

## Cyberspace

### Großer Bruder im Netz

Jeder Klick hinterlässt eine Spur – zur Freude von Polizei, privaten Firmen und Datendieben

Von Thomas Fischermann

Am 7. November 2002 klopfen die Agenten der chinesischen Polizei an die Tür von Liu Di. Es würde keine offizielle Anklage geben, kein Besuchsrecht für Familie und Freunde im Qincheng-Gefängnis, wurde der Frau beschieden. Liu Di war eine Psychologiestudentin in Peking, im dritten Studienjahr. Doch Liu Di hatte noch eine andere Identität, im Cyberspace: Jahrelang war sie die „Rostfreie Stahlmaus“ gewesen, Verfasserin satirischer Systemkritiken und Webmaster einer der bekannteren Anti-Regierungs-Web-Seiten im Internet. Eine Cyber-Dissidentin, die dank ihres technischen Geschicks jahrelang den Fahndern entkommen konnte.

Sie ist nicht allein. Rund 40 Cyber-Dissidenten sind in den vergangenen Jahren in China verschwunden oder haben das Land verlassen, eine „Internet-Polizei“ überwacht den Cyberspace und hat ein gigantisches Filter- und Beobachtungsnetz um den gesamten chinesischen Teil des Internet gezogen. Doch autoritäre Regime wie China, Burma oder Singapur sind längst nicht mehr die größten oder gar einzigen Schnüffler im Internet. Die Lauscher mit den größten Ohren, sagen Sicherheitsexperten, seien Behörden der westlichen Welt.

Die wachsende Leistungsfähigkeit von Computersystemen erlaubte der amerikanischen Bundespolizei FBI den Aufbau eines Systems namens Carnivore, das nach Belieben E-Mails lesen und jeden Klick eines Individuums auf Web-Seiten erfassen kann. Ein streng geheimes und stetig wachsendes Spionagesystem namens Echelon belauscht derweil offenbar weltweit den Telefon- und Datenverkehr. Und selbst wer sich off line bewegt, hinterlässt bei solchen Behörden immer deutlichere Datenspuren: In vielen Ländern wird das Netz aus Videoüberwachungsanlagen engmaschiger, Reisedaten und Hotelbuchungen werden immer gründlicher erfasst, Kreditkartenzahlungen zusammengestellt. In den Vereinigten Staaten wandert sogar schon in eine Datenbank, wer bestimmte Bücher in öffentlichen Bibliotheken ausleiht.

Auch private Firmen in aller Welt schnüffeln inzwischen eifrig mit – aus rein wirtschaftlichen Motiven, weil sie ihre Kundschaft besser kennen lernen wollen. Eine Reihe großer Finanzhäuser, darunter auch die Allianz, hat gemeinsam die Firma Regulatory Data Corp (RDC) gegründet. Sie baut fieberhaft eine gigantische weltweite Datenbank über Menschen in aller Welt auf, die zweifelhafte Schuldner oder gar Geldwäscher sein könnten. „Wenn ein Bankkunde in New York einmal Schwierigkeiten mit den schweizerischen Aufsichtsbehörden hatte – wir wollen das wissen“, hat der RDC-Chef Bill Catucci einmal gesagt. Mit einer Fülle von Techniken forschen Web-Seiten-Betreiber ihre Besucher aus. Cookies, die das Surf-Verhalten des Internet-Benutzers nachzeichnen, und so genannte Spyware – Computerprogramme, die sich auf dem PC unerkannt installieren und jeden Klick über Monate registrieren – sorgen für kommerziell interessante Informationssplitter.

So richtig wertvoll werden diese Splitter, wenn man sie mit anderen Daten kombiniert, wenn Banken, Versicherungen, die Veranstalter von Preisausschreiben, Fluggesellschaften, Buchhändler, Supermärkte zusätzliches Wissen über virtuelle Besucher beisteuern. Auf diese Weise kommen erschreckend komplette Profile von Personen zustande: monatliches Einkommen, politische Überzeugungen, die Zahl der Familienmitglieder, gesundheitliche Probleme, das Flirtgehabe auf match.com, Einkäufe bei amazon.de, quelle.de und duftende-unterwaesche.de.

Strafverfolgungsbehörden in aller Welt sind von dieser Entwicklung begeistert: Das Patriot-Gesetzespaket, das nach den Anschlägen vom 11. September verabschiedet wurde, erlaubt dem FBI mehr Zugriffe denn je auf solche privat gesammelten Daten – ohne Durchsuchungsbefehl.

Doch nicht nur Gesetzeshüter nutzen die neuen Überwachungstechniken. In den Vereinigten Staaten macht der Musikindustrie-Verband RIAA gerade kontroverse Schlagzeilen: Er hat Tausende Internet-Surfer verklagt, die Musikstücke über Tauschbörsen gehandelt haben – die Schuldigen fand der Verband durch eine gewaltige Schnüffelaktion im Internet.

Zahlreiche Konzerne setzen Überwachungsprogramme gegen die eigenen Mitarbeiter ein – um Surfgewohnheiten zu kontrollieren und betriebsfremden Zeitvertreib im Netz zu stoppen. Und auch Hacker und Datendiebe nutzen eine Vielzahl von Schnüffeltechniken, um ahnungslosen Surfern ihre Passwörter und Kreditkartennummern zu entlocken. Zum Einsatz kommen dabei so genannte Keylogger-Programme, die sich heimlich auf Computern installieren und jeden Klick und Tastendruck in den Cyberspace hinausposaunen.

Liu Di ist inzwischen wieder frei, zusammen mit zwei anderen chinesischen Cyber-Dissidenten. Das meldete am Wochenende eine Hongkonger Menschenrechtsgruppe und wertete die Freilassung als diplomatische Geste gegenüber den USA. Etliche andere Aktivisten bleiben freilich hinter Gittern. Und manchmal, wenn man Bürgerrechts-Web-Seiten im Internet besucht, kann man den Griff der fernen, staatlichen Kontrolleure auf dem eigenen Bildschirm spüren. „Hier gibt es nichts für Sie zu sehen“, stand zum Wochenbeginn auf einer bekannten Dissidenten-Web-Seite. Offensichtlich waren Unbekannte eingedrungen. Die Links zu kritischen Papieren gegen die chinesische Regierung waren allesamt blockiert.

Quelle: ZEIT.de

