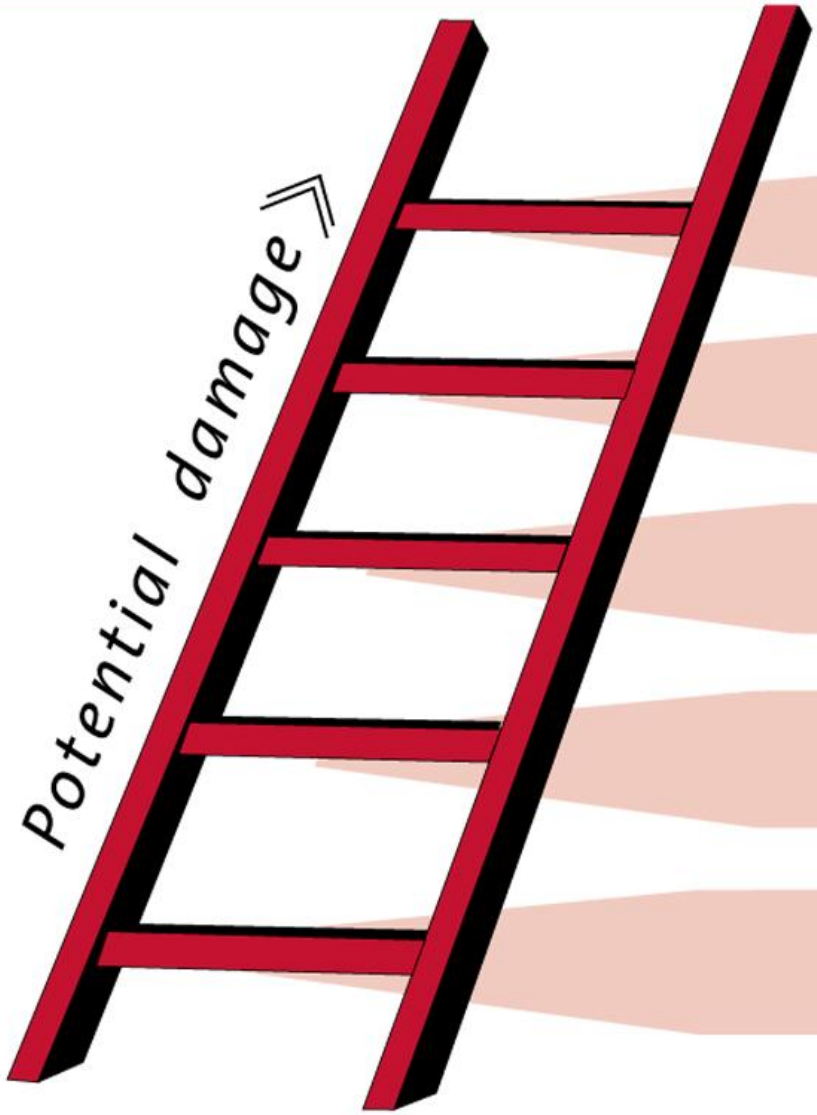
# Cybersecurity und Nationale Sicherheit: 1990er

- Zunehmend vernetze Systeme
- Erfahrung im Golfkrieg von 1990/91
- Quantitative Zunahme von IT Vorfällen (Statistiken)
- Militär/ Pentagon vermehrt Ziel von Angriffen
  - 1994, Rome Lab incident
  - 1998, Solar Sunrise
  - 1998, Moonlight Maze
- Übungen: 1996, RAND "The Day After" Exercise / 1997, Eligible Receiver
- PCCIP: President's Commission on Critical Infrastructure Protection (1997)



- Die moderne Gesellschaft stark vom reibungslosen Funktionieren der Informationsinfrastruktur abhängig
- Sie ist
  - wichtiger Bestandteil der ökonomischen Wertschöpfung,
  - vernetzendes Führungselement zwischen Elementarbereichen,
  - Grundvoraussetzung für das Funktionieren von Infrastrukturen
- Kritische Infrastrukturen:
  - „Organisationen 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“

# Types of Cyberconflict




CYBERWAR

CYBERTERRORISM

CYBERESPIONAGE

INTERNET CRIME

CYBERVANDALISM

CSS Analysis in Security Policy No. 71, April2010 (Center for Security Studies)

# Eskalationsstufen

- Cybervandalismus / Hacktivismus: Kombination von „hacking“ und Aktivismus, beinhaltet Angriffe auf Internetseiten, um Ziele zu erreichen.
  - Beispiele: Web „sit-ins“, virtuelle Blockaden, automatisierte Email-Bomben, Web Hacks, Computer Break-ins, Viren, Würmer, DoD Attacken.
- Internetkriminalität: vielfältige Erscheinungsformen, Straftaten, die auf dem Internet basieren oder mit den Techniken des Internets geschehen
- Cyberspionage: Spionage mit Hilfe von Computern / moderner ICT
- Cyberterrorismus: “generally understood to mean unlawful attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. [A]n attack should result in violence against persons or property, or at least cause enough harm to generate fear”.
- Cyberwar: von Staaten gegen Staaten geführte Computer Network Attacks

# Gefahr oder Hype?

- Läutet Stuxnet eine neue Ära des Cyberwar ein?
- Cyberwar hat viele Vorteile, wenn man ihn mit dem konventionellen Krieg vergleicht: billiger, weniger blutig, etc.
- Aber: Wie verwundbar ist die (kritische) Infrastruktur wirklich?
  - Mangel an Daten und Erfahrung
  - Grosse praktische Schwierigkeiten
  - Haben Akteure überhaupt ein Interesse daran anzugreifen? (Blowback Effekte, Weltwirtschaft, etc.)
- Unklare zukünftige Entwicklung: Die Frage von wer-wie-wo-was-warum-wann kann kaum beantwortet werden

# Cyberangst (und ihre Gründe)

- Szenarios, in denen hackende Terroristen Tod und Verwüstung anrichten schüren sog. Cyberangst
- Psychologische Gründe:
  - Willkürliche terroristische Gewalt
  - Misstrauen gegenüber Computertechnologie
  - Massenmedien schüren die Angst
- Ökonomische Gründe:
  - Neue Einkommensquellen für IT-Firmen
  - Neue Gelder für think tanks
- Politische Gründe:
  - Politische Instrumentalisierung, Versicherheitlichung eines Themenfeldes
  - Führt zur Ausweitung der Regierungskompetenzen
  - Ende des Kalten Krieges

# „Neue“ Risiken

- Gefahrenperzeption muss gesehen werden im grösseren Zusammenhang einer substantiellen Verbreiterung des wahrgenommenen Gefahrenspektrums nach Ende des KK
- Federführend bei dieser sicherheitspolitischen Neuorientierung waren Strategen in den USA, die den Blick verstärkt auf nichtstaatliche Akteure lenkten, die mit terroristischen Anschlägen eine Bedrohung darstellen könnten
- Beunruhigend an diesem „neuen Gegner“ war, dass er nicht mehr klar und mit gängigen nachrichtendienstlichen Mitteln identifiziert werden konnte.
- Als Folge davon begann man, Unsicherheitsabschätzungen verstärkt von der wahrscheinlichen Gefährlichkeit der Mittel abhängig zu machen, die zur Verfügung stehen *könnten*

# Und was heisst das nun?

- Vorsichtig sein, keine „Cyberangst“ zu schüren
  - Führt zu Platitüden und unnötiger Hysterie
  - Kann Lösungsfindung verhindern
- Schutzpraktiken, wie sie heute bestehen, sind auf gutem Weg
  - Zusammenarbeit über Public-Private Partnerships verstärken und pflegen
  - Stete Bemühung um mehr Sicherheit durch Risikoanalysen
- Gefahr immer wieder neu einschätzen
- Forschung im Bereich stärken
  - Interdisziplinäre Sichtweise nötig: Tunnelblick vermeiden

# Contact Details

## Danke!

Dr. Myriam Dunn Cavelty
Center for Security Studies
dunn@sipo.gess.ethz.ch