Proseminar "Ethische Aspekte der Informationsverarbeitung"

Thema 19:Cyberkriegs-Debatte und Verwundbarkeit

[Ralf Bendrath]

Lu, Guo

Inhalt

Einleitung

- Die Dynamik der Informationstechnologien wird als globalisierte Medienökonomie der entstehenden Wissensgesellschaft begriffen, auch als Risiko betrachtet.
- Die große Abhängigkeit moderner Industrienationen von informationstechnischen Systemen macht sie anfällig für Störungen durch verschiedene Ursachen.
- Die zunehmende Abhängigkeit der westlichen Staatenwelt von funktionierenden Kommunikationssystemen und die immer höhere Saturierung und Durchdringung dieser Gesellschaften durch Medien eröffnen eine neue Ebene der Konfliktaustragung.

Cyberkrieg im Cyberspace

Cyberkrieg

- Der Krieg findet mittels Software und Hardware auf Computer- und Informationssystemen der gegnerischen Streitkräfte statt.
- Im Zentrum steht jedoch immer die Verarbeitung von Daten, Informationen und Wissen.

Waffen

- Werkzeuge aus dem Bereich der Informatik.

Ziel

- Die Computersysteme des bzw. der Gegner so zu beeinträchtigen, dass sie nicht ihren Zweck erfüllen. Dabei können im einfachsten Fall rechnergestützte Verbindungen lahmgelegt werden.

Gründe

- Patriotismus und Zorn.

Bedingungen

- Nach dem Land, der See, der Luft und dem Weltraum scheinen kriegerische Auseinandersetzungen auf der Basis von digitalen Informationen im Cyberspace möglich.
- Herstellung verursacht geringe Kosten und bietet schwächeren Staaten (z.B. China) das Potenzial, im

Rahmen einer asymmetrischen Kriegsführung die zivile oder militärische Infrastruktur stärker vernetzter Gesellschaften zu treffen.

Verwundbarkeit des Cyberspace in den USA

- Auf diesem Gebiet am verletzlichsten.
- Viele Mittel in Kapazitäten zum Führen von Cyberkriegen investiert.
- klassisches Sicherheitsdilemma: andere Staaten werden versuchen, einer möglichen Bedrohung durch diese amerikanischen Kapazitäten entgegenzuwirken.

Neuer Rüstungswettlauf

- welcher durch den globalen Charakter des Mediums Internet und durch die relativ geringen Einstiegskosten ein ungeahntes Ausmaß annehmen könnte.

Debatte zum Thema Cyberkrieg

Die Debatte, wie sie sich etwa Mitte der neunziger Jahre darstellte, basierte auf drei grundlegenden Annahmen:

1. wachsende sicherheitspolitische Ungewißheit über mögliche Gegner, verbunden mit der unkontrollierbaren Diffusion von Software und Know-How über Cyber-Angriffstechniken;
2. wachsende militärische Angst vor der elektronischen Verwundbarkeit der US-Streitkräfte, basierend auf einer möglichen asymmetrischen Cyberkriegführung durch konventionell unterlegene Gegner;
3. anarchische Struktur des Internet als sozialer Raum, der sich staatlichen Kontrollversuchen und damit auch dem staatlichem Sicherheitsbedürfnis zu widersetzen schien.

Untersuchung zur Verwundbarkeit

Für eine Verwundbarkeitsuntersuchung zu prüfende, wichtige Variablen:

- die erwartete Abhängigkeit einzelner oder der Gesellschaft von bestimmten Techniksystemen,

- das mögliche Schadensausmaß eines Versagens der Technik, oder eines gelungenen Missbrauchs,

- die Möglichkeiten, das potenzielle Schadensausmaß zu vermindern oder Missbrauchsmöglichkeiten auszuschließen.

- aber auch die sozial begründete Verlässlichkeit solcher Sicherungsmaßnahmen und ihre sozialen Auswirkungen.

Netwar, Infowar und Cyberkriege

Unterschied zwischen Netwar und Cyberkriegen

- In den USA wird zur konzeptionellen Differenzierung von Information Warfare daher folgerichtig zwischen Netwar und Cyberkrieg getrennt.
- Während Cyberkrieg im herkömmlichen Sinne kriegerische Aktivitäten gegen die Informationsinfrastruktur eines Gegners bedeutet, werden unter Netwar Aktivitäten außerhalb bewaffneter Auseinandersetzungen verstanden, bei denen die Sabotage der Infrastruktur zur permanenten Bedrohung wird.
- Die Netwar-Definition integriert alle Aspekte einer Kriegsführung im Cyber- und Infospace in eine Theorie.
- Erweitert wird überdies der Kreis jener, die als Gegner in einem Netwar gesehen werden. Zu den möglichen Konfliktparteien werden nun auch Umwelt- oder Menschenrechtsgruppen gezählt.

Unterschied zwischen Cyberkriegen und Infowar

- Ein Cyberkrieg richtet sich dabei nach dem hier vertretenen Begriffsverständnis gegen die Infrastrukturen.
- Ein Infowar hingegen setzt an den in diesen Infrastrukturen übertragenen Inhalten an.

Arten von Cyberangriffen

Web-Vandalismus

- Webseiten verunstalten, die häufigste Art des Cyberangriffs, leichte Form der Verletzung.

Propaganda

- Politische Meldungen können rasch verbreitet werden durch das Internet.

Vermischung von Dateien

- Vertrauliche Information abfangen und sogar modifizieren.

Distributed Denial-of-Service Attacks:

- Als DOS (zu Deutsch etwa: Dienstverweigerung) bezeichnet man einen Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen.
- In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von Verteilter Dienstblockade bzw. DDoS (Distributed Denial of Service).
- Normalerweise werden solche Angriffe nicht per Hand, sondern mit Backdoor-Programmen oder Ähnlichem durchgeführt, welche sich von alleine auf anderen Rechnern im Netzwerk verbreiten und dem Angreifer durch

solche Botnetze weitere Wirte zum Ausführen seiner Angriffe bringen.

Angriff auf kritische Infrastrukturen

- Telekommunikation, Energieversorgung, Finanzwirtschaft, Transport, Rettungsdienste und öffentliche Verwaltung sind die Objekte, die in Cyberkriegen angegriffen werden.
- Aufgrund der Komplexität der heutigen Technik fällt eine Einordnung eines entstandenen Schadens zunehmend schwer.

Der erste Cyberkrieg

Hackerangriffe gegen estnische Webserver

- Am 27. April 2007 begann eine Welle von Hackerangriffen gegen estnische Webserver. Hinter den Angriffen wurde von estnischer Seite der russische Staat verdächtigt, was die Ereignisse zum ersten Angriff eines Staates auf die Internet-Infrastruktur eines anderen gemacht hätte.

Auslöser des Krieges

- Estland wollte ein russisches Kriegerdenkmal in Tallinn verlegen.

Verlauf

- Während in Tallinn estnische Russen am Denkmal protestierten und es zu gewalttätigen Auseinandersetzungen kam, blockierten russisch-nationale Jugendbewegungen die estnische Botschaft in Moskau. DoS-Angriffe legten viele Webseiten der estnischen Regierung, aber auch von Zeitungen, Banken oder Unternehmen lahm.
- Estland ist eines der am stärksten auf das Internet setzenden Länder der EU und Vorreiter beim e-Government. Die Angriffe haben auch nach drei Wochen nicht aufgehört.
- Viele Websites sind weiterhin vom Ausland aus unzugänglich, weil Zugriffe aus dem Ausland blockiert werden, um die Angriffe abzuwehren. So wurde erst die Website der zweitgrößten Bank angegriffen, nachdem eine Woche zuvor bereits Hansapank, die größte Bank, zum Ziel von DoS-Angriffen wurde. Hillar Aarelaid, der Leiter von CERT **(**Computer Emergency Response Team**)** Estonia, weist darauf hin, dass die neuen Angriffe zwar aus der ganzen Welt kämen, aber wohl immer noch von Russland aus gesteuert würden.

Nachwirkungen und Fazit

- Das Denkmal wurde an einem anderen Ort wieder aufgestellt.
- Die Auffassung herrscht vor, dass die öffentliche Darstellung von Mitteln und Wegen zur Manipulation oder Störung grundlegender IT-Funktionen vermieden werden sollte.
- Diskussionen um Cyberkriege und terroristische Angriffe im Internet sollten potenziellen Tätern weder szenarische Anregungen noch praktische Hilfestellungen bieten.
- Ein so verlaufender Diskurs führt am eigentlichen Ziel der systematischen und proaktiven Absicherung digitaler und von ihnen abhängiger analoger Systeme vorbei.
- Die freiwillige Beteiligung von Internet-Usern an Botnetzen zeigt, dass Anwender nicht nur lernen müssen, wie sie ihre Systeme technisch schützen (etwa durch sicher konfigurierte Firewalls und aktuelle Antivirenprogramme), sondern auch, welch verheerende internationale Auswirkungen es haben kann, wenn man sich unbedacht an DDoS-Attacken im Rahmen politischer Aktionen beteiligt und einem noch größer angelegten Cyberkrieg den Weg bereitet.

Literatur

- Ralf Bendrath: The cyberwar debate: Perception and politics in US critical infrastructure protection. http://cms.isn.ch/public/docs/doc_705_259_en.pdf (1. 4. 2006).
- Carsten Kaefert :der erst cyberwar, Kapitel 3: Estlands Ankunft im Westen und der Denkmalstreit mit Russland. http://www.scribd.com/doc/1153957/Der-erste-Cyber-War (7. 5. 2007)
- Olivier Minkwitz: Ohne Hemmungen in den Krieg? HSFK-Report, Seite 24: Die Wirkung von Computernetzwerkangriffen auf Normen der Kriegsführung. http://edoc.vifapol.de/opus/volltexte/2007/201/pdf/report1003.pdf (1. 10. 2003)
- Krieg-Jörg Wollscheid: Postmoderner Krieg, Seite-118: Netzwerke und Netwar_Die Weiterentwicklung der Organisationsschemata durch die Kriegsführung der dritten Welle, Seite-135: Cyberwar und Infowar. http://www.politik.uni-trier.de/pubs/prom/Postmoderner_Krieg_Web.pdf (27. 8. 2004)
- Martin Kahl: Strategische Kontexte des Cyberwar in den USA, Kapitel 2: Vorbereitung auf den Cyberwar.

http://www.ifsh.de/IFSH/printversionen/gesamtliste.html (Jan. 2001).

- Ralf Bendrath: Interview zum Thema "Cyberwar". http://de.wikipedia.org/wiki/Cyberwar (Juni 2006).
- Ute Bernhardt und Ingo Ruhmann: Überwachung der Überwacher, Seiten 2, 3. http://www.heise.de/tp/r4/artikel/6/6768/1.html (Sept. 2002).
- Christian Mölling & Götz Neuneck: Präventive Rüstungskontrolle und Information Warfare. Kapitel 5: Information Warfare und präventive Rüstungskontrolle. In: Rüstungskontrolle im Cyberspace. Perspektiven der Friedenspolitik im Zeitalter von Computerattacken. Dokumentation einer Internationalen Konferenz der Heinrich-Böll-Stiftung am 29./30. Juni 2001 in Berlin, S. 47-53.
- Ute Bernhard / Ingo Ruhmann: Krieg und Frieden im Internet. http://www.heise.de/tp/r4/artikel/6/6271/1.html (letzter Zugriff 14. 4. 2008).
- Peter Ansorge / Ralf E. Streibl: Computer und Krieg. FIfF-Texte, http://fiff.informatik.uni-bremen.de/ruin/10jahre.htm (letzter Zugriff 14. 4. 2008).
- **http://www.wikipedia.org**: Cyberwar. (Feb. 2008).
- **http://archive.infopeace.de**

Ralf Bendrath: USA und Estland wollen gemeinsam gegen Cyber-Attacken vorgehen (http://archive.infopeace.de/msg03903.html, letzter Zugriff 14. 4. 2008).

Ralf Bendrath: "Cyber Command" soll Überlegenheit der USA im Cyberspace sichern (http://archive.infopeace.de/msg03891.html, letzter Zugriff 14. 4. 2008).