UNENDLICHE WEITEN …?

UMKÄMPFTE GRENZEN IM INTERNET

Ξ Thorsten Thiel

»Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.«[1]

Diese Auftaktzeilen der 1996 verfassten »Declaration of the Independence of Cyberspace« stehen sinnbildlich für ein Verständnis, das noch heute die populären Erzählungen vom Internet dominiert: Die Ubiquität, Globalität und Aktualität des Netzes und die unendliche Leichtigkeit der Vernetzung im Web 2.0 werden so gedeutet, dass Staaten und ihre Grenzen im Internet völlig bedeutungslos geworden sind. Das je nach Standpunkt daraus folgende utopische oder dystopische Raunen, dass niemand das Internet kontrollieren könne, ist ein Topos von großer Kraft.

Dass das Internet grenzenlos und seine Entwicklung nicht zu steuern sei, ist dennoch nicht ganz richtig. Natürlich wird das Internet reguliert – und zwar immer und überall. Durch private Firmen, technische Standards,

1 John Perry Barlow, A Declaration of the Independence of Cyberspace, online einsehbar unter https://projects.eff.org/~barlow/Declaration-Final.html [eingesehen am 27.07.2012].

Programmcodes etc. Und natürlich gelten auch im virtuellen Raum Gesetze nationaler Art. Staaten mögen verspätet auf die Entwicklung reagiert haben; ihre Versuche zu begrenzen, zu regulieren und zu kontrollieren, sind aber überall sichtbar.

Dies erklärt sich schon dadurch, dass das, was auf dem Spiel steht, weit mehr ist als nur die Möglichkeit zu digitalem Preisvergleich und zur Pflege digitaler Netzwerke. Der reale Raum wird zunehmend durch virtuelle Kommunikation überschattet, Kommunikationsweisen und in deren Folge Interessenlagen werden grundlegend transformiert – die Musikindustrie kann ein Liedchen davon singen. Es erklärt sich daher von selbst, dass die Cyberutopie von einer sich den materiellen Zwängen entziehenden, grenzenlosen Interaktion auf Schranken stößt. Denn es sind nicht nur wirtschaftliche Rahmenbedingungen, die sich verschoben haben, sondern auch die Staaten selbst sind direkt von der grenzenauflösenden Kraft des Internets betroffen. Und für sie liegt der Einsatz ungleich höher, da sich für sie, im Gegensatz zu Unternehmen, die Risiken und Chancen des Netzes nicht die Waage halten. Das Internet stellt nichts Geringeres als das Grundprinzip von Staatlichkeit in Frage: den Staat als einheitlich verfassten und kontrollierten Raum, als souveräne Entität. Gerade in den Kernbereichen von Souveränität bewirkt die zunehmende Digitalisierung epochale Veränderungen, z. B. bei der Gewährleistung kollektiver Sicherheit oder bei der Durchsetzung der Eigentumsordnung. Der Versuch der Re-Etablierung von Grenzen im Netz ist daher wenig überraschend. Doch wie kann eine solche Grenzziehung überhaupt angegangen werden, wenn der Raum, in dem sich das Internet erstreckt, ein virtueller ist, theoretisch unendlich weit und beliebig formbar?

Grenzen im realen Raum sind weit einfacher zu konkretisieren als im virtuellen Feld, wo das, was man abzutrennen versucht, die ätherische Qualität digitaler Kommunikation hat. Jede Grenze – die physisch-territoriale wie die virtuelle – basiert auf den Faktoren Kontrolle und Beachtung. Kontrolle bedeutet die Fähigkeit, den sich an der Grenze ergebenden Verkehr zu überwachen, ihn zu regulieren und gegebenenfalls zu sanktionieren. Hierfür ist technische Superiorität zentral: An der Grenze muss man identifizieren und selektieren können. Im Grenzraum selbst muss Eindeutigkeit hergestellt werden, damit er administrierbar wird. Es ist jedoch nicht nur die Möglichkeit von Kontrolle, die eine Grenze funktionieren lässt. Ebenso bedarf es der Beachtung, der Anerkennung ihrer Legitimität. Zumindest von denen, die durch sie eingegrenzt werden, muss eine Grenze als berechtigt, gut und notwendig empfunden werden. Sie müssen für deren Verteidigung eintreten und die Grenze bestenfalls als natürlich empfinden. Wird die Grenze weder von

außen noch von innen anerkannt, wird ihr Erhalt so mühsam und kostspielig, dass wohl kein Regime sie über kurz oder lang bewahren kann.

Wie ist es nun um diese Faktoren im Feld des Digitalen bestellt? Kontrolle ist einfach und schwierig zugleich. Schwierig, da die Konstruktionsweise des Netzes in hohem Maße der Kontrollierbarkeit durch zentrale Steuerung widerspricht. Dies hat historische Gründe und wurde gerade von Staaten so gewollt, da in den Frühphasen des Internets die Staats- und Ökonomiefreiheit des Internets als zentral erachtet wurde, um die Widerstandsfähigkeit des Netzes zu gewährleisten.[2] Das Internet ist sehr bewusst auf einem »dummen« Protokoll errichtet, welches gerade nicht nach Inhalten diskriminiert, sondern alle Daten gleichberechtigt überträgt und damit das Prinzip der Netzneutralität durchzusetzen hilft. Dieses ermöglicht völlig unterschiedliche Anwendungen und begründet daher die hohe Innovationskraft des Netzes mit.[3] In einer Zeit, in der die Anzahl und Varianz der Anwendungen, die im Netz ausgeführt werden, nahezu unendlich ist und alle Aspekte des öffentlichen Lebens und privater Kommunikation vernetzt sind, ist ein Zurückfahren dieser offenen Infrastruktur per se schwierig – wenn auch nicht unmöglich, wie das leidlich erfolgreiche Beispiel der chinesischen Internetzensur zeigt.

VOLLÜBERWACHUNG IM KONTRAST ZUR LIBERALEN ARCHITEKTUR DES NETZES

Die Folge der offenen, dezentralen Grundstruktur des Netzes ist, dass man tief eingreifen muss, will man Datenkommunikation kontrollieren oder das Netz gar in nationale Container einfassen. Kein IP-Paket darf unbeachtet bleiben, alles und jede Kommunikation muss kategorisiert und vorsortiert werden. Es müssen Instrumente geschaffen werden, um automatisch und auf der Stelle zu entscheiden, welche Bedeutung welche Kommunikation trägt. Nötig ist also eine Tiefenüberwachung und ein In-die-Pflicht-Nehmen der Unternehmen, die den Bau der Infrastruktur des Webs betreiben bzw. dessen Navigation und Vernetzung gewährleisten (von Suchmaschinenanbietern zu sozialen Netzwerken bis hin zu Providern von Webspace). Diese Vollüberwachung, in Deutschland exemplifiziert durch die Vorratsdatenspeicherung, steht in starkem Kontrast zur liberalen Architektur des Netzes, seinem horizontalen Ethos und auch der privatwirtschaftlichen Ökonomie, die sich auf diesen Anlagen aufbauend entwickelt hat. Wie groß die Anpassungen und Einschränkungen schon heute sind, weiß jeder, der einmal bei YouTube ein Musikvideo aufzurufen versucht und dann die Meldung erhalten hat: »Dieses Video ist in Ihrem Land nicht verfügbar«. Noch weiter ging der Versuch, ein rein nationales und staatlich betriebenes Netz zu errichten, das französische

2 Eine kurze Geschichte des Internets sowie eine allgemein gut verständliche Einführung finden sich bei Martin Warnke, Theorien des Internets, Hamburg 2011. Dass auch in der Entwicklung des Netzes und seiner Standards Staaten eine zentrale Rolle spielten, argumentiert Daniel Drezner, The Global Governance of the Internet: Bringing the State Back In, in: Political Science Quarterly, Bd. 119 (2004) H. 3, S. 477–498.

3 Die klassische Verteidigung dieses Prinzips und der Vorteile eines »dummen« Protokolls findet sich bei Doc Searls u. David Weinberger, World of Ends. What The Internet Is and How to Stop Mistaking it For Something Else, online einsehbar unter http://www.worldofends.com [eingesehen am 27.07.2012].

Minitel-System, das aber, dem freien Internet hoffnungslos unterlegen, nach dreißig Jahren am 30. Juni 2012 endgültig abgeschaltet wurde. Um die Verhältnismäßigkeit tiefer Eingriffe und der Projektion nationaler Grenzen ins Netz zu belegen, bedarf es also einer starken Rechtfertigung.

Aus dem invasiven Charakter aller Maßnahmen zur technischen Kontrolle virtuell gezogener Grenzen folgt, dass es umso wichtiger wird, Beachtung für diese zu erzielen. Notwendigkeit und Legitimität werden zu Ankern des Diskurses. Gerade weil die Eingriffe massiv und flächendeckend sind, wird daher eine stark paternalistische Version des staatlichen Vorsorgeprinzips zur Begründung angeboten: Die Identifizierung einer übergroßen Gefahr, die jeden betrifft, ist der erste Schritt; sodann muss deren Abtrennbarkeit und Beherrschbarkeit suggeriert werden und für eine präventive Eindämmung argumentiert werden: besser jetzt als nie. Das existierende Regime des Internetverkehrs wird dabei als der heutigen Bedeutung des Netzes nicht mehr gerecht werdende Nerd-Utopie diffamiert, ihm wird die Notwendigkeit von Verantwortung und Supervision entgegengestellt. Nicht zufällig wird dabei eine besonders chaotische Form der Anarchie als Gegenbild beschworen, die zu eskalieren drohe, wenn man dem Treiben seinen Lauf ließe. Genau das soll nun exemplarisch an zwei Diskursen gezeigt werden, die gerade den Zusammenhang von nationaler Souveränität, Abgrenzung und Gefahr betonen.

Nahezu in Reinform lassen sich der Aufbau eines Bedrohungsszenarios und die versuchte Re-Etablierung nationaler Grenzen im Feld digitaler Sicherheitspolitik beobachten. Das Thema Cyber-Security blüht und bei seiner Diskussion fällt sofort auf, wie unterschiedlich die Gefahren sind, die unter diesem Label zusammengefasst werden. Den übergreifenden Nenner bildet die Allgegenwart der Vernetzung, die eine allgemeine Verletzlichkeit gesellschaftlicher Strukturen wie des Individuums begründen und damit die Betroffenheit eines jeden plausibel machen soll. Handlungsdruck wird erzeugt und das Diffuse der Gefahr trägt zu deren Potenzierung bei. Unter der inkludierenden Logik der Sicherheit im Netz werden Cyber-Kriminalität und Cyber-Kriegsführung (in den Sub-Varianten Cyber-War und Cyber-Terrorismus) zusammengeführt und als eine amalgamierte Gefahr mit höchst unterschiedlichen Bedrohungsmechanismen (Spionage, Angriffe auf öffentliche Infrastruktur, Lahmlegen privater Dienstleistungen, Gefährdungen des Alltags komplexer Gesellschaften) begriffen. Schon die Breite der Gefahr suggeriert dann, dass die Antwort nur in kollektiver Koordination und Zentralisierung liegen kann und angesichts der Aufrüstung anderer Staaten notgedrungen auch eine nationale sein muss. In Deutschland hat sich dies in der Errichtung eines nationalen Cyber-Abwehrzentrums manifestiert.

Weiter illustrieren lässt sich dies am Fall WikiLeaks, der eigentlich nur schwerlich in das Schema von neuartigen Internetbedrohungen passen will. Zumindest die Bradley Manning zugeschriebenen Leaks amerikanischer Geheimdokumente sind schließlich ein relativ klassischer Fall von Whistleblowing, dem allein durch die globale Distributionsweise und die Möglichkeit der unmittelbaren Einsicht in (Teile der) Originaldokumente ein digital schimmernder Mantel umgelegt wird. Am WikiLeaks-Diskurs ist auffällig, wie grotesk überzogen die Schadensbehauptungen und die daraus abgeleiteten Maßnahmen sind. Nicht nur wird ein »Framing« des Diskurses gesucht, der pauschal allein auf die Gefahr der Veröffentlichungen hinweist, diese werden auch als ein national zu regulierendes Thema aufgegriffen. Wie schlecht diese Schublade passt, wird schon deutlich, wenn man sich die juristischen Verwicklungen um die Person Assange vor Augen führt: jener Australier, der Enthüllungen über amerikanische Außenpolitik verbreitete, die in vielen Regionen der Welt diplomatische Erdbeben auslösten – und die nicht zuletzt in Island für die Veröffentlichung präpariert wurden. Nachdem Assange darüber mit einem deutschen Mitstreiter brach, sitzt er nun wegen eines mutmaßlich in Schweden begangenen Verbrechens nach der Flucht aus der britischen Haft im ecuadorianischen Asyl. Noch komplexer wird es, wenn man als Beispiel das Wirken der Aktivisten von Anonymous oder von Virenprogrammierern heranzieht; aber selbst im genuin staatlichen Bereich – Beispiel: Stuxnet – bleiben große Fragen und Zweifel an Identität/Identifizierbarkeit, Kontrolle und der Adäquatheit nationalstaatlicher Reaktion.

Nicht anders sieht es aus, wenn man auf die Debatte um den Schutz von (geistigen) Eigentumsrechten im Netz fokussiert. Diese geht der Debatte um Cyber-Security zeitlich und an Bedeutung voraus und auch hier ist ein starkes Moment nationalstaatlicher Zuständigkeitsbehauptung zu beobachten. Die Debatte tritt in mehreren Mutationen auf: so zunächst mit Blick auf Open-Source-Software, später dann in Bezug auf Tauschbörsen und jüngst in den Auseinandersetzungen um die Reform des Urheberrechts. Sie dreht sich vor allem um die durch die Digitalisierung veränderte Beschaffenheit von Gütern und Vertriebswegen und insbesondere um die Möglichkeit der verlustfreien Vervielfältigung durch Kopieren. Gerade letzterer Aspekt gibt dem Ganzen staatliche Bezüge, da der grenzüberschreitende Verkehr von Daten – Stichwort: Peer-to-Peer-Verbindungen – die Problematik unterschiedlicher Jurisdiktionen unmittelbar evident macht. Die Suche nach nationalen Regelungen auf diesem Feld hat stark zugenommen und erstreckt sich von der Kooperation und Angleichung von Standards – man denke nur an die heftigen Debatten um ACTA und SOPA – vor allem auch auf technische Möglichkeiten

der Unterdrückung illegalen Datenverkehrs bzw. dessen unmittelbarer Sanktionierung (am bekanntesten ist hier wohl die Three-Strikes-Regel in Frankreich, die nach dreimaligem Verstoß gegen das Urheberrecht unter anderem ein temporäres Abklemmen vom Internetzugang erlauben soll). So klar auf den ersten Blick die Trennung von Urheberrechten und illegaler Verwendung scheint, so schwierig wird es, wenn man sich konkrete Fälle genauer anschaut. Das Urheberrecht stößt im Netz permanent an seine Grenzen und die Idee des Originals und seiner kontrollierten Nutzbarkeit wird durch die Möglichkeiten von digitaler Vervielfältigung und Veränderung (Remix) konterkariert.[4] Da die Unterbindung des Austauschs von Daten über Peer-to-Peer-Netzwerke auch eine Vielzahl von legalen Nutzungen betreffen würde, werden Strategien der Delegitimierung herangezogen, die zugleich den Aufbau von Kontrollapparaturen und die rechtliche Sanktionierung außerhalb des virtuellen Raums erlauben sollen. Auch hier lassen sich daher Momente der »Versicherheitlichung« beobachten, wobei es nun zum Schutz privaten Eigentums errichtete Filter sind, die ein nationales Ordnungsverständnis durchzusetzen versuchen. Rhetorisch auf den Punkt gebracht wird dies in der Metapher der Piraten, in der sowohl die Rechts- und Hoheitslosigkeit als auch die überfallartige Schädigung mitschwingen, die dem Gemeinwohl durch gänzlich unverantwortliche Horden drohen.[5] Dass diese negative Stigmatisierung durch den Begriff der Piraterie gegenwärtig zumindest teilweise in das Bild von Freiheitsliebe und Horizontalität umgekehrt wird und in Deutschland die Piraten gar in Form einer Partei im großen Stil im System angekommen sind, entbehrt nicht einer gewissen Ironie.

1:1-PROJEKTION NATIONALER SOUVERÄNITÄT IST SCHÄDLICH

Sowohl im Feld der Sicherheitspolitik als auch mit Blick auf die Durchsetzung der Eigentumsordnung zeigt sich also, dass Grenzen im virtuellen Raum nicht etwas von gestern sind, sondern vielmehr etwas, das heute zu etablieren versucht wird. Und dies geschieht nicht nur jenseits der OECD-Welt in autokratischen Regimen, wo man sich vor der Kraft von Facebook und Twitter fürchtet, sondern auch in den liberalen Demokratien des Westens, in denen die offenen Prinzipien des Internets zuerst formuliert wurden. Ganz unabhängig von der Frage, wie groß der wahre Kern der Argumente jeweils ist – immerhin wäre die cyber-romantische Gleichsetzung eines eingriffsfreien Raums mit demokratischer Selbstregierung ebenfalls kritisch zu erörtern –, muss diskutiert werden, ob die Strategie der lautstarken Grenzziehung nicht enorme Kollateralschäden nach sich zieht. Dass die 1:1-Projektion nationaler Souveränität schädlich ist, ändert sich daher auch nicht, wenn man feststellt,

4 Das wohl bekannteste Plädoyer für einen neuen Umgang mit Wissen und Kreativität im Netz stammt von Lawrence Lessig, Freie Kultur. Wesen und Zukunft der Kreativität, München 2004.

5 Dass in der gesamten Debatte eine rhetorische Abrüstung Not tut, wurde zuletzt mit Blick auf die innerdeutsche Urheberrechtsdebatte in den deutschen Feuilletons diskutiert. Siehe Frank Schirrmacher, Schluss mit dem Hass, in: Frankfurter Allgemeine Zeitung, 13.05.2012.

dass die Grenzziehung zwar mit Vehemenz propagiert wird, doch über die Frage ihres Erfolges noch lange nicht entschieden ist, sich vielmehr gerade wegen ihrer Plumpheit nun auch Gegenkräfte regen.

Bisher wurde bewirkt dass die Diagnose des Internets als etwas Ambivalentes und in mancher Hinsicht Bedrohliches – im traditionell eher technikskeptischen Deutschland ohnehin – viel Präsenz in der öffentlichen Diskussion einnimmt. Dass diese negative Politisierung nun Widerstandskräfte hervorruft, welche die Gefahr für die etablierte Kommunikationskultur erkennen und die (relative) Grenzenlosigkeit des Internets zu verteidigen suchen, ist eine logische Folge und wünschenswert.[6] Doch solange das Thema eines von Sicherheit und Bedrohung bleibt, so lange bleibt eine Durchsetzung des alten Denkens in Grenzen und Territorien wahrscheinlich. Es kommt daher alles auf das »Wie« der Regulierung an; und dieses »Wie« ist nicht nur technisch zu verstehen, sondern es umfasst auch die Rhetorik des Regulierungsdiskurses. Die Re-Etablierung nationaler Grenzen auf den Schultern wackeliger Metaphern und pauschalisierender Gleichsetzungen realweltlicher Raumvorstellungen mit digitaler Kommunikation unterschlägt die Möglichkeiten und das Potenzial des digitalen Raums.

Und darüber hinaus zieht die Debatte um staatliche Grenzziehung auch noch Aufmerksamkeit ab von einer anderen, viel subtileren Form der Grenzziehung, die gegenwärtig durchaus erfolgreich vorgenommen wird: die Parzellierung der Netzlandschaft in die Domänen weniger großer Internetunternehmen, die meist alle Nutzung in einem Angebot vereinen und es dann implizit über Anreize, Filter und zustimmungsbedürftige Geschäftsordnungen schaffen, das virtuelle Feld so einzugrenzen, dass Verbindungen aktiv kontrolliert, abgeschnitten und überwacht werden können. Apps treten an die Stelle freier Netzstandards und stellen einen ähnlichen Konterpunkt zur ursprünglichen Version des horizontalen Netzwerks dar, wie es auch staatliche Grenzen tun.[7] Ironischerweise bedarf es zur Entgegnung dieses Trends und zur Kontrolle der Unternehmen einer Regulierung, die zumindest nicht ohne staatliche Instanzen und deren realweltliche Zusammenarbeit gelingen kann. Diese müsste aber über Grenzen hinweg und mit dem Ziel der Erhaltung eines freien virtuellen Raums erfolgen.

6 Die Entwicklung des Politikfelds der »Netzpolitik« samt starker zivilgesellschaftlicher Akteure ist hierfür ein Zeichen. Den Versuch, ein solches Anliegen so programmatisch wie pragmatisch zu formulieren, unternehmen Markus Beckedahl u. Falk Lüke, Die digitale Gesellschaft, München 2012.

7 Diese Gefahr wird ausgeführt in Jonathan Zittrain, The Future of the Internet. And How to Stop It, London 2009.

Dr. Thorsten Thiel ist Politikwissenschaftler und arbeitet als Postdoc am Exzellenzcluster »Die Herausbildung normativer Ordnungen« an der Goethe-Universität in Frankfurt am Main. Schwerpunkte seiner Forschung sind Politische Theorie und Internationale Politik. Er ist Mitbegründer und Autor beim Theorieblog, ein Forum für Politische Theorie und Philosophie im Internet.