

Risiken und Chancen der elektronischen Kommunikationstechnologien

ein Thesenpapier der Jusos Gießen

Daniel Guterding

4. April 2009



Inhaltsverzeichnis

| | |
|---|----------|
| I. Einleitung | 3 |
| II. Analyse | 3 |
| 1. Der Alltag in der Informationsgesellschaft | 3 |
| 2. Soziale Netzwerke | 4 |
| 2.1. Struktur und Funktion | 4 |
| 2.2. Risiken bei der Benutzung | 5 |
| 3. Internetkapitalismus | 6 |
| 4. Googles Meinungsmonopol | 6 |
| 5. Das Internet als Mittel gesellschaftlicher Teilhabe am Beispiel Estlands | 7 |
| 5.1. Allgemeine Situation | 7 |
| 5.2. Angriff auf die estnische Internetinfrastruktur vom 27. April 2007 bis 18 Mai 2007 | 7 |

| | |
|--|-----------|
| 5.3. Unmittelbare Folgen des Angriffs | 8 |
| 5.4. Schlussfolgerung | 8 |
| 6. Internet und Terrorismus | 9 |
| 7. Das Verhältnis von Staat und Internet | 9 |
| 8. Was bleibt übrig vom Traum der Völkerverständigung ? | 10 |
| III. Prognose und Ausblick | 11 |
| IV. Anhang | 13 |
| A. Quellen | 13 |

Teil I.

Einleitung

Die Bourgeoisie reißt durch die rasche Verbesserung aller Produktionsinstrumente, durch die unendlich erleichterte Kommunikation alle, auch die barbarischsten Nationen in die Zivilisation. Die wohlfeilen Preise ihrer Waren sind die schwere Artillerie, mit der sie alle chinesischen Mauern in den Grund schießt, mit der sie den hartnäckigsten Fremdenhass der Barbaren zur Kapitulation zwingt. Sie zwingt alle Nationen, die Produktionsweise der Bourgeoisie sich anzueignen, wenn sie nicht zugrunde gehen wollen; sie zwingt sie, die sogenannte Zivilisation bei sich selbst einzuführen, d.h. Bourgeois zu werden. Mit einem Wort, sie schafft sich eine Welt nach ihrem eigenen Bilde. [1, 1]

Selbst Marx und Engels konnten die wirtschaftlichen und gesellschaftlichen Folgen der Weiterentwicklung der Kommunikationstechnologien nur ansatzweise abschätzen. Und doch entspricht das, was wir heute Globalisierung nennen und durch die fortschrittliche Kommunikationstechnologie möglich wurde, den Beobachtungen der beiden Philosophen.

Neue Möglichkeiten basisdemokratischer Partizipation, jedoch auch neue Mechanismen der Ausgrenzung entstehen. Kommunikationstechnologie reißt Mauern ein, schafft jedoch auch neue.

Im folgenden möchte ich dieses Technologiegebiet näher betrachten, gesellschaftliche Auswirkungen aufzeigen und eine Prognose für die Zukunft geben.

Teil II.

Analyse

1. Der Alltag in der Informationsgesellschaft

So wie das Telefon die Kommunikation zwischen Personen und Unternehmen vereinfacht hat, vereinfacht nun das Internet den Zugriff auf Information. Im Vergleich zu Büchern sind Informationen durch moderne Suchalgorithmen (Google) und offene Wissensdatenbanken (Wikipedia) schneller, einfacher und in komprimierter Form abrufbar. Wissen ist so für alle Menschen mit einem Internetanschluss leichter verfügbar also noch vor 15 Jahren. Scheinbar wurde im Internet das Wissen der Menschheit gesammelt, katalogisiert und demokratisiert. Ebenso wurde die Kommunikation weiter erleichtert. Waren über das Telefon nur Gespräche mit wenigen Personen gleichzeitig möglich und mussten alle Gesprächspartner zur gleichen Zeit anwesend sein, so ist durch E-Mails (auch SMS) und Text-Chats asynchrone Kommunikation mit vielen Menschen gleichzeitig möglich.

Während viele Menschen diese Art der Kommunikation als unpersönlich empfinden, ist im Internet eine Vielzahl neuer Möglichkeiten zur Partnersuche entstanden, die von

¹aus dem *Manifest der Kommunistischen Partei*

Millionen Menschen genutzt wird.

Ein ähnliches Phänomen sind sogenannte „soziale Netzwerke“, in denen sich Menschen ähnlicher Interessen leichter und unverbindlicher zusammenfinden können als dies beispielsweise in einem realen Verein möglich wäre. Diese „sozialen Netzwerke“ bilden die Grundlage des sogenannten „Web 2.0“, das jedem Internetnutzer ermöglichen soll, die Inhalte des Internets mitzugestalten.

2. Soziale Netzwerke

2.1. Struktur und Funktion

Soziale Netzwerke umfassen Diskussionsplattformen („Foren“), Wissensdatenbanken (Wikipedia), Personenverzeichnisse (StudiVZ, Facebook, etc.), Videoportale (YouTube, etc.), Webtagebücher („Blogs“) und Karriereplattformen (Xing).

Foren führen im allgemeinen anonyme Diskussionsteilnehmer mit ähnlichen Interessen zusammen. Wissensdatenbanken wie Wikipedia haben sich zur Aufgabe gemacht Wissen zu sammeln und zu katalogisieren. Die daran teilnehmenden Personen eint vor allem das gemeinsame Ziel einer möglichst fehlerfreien und umfassenden Datenbank. Sowohl in Foren als auch Wikis tritt der soziale Aspekt hinter den eigentliche Zielen der Teilnehmer zurück. Dennoch beruht ihr Erfolg auf der Synergie zwischen den Fähigkeiten vieler Einzelpersonen.

Charakteristisch für Foren und Wikis ist eine hierarchisch organisierte Qualitätssicherung. Beiträge werden kontrolliert, korrigiert und zensiert. Entweder um Beleidigungen und bewusste Falschaussagen zu entfernen oder um inhaltliche Fehler auszumerzen.

Wikipedia hat Versuche unternommen z.B. Entscheidungen über die Löschung von Artikeln durch Abstimmungen zu demokratisieren. Dabei muss jedoch bedacht werden, dass Abstimmungen innerhalb der Gemeinschaft der Wikipedia-Editoren längst nicht das Meinungsspektrum der Wikipedia-Nutzer wiedergeben können. Der Kreis der Editoren steht zwar theoretisch jedem offen, bleibt jedoch aufgrund des damit verbundenen Zeitaufwandes dem Nutzer, der nur schnell etwas nachschlagen möchte, verschlossen und damit elitär.

Grundsätzlich anders strukturiert sind Personenverzeichnisse und Videoportale. Meistens sind diese kommerziell betrieben, wobei die Leistung der Nutzer darin besteht das vom Betreiber bereitgestellte technische System mit Inhalten zu füllen oder zumindest dem Betreiber persönliche Informationen bereitzustellen. Den Anreiz zur Teilnahme stellt dabei für viele Menschen die Möglichkeit zur Darstellung ihrer eigenen Person und die Möglichkeit die Selbstdarstellungen anderer zu lesen und anzuschauen dar. Die Nutzer nehmen also keineswegs anonym teil, sondern veröffentlichen Informationen bewusst unter ihrem realen Namen, damit diese mit ihrer real existierenden Person in Verbindung gebracht werden.

Eine Qualitätskontrolle findet oft nur rudimentär statt und ist weder vom Betreiber, noch von der Mehrzahl der Nutzer erwünscht. Die Nutzer empfinden den besonderen Reiz des Systems oft darin, dass niemand die Richtigkeit der gemachten Angaben überprüft

und somit aus ihrer Sicht alles möglich ist, während der Betreiber möglichst viele Informationen über die Nutzer und deren Interaktion gewinnen will.

Die Karriereplattform Xing stellt insofern einen Sonderfall eines Personenverzeichnisses dar, als dass die Nutzer größtenteils beruflich relevante Daten bereitstellen und sich vor allem als qualifizierte Arbeitskräfte präsentieren wollen.

Sogenannte Weblogs stellen meist Tagebücher einzelner oder weniger Personen dar, die diese im Internet veröffentlichen, um möglichst viele Leser zu erreichen. Oft stellen die Autoren dabei weniger persönliche Probleme als gesellschaftlich oder politisch relevante Themen in den Vordergrund. Durch die Veröffentlichung im Internet ist es den Autoren möglich innerhalb kurzer Zeit eine große Leserschaft zu gewinnen.

2.2. Risiken bei der Benutzung

Oft haben besonders die minderjährigen Nutzer von Personenverzeichnissen noch kein Bewusstsein für die möglichen Folgen ihres digitalen Exhibitionismus entwickelt und veröffentlichen privateste und intimste Informationen, die so in die Gemeinschaft des Netzwerks, aber auch in die Datenbank des Anbieters, der diese kommerziell verwenden möchte, gelangen. Probleme des Datenschutzes sind dabei offensichtlich, aber im Bewusstsein der Mehrheit der Nutzer noch nicht angekommen. Die zukünftigen Verwendungsmöglichkeiten für die gesammelten Daten sind vielfältig. So könnte beispielsweise ein Arbeitgeber bereits vor der Einstellung eines potenziellen Mitarbeiters dessen Persönlichkeitsprofil von einem Datendienstleistungsanbieter erwerben, der jenes aus den gesammelten Daten der sozialen Netzwerke zusammengestellt hat, an denen der Bewerber beteiligt ist – die Umgehung aller derzeitigen Datenschutzgesetze oder die Einwilligung des Nutzers vorausgesetzt.

In jüngster Zeit häufen sich die Fälle des sogenannten Cyber-Mobbings, bei dem Personen durch Dritte im Internet bloßgestellt, angegriffen oder diffamiert werden. Dies korrespondiert mit der fehlenden inhaltlichen Kontrolle vieler sozialer Netzwerke. Die Täter benutzen hierbei oft Tarnidentitäten, um sich einer eventuellen Rache zu entziehen.

Ebenso ermuntert die Preisgabe von intimen Informationen und das Angebot zur anonymen Teilhabe am Leben anderer zum sog. Stalking. Dieser Effekt ist von einigen „Opfern“ jedoch erwünscht.

Man kann an dieser Stelle einwerfen, dass die Teilnahme an Personenverzeichnissen und die Veröffentlichung privater Daten freiwillig geschieht. Oft steht der Einzelne dabei jedoch unter Druck. Entweder unter dem Druck der Gemeinschaft des Netzwerks, wenn er vollwertiges Mitglied sein möchte, oder unter dem Druck realer Personen, die ihn zur Teilnahme bewegen wollen. Da eine Nichtteilnahme jedoch auch ein Informationsdefizit in der Realität bedeuten könnte, kann das Gefühl „etwas zu verpassen“ auftreten und dadurch Personen zur Teilnahme bewegt werden.

Neben den Betreibern der sozialen Netze können auch Kriminelle über Sicherheitslücken in der Betreibersoftware an die Datensätze der Nutzer gelangen, diese verwerten und verkaufen. Besonders interessant ist die Möglichkeit der Kombination der einzelnen Verhaltensmuster des Nutzers in sozialen Netzwerken mit (zum Beispiel) den von ihm in

Google eingegebenen Suchbegriffen. Dadurch ist die Erstellung eines umfassenden Profils möglich.

Das kürzliche Erscheinen ganzer Sätze von Kreditkartendaten im Internet zeigt, dass definitiv mit privaten Daten Handel getrieben wird. Dazu kommt, dass Daten, die einmal in das Internet eingegeben wurden, nicht mehr entfernt werden können, da Google nahezu das gesamte Internet speichert. Daher ist im Grunde jede Eingabe auf ihre Folgen hin zu untersuchen. Da die Sicherheit der Daten bei Dritten, die man eigentlich für vertrauenswürdig hält (z.B. Kreditinstitute), leider nicht beeinflusst werden kann, sollte auf alle unnötigen Angaben verzichtet werden. Die Gefährlichkeit der veröffentlichten Kreditkartendaten hätte dies selbstverständlich nicht gemindert.

3. Internetkapitalismus

Besonders die Betreiber von Personenverzeichnissen und Videoportalen wurden innerhalb kurzer Zeit durch eine relativ simple Idee zu Millionären. Wie ist dies möglich?

Der Betreiber muss nur das technische System zu Verfügung stellen. Dieses wird dann nach der Anwerbung einer ersten Nutzerbasis von selbst mit neuen Nutzern und Inhalten gefüllt. Ein Großteil der Arbeit, die den Wert des Produkts ausmacht, wird also nicht nur von Freiwilligen unentgeltlich geleistet, der Betreiber verdient sogar direkt an dieser Arbeit, indem er sie statistisch auswertet oder anonymisiert verkauft. Indirekt verdient er, indem er Werbung für die wachsende Nutzergemeinde schaltet, eventuell sogar personalisiert, deren Wert mit der Gemeinde wächst. So ist es möglich innerhalb kurzer Zeit große Mengen Kapital anzuhäufen ohne Wertschöpfung zu betreiben.

4. Googles Meinungsmonopol

Der Konzern hinter der effizientesten Suchmaschine der Welt hat sich in kürzester Zeit zu einem undurchsichtigen, Daten sammelnden Moloch entwickelt. Durch den bisher unübertroffenen Suchalgorithmus war Google in der Lage sich auf legalem Wege zum Quasi-Monopolisten zu entwickeln. Wettbewerber wie MSN oder Yahoo stellen aufgrund der niedrigen Qualität der Suchergebnisse keine Alternativen dar.

Somit haben Googles Werbeflächen einen unvorstellbaren Wert, da die Webseiten täglich von Millionen Menschen auf der ganzen Welt besucht werden. So wurde es Google mit den Werbeeinnahmen möglich in weitere Bereiche der Internetdienstleistungen zu expandieren. So stellt Google heute auch Systeme für E-Mails (GMail), Terminplanung (Google Calendar), Dokumentenverwaltung (Google Docs), Instant Messaging (Google Talk), Bilderverwaltung (Picasa), Routenplanung (Google Maps) und Nachrichten (Google News) bereit. Zudem expandierte Google mit dem Kauf von YouTube, des größten Videoportals, und der Kooperation mit MySpace, einem Personenverzeichnis, in alle wichtigen Bereiche des Web 2.0.

Somit ist Google in fast allen wirtschaftlich relevanten Bereichen des Internets aktiv, bietet jedoch gleichzeitig das mächtigste Werkzeug zum Durchsuchen des WWW. Dem

Missbrauch ist an dieser Stelle Tür und Tor geöffnet.

Google ordnet alle bei der Benutzung seiner Dienste anfallenden Daten eindeutig der realen Person zu, die die Dienste nutzt. Somit ist es dem Konzern nicht nur möglich, die Bewegungen einer Person im Internet zu verfolgen, sondern über Analyse von Mails und Kalendereinträgen auch das reale Leben zu rekonstruieren.

Genauso ist Google jedoch auch in der Lage, die im Internet abgerufenen Inhalte über die Reihenfolge der Ergebnisse seiner Suchmaschine massiv zu beeinflussen und hierdurch zu bestimmen, wer welche Inhalte des Internets über Google abrufen kann. Somit kann Google nicht nur Meinungen aufzeichnen und analysieren, sondern auch Meinungen schaffen. Insbesondere der Nachrichtendienst Google News zielt auf die Bereitstellung eines zeitungähnlichen Formats aus Artikeln der Internetausgaben verschiedener Tages- und Wochenzeitungen ab, wobei die Artikel von Google ausgewählt werden.

Seit Anfang 2006 arbeitet Google bei der Zensur von Suchergebnissen mit der Volksrepublik China zusammen. Offenbar kann der Konzern den moralischen Anforderungen seiner Stellung nicht gerecht werden.

5. Das Internet als Mittel gesellschaftlicher Teilhabe am Beispiel Estlands

5.1. Allgemeine Situation

Als Estland nach dem Zusammenbruch der Sowjetunion vor einem staatlichen Neuanfang stand, entschied sich das Land die modernste damals verfügbare Kommunikationstechnologie in die Grundlagen des staatlichen Systems einzubinden – das Internet. So können alle Behördengänge per Internet erledigt werden und Wahlen werden auch über das Internet durchgeführt. Die Akzeptanz elektronischer Kommunikation stieg in Estland sehr stark an. Über 90

Estland ist das einzige Land der Europäischen Union, das seiner Bevölkerung einen kostenlosen Internetzugang gesetzlich garantiert. In allen Postämtern und Bibliotheken stehen kostenlose Internetterminals bereit.

Somit wurde eine Entstehung schlecht mit Internet versorgter Gebiete auf dem Lande, die eine Ungleichheit der Zugangsmöglichkeiten zu Verwaltungsstellen und Internetdienstleistungen bedeutet hätte, wirksam unterbunden.

In Estland konnten so durch die Nutzung des Internets Kosten für Unternehmensfilialen und öffentliche Verwaltung erheblich reduziert werden. Filialen und örtliche Ämter wurden eingespart, was die Abhängigkeit vom Internet verstärkte. Umgekehrt wurden diese Stellen jedoch leicht und zu jeder Zeit von zu Hause oder von den vielen öffentlichen Zugangspunkten aus zugänglich.

5.2. Angriff auf die estnische Internetinfrastruktur vom 27. April 2007 bis 18 Mai 2007

Über drei Wochen hielten russische Hacker die Internetseiten der estnischen Regierung und der beiden größten Banken des Landes unter Beschuss. Am ersten Tag des Angriffs

begannen die Angreifer mittels in sozialen Netzwerken verteilter Skripte und mehrerer Botnetze (Vermutlich wurde unter anderen das Botnet „Storm“ benutzt, das manche Experten für den leistungsfähigsten Rechner der Welt halten.) die Rechner der estnischen Regierung durch simple Überlastung unerreichbar zu machen. Der erzeugte Datenverkehr überstieg die maximale Kapazität der estnischen Rechnernetze um mehr als das Tausendfache. Einem solchen Angriff konnte logischerweise nichts entgegengesetzt werden, wenngleich durch falsche Konfiguration einiger Geräte die Effekte des Angriffs unnötig verstärkt wurden.

Begleitet wurden die Angriffe durch anti-estnische Propaganda in vielen russischsprachigen sozialen Netzwerken, wo an Privatpersonen Anleitungen zur Teilnahme an dem Angriff verteilt wurden.

Am 1. Mai wurden die Angriffe auf die Seiten russischer Oppositionsgruppen ausgedehnt und noch weiter verstärkt. Am 4. Mai fiel die Internetseite Estlands größter Tageszeitung aus. Am 6. Mai folgte das Internetportal der größten estnischen Bank – in einem Land, das derart großes Vertrauen in Online-Banking setzt eine Katastrophe.

Am 9. Mai, dem Tag des Sieges der Sowjetunion über das Dritte Reich, erreichten die Angriffe ihren Höhepunkt. Danach verringerte sich die Intensität der Angriffe. Am 16. Mai fiel jedoch auch die Internetseite von Estlands zweitgrößter Bank aus. Am 18. Mai waren schließlich alle Bank- und Regierungsseiten wieder erreichbar.

Eingebettet waren die Internetangriffe in den Kontext von teilweise gewalttätigen Protesten russischstämmiger Estländer gegen die Verlegung eines sowjetischen Kriegerdenkmals in Tallinn.

Die Angreifer traten in keiner Weise mit den Opfern in Kontakt. Es wurden keinerlei Forderungen gestellt, keine Daten gestohlen und keine kritischen Systeme zerstört.

5.3. Unmittelbare Folgen des Angriffs

Die gesamte im Internet organisierte staatliche Verwaltung war fast über den gesamten Zeitraum der Attacke arbeitsunfähig. Zudem wurde der E-Mail-Verkehr des estnischen Parlaments völlig blockiert. An mehreren Tagen brach der elektronische Zahlungsverkehr vollständig zusammen, wodurch es vielerorts nicht möglich war zu tanken oder einzukaufen, da Kreditkarten nicht mehr funktionierten. Die Angriffe auf Seiten von Zeitungen störten den Zugriff auf Nachrichten und sonstige Informationsdienste.

5.4. Schlussfolgerung

An Estland wurde das Modell eines Cyber-Krieges getestet. Eine Beteiligung russischer Regierungsstellen an dem Angriff konnte nicht nachgewiesen werden. Es bleibt jedoch die Vermutung, dass Staaten und Unternehmen in Zukunft mit virtuellen Angriffen zu rechnen haben – durch andere Staaten, Kriminelle, Terroristen und andere Interessengruppen.

Somit muss der Begriff der kritischen Infrastruktur neu definiert werden. Energieversorgung und Militär waren nicht Ziele der Attacke, dafür jedoch der bargeldlose Zahlungsverkehr und die staatliche Verwaltung. Beides wird von der estnischen Bevölkerung

mit großem Vertrauen mittels des Internets genutzt. Durch die Abhängigkeit der staatlichen und wirtschaftlichen Abläufe vom Internet wurden erhebliche Schäden durch Internetkriminelle möglich. Die Verletzlichkeit der elektronischen Kommunikation hat sich damit auf alle Lebensbereiche der Informationsgesellschaft übertragen.

Einem Staat von der Größe Estlands ist es kaum möglich sich wirksam gegen Attacken der aufgetretenen Größenordnung zu verteidigen, da hierfür enorme Überkapazitäten aufgebaut werden müssten.

6. Internet und Terrorismus

Wie der Fall Estland zeigt, wird das Internet immer mehr zur Spielwiese von Kriminellen und Terroristen. Virtuelle Angriffe können reale Gewalt unterstützen, ergänzen oder völlig ersetzen.

Oft ist es unmöglich Verantwortliche zu ermitteln, besonders wenn Rechner Dritter gekapert und für die Angriffe missbraucht werden. Eine Vielzahl an im Umlauf befindlichen Trojanern sorgt dafür, dass die Rechnerbasis der Botnetze, Schwärme gekapert Rechner, die sich ohne Wissen der Eigentümer gegen Entgelt für Attacken nutzen lassen, kontinuierlich wächst.

Sicherheitslücken in weit verbreiteter Software werden von Kriminellen benutzt um Würmer einzuschleusen, die ganze Rechnernetze lahmlegen. Dabei sind die Experten für Computersicherheit oft einen Schritt hinter den Angreifern zurück und können nur auf auftretende Bedrohungen reagieren. Sicherheitslücken sind in komplexen Programmen immer noch zu schwer zu entdecken. Die Durchschnittsqualität verbreiteter Software ist weiterhin zu gering.

Erschwerend kommt für die Sicherheitsfachleute hinzu, dass die Angreifer sich nicht in der Nähe des angegriffenen Objekts befinden müssen. Die zu verteidigende Grenze ist nicht festgelegt. Angriffe sind jeder Zeit von jedem Ort der Welt aus möglich, schließlich ist das Internet öffentlich zugänglich. Die Gefahr für die Angreifer bleibt somit relativ gering. Ebenso hält sich der finanzielle Aufwand für Internetsabotage in engen Grenzen.

Daneben hat das Internet jedoch auch die Kommunikation von Terroristen und Kriminellen untereinander erheblich erleichtert. Persönliche Treffen der an einem Plan beteiligten Personen sind nicht mehr zwingend notwendig. Anleitungen zum Bombenbau sind frei im Internet verfügbar. Propaganda kann weitgehend unkontrolliert im Internet verbreitet werden, was neue Möglichkeiten zur Rekrutierung neuer Mitglieder bietet. Dem internationalen Terrorismus war somit eine weitere Dezentralisierung seiner Strukturen möglich.

7. Das Verhältnis von Staat und Internet

Spätestens seit der EU-Vorgabe zur Vorratsspeicherung von Verbindungsdaten ist klar, dass Staaten das Internet zur Überwachung ihrer Bürger nutzen wollen. Dabei können staatliche Gesetzgebungsverfahren jedoch nicht mit der Innovationsgeschwindigkeit der

Internetgemeinde Schritt halten, weshalb die Avantgarde der Nutzer dem Staat permanent einen Schritt voraus ist.

Angesichts der Entwicklungen im Bereich der sozialen Netzwerke ist einleuchtend, dass der Staat die bereitwillig veröffentlichten Informationen in Kombination mit geheimdienstlich gewonnenen Informationen hervorragend nutzen kann. Es bleibt jedoch die Frage, inwieweit demokratische Verfassungen die nachrichtendienstliche Nutzung der gewonnenen Daten erlauben.

Daneben ist jedoch auch die Möglichkeit einer militärischen Nutzung informationstechnischer Systeme von großer Bedeutung. Moderne Kommunikationstechnologien erleichtern die Koordination von militärischen Operationen ebenso wie diplomatische Kontakte. Durch Satelliten und Drohnen ist es hochtechnisierten Armeen möglich, einen Informationsvorteil gegenüber dem Feind zu erlangen, der den Verlauf von Konflikten entscheidend beeinflussen kann.

Möglich ist auch die Manipulation der Meinung der eigenen und fremden Bevölkerung durch Internetpropaganda.

8. Was bleibt übrig vom Traum der Völkerverständigung ?

Ursprünglich sahen Visionäre das Internet als positive Erfüllung von Marx Vorhersage bezüglich der neuen Kommunikationstechnologien. Das Internet sollte die Völkerverständigung verbessern und demokratische Werte in die ganze Welt tragen. Kultureller Austausch sollte gefördert und autoritäre Gesellschaften revolutioniert werden.

Tatsächlich scheint das Internet die Hoffnungen nicht erfüllt zu haben. Millionen von Spam-Mails verstopfen die Postfächer der Mail-Kunden. Die wirtschaftlichen Schäden durch Spam gehen in die Milliarden. Kriminelle treiben ihr Unwesen. Die größte Nutzung, gemessen am Volumen des Datenverkehrs, erfährt das Internet durch die Verbreitung von Pornographie und anderen urheberrechtlich geschützten Inhalten wie Musik und Filmen. Zudem treten unter Vielnutzern vermehrt Suchterscheinungen auf. Mit dem Internetterrorismus ist eine neue Gefahr am Horizont aufgezogen.

Andererseits hat das Internet das Prinzip der Informationsgesellschaft endgültig Realität werden lassen. Nie war es Nichtregierungsorganisationen und Einzelpersonen leichter sich in der Öffentlichkeit Gehör zu verschaffen. Selbst die Volksrepublik China vermag das Drängen ihrer Bürgerrechtsaktivisten ins Internet nicht mehr aufzuhalten. Die Bevölkerung autoritärer Regime kann im Internet unabhängige Informationen gewinnen.

Und natürlich förderten die neuen Kommunikationstechnologien die Globalisierung und damit das Zusammenrücken der Nationen. Das Internet bleibt ein Ort von Licht und Schatten.

Teil III.

Prognose und Ausblick

Die größte Veränderung des nächsten Jahrzehnts hat Google bereits begonnen. Dienstleister werden vermehrt Werkzeuge im Internet bereitstellen, die fest installierte Programme auf dem lokalen Rechner ersetzen. Googles Suchmaschine, sein Routenplaner oder Wikipedias Enzyklopädie sind die ersten Beispiele für etwas viel größeres, das noch bevorsteht.

In den vergangenen Jahrzehnten sind die Ausgaben für Informationstechnologien in Unternehmen ständig gestiegen. Experten prognostizieren, dass die Entwicklung zu Gunsten spezialisierter Informationsdienstleister verlaufen wird, die den Unternehmen eigene IT-Abteilungen ersetzen, um so Kosten einzusparen. IT-Dienstleistungen würden in Zukunft so einfach verfügbar sein wie elektrische Energie, deren Erzeugung vor über einem Jahrhundert eine ähnliche Revolution erfahren hatte. Dem festgefahrenen Markt der Betriebssysteme und Hardwarekomponenten stehen folglich nach Jahrzehnten des Monopol- bzw. Oligopol große Veränderungen bevor. Jedoch ist zur Gewinnung einer großen Nutzerbasis für die neuen Dienstleistungen eine Erhöhung der durchschnittlichen Zugangsbreiten notwendig.

Ein weiterer Trend, der mit wachsenden Bandbreiten einhergeht, ist das sogenannte Cloud-Computing, d.h. die Verlagerung von Berechnungen vom Einzelrechner auf eine ganze Wolke unabhängiger an ein Netzwerk angeschlossener Rechner. Dies trägt dem wachsenden Bedürfnis an Berechnungskapazität Rechnung. Cloud-Computing stellt einen Weg dar, um den Zwang zur ständigen Erhöhung der Geschwindigkeit von Privatcomputern zu verringern. Da ungenutzte Kapazitäten ohnehin laufender Rechner für sinnvolle Berechnungen genutzt werden könnten, stellt dieses neue Verfahren eine große Hoffnung für viele Wissenschaftler dar.

Mit der Einführung von Datendienstleistungen stellen sich für den Nutzer jedoch neue Fragen. So muss in der Wolke geregelt werden, wer auf welche Daten zugreifen kann und was privat ist. Der Nutzer kann eventuell nicht mehr feststellen, welche Informationen sich noch unter seiner Herrschaft befinden und welche davon auch anderen Personen bekannt sind.

Die Problematik des Datenschutzes wird in Bezug auf die freiwillige Veröffentlichung persönlicher Informationen neu diskutiert werden, wenn die ersten Bewerber auf eine Stelle aufgrund ihrer Google-Suchanfragen und Einträge in Personenverzeichnissen abgelehnt werden.

Ohnehin kommt dem zukünftigen Verhalten einiger weniger Unternehmen große Bedeutung zu. Wenn Google weiterhin seine Vorherrschaft in den Bereichen des Ordens von Informationen und des automatisierten Erkennens von Zusammenhängen behaupten kann, wird vom Verhalten dieses Unternehmens der Erfolg oder Misserfolg von Bürgerrechtsbewegungen und vielen anderen Internetkampagnen abhängen. Falls Google seine Macht eines Tages politisch nutzen sollte, kann dem vielleicht kein Staat mehr etwas entgegensetzen, weil er Gefahr läuft, dass Google die Bevölkerung durch gezielte

Weitergabe von kompromittierenden Informationen gegen bestimmte Politiker aufwiegelt.

Man wird sehen, ob Microsoft sein Betriebssystem an die neuen Anforderungen anpassen kann. Der Online-Händler Amazon wird vielleicht zu einem Pionier des Cloud-Computings. Eine erste Implementierung dieses Prinzips unter dem Namen „Amazon Elastic Compute Cloud“ existiert bereits. Oder gewinnen nach langer Zeit des Schattendaseins doch die Unix-ähnlichen Systeme wie Linux die Oberhand ? Wird IBM die richtigen Konzepte für Cloud-Computing Rechner finden können ? Die nächsten Jahre versprechen für die IT-Branche eine interessante und turbulente Zeit.

Teil IV.

Anhang

A. Quellen

Literatur

- [1] Karl Marx, Friedrich Engels: *Manifest der Kommunistischen Partei*. Verlag Philipp Reclam jun., Stuttgart, 2005.
- [2] Nicolas Carr: *The big switch: rewiring the world, From Edison to Google*. W. W. Norton & Company, New York, 2008.
- [3] Hartmut Rosa: *Im Wirbel der Beschleunigungsspirale*. Spektrum der Wissenschaft 02/08, S. 82-87.
- [4] Lee Feigenbaum et al.: *Mein Computer versteht mich – allmählich*. Spektrum der Wissenschaft 11/08, S. 92-99.
- [5] Gunter Dueck: *Virtuelle Gartenzwerge im Web 7.0*. Spektrum der Wissenschaft 12/08, S. 102-104.

Internet

- Gadi Evron: *Estonia and information warfare*. Vortrag auf dem ChaosComputer-Camp 2007, abzurufen unter: http://audio.textfiles.com/cons/ccc/2007/cccamp07-en2050-Estonia_and_information_warfare.m4v 04.01.2009, 18:06 Uhr
- <http://www.heise.de/newsticker/InEstlandwurdederCyberKrieggetestet/meldung/-90340> 03.01.2009, 17:49 Uhr
- http://www.iaik.tugraz.at/downloads/public/KIIS/tittelbach_angriff_auf_estland.pdf 03.01.2009, 18:13 Uhr
- <http://de.wikipedia.org/w/index.php?title=Google&oldid=54867016>
- <http://de.wikipedia.org/w/index.php?title=Facebook&oldid=54826505>
- <http://de.wikipedia.org/w/index.php?title=MySpace&oldid=54873396>
- http://de.wikipedia.org/w/index.php?title=Cloud_Computing&oldid=54531407