



Die Freiheit kommt Bit für Bit

Handyfotos und Blogs sind die neuen Werkzeuge der Demokratiebewegungen. Doch der Zensor twittert mit **VON CHRISTOPH DRÖSSER UND STEFAN SCHMITT**

Der Goliath Totalitarismus wird vom David Mikrochip besiegt werden, prophezeite der US-Präsident Ronald Reagan im Jahr 1989. Sein Widersacher und Partner bei der Beendigung des Kalten Kriegs, Michail Gorbatschow, hatte sich ein Jahr zuvor ähnlich geäußert: »Die internationale Kommunikation ist heute leichter als je zuvor. Heute kann praktisch keine Gesellschaft völlig geschlossen sein.«

Diese Sätze stammen aus einer Zeit, als das Internet noch in den Kinderschuhen steckte und kofferschwere Mobiltelefone Spielzeuge für ein paar Reiche waren. Zwanzig Jahre später scheint sich die Vision der beiden Staatsmänner zu bestätigen: Weltweit haben die Bürger per elektronischer Datenleitung Zugang zu politischen Informationen aus dem In- und Ausland. Das Netz, so scheint es, ist zum Instrument der Freiheit geworden. Amateurfotos erreichen uns vom brutalen Einsatz der chinesischen Sicherheitskräfte gegen die Uiguren ebenso wie von den Schüssen der birmanischen Militärjunta auf friedliche Mönche. Per Internet schaut die Welt zu, wenn die Machthaber in Kenia oder Simbabwe Zivilisten verfolgen lassen. Und als in Iran gegen den Ausgang der Präsidentschaftswahl protestiert wurde, machte das Wort von der »Twitter-Revolution« die Runde. Vernetzt die Menschen miteinander, so die einfache Formel, und sie begehren gegen ihre Unterdrücker auf.

Doch die neuen Informationstechniken verändern die politische Szenerie in autoritär regierten Ländern auf eine sehr viel komplexere Weise. Das westliche Klischee von einer technisch versierten, aufmüpfigen iranischen Jugend einerseits und technikfeindlichen Mullahs andererseits, die ihre Propaganda auf altmodische Weise von den Minaretten rufen, ist ebenso abgedroschen wie falsch.

»Wir wissen so viel über die Onlineaktivitäten der Mussawi-Unterstützer – und fast nichts über die der konservativen Hardliner«, sagt Evgeny Morozov vom Thinktank Open Society Institute in New York. Dass die Stimmen der Konservativen nicht auf Twitter zu hören gewesen seien, bedeute noch lange nicht, dass sie sich nicht auch dieses Mediums bedienen. »Sie tun es nur auf Farsi und auf lokalen Websites – wir wissen einfach nicht, wo wir hinschauen müssen.«

Tatsächlich bietet die iranische Internetszene ein erstaunlich buntes Bild. Forscher vom Berkman Center for Internet and Society an der Harvard-Universität haben eine Landkarte der persischen Blogosphäre erstellt, die schon vor den

jüngsten Ereignissen aus 60 000 regelmäßig gepflegten Blogs bestand. Die säkularen, reformorientierten Einträge machten dabei nur einen Teil aus – zahlenmäßig ebenbürtig waren neben kulturellen oder rein persönlichen Inhalten auch die politisch konservativen und religiösen Webauftritte. Schließlich waren die Mullahs neuen Techniken gegenüber schon immer aufgeschlossen. Als der Ajatollah Chomeini noch im Pariser Exil saß, wurden seine Botschaften auf Video- und Audiokassetten nach Iran geschmuggelt. Und bereits 2006 wurde in Qum, der religiösen Kaderschmiede der islamischen Republik, ein »Büro für die Entwicklung religiöser Weblogs« eingerichtet.

»Statt die Todesglocke für den Autoritarismus zu läuten, bietet die globale Verbreitung des Inter-

nets sowohl Gelegenheiten als auch Herausforderungen für autoritäre Regime.« Das schrieb bereits im Jahr 2003 die amerikanische Carnegie-Stiftung in ihrer Studie *Open Networks, Closed Regimes*. Und Evgeny Morozov hat für die Netzwerke staats-treuer Propaganda den Begriff »Spinternet« geprägt – das soll zum Ausdruck bringen, dass die Herrschenden als Spindoktoren die neuen Informationskanäle nutzen, um der öffentlichen Meinung ihren eigenen Dreh (*spin*) zu geben. Das geschieht nicht nur in Iran; in Russland beispielsweise rief der regierungsnahen Fonds für effektive Politik (FEP) die Website *liberty.ru* ins Leben, eine moderne, mit Web-2.0-Elementen gespickte Plattform. Die Kreml-Strategen erhoffen sich davon, jene Bevölkerungskreise zu erreichen, die weder

loyal zur Regierung stehen noch deren Kritiker sind – Journalisten, Kreative, Computerspezialisten. Die Kommunisten scheinen dabei das Netz und seine Mechanismen besser verstanden zu haben als viele westliche Politiker, die im Internet nicht viel mehr als eine weitere Plakatwand sehen.

Auch in China ist der kommunistischen Partei eine gewisse Partizipation via Internet durchaus willkommen – solange nicht die Systemfrage gestellt wird. Mit entsprechenden Websites will die Regierung die Korruption eindämmen und sich einen modernen Anstrich geben – die ultimative Kontrolle sowohl über die Themen als auch über die Ergebnisse bleibt natürlich bei der Partei. Das erinnert an die Zeit, als Mao unter dem Motto »Lasst hundert Blumen blühen« das Volk auf

Wandzeitungen seine Meinung sagen ließ, bevor die Kulturrevolution den Keim der Freizügigkeit erstickte.

Blühen die Blumen zu üppig, dann werden die Regime nervös und repressiv. In den vergangenen Tagen schloss die chinesische Regierung mehr als fünfzig uigurische Internetforen, die Webseiten von Twitter und YouTube waren in der Provinz Xinjiang nicht mehr erreichbar. Schon vor drei Jahren stellte die Open Net Initiative (ONI), zu der sich Institute der Universitäten Harvard, Toronto, Oxford und Cambridge zusammengeschlossen haben, fest, dass weltweit in insgesamt 26 Staaten Internet-Inhalte gefiltert würden. Soeben wird die Untersuchung wiederholt – mittlerweile hat sich die Zahl schon auf 36 erhöht.

Die Technik für die Netzkontrolle stammt meist aus dem Westen. Hard- und Software, die etwa in Deutschland für die Vorratsdatenspeicherung eingesetzt wird, »eignet sich theoretisch auch dafür, Nutzer auszuspionieren und unerwünschte Inhalte zu blockieren«, sagt der ONI-Forscher Rafal Rohozinski. Es sei eine bittere Ironie, dass ausgerechnet im Namen der Cybersicherheit solche Technologien im Westen kommerziell verfügbar würden.

Zugleich liefert der Westen allerdings auch die Gegenmittel. So nutzten iranische Surfer in den vergangenen Wochen verstärkt den Anonymisierungsdienst Tor. Dafür stellen Freiwillige aus vielen Ländern Server zur Verfügung; in einer Art Stille-Post-Technik ermöglichen diese dann Surfern aus unfreien Ländern den Aufruf blockierter Websites auf Umwegen. Auch der Dienst Psiphon leitet die Inhalte geblockter Seiten so um, dass sie an der Zensur vorbei gelesen werden können.

Letztlich kann heute kein Diktator mehr verhindern, dass Nachrichten über menschliches Elend und undemokratische Zustände nach außen dringen. Selbst Skeptiker wie Morozov sind überzeugt: »Ein zensuriertes Netz ist besser als gar keins.« Und mit Blick auf Iran sagt Konstantin Kosten von der Deutschen Gesellschaft für Auswärtige Politik: »Die Vorteile und der Einfluss des Internets auf verschiedene gesellschaftliche Gruppen überwiegen bei Weitem die negativen Folgen.«

Der Preis für eine totale Informationskontrolle wäre die totale Abschottung nach außen, und die kann sich in der globalisierten Welt nur noch Nordkorea leisten. Das Netz ist also nicht zu stoppen – automatisch zur Freiheit führt es allerdings nicht. Die müssen sich die Menschen immer noch selbst erkämpfen.

Die Kehrseite des Digitalen

Wie Regimekritiker kontrolliert und zum Schweigen gebracht werden

Zensieren: Thailand gibt sich fortschrittlich, wenn es um die Beschränkung der freien Meinungsäußerung geht. In bester Web-2.0-Manier lagert der Staat die Fahndung nach anstößigen Webinhalten aus: Unter Protect-TheKing.net (»Schützt den König«) können thronerhebene Untertanen königskritische Webseiten melden. Die Behörden wenden dann drakonische Gesetze an.

Blockieren: Autoritäre Staaten kappen gern den Zugang zu ausländischen Seiten. Immer wieder hat etwa Iran den persischen BBC-Dienst blockiert. Internetnutzer sahen nur eine Fehlermeldung. Solche schwarzen Listen zu erstellen ist für die Machthaber in Teheran besonders einfach, weil jeglicher Datenverkehr ins Ausland über einen einzigen, staatlich kontrollierten Übergabepunkt läuft. Syrien verhindert alle Zugriffe auf Webseiten mit der israelischen Länderkennung .il. Und Chinas »Great Firewall« (etwa: Große Internet-Mauer) blockiert nicht bloß einzelne Webseiten, sondern auch Adressen, die bestimmte Schlüsselwörter enthalten.

Analysieren: An einem Netzwerkknoten lassen sich praktisch alle durchgehenden Datenpakete öffnen, mitlesen, analysieren und bei Bedarf protokollieren. Informatiker sprechen von *deep packet inspection* (kurz DPI), also von Tiefeninspektion. Wissenschaftler der Open Net Initiative (ONI) fanden Belege für DPI in China und Tunesien. Aber auch in Iran, so mutmaßen Regimekritiker, könnte in den vergangenen Wochen DPI eingesetzt worden sein. Dafür spricht, dass am Wahltag Datenverkehr zwischen Iran und dem Rest der Welt spürbar langsamer wurde.

Belauschen: Chat oder Telefonie über das Internet (*voice over IP*, kurz VoIP) ersetzt für viele Menschen das Telefon. Sie mitzuhören oder mitzulesen ist aufwendig, aber nicht unmöglich. Besonders leicht macht es die chinesische Software Tom-Skype den Sicherheitskräften. Kanadische Forscher konnten vergangenes Jahr belegen: Nicht nur Verbindungsdaten werden festgehalten, Schlüsselwörter fischt das Programm heimlich aus dem Datenstrom und hinterlegt sie auf einem Server – ein Datenschatz für Ermittler.

Zumüllen: Masse macht Meinungsmacht, nach diesem Prinzip verfahren viele Autokratien

und bedienen sich dabei sowohl freiwilliger Unterstützer als auch bezahlter Helfer. Russland ist ein herausragendes Beispiel für diese Praktik. Kreml-freundliche Positionen prägen den Ton vieler Onlinedebatten. Hier dient das Internet zwar dazu, Dampf abzulassen, die Obrigkeit verliert aber nie die Kontrolle. Politikwissenschaftler sprechen von »autoritärer Deliberation«.

Manipulieren: Hackerattacken sorgen dann für Aufsehen, wenn prominente Ziele wie das Pentagon und Server der Bundesregierung betroffen sind. Über Verbindungen nach Peking oder Moskau wird meist nur gemunkelt. Auch Angriffe gegen die Informationsinfrastruktur von Staaten wie Estland, Georgien oder im israelisch-palästinensischen Dauerkonflikt sorgen wiederholt für Schlagzeilen. Diese Form von Cyberkrieg wird auch von Staaten gegen einzelne Bürger, Firmen oder Interessengruppen eingesetzt. So verschwanden am ersten Jahrestag des Aufstands birmanischer Mönche gegen das Militärregime in Myanmar drei prominente Seiten von Exilbirmanen aus dem Netz. Sie waren unter massenhaften Aufrufen ferngesteuerter Server (DDoS, kurz für *distributed denial-of-service attack*) zusammengebrochen.



Kein Mensch ist wie der andere. Das wissenschaftliche PARSHIP-Prinzip vergleicht 30 wesentliche Persönlichkeitsmerkmale und schlägt Ihnen Partner vor, mit denen Sie sich optimal ergänzen.



www.zeit.de/partnersuche
DIE ZEIT

Wer passt zu Ihnen?
Jetzt kostenlos anmelden.