Proseminar

„Ethische Aspekte der Informationsverarbeitung“
WS 2003/2004
(Prof. Dr. W. Kurth)

Informations-Krieg / Information Warfare

(Referent: P. Brinkmann)

Definition(en)

- Handlungen, deren Ziel es ist einen Informationsvorteil gegenüber einem/dem Gegner zu erhalten
(Informationen, informationsverarbeitende oder informationsbasierende Prozesse, Informationssysteme oder computerbasierte Netzwerke beeinflussen)
Joint Chiefs of Staff

- IK/IW besteht aus Handlungen, deren Ziel es ist Daten oder Datenverarbeitung zu schützen, zu korrumpieren, auszunutzen, zu verweigern oder zu zerstören um einen entscheidenden Vorteil gegenüber einem Gegner zu erhalten
Alger

- Konflikt zwischen zwei Parteien, in dem IT das Hauptmittel ist um einen Vorteil zu erringen
King

Geschichte/Entwicklung des IK

- Informationsvorteile seit Urzeiten von Bedeutung in Konflikten
-> Späher/Kundschafter, Spione, etc.

- gewinnen mit weiteren Entwicklung von Datenübertragung an Bedeutung
(Feuer-/Rauchsignale, Telegraphie (optisch, später elektronisch), Telekommunikation, Übertragung optischer Informationen)

- Boten/Späher/Läufer

- Feuersignale (Griechen)

- Telegraphstationen (Napoleon)

- elektrische Telegraphie

- Digitale Bilder

- Satelliten/Spionagesonden

- Datenverarbeitung (Ver- und Entschlüsselung, später Auswertung)

- Enigma

- Computer
- Text- später immer feinere Bildanalyse und –verfälschung
(Bsp. Morphen)

Wandel im Militär
("RMA" <- "Revolution in military affairs")

Die „Revolution" bezieht sich teilweise auf das Vermögen/Können von Präzisionswaffen und die Kontrolle eigener Truppen, und darüber hinaus - vielleicht zum bedeutenderen Teil – auf eine technologische Änderung in der Ver-/Bearbeitung und Nutzung von Daten über den Feind und sein Territorium.

Beispiele:

- Präzisionsschläge
- Aufklärung (Sonden, Satteliten)
- De-/Moralisierung / generelle Beeinflussung
- Verringerung direkter Feindkontakte

IK – Offensive und Defensive (allgemein)

Offensive:

- physische Zerstörung von Informationen, -systemen und/oder Netzwerken
- unerkannte Infiltration gegnerischer Informationssysteme um Daten, -verarbeitung zu manipulieren

Defensive:

- Bedrohungseinschätzung (Möglichkeiten, Motive)
- Bedrohungseindämmung (Demotivierung, Schutz eigener Infrastruktur)

Typologie

(Stufe 1)	Zerstörung von kommandorelevanter Ausrüstung mittels herkömmlicher Mittel
Stufe 2	Beeinträchtigung der Arbeit des gewählten Ziels (DoS)
Stufe 3	Zerstörung bzw. Entwertung des Inhalts eines Informationssystems („malware“)
Stufe 4	Infiltration mit dem Ziel Spionage
Stufe 5	Unbemerkte Manipulation von Daten – Ziel: „mind games“

Eindringen:
- packet sniffers („Abhör“-programme für den Datenverkehr)
- password grabbers (gespeicherte/eingegebene Passwörter weiterleiten)
- password crackers (Zum umgehen von Sicherheitsabfragen)
- password guessing (Passwort-(er)raten)
- social engineering ()

Manipulation:
- trojan horses ()
- logic bombs (Ein mit einem Auslöser gekoppeltes Programm)
- trap doors (Falltüren)
- computer viruses (Comp.-viren bezeichnen umgangssprachlich eine Vielzahl von schädlichen Programmen)
- worms („Würmer“ sammeln Daten und verbergen sich mit diesen)

Dadurch entstehende Asymmetrie

- Abhängigkeit großer Armeen von komplexen Informationssystemen
- IK-Angriff unabhängig von militärischer Stärke

- Unterentwickelte Infrastruktur -> IK-Angriff wirkungsloser

Vorteil des Angreifers:

- Unregelmäßige Angriffe (Herkunftsorte, Ziele)
- „Unsichtbarkeit“
- Keine Warnung/Vorzeichen
- Keine Verzögerung /unmittelbarer Angriff
- Flüssiger Wechsel zwischen den Angriffsmodi
- Fähigkeit Frequenz und Intensität des Angriffs zu wechseln
- Vervielfältigungseffekte
- Einfache Abwägung
- Ziel in Defensive
- Ziel muss Streuschäden vermeiden/eindämmen
- allgemein Änderung im Verhalten erzwungen
- Ziel u.U. in Reaktionen eingeschränkt

Wegfall einiger herkömmlicher Aspekte

- Reichweite
- Umwelt (herkömmlicher Sinn)
- Logistik

Neue Aspekte

- Anonymität
- unbegrenzte Reichweite

Gesetzliche und ethische Aspekte

Bisher keine internationalen und kaum nationale Regelungen

Beispiel:

Eine Falschmeldung in der ein gemorphter Anführer seine Truppen zur Kapitulation aufruft

Auszug zu klärender Punkte:

- Erstschläge
  (Was ist als Angriff zu werten? Darf es Erstschläge geben?)
- Angriffe auf zivile Ziele

- Definition zivile/militärische Ziele
  (Kompliziert, da die Verflechtung tiefgehend und komplex ist)
- Beziehung Schaden – Angriff (Verantwortung)
  (Welcher Schaden geht zulasten des Angriffs? … des Verteidigers?)
- Ausmaß von gerechtfertigten Gegenschlägen

- Gerichtsbarkeit internationaler Angriffe

- internationale Kooperation (Angriff als auch Abwehr)

(letzten beiden Punkte sind sehr komplex, da selbst nationales Recht diesbezüglich noch in Kinderschuhen steckt)

Beispiel hierzu:

1992 attackierten Schweizer Hacker ein Supercomputerzentrum in den USA und konnten nicht von USA dafür belangt werden.

Infrastrukturelle Verwundbarkeit

- IK nicht nur militärisch relevant
  (Informationsterrorismus)

- Vernetzung in wirtschaftlichen Bereichen ebenfalls vorangeschritten

- Faktoren: Energie, Verkehr, Bank-, Finanzwesen, …

- Notwendigkeit auch zivile Systeme/Netzwerke zu schützen
  (in Regel verwundbarer als militärische Ziele)

- Umfassende Analyse (Schwachstellen, Knoten-/Schlüsselpunkte, -systeme)

- Beispiel: in USA entstand NIPC (sitz derzeit im FBI, kritisiert)

- „Information surety“ („I-verlasslichkeit/-sicherheit)
  (Schutz, Sicherheit, Verlässlichkeit, Integrität, Authentifizierung)

- Definition:
  IS beginnt bei der Bestimmung von Konsequenzen bestimmter Störungen, gefolgt von der Erkennung kritischer Knotenpunkte, die so wichtig sind, dass ihr Versagen ernste Folgen hätte und endet bei der Skizierung von Schutzmechanismen und der Berechnung der Kosten um diese Punkte zu schützen. …
  Dadurch sollen die Kosten von Unterbrechungen unabhängig von der Störungsursache ermittelt werden können.
  Robinson

IK in der Wirtschaft

Teile des IK aus Wirtschaftalltag

- Betrug
- Spionage
- DoS
- Suck-Sites

- Verschlüsselung
- Firewalls

- Internet/Intranet

mögliche Aggressoren:
Konkurrenten, Hobbyhacker, Kriminelle, feindliche Regierungen, ehemalige Angestellte, …

mögliche Ziele:
Daten bzw. Informationssysteme zerstören, manipulieren oder ausspionieren

durch IK entstandene **neue Wirtschaftszweige**

- Firewall, Ver-/Entschlüsselung

- Anti-Spyware

- Spyware

- …

- Ansir ("Awareness if National Security Issues and Response Program")

“Ziviler Informationskrieg”

- Internet als Plattform auch Einzelpersonen zugänglich (Megafon)

- wird weitestgehend auch genutzt

  - „Netz-basierter Aktivismus“
  - „Hacktivismus“
  - „Cyberterrorismus“

Beispiel:
- EDT
  (Vereinigung, die mittels „Fluten“ gegen bestimmte Seiten/etc. vorgeht. (DoS))
- 1998 Angriff auf Pentagon
- Reaktion: DoS-Angriff, dann von Öffentlichkeit scharf kritisiert

Informationsterrorismus

I-ter. bezeichnet allgemein die Nutzung des Internets durch Terrororganisationen

(Soziale) Bewegungen Online/im Internet

Beispiele:

- Amnesty International
  http://www.amnesty.de/

- Greenpeace
  http://www.greenpeace.de/

- ATTAC
  http://www.attac.de/

- …

Persönlicher IK

Cyber-Stalking

"*Cyberstalking is defined as the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals.*"
(http://www.cyber-stalking.net/about_cyberstalking.htm)

Cyber-impersonation

Unkenntlich machen der (eigenen) Identität

ID-theft

Annehmen der virtuellen Identität eines anderen

Digitale Diffamierung

Erstellen/Verbreiten von diffamierenden Seiten/Daten/Emails

Hackbacks

(Automatischer) Gegenangriff

Quellen

„Information warfare: peering inside Pandora's postmodern box"
(Library Review, V50 N6 2001 pp. 279-294
MCB University Press ISSN 0024-2535)
http://www.tukkk.fi/tjt/OPETUS/TJTS11/Kirjallisuusartikkelit/Article%201.pdf

http://www.albany.edu/~rs6021/research/

http://www.cyber-stalking.net/

http://www.amnesty.de/

http://www.greenpeace.de/

http://www.attac.de/