Gefordert sei die EU in der Elfenbeinküste darüber hinaus als ordnungspolitische Kraft in der Postkonfliktphase.

Insgesamt betrachtet ist Dialer eine umfassende politikwissenschaftliche Einführung in die Systematik und Problematik des Cotonou-Abkommens gelungen. Trotz des streckenweise technisch-deskriptiven Stils bleibt der Band gut lesbar sowie für entwicklungs- und europapolitisch Interessierte gleichermaßen aufschlussreich. Ein vollständiges Abkürzungs- und ein umfangreiches Literaturverzeichnis erleichtern den Gebrauch. Als sinnvoll erweist sich auch die angehängte Übersicht über die zwischen 1996 und 2004 geführten politischen Konsultationsverfahren im Krisenfall nach Artikel 366a des Lomé- bzw. Artikel 96/97 des Cotonou-Abkommens. Die Tabelle wirft jedoch auch Fragen auf und lässt erneut den Wunsch nach mehr Empirie im Hauptteil aufkommen. Unter welchen Bedingungen führen solche Konsultationen z. B. zum Erfolg? Wie kann ein Aussetzen der Vertragsbeziehungen in der Praxis vermieden werden? Werden die Sanktionsmöglichkeiten durch die EU einheitlich angewendet? Hier besteht zweifelsohne weiterer Forschungsbedarf.

Axel Biallas,
Berlin

RONALD DEIBERT / JOHN PALFREY / RAFAL ROHOZINSKI / JONATHAN ZITTRAIN (Hrsg.):
Access Denied. The Practice and Policy of Global Internet Filtering

Cambridge / USA 2008

MIT Press, 457 S.

In den 1990er Jahren löste das Internet insbesondere in den zivilgesellschaftlichen Segmenten vieler Staaten einen Enthusiasmus aus, der auf eine breiter angelegte politische Partizipation nicht nur in den westlichen Demokratien, sondern insbesondere auch in autoritär regierten Staaten abzielte. Die angenommene Unkontrollierbarkeit des Cyberspace sollte oppositionellen Parteien und Nichtregierungsorganisationen (NGOs) die Möglichkeit geben, ihre politischen Standpunkte zu verbreiten, ihre Anhängerschaft zu erweitern und langfristig einen Demokratisierungsprozess einzuleiten. Ignoriert wurde allerdings vielfach die Tatsache, dass in den jeweiligen Staaten nur ein Bruchteil der Bevölkerung überhaupt Anschluss an das Netz hatte, was in den folgenden Jahren auch weitestgehend so bleiben sollte. Der Informationsfluss konnte also hauptsächlich von besagten Staaten in z. B. westliche Demokratien laufen, von wo man sich Hilfe beim Aufbau demokratischer Strukturen erhoffte. So auch in Burma/Myanmar, wo sich zuletzt im September 2007 eine von Mönchen angeführte Protestbewegung den Weg in die weltweite Öffentlichkeit verschaffte, indem sie

Bilder und Filme ihrer Demonstrationen und Konfrontationen mit der Militärregierung über das Internet verbreitete. Anders als bei früheren Unruhen im Jahr 1988 dauerte es nun nicht mehr mehrere Tage, sondern lediglich wenige Stunden, bis Informationen den Weg in die weltweite Öffentlichkeit fanden. Doch auch die Militärregierung des Landes hatte nicht tatenlos zugesehen, wie ihr die Kontrolle des Informationsflusses entglitt. Entsprechend blockierte sie nach wenigen Tagen landesweit den Zugang zum Internet und schnitt das Land somit vom elektronischen Informationsaustausch ab.

Wie in dem gerade beschriebenen Fall nehmen weltweit zunehmend Regierungen Einfluss auf die Inhalte, die der Bevölkerung des jeweiligen Landes im Netz zur Verfügung stehen. Zuletzt wurde während der Olympischen Spiele in China in breiterem Umfang darüber berichtet, dass das Land bestimmte Bereiche des Internets blockiert. Dazu zählen vor allem Webseiten mit Bezug zu globalen Themen wie Menschenrechte und Demokratie, aber auch nationale Fragen wie die Situation von Uiguren, Mongolen und Tibetern in China. Mit »Access Denied« haben nun Wissenschaftler der OpenNet Initiative (ONI) die erste strikt akademische Studie zum Thema »Internet Filtering« vorgelegt. Die OpenNet Initiative ist ein Zusammenschluss von Mitarbeitern des Citizen Lab der Universität von Toronto, des Berkman Centre der Harvard Law School, der Advanced Network Research Group der Universität Cambridge und des Oxford Internet Institute. Die Studie befasst sich mit der Untersuchung von 40 Staaten im Jahr 2006 mit dem Ergebnis, dass 26 von ihnen Internetfilter nachweislich anwendeten. Bei der Auswahl der Staaten begrenzte das Forscherteam die Fälle hauptsächlich auf asiatische und afrikanische Staaten, mit einzelnen Ausnahmen aus Europa (Weißrussland, Moldawien und Ukraine) und Lateinamerika (Kuba und Venezuela). Die Tatsache, dass das Internet auch in westlichen Industriestaaten gefiltert wird, ließen sie mit dem Hinweis außen vor, dass zu diesen Ländern bereits an anderer Stelle publiziert wurde. Das Buch besteht aus sechs Kapiteln und einer anschließenden 280-seitigen Darstellung der Internetnutzung und Blockierung in allen Regionen der Welt sowie in den der Studie zugrunde liegenden Staaten.

Die Motive für das Filtern von Internetinhalten lassen sich Robert Faris und Nart Villeneuve von der ONI zufolge in drei Hauptbereiche teilen: politische Interessen, soziale Normen und Moralvorstellungen sowie Sicherheitsinteressen (S. 9). Hinzu fügen sie einen vierten Bereich, den sie als relevant für die Nutzung von Informationen aus den ersten drei Gebieten ausmachen: Internettools wie automatische Übersetzungsseiten, Webseiten zur anonymen Netznutzung (z. B. Proxyserver) oder Blogangebote. Dazu kommen Filtersysteme aus wirtschaftlichen Interessen, wie etwa zum Schutz geistigen Eigentums (so vor allem in Westeuropa und Nordamerika) oder auch »VoIP«-Angebote zum Telefonieren über das Internet, die zum Beispiel in Vietnam und Syrien blockiert werden. Den Autoren zufolge geschieht dies zum Schutz der einheimischen Telekommunikationsbranche, die von ausländischen Anbietern unterboten würde. Dabei findet

der Filtervorgang auf zwei Ebenen statt: auf nationaler Ebene über die gesamte Infrastruktur oder auf Ebene der Internet Service Provider (ISP). Die Techniken selbst beschreiben die Verfasser als »IP-Blocking«, »DNS-Tampering«, »Blockpage« und »Keyword«. Bei »IP-Blocking« handelt es sich um eine preiswerte, aber auch ungenaue Option, bei der einzelne IP-Adressen von ungewünschten Servern blockiert werden. Dadurch werden aber nicht einzelne auf diesem Server befindliche Seiten zensiert, sondern der gesamte Inhalt des Servers, so dass auch Inhalte betroffen sein können, die dem Zensurregime ihrem Inhalt zufolge nicht unterliegen würden. Beim »DNS-Tampering« wiederum sorgt eine ISP-interne Konfiguration dafür, dass mittels einer Veränderung von IP-Adressen bestimmte Webseiten nicht oder fehlerhaft angezeigt werden. Die dritte Technik wendet eine Liste bestimmter Webseiten an, bei deren Aufruf automatisch eine »Blockpage« angezeigt wird, also eine Webseite mit dem Hinweis darauf, dass die eigentlich aufgerufene Seite blockiert wurde. In einigen Staaten wie z. B. Tunesien haben »Blockpages« das Erscheinungsbild einer Internet-Explorer-Fehlermeldung, wodurch verschleiert wird, dass die gesuchte Seite gefiltert wurde. In anderen Fällen (z. B. Usbekistan) werden automatische Weiterleitungen eingesetzt, die den Anwender beim Aufruf einer gefilterten Seite auf eine offizielle Microsoftseite umleiten, um die stattgefundene Filterung nicht direkt zu offenbaren (S. 16). Der Keywordfilter funktioniert nach dem Suchprinzip innerhalb der Webseite. Während bei den vorherigen Techniken die Adressen der Webseiten durchsucht werden, findet in diesem Fall eine Suche auf der gesamten Seite statt – eine Technik, die allerdings zum Zeitpunkt der Untersuchung von keinem der in der Studie genannten Staaten nachweislich genutzt wurde. Interessant erscheint dabei, dass Filterregime nicht zwangsläufig zentral gesteuert werden und als eine direkt von Regierungsseite ausgehende Zensur betrachtet werden können. So ist es in einigen Ländern möglich, schriftlich Beschwerde gegen die Blockierung einzelner Webseiten einzulegen (z. B. in Iran, Saudi Arabien und Oman). Die Autoren gehen an dieser Stelle nicht weiter auf die Frage ein, auf welche Weise derartige Beschwerden bearbeitet werden. In anderen Fällen stellten die Autoren fest, dass einzelne ISP die Auswahl der zu filternden Seiten selbst bestimmten. Dies ist ein eindeutiger Hinweis darauf, dass keine zentralen Vorgaben zur Blockierung bestimmter Webangebote vorlagen.

Die Möglichkeit der Beschwerdeeinreichung lässt sich sogar als Eingestehung von Schwachpunkten im Internetfilterregime einzelner Staaten interpretieren. Denn kein Filtersystem schafft es bisher, sein Ziel exakt zu erreichen. Dort, wo eine große Zahl an Webseiten geblockt werden soll, fallen regelmäßig einzelne (oder auch viele) durch das Filtersystem. In anderen Fällen werden Webseiten geblockt, obwohl ihr Inhalt der jeweiligen Regierung als unbedenklich erscheint. »Overbreadth« und »underbreadth« nennen Jonathan Zittrain und John Palfrey dieses Phänomen (S. 46ff). Verantwortlich für diese Ungenauigkeit der Filterung ist die von den Staaten angewandte Methode. Viele nutzen kommerzi-

elle Serviceangebote von US-amerikanischen Firmen wie SmartFilter, Websense oder Fortinet. Im Angebot dieser Firmen befinden sich u. a. Filterlisten zu verschiedenen Themen wie Drogen, Glückspiel, Pornografie usw. Diese vorgefertigten Angebote können bei der Vielzahl an existierenden Webseiten kaum eine genaue Trefferquote erreichen. Dies liegt neben technischen Gründen auch daran, dass zwar englischsprachige Webangebote in die entsprechenden Listen aufgenommen werden, Webseiten in anderen Landessprachen aber oft nicht registriert werden. Zittrain und Palfrey zufolge kann aber auch ein ungenaues Filtersystem seine eigene Effizienz entfalten, indem es Anwendern deutlich macht, dass bestimmte Internetangebote als nicht erwünscht betrachtet und überwacht werden. Dadurch kann es zu einer Selbstzensur der Anwender kommen (S. 35). Aufgrund der je nach Staat variierenden Filtersysteme sprechen die Verfasser gar statt vom World Wide Web von einem Saudi Wide Web, einem Thai Wide Web oder einem Uzbek Wide Web. (S. 31). Das Resultat der Filterregime sei »(…) the emergence of an increasingly balkanized Internet« (S. 30).

Auf die technischen Aspekte des Filterns gehen Steven J. Murdoch und Ross Andersson in ihrem Beitrag »Tools and Technology of Internet Filtering« ein. Während die technischen Fragen in den vorherigen Beiträgen zwar erwähnt, aber nicht weiter erläutert wurden, beginnen die beiden Verfasser quasi bei null und geben eine kurze Einführung in die Funktionsweise des Internets. Dies geschieht sehr knapp und wird von einigen Grafiken unterstützt, was besonders für Einsteiger in die Materie eine große Hilfe sein wird. Denn ohne das Verständnis vom »Domain Name System« (DNS) oder »Proxyservern« lässt sich nicht nachvollziehen, wie eine Webseite tatsächlich geblockt werden kann. In kurzen Unterkapiteln werden hier verschiedene Filtermethoden dargestellt, wie »TCP/IP Header Filtering«, »TCP/IP Content Filtering«, »DNS Tampering« und »HTTP Proxy Filtering«. Darüber hinaus werden auch andere Sicherheitsaspekte wie »Denial of Service Attacks« (DoS) sowie Themen wie Zuverlässigkeit und Kosten kurz angesprochen, aber nicht sehr ausführlich behandelt.

Im vierten Kapitel, »Filtering and the International System«, führen Mary Rundle und Malcolm Birdling eine juristische Analyse durch, die sich zunächst mit grundsätzlichen Fragen und Akteuren des internationalen Systems auseinandersetzt und anschließend auf die Frage der Menschenrechte und insbesondere den Aspekt der Meinungsfreiheit eingeht. Dieser letztgenannte Punkt ist es auch, der sich anschließend durch das gesamte Kapitel zieht. An manchen Stellen erscheint es, als seien die Verfasser darum bemüht gewesen, in ihren rein juristischen Beitrag zumindest einen Hauch der Buchthematik einfließen zu lassen. So greifen sie stellenweise (z. B. auf S. 77) auf den Meinungsfreiheitsdiskurs im Rahmen des »World Summit on the Information Society« (WSIS) Prozesses zurück oder analysieren das Verhältnis zwischen Meinungsfreiheit und internationalem Handel unter Einbeziehung von eventuellen Filtervorgängen (S. 88ff). Auch wenn es sich insbesondere beim zweitgenannten um einen interessanten

Gedankengang handelt, so überwiegt im gesamten Kapitel doch eher die juristische Diskussion um Meinungsfreiheit an sich. Die Internetfilterthematik wird nur stellenweise erwähnt.

Das fünfte Kapitel befasst sich wieder mit dem zentralen Thema des Buches und geht auf die Problematik der beteiligten Akteure aus der Privatwirtschaft ein, die in Filterprozesse in verschiedenen Ländern gewollt oder ungewollt involviert sind. Wie bereits in den vorherigen Kapiteln dargestellt wurde, befindet sich die Mehrzahl der filternden Staaten in den Regionen Asien, Nordafrika, Mittlerer Osten, in Zentralasien und anderen GUS-Staaten. Bei den Softwarefirmen, die die benötigte technische Unterstützung anbieten, handelt es sich dagegen in der Regel um westliche, insbesondere US-amerikanische Firmen. Beim Eintritt in die Märkte der genannten Regionen müssen diese Firmen eine Selbstzensur durchführen, da ihnen ansonsten der Zugang von den jeweiligen Regierungen untersagt wird. Global Player wie Microsoft, Google oder Cisco waren aus diesem Grunde in der Vergangenheit internationaler Kritik ausgesetzt. Sie sahen sich mit dem Vorwurf konfrontiert, demokratische Grundregeln und insbesondere die Menschenrechte zu missachten und sich dem Wunsch autoritärer Regime zu beugen. Dabei sind es nicht nur die großen Firmen der Branche, die sich in dieser Situation befinden. Zittrain und Palfrey zufolge sind fast alle IT-Firmen von diesem Problem betroffen, wenn sie in den genannten Regionen tätig werden wollen. Gleichzeitig ist die Liste der filternden Staaten in den vergangenen Jahren immer weiter gewachsen. »As this book makes plain, over the past five years there has been a steady rise of Internet filtering practices from a handful of states in 2002 to over three dozen states in 2007« (S. 105). Die Verfasser schlagen zur Lösung des Konflikts die Selbstregulierung der Industrie in Form eines »code of conduct« vor. Und tatsächlich haben bereits einige der weltweit agierenden Firmen damit begonnen, gemeinsame Verhaltensnormen im Umgang mit filternden Staaten zu entwickeln. Es bleibt abzuwarten, welche Firma als Erste diese Normen unterläuft, um einen »ethisch orientierten« Konkurrenten auszuschalten oder ob der Verhaltenskodex der Industrie tatsächlich in einer juristischen Festlegung auf internationaler Ebene resultieren wird.

Bevor die ausführliche Darstellung aller in der Studie untersuchten Staaten beginnt, befassen sich Ronald Deibert und Rafal Rohozinski im sechsten Kapitel mit der Rolle der Zivilgesellschaft und der Funktion, die das Internet für ihre Arbeit hat. Sie unterscheiden dabei »civic networks«, »resistance networks« und »dark nets« (S. 124). »Civic networks« arbeiten demzufolge schwerpunktmäßig in den Bereichen Umwelt, Frieden und soziale Gerechtigkeit, während »resistance networks« radikale Gruppen beinhalten, die durch zivilen Ungehorsam oder andere Methoden agieren und die von den von ihnen kritisierten Regierungen unter Umständen als illegal betrachtet werden. In die Kategorie »dark nets« fallen bewaffnete soziale Bewegungen ebenso wie kriminelle Organisationen. Zugehörige aller drei Kategorien haben in den vergangenen Jahren ver-

stärkt von der Verbreitung des Internets profitiert – sei es durch virtuelle Fundraisingkampagnen, Onlineproteste, Vernetzungsaktivitäten oder die Verbreitung von Propagandavideos. Hinzu kommen herkömmliche kriminelle Aktivitäten wie Betrug oder Diebstahl, die in einer virtuellen Variante betrieben werden und deren Täter Schutz durch die Anonymität des Internets genießen. Die international kritisierten und bekämpften »Dark net«-Gruppen werden von Regierungen oft als Begründung für die Einschränkung der Internetnutzung herangezogen. Der ONI-Studie zufolge werden dadurch jedoch auch (bewusst oder unbewusst) »civic« und »resistance networks« in ihrer Arbeit eingeschränkt. An dieser Stelle gehen die Verfasser auf einzelne Themen wie unabhängige Medienwebseiten, Internettools und Blogs ein, verpassen es jedoch, überzeugende Beispiele für die Benachteiligung von beispielsweise NGOs durch die staatliche Bekämpfung von »dark nets« zu liefern. Das einzige Beispiel, das in diese Richtung geht, ist die Blockierung von Hackingwebseiten, die illegale Softwaredownloads und andere auch für NGOs nützliche Internetanwendungen anbieten. Deibert und Rohozinski zufolge werden NGOs dadurch eingeschränkt, dass durch die Blockierung besagter Webseiten »Dark net«-Bewegungen der Zugriff auf illegale Softwarekopien erschwert werden soll. Was sie anscheinend aus ihrer westlichen Perspektive nicht bedacht haben, ist die Tatsache, dass im Rest der Welt auch Mitglieder der von ihnen durchgehend als ehrenvoll dargestellten »civic networks« illegale Software nutzen, da ein kommerzieller Erwerb für die Masse kleiner Organisationen in Asien, Afrika und Lateinamerika kaum möglich ist.

Die in den vergangenen Jahren stark gewachsene Zahl der Staaten, die Internetfilter anwenden, zeigt, dass dieses relativ neue Thema eine größere Aufmerksamkeit verdient, als dies bisher geschehen ist. Das vorliegende Buch »Access Denied« ist als erste umfassende wissenschaftliche Studie zu diesem Thema ein wichtiger Beitrag und (nicht nur) deshalb sehr zu empfehlen. Die Verfasser sprechen verschiedene politische, juristische und technische Aspekte an und bieten zudem eine interessante Darstellung des Internets in allen 40 untersuchten Staaten. Passend zum Thema kündigen sie außerdem an, im Laufe der Zeit Aktualisierungen zu den einzelnen Staaten auf der Webseite der OpenNet Initiative (http://www.opennet.net) hinzuzufügen.

Daniel Oppermann,
Universität von Brasília