



Das Weihnachtsgeschäft zeigt vollends, dass der Begriff des Postmaterialismus nichts mehr taugt S. 15

Bedrohter Kulturraum

Cyberwar Das Internet nimmt als Schlachtfeld Formen an. Auf „Cablegate“ folgt nun der Info-Bürgerkrieg

■ Niels Boeing

Es mutet an wie ein Hollywood-Thriller in Echtzeit, was die Weltöffentlichkeit in den vergangenen drei Wochen erlebt hat: Kurz nachdem die Whistleblower-Plattform Wikileaks, unterstützt von fünf internationalen Zeitungen, begonnen hat, eine Viertelmillion vertraulicher Depechen aus dem diplomatischen Korps der USA zu veröffentlichen, werden die Webserver der Organisation heftig angegriffen. Dann sperren mehrere US-Konzerne ihre Online-Dienste für Wikileaks, derweil deren Gründer Julian Assange zum Staatsfeind Nr. 1 ausgerufen wird. Mit einem internationalen Haftbefehl wegen mutmaßlicher Vergewaltigung gesucht, stellt er sich schließlich der britischen Polizei – und löst damit eine Netzangriffswelle gegen die Konzernserver durch Sympathisanten aus aller Welt aus. „Der erste Info-war hat begonnen“, proklamieren Hacker aus dem Umfeld der so genannten Anonymous-Gruppe und versprechen, ihn fortzusetzen.

Das klingt martialisch. Für Militär- und Sicherheitsanalysten ist ein Krieg im Internet als fünftem Gefechtsraum – neben Land, See, Luft und Weltraum – jedoch eine Option, seit 1993 die Rand Corporation, eine Denkfabrik für den militärisch-industriellen Komplex, den reißerisch betitelten Report *Cyberwar is coming!* veröffentlichte. Nur: „Wir haben keine eindeutigen Definitionen, was ein Cyberwar eigentlich ist“, schreibt der amerikanische Computersicherheitsexperte Bruce Schneier in seinem Blog. Das liegt daran, dass die bislang zugänglichen Analysen oft von Allmachtsphantasien und Dystopien erfüllt sind, und dass die Grenzen zwischen Kriegsführung, Überwachung, Desinformation und Kriminalität im Netz verschwimmen.

Kein feinmaschiges Netz

Es wäre also leicht, die Vorstellung eines Cyberwar in der gegenwärtigen Aufregung um „Cablegate“ als heiße Luft abzutun. Tatsächlich aber sollte man die Bedrohung des Netzes nicht unterschätzen. Zum einen ist es zur Infrastruktur geworden: Handel, Produktionsketten oder Finanzmärkte sind ohne das Internet heute nicht mehr denkbar. Zugleich haben sich mit seinem rasanten Wachstum Teile der Kulturproduktion, sozialen Gemeinschaften und Medien dort hin verlagert und es zu einem Kulturraum gemacht, den William Gibson in seinem Science-Fiction-Roman *Neuromancer* als Cyberspace vorwegnahm. Für zig Millionen Mensch ist das Netz ein kommunikativer Ort ihres Alltagslebens geworden.

Betrachtet man das Internet als Infrastruktur, stellt sich der Cyberwar vor allem als Ausweitung herkömmlicher Kriege dar. Darin könnte das Internet als Vehikel dienen, um einen Gegner mit informationstechnischen Mitteln anzugreifen, als militärische Aufmarschroute gewissermaßen. Die Datenangriffe auf Estland im April 2007 richteten sich gegen Banken und Behörden und trennten den baltischen Staat de facto vom Netz. Mit der zunehmenden Anbindung von herkömmlichen Infrastrukturen ans Netz eröffnen sich neue Einfallstore, direkt in die Computer etwa von Kraftwerken. Einen Vorgeschmack gab im Sommer der Stuxnet-Wurm, der auf eine Siemens-Software für Industrieanlagen zugeschnitten ist. Zwar muss er noch per USB-Stick ans Ziel, die eigentlichen Steuerrechner, transportiert werden. Seine Komplexität und Raffinesse, für die wohl ein mehrköpfiges Team mit einem Millionenbudget verantwortlich zeichnete, machen ihn für Ex-



Kriegslist: Die Internet-Aktivisten von „Anonymous“ verbergen sich gerne hinter der Maske des Verschwörers Guy Fawkes

perten zum ersten echten Prototyp einer Cyberwaffe: Auf Stuxnet geht wahrscheinlich ein plötzlicher Ausfall zahlreicher Zentrifugen zur Urananreicherung im Iran zurück.

Das Netz ist aber potenziell auch selbst ein Angriffsziel. Was dies bedeutet, zeigt das Beispiel des Computerwurms Slammer, der im Januar 2003 innerhalb weniger Stunden das Netz mit enormen Mengen von Datenpaketen – die tatsächlich Kopien seiner selbst waren – überflutete. Der globale Datenverkehr verlangsamte sich vorübergehend drastisch. Dieselbe Wirkung hatte 2008 das physische Durchtrennen einer Hauptleitung im östlichen Mittelmeer. Kurzzeitig tröpfelten in Teilen von Asien die Daten mehr, als dass sie flossen.

Der neue Cyber-Konflikt entsteht aus den westlichen Industriegesellschaften

Nun hält sich bis heute der Mythos, das Internet sei als dezentrales militärisches Kommunikationsnetz angelegt worden, um auch bei einem teilweisen Ausfall in einem Atomkrieg nahtlos weiter zu funktionieren. Tatsächlich ging es den Entwicklern aber nur darum, eine Technologie zu entwickeln, die effizienter als die damaligen Telefonnetze Daten übertragen konnte. Ein Blick auf die Hauptleitungen des Netzes zeigt denn auch, dass es mitnichten wie ein gleichmäßiges, feinmaschiges Netz den Globus überzieht. Vielmehr sind diese „Backbones“, etwa über den Atlantik, äußerst ungleichmäßig verteilt – was das Netz viel verwundbarer macht, als es der My-

thos glauben macht. Neben solchen Bedrohungen, die Sicherheitsexperten beschäftigen, ist in der Auseinandersetzung um die jüngste Wikileaks-Enthüllung noch eine weitere Dimension des Cyberwar sichtbar geworden: Man könnte sie einen „Info-Bürgerkrieg“ im Kulturraum Internet nennen. Die Akteure, und das ist das Erschreckende daran, sind nicht repressive Regime und Dissidenten wie in China, Syrien oder dem Jemen. Der neue Cyber-Konflikt entsteht aus den westlichen Industriegesellschaften heraus, in denen Unternehmen staatlichen Akteuren zur Seite springen und die Informationsfreiheit angreifen.

Den Anfang machte der Online-Händler Amazon: Er sperrte Wikileaks von seinen so genannten Web Services aus. Das ist eine verteilte Infrastruktur aus Großrechnern, die diejenigen mieten, die große Datenmengen halten möchten, aber selbst keine derartigen Infrastrukturen aufbauen wollen oder – wie Wikileaks – können. Dann folgten der Bezahldienst Paypal und die Kreditkartenunternehmen Mastercard und Visa mit einer Aussperrung. Über sie sammelte die Whistleblower-Plattform bis dahin große Teile seiner Spendengelder ein.

Bemerkenswert ist die rein rechtliche Begründung der vier Unternehmen: Wikileaks habe mit seiner Operation die Geschäftsbedingungen verletzt, weil diese „illegal“ sei. Dass die Bezahlendienste keine Probleme damit haben, offen rassistische Organisationen wie den Ku-Klux-Klan zu unterstützen, fiel ihnen erst auf Nachfrage der Medien auf.

Diese Bigotterie muss niemanden überraschen. Sie zeigt aber einmal mehr, wie über das bürgerliche Vertragsrecht Machtverhältnisse durchgesetzt werden können. Da macht auch der Cyberspace keine Ausnahme. Er ist nicht jener abstrakte, freie Raum, an den noch John Perry Barlow in seiner berühmten *Unabhängigkeitserklärung des Cyberspace* 1996 glaubte. Vielmehr wird er von allen Akteuren beständig erzeugt produziert. Diese sind freilich nicht alle gleich, sondern bilden in ihren Kräfteverhältnissen dieselben Konzentrationspro-

zesse ab, die seit jeher im „realen“ Kapitalismus ablaufen. Auch in dieser Hinsicht ist das Internet nicht ein feinmaschiges, gleichmäßiges Netz, in dem alle Knoten dieselbe Bedeutung hätten. Daran ändert auch die Tatsache nichts, dass Unterstützer die Inhalte von Wikileaks bald auf Hunderten von „Mirror Sites“, Ersatz-Servern, zur Verfügung stellten. Denn, wie Barlow vor einigen Tagen schrieb: „Wenn sie Wikileaks zum Schweigen bringen können, können sie jeden mundtot machen“ – im Prinzip jedenfalls, und darum geht es.

Ein Friedensabkommen

Die Reaktion der Netzbürger ließ nicht lange auf sich warten: In der „Operation Payback“ versuchten Tausende mit einem simplen zu bedienenden Angriffsprogramm der Anonymous-Gruppe, die Rechner von Mastercard und anderen Unternehmen zu blockieren. Kurzzeitig gelang dies sogar. So verständlich die Empörung ist, muss dieser Prototyp einer „Online-Guerilla“ auch nachdenklich machen. Das Software-Werkzeug für die Operation Payback war bereits vor der Auseinandersetzung um Wikileaks entwickelt worden, und wer es wann aus welchen Motiven einsetzen könnte, ist nicht abzusehen. Hamadou Touré, Generalsekretär der internationalen Telekommunikations-Union, hat bereits ein „Cyber-Friedensabkommen“ vorgeschlagen. „Ein Cyberwar wird schlimmer sein als ein Tsunami – wir müssen ihn verhindern“, sagte Touré im September in London. Dabei dürfte er allerdings nur die Cyberwar-Programme von Staaten wie China, Russland oder den USA im Sinn gehabt haben, nicht die aufkeimende Militanz im kulturellen Raum Internet. Die aber wird genährt von den ökonomischen Machtverhältnissen im Netz – und gegen die hilft auch ein internationales Friedensabkommen nicht.

Niels Boeing ist Technikjournalist aus Hamburg und schrieb im Freitag zuletzt über Vorratsdatenspeicherung

Kulturkommentar
Arnd Pollmann

Der kommende Angstschweiß: Ein Eau de Revolution

Wer sich in diesen Tagen eine Winterausrüstung zulegen will, muss einsehen: Der warenproduzierende Kapitalismus ist am Ende. Im letzten Sommer bekam man schon keine Tisch-Ventilatoren mehr. Dafür wird es Schlitten erst wieder zu kaufen geben, wenn es warm ist. In den Worten eines ICE-Schaffners im letzten Juli kurz vor Köln: „Eigentlich funktionieren die Klimaanlage ganz gut. Nur wenn es heiß wird, fallen die manchmal aus.“ Wird die Warenwelt auch diese Hürde nehmen?

Jüngst ist es immerhin gelungen, aus der konsumkritischen Rebellion ein rares und deshalb begehrtes Luxusprodukt zu machen. Die New Yorker Künstlerin Lisa Kirk hatte – generiert von der Terror-Hysterie der Bush-Ara – einen Duft namens *Revolution* kreiert. Kirk befragte politische Aktivistinnen, Barrikadenkämpfer und Journalisten aus aller Welt, wie die Revolution „riecht“. Die Antworten: nach Tränengas, Urin, Schweiß, verbranntem Gummi, verwesten Körpern. Diesen Cocktail bannte Kirk in einen Metallflakon, der wie eine Rohrbombe aussah und dessen Platinum-Version in ihrer Galerie für 4750 Dollar zu haben war.

Ursprünglich ist das ein Kunstprojekt und durchaus witzig gewesen. Zumal Kapitalismuskritik ansonsten fast immer ohne Humor auskommt – was zuletzt eindringlich unter Beweis gestellt wurde durch das fast lächerlich ernsthafte Pamphlet *Der kommenden Aufstand* (Freitag vom 20. Mai). Und doch haben wir es bei Kirks Duftwasser mit dem passenden Parfum zum Buch zu tun. Beide Produkte eint das trotzige Credo: capitalism sucks! Und die im Flakon versteckte Botschaft ergänzt scharfsinnig: revolution stinks!

Die Bombe zündete aber nicht; stattdessen wurde man Zeuge eines Ausverkaufs. Ein ehemaliger Duftdesigner von L'Oréal überredete die Künstlerin, eine Discount-Version ihres Revolutionparfums herzustellen und zum Preis von 55 Euro in exklusiven Konsumenttempeln zu vertreiben. Der einst so bombige Flakon, der in einem New Yorker Kaufhaus schon einmal Terroralarm ausgelöst hatte, wurde entcoolt. Ihm wurde das Outfit eines Molotowcocktails übergestülpt, wie man ihn sich an jeder Tankstelle zusammenbasteln kann. Seither kann man auf der Berliner Friedrichstraße eine gut betuchte, aber doch minder bemittelte Käuferschaft dabei beobachten, wie diese immer häufiger zur Waffe greift. Kurz vor dem Weihnachtssfest will man sich den Hauch einer waschechten Rebellion zulegen. Man verspricht das verruchte Odeur eines gewaltsamen Umsturzes, von dem man hofft, dass man ihn nicht mehr erleben wird, weil man ihn ohnehin nicht überleben würde. Wie geil ist das denn? Die Kulturindustrie hat gesiegt. Aus dem erfrischenden Schlachtruf „Vive la revolution!“ ist ein muffiges Eau de Toilette geworden.

Aber ist das schon die ganze Wahrheit? Nein, denn am Ende haben wir es mit einer offfaktorischen List der Unvernunft zu tun. Deren Geheimnis liegt im menschlichen Geruchssinn begründet: Düfte, die man längere Zeit um sich hat, nimmt man schon bald nicht mehr als störend wahr. Die frohe Botschaft zum Weihnachtseinkauf lautet also: Die Reichen und Schönen mögen sich ruhig schon einmal daran gewöhnen. Es riecht nach Revolution!

Arnd Pollmann lehrt an der Otto-von-Guericke-Universität Magdeburg Praktische Philosophie und veröffentlichte zuletzt bei C.H. Beck: *Unmoral. Ein philosophisches Handbuch. Von Ausbeutung bis Zwang* (2010)