h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Informatik und Gesellschaft

Sommersemester 2013

Victor Hahn, Donia Dhaouadi

Internetzensur:

Freiheitsberaubung zum Wohle der Gesellschaft?

Inhaltsverzeichnis

1 Einleitung

Diese Arbeit untersucht den Themenkomplex der Zensur in seiner besonderen Anwendung auf die Kommunikation über das Internet. Zunächst werden wir im nächsten Kapitel die spezifischen Voraussetzungen des Internets analysieren. Wir werden verschiedene typische Angriffsszenarien formulieren sowie deren technische Umsetzbarkeit aufzeigen. Weiter diskutieren wir typische Schutzmaßnahmen vor Zensurversuchen und deren Probleme sowie Grenzen. Hierbei versuchen wir, die technischen Aspekte so ausführlich, akkurat und gleichzeitig behutsam vereinfacht darzustellen, dass sie auch für fachfremde Leserinnen und Leser verständlich sind.

Anschließend werden wir anhand einiger Beispiele aus verschiedenen Regionen der Welt das politische und gesellschaftliche Potenzial der freien Kommunikation über das Internet untersuchen. Wir werden anhand einiger ausgewählter Szenarien der Gegenwart sowie der letzten Jahre zeigen, in welchen Situationen und aus welchen politisch-gesellschaftlichen Motiven Wünsche nach Zensur entstanden und auf welche Art diese umgesetzt wurden.

Diese grobe Zweiteilung – technische Grundlagen sowie isolierte Beispiele aus der Praxis – erschien uns als eine geeignete Darstellungsform für dieses Thema, um mit ausreichend fachlichen und praxisbezogenen Informationen eine eigene Meinungsbildung zu ermöglichen. Neben einer Einführung in die Begriffe und eines technischen Angriffsmodells haben wir die Schwerpunkte auf einzelne Beispiele gelegt, die uns zur Verdeutlichung der Natur der Zensur besonders nützlich erschienen. Es ergibt sich von selbst, dass wir mindestens ebensoviele gleichermaßen oder, je nach Sicht des Lesers, sogar bessere Beispiele ausgelassen haben.

Zensur ist kein internetspezifisches Phänomen. An zahlreichen Stellen dieser Arbeit werden Parallelen zur klassischen Zensur nichtelektronischer Medien deutlich erkennbar sein. Die Beschränkung dieser Arbeit auf das Medium Internet ist eine Spezialisierung, keine Abgrenzung. Jedoch kommt dem Internet als sehr schnellem, direktem und leicht zugänglichem Medium gerade in unruhigen Zeiten durchaus auch eine besondere Rolle zu, wie einige unserer Beispiele zeigen werden.

1.1 Begriffsdefinitionen

Wikipedia definiert[WIKI-2013a] den Begriff **Zensur** wie folgt:

> »*Zensur (...) ist ein restriktives Verfahren von in der Regel staatlichen Stellen, um durch Massenmedien oder im persönlichen Informationsverkehr (...) vermittelte Inhalte zu kontrollieren, unerwünschte beziehungsweise Gesetzen zuwiderlaufende Inhalte zu unterdrücken und auf diese Weise dafür zu sorgen, dass nur erwünschte Inhalte veröffentlicht oder ausgetauscht werden.*«

Auf diese Definition werden wir uns im Weiteren beziehen. In diesem Zusammenhang verwenden wir auch den Begriff *Zensor*, um eine Person oder Institution zu beschreiben, die Maßnahmen im Sinne dieser Definition ausübt, sowie das Adjektiv *zensiert* als Eigenschaft von Daten, gegen die solche Maßnahmen unternommen wurden.

Der Begriff der Zensur ist kein eindeutiger. Wikipedia verweist zusätzlich auf zwei weitere Definitionen.

> »*von zuständiger, besonders staatlicher Stelle vorgenommene Kontrolle, Überprüfung von Briefen, Druckwerken, Filmen o. Ä., besonders auf politische, gesetzliche, sittliche oder religiöse Konformität*«
>
> – Duden online[DUD-2013]

> »*[lat.] Z. bezeichnet die in modernen Demokratien strikt abgelehnte (politische) Kontrolle öffentlich geäußerter Meinungen (in Presse, Funk und Fernsehen, aber auch im Bereich der Literatur, Kunst etc.). Die Ausübung der Z. wird in nicht- oder vordemokratischen Ländern durch neue Medien (Satellitenfunk, -fernsehen, Internet) erschwert.*«
>
> – Bundeszentrale für politische Bildung[BPB-2013]

Diese beiden Definitionen vermitteln ein sehr klassisches, fast schon altmodisches Verständnis des Zensurbegriffs, indem sie sich sehr auf Medien jenseits eines Alters von etwa dreißig Jahren stützen. Insbesondere die Definition, die die Bundeszentrale für politische Bildung aus der Literatur übernommen hat, wirkt aus heutiger Sicht fast schon etwas hilflos, wenn sie in einem Nachsatz den Begriff *neue Medien* auf im Gegensatz dazu „aktuelle" Entwicklungen wie Satellitentechnik oder eben das Internet anwendet.

Bei der Betrachtung des Begriffs *Zensur* sind die beiden Varianten *Vorzensur* und *Nachzensur* voneinander zu unterscheiden. Die beiden Definitionen von Duden online und der Bundeszentrale erwecken dabei den Eindruck, sich nur auf erstere zu beziehen.

Vorzensur beschreibt die Möglichkeit des Zensors, Informationen noch vor ihrer Publikation zu prüfen und gegebenenfalls die Verbreitung von vornherein zu vebieten.

Bei der **Nachzensur** dagegen ist die Publikation zunächst frei, kann durch den Zensor jedoch im Nachhinein unterbunden und sanktioniert werden.

Wir beziehen uns in dieser Arbeit stets auf beide Varianten. Im Rahmen unseres in Kapitel 2 vorgestellten Angriffsmodells werden wir auf diese Begriffe eingehen.

Auf eine Definition des Begriffs *Internet* verzichten wir an dieser Stelle.

Den Begriff der **Gesellschaft** definiert Reinholds Soziologielexikon wie folgt[HIL-1997]:

> »*Als soziologischer Grundbegriff bezeichnet G. die umfassende Ganzheit eines dauerhaft geordneten, strukturierten Zusammenlebens von Menschen innerhalb eines bestimmten räumlichen Bereichs.*«

Freiheitsberaubung ist in Deutschland ein definierter Begriff des Strafrechts.

> »*Wer einen Menschen einsperrt oder auf andere Weise der Freiheit beraubt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.*«
>
> – § 239 Abs. 1 StGB

Wie unschwer zu erkennen ist, handelt es sich bei der Verwendung des Begriffs im Titel dieser Arbeit lediglich um eine Metapher.

Im Zuge der seit etwa zehn Jahren bestehenden Diskussion um den Begriff der „Digital Natives“ – also der Frage, in wie weit digitale Medien und insbesondere das Internet für die Generationen, die bereits mit diesen Technologien aufgewachsen sind, eine besondere Bedeutung haben, die sich durch den klassischen Medienbegriff nicht mehr fassen lässt – möchten wir im Hintergrund stets die Frage stellen, in wie weit eine solche Analogie mit entsprechenden Konsequenzen gezogen werden muss.

Eine Antwort geben wir nicht vor.

1.2 Problem der Inhaltsbestimmung digitaler Daten

Zensur zielt, wie auch der von uns verwendeten Definition zu entnehmen ist, darauf ab, die Verbreitung bestimmter Kommunikationsinhalte zu unterdrücken.

In der Informationstechnik werden Daten durch digitale Symbolsequenzen ausgedrückt. Dies ist zunächst kein Unterschied zu einem der ältesten bekannten Kommunikationshilfsmittel, der Buchstabenschrift. Im Gegensatz zu dieser setzen elektronische Systeme jedoch maschinenlesbare Codierungen ein, die erst nach Übersetzung z.B. eben in Buchstabenschrift wieder einen Wert für die menschliche Kommunikation erhalten.

Während manche dieser Darstellungen, wie z.B. die grundlegende Zeichencodierung mittels ASCII oder Unicode, mit etwas Aufwand und Übung auch ohne technische Hilfsmittel lesbar sind, ist bei anderen, etwa komprimierten Daten, der Einsatz von Computern zur Decodierung unverzichtbar.

4 85650 78965 73978 29309 84189 46942 86137 70744 20873 51357 92401
96520 73668 69851 34010 47237 44696 87974 39926 11751 09737 77701
02744 75280 49058 83138 40375 49709 98790 96539 55227 01171 21570
25974 66699 32402 26834 59661 96060 34851 74249 77358 46851 88556
74570 25712 54749 99648 21941 84655 71008 41190 86259 71694 79707
99152 00486 67099 75923 59606 13207 25973 79799 36188 60631 69144
73588 30024 53369 72781 81391 47979 55513 39994 93948 82899 84691
78361 00182 59789 01031 60196 18350 34344 89568 70538 45208 53804
58424 15654 82488 93338 04747 58711 28339 59896 85223 25446 08408
97111 97712 76941 20795 86244 05471 61321 00500 64598 20176 96177
18094 78113 62200 27234 48272 24932 32595 47234 68800 29277 76497
90614 81298 40428 34572 01463 48968 54716 90823 54737 83566 19721
86224 96943 16227 16663 93905 54302 41564 73292 48552 48991 22573
94665 48627 14048 21171 38124 38821 77176 02984 12552 44647 44505
58346 28144 88335 63190 27253 19590 43928 38737 64073 91689 12579
24055 01562 08897 87163 37599 91078 87084 90815 90975 48019 28576
84519 88596 30532 38234 90558 09203 29996 03234 47114 07760 19847
16353 11617 13078 57608 48622 36370 28357 01049 61259 56818 46785
96533 31007 70179 91614 67447 25492 72833 48691 60006 47585 91746
27812 12690 07351 83092 41530 10630 28932 95665 84366 20008 00476
77896 79843 82090 79761 98594 93646 30938 05863 36721 46969 59750
27968 77120 57249 96666 98056 14533 82074 12031 59337 70309 94915
27469 18356 59376 21022 20068 12679 82734 45760 93802 03044 79122
77498 09179 55938 38712 10005 88766 68925 84487 00470 77255 24970
60444 65212 71304 04321 18261 01035 91186 47666 29638 58495 08744
84973 73476 86142 08805 29443

Abb. 1: Erste illegale Primzahl

Hieraus ergibt sich das prinzipielle Problem, dass digitale Daten nicht eindeutig sind. Sie besitzen keine intrinsische Decodiervorschrift, so dass sich ihre Bedeutung erst aus dem verwendeten Decodieralgorithmus ergibt.

Dieser Umstand wurde sich bereits mehrfach zu Nutze gemacht, um Zensurversuche zu umgehen.

Insbesondere die Interpretation als Zahl ist dabei bei jeder Art durch Computer verarbeitete Daten naheliegend. 1999 entwickelten[WIKI-2013b] der Norweger Jon Lech Johansen, der Brite Mark Roberts sowie ein unbekannter Dritter *DeCSS*, ein Programm zur Umgehung des *Content Scrambling Systems*, des Kopierschutzes der damals noch recht neuen Video-DVDs. Als Folge aus dem von inzwischen 90 Ländern[WIPO-2013] ratifizierten WIPO-Urheberrechtsabkommen, das die Vertragsstaaten verpflichtet, „angemessenen rechtlichen Schutz und effektive rechtliche Mittel“[1] gegen Kopierschutzumgehung bereitzustellen, ist die Verbreitung derartiger Software in den meisten Teilen der Welt verboten und mit Strafe bedroht[2].

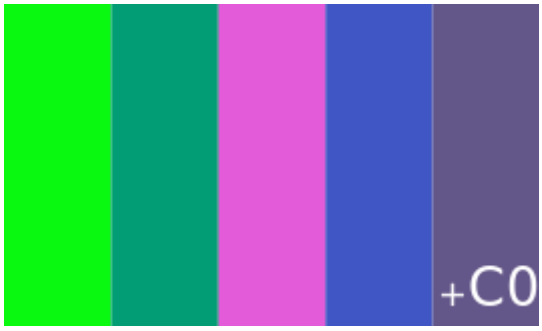

Abb. 2: „Free Speech Flag“

Neben verschiedenen weiteren Personen versuchte auch der Mathematiker Phil Carmody[CAR-2010], diesen Zensurversuch zu umgehen. Hierzu fand er 2001 mehrere Darstellungen von *DeCSS* sowohl im Quellcode sowie auch als ausführbares Kompilat, die sich ebenso als Primzahlen interpretieren lassen[WIKI-2013c][CAR-2001]. Primzahlen, insbesondere lange Primzahlen, werde in der Mathematik alleine auf Grund ihrer Primzahl-Eigenschaft archiviert und öffentlich zugänglich gemacht. Die Verbreitung dieser Information ist nicht sinnvoll zensierbar.

Zu einem ähnlichen Zensurversuch mit kreativer Gegenmaßnahme kam es 2007, als einer der Schlüssel des *Advanced Access Content System*, dem auf Blu-Ray-Discs eingesetzten Kopierschutzsystem, im Internet veröffentlicht wurde.

---

1 Artikel 11: „Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.“ [WIPO-1996]

2 In Deutschland ist das Verbot in §108b UrhG normiert und mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bedroht. In den USA ist das Verbot in 17 USC §1204 normiert und mit Freiheitsstrafe bis zu zehn Jahren oder Geldstrafe bis zu einer Million Dollar bedroht.

Zahlreiche Benutzer begannen daraufhin, ein Bild einer aus fünf farbigen Streifen und der Aufschrift „+C0“ bestehenden Flagge zu verbreiten, das als „Free Speech Flag“ bekannt wurde[WIKI-2013d].

Jede dieser Farben wird im RGB-Farbsystem mit Hilfe von drei Farben beschrieben, die für den jeweiligen Rot-, Grün- und Blauanteil der Farbe stehen. Interpretiert man diese fünf mal drei Zahlenwerte als zusammenhängende Zahl und hängt an deren Hexadezimaldarstellung schließlich noch die Ziffern „C0“ an, ergibt sich genau der zensierte Schlüssel.

Solche Versuche, Zensurmaßnahmen durch mehrdeutige digitale Daten zu umgehen, sind Teil der *Steganographie*. Hierauf gehen wir in Abschnit 2.2.1 genauer ein.

Das Problem, dass digitale Daten inhärent mehrdeutig sind, führt uns dazu, zusätzlich folgende technische Hilfsdefinition für den Begriff der Zensur zu treffen.

> »*Einschränkung oder Verbot bestimmter Datenübertragungen aufgrund ihres Inhalts bzw. einer bestimmten Decodierbarkeit* «

2 Zensuransätze und Gegenmaßnahmen

Aus Sicht des Internets – eines dezentralen, ausfallresistenten und auf dem Best-Effort-Prinzip basierenden Kommunikationsnetzes – kann der Versuch von Zensur, d.h. der Versuch, bestimmte Datenübertragungen zu stören, als Angriff aufgefasst werden. Das möchten wir an dieser Stelle tun und, wie das in der IT-Sicherheit üblich ist, zunächst ein Modell aufstellen, das realistische Zensurmaßnahmen beschreibt.

Selbstverständlich ist dieses Modell nicht vollständig. Es beschreibt jedoch die Szenarien, die aus unserer Sicht besonders typisch und relevant sind. Vergleiche hierzu auch die praktischen Beispiele in Kapitel 3.

2.1 Modell möglicher Zensurmaßnahmen

Fünf verschiedene Maßnahmen möchten wir hier als besonders relevant vorstellen. Diese sind nicht disjunkt. In einem Zensurvorhaben können – und werden zumeist – mehrere parallel angewendet. Teilweise bestehen semantische Zusammenhänge zwischen diesen Maßnahmen. Wo das der Fall ist, weisen wir darauf hin.

Zur Visualisierung des Modells verwenden wir in den Abbildungen dieses Abschnitts drei Grundsymbole: Die Dame mit dem Dokument stellt die Kommunikatorin dar. Sie möchte eine unerwünschte Information publizieren. Der Herr mit dem Polizeihelm steht für den Zensor – unabhängig davon, ob dieser für eine staatliche oder private Stelle agiert. Die Person im Anzug stellt einen Dienstleister dar, den die Kommunikatorin für ihre Publikation benötigt. Das kann beispielsweise ein Webhoster, Serveradministrator, oder Rechenzentrumbetreiber – aber auch ein Journalist oder Blogger sein, der für die Kommunikatorin die öffentliche Bereitstellung übernimmt.

Der Einfachkeit halber bezieht dieses Modell sich zunächst immer auf mögliche Zensurmaßnahmen gegen Kommunikatoren. Grundsätzlich – wenn auch unter in der Regel wesentlich höherem Aufwand, da mehr Personen betroffen sind – kann Zensur aber auch gegen den Rezipienten geübt werden. Wann immer dies anwendbar ist, weisen wir darauf hin.

2.1.1 Vorgaben an den Kommunikator selbst

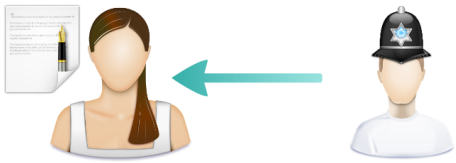

Abb. 3: Angriffsszenario 1

Die Basismethode nahezu jeder Zensur. Durch Gesetze, Verordnungen oder auch privatrechtliche Vorschriften werden der Kommunikatorin noch im Vorfeld unerwünschte Veröffentlichungen untersagt. Dies kann pauschal für eine gesamte soziale Gruppe (z.B. Staatsbürger, Einwohner, Mitarbeiter), für eine einzelne Person verdachtsunabhängig oder auch als Reaktion auf einen konkreten Veröffentlichungsplan erfolgen.

In aller Regel wird dieses Verbot mit Androhung eines empfindlichen Übels[3] (z.B. Geldstrafe, Freiheitsstrafe, Verlust von Rechten / Status / Ehre, Verlust des Arbeitsplatzes, Ausschluss aus einer Organisation, Tod) gestützt.

Nach dem gleichen Prinzip kann ein Kommunikator auch nach seiner Publikation zu deren Rücknahme bzw. Löschung bewegt werden.

Diese Maßnahme ist auch gegen Rezipienten anwendbar. In diesem Fall bezieht sich das Verbot auf den Empfang oder den Besitz bestimmter Informationen.

3 Formulierung in Anlehnung an den Tatbestand der Nötigung im deutschen Strafrecht, vergleiche § 240 StGB.

2.1.2 Vorgaben an den Dienstleister

Kaum ein Kommunikator ist in der Lage, Internetveröffentlichungen komplett selbstständig vorzunehmen. Wie eingangs erwähnt, werden zumeist ganz spezifische Dienstleister benötigt, die der Zensor konkret in Bezug auf eine bestimmte Publikation zur Kooperation auffordern kann. Nach einer unerwünschten Veröffentlichung kann er von diesen zumeist schlicht die Löschung fordern.

Abb. 4: Angriffsszenario 2

Auch diese Maßnahme wird in nahezu allen Bereichen angewandt, in denen bestimmte Publikationen unerwünscht sind. Im privatrechtlichen Bereich sind hier insbesondere Löschungsaufforderungen an Webhoster zur Wahrung von Urheberrechten zu nennen.

2.1.3 Scan auf unerwünschte Inhalte

Die klassische Vorzensur existiert auch im Internet. Veröffentlichungen können im Zuge ihres Publikationsprozesses auf unerwünschte Inhalte kontrolliert werden. Relevanter als die klassische Vorkontrolle durch einen menschlichen Zensor ist im Internet jedoch der automatische Scan.

Von der Kommunikatorin genutzte Dienstleister können – freiwillig oder auf Zwang des Zensors – übermittelte Inhalte auf bestimmte allgemeine Muster oder auf Ähnlichkeit mit bekannten unerwünschter Inhalten untersuchen. Allgemeine Muster können beispielsweise bestimmte Worte, Klänge, geometrische Figuren oder Sprachmuster sein. Bekannte unerwünschte Inhalte können über Listen erfasst werden.

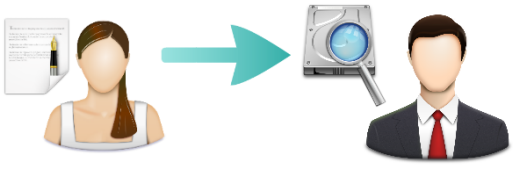

Abb. 5: Angriffsszenario 3

Eine Überprüfung übermittelter Inhalte kann daneben auch zur Nachzensur genutzt werden, beispielsweise um physische Repression gegen die Kommunikatorin zu üben (Angriffsszenario 5). Hierzu gehört auch der Bereich der Telekommunikationsüberwachung, also im Bereich der Internetzensur das Abhören des Internetanschlusses.

2.1.4 Sperren von Diensten

Von der Kommunikatorin genutzte Dienstleister können durch den Zensor unverfügbar gemacht werden. Dieses Mittel wird in der Regel angewandt, wenn sich Versuche der Einflussnahme (vorherige zwei Abschnitte) als nicht zielführend oder zu aufwendig erweisen.

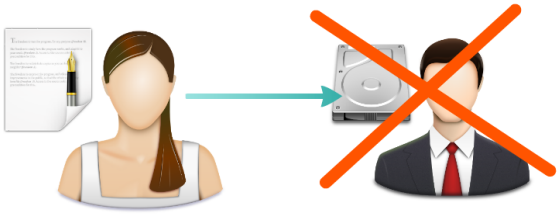

Abb. 6: Angriffsszenario 4

Hierbei sind zumeist keine Maßnahmen gemeint, die den Geschäftsbetrieb des Dienstleisters als solches schädigen (z.B. durch Sabotage). Vielmehr geht es meist darum, die Erreichbarkeit eines Dienstes für eine definierte Benutzergruppe zu schädigen. Insbesondere staatliche Zensoren können sich dabei meist der Hilfe des Internet Service Providers der Kommunikatorin bedienen. Oft werden derartige Zensurmaßnahmen für ganze Staaten vorgenommen.

Diese Maßnahme ist gleichermaßen gegen Kommunikatoren wie auch gegen Rezipienten einsetzbar.

Zwei technische Verfahren zur Zugangsverhinderung sind hierbei besonders zu nennen.

Einflussnahme auf das Domain Name System

Beim Zugriff auf eine Webseite über deren (auf menschliche Lesbarkeit ausgelegte) **Domain** muss diese zunächst in die (zur technischen Abwicklung verwendete) **IP-Adresse** aufgelöst werden. Diese Aufgabe übernehmen spezielle Verzeichnisdienste, die **DNS-Server**.

Zwei verschiedene Rollen von DNS-Servern sind zu unterscheiden: Autoritative DNS-Server werden vom Dienstleister selbst betrieben und mit den korrekten Informationen bespielt. Sie sind als zuständig für die jeweiligen Dienste anerkannt – „ihr Wort gilt". Auf diese Server hat der Zensor nur selten Einfluss.

Nicht-autoritative DNS-Server sind dagegen nur für die Verteilung dieser Informationen zuständig. So betreibt in der Regel jeder Internet Service Provider einen DNS-Server, den die Kunden für ihre Anfragen nutzen können und sollen. Dieser bezieht seine Informationen in gewissen Zeitabständen und wannimmer benötigt von den autoritativen Servern.

Nicht-autoritative DNS-Server können bestimmte Dienste zensieren, indem sie Kunden für diese schlicht keine Antworten liefern oder aber die Nutzeranfragen mittels gefälschter Antworten auf andere Dienste umleiten. Ein Zensor mit Einfluss beispielsweise auf einen bestimmten Internet Service Provider kann dies veranlassen.

Solche DNS-basieren Sperren lassen sich durch den betroffenen Nutzer recht leicht umgehen, indem dieser einen anderen DNS-Server nutzt. Neben Servern anderer Internet Service Provider stehen auch eine Reihe öffentlicher Server zur Verfügung. Besonders bekannt ist beispielsweise der vom Unternehmen Google Inc. unter der IP-Adresse 8.8.8.8 betriebene.

Einflussnahme auf das Routing

Auch nachdem die IP-Adresse eines gewünschten Dienstes bestimmt wurde, ist noch nicht gesichert, dass Anfragen auch tatsächlich bei diesem Dienst ankommen. Auf welchem Weg Daten in Rechnernetzen wie dem Internet transportiert werden, bestimmen spezielle, meist an Knotenpunkten untergebrachte Geräte, die sogenannten **Router**. Über verschiedene Kommunikationsprotokolle teilen sich die Router dabei gegenseitig mit, welche Netz-Teile über sie zu erreichen sind. Für das Routing zwischen verschiedenen Netzsegmenten (den sogenannten *Autonomen Systemen*) wird im Internet hierfür das **Border Gateway Protocol** (BGP) eingesetzt.

Auch hier gilt, dass ein Zensor meist nur Zugriff auf die Router einzelner Internet Service Provider hat. Hat er Zugriff auf das Routing des von der Kommunikatorin genutzten Providers, kann er wiederum den Zugriff unterbinden (durch Einstellung in den Routern, die Anfrage trotz eigentlich bekannter Route zu verwerfen) oder an einen anderen Dienst umleiten (durch manuelle Einstellung einer gefälschten Route).

Bei Einstellung einer gefälschten Route ist es auch möglich, dass diese über BGP an andere Internet Service Provider übermittelt wird. Theoretisch ist damit auch eine über diesen Provider hinausgehende Zensur möglich. In der Praxis führt dies seitens der Fremdprovider zu einem Ausschluss aus dem BGP-Routenaustausch.

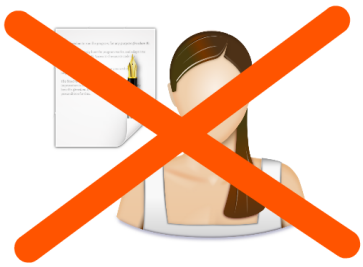

Abb. 7: Angriffsszenario 5

2.1.5 Direkte Repression

Diese einfachste denkbare Zensurmaßnahme ist vollkommen internetunspezifisch. Die Kommunikatorin selbst kann beispielsweise durch Entzug der Internetanbindung, Freiheitsentzug oder Tötung von Veröffentlichungen abgehalten werden.

2.2 Gegenmaßnahmen

Zensurmaßnahmen sind nicht perfekt. Mit verschiedenen technischen Maßnahmen ist es meist möglich, sie zum umgehen. Nach bewährtem Muster möchten wir auch hier wieder eine Auswahl bekannter und besonders relevanter Abwehrmaßnahmen vorstellen. Zu jeder Gegenmaßnahme werden wir kurz erläutern, gegen welche Zensurmaßnahmen sie Schutz bietet und welche Risiken hierbei bestehen.

Eine Ausnahme bilden hier unsere Angriffsszenarien 1 und 5 aus dem vorangehenden Abschnitt. Ersteres basiert lediglich auf Angst und anderem psychologischen Druck auf die Kommunikatorin und kann damit jederzeit mit dem Willen, entsprechende Folgen zu riskieren, „umgangen“ werden. Angriffsszenario 5 ist, zumindest in seiner endgültigen Ausprägung, nicht umgehbar.

Auch für die Darstellung der Gegenmaßnahmen setzen wir wieder auf Symbolbilder zur Visualisierung. Die Kommunikatorin ist nur noch als Relief zu sehen, um zu verdeutlichen, das sie sich nun im Veborgenen bewegt. Wannimmer wir genauer auf ein spezielles technisches Systems zur Zensurabwehr eingehen und das in Abschnitt 2.1 beschriebene Kommunikations- und Zensurmodell in den Hintergrund tritt, werden wir unsere Kommunikatorin auch schlicht als Benutzerin beschreiben. Ebenso wird der Dienstleister aus unserem Kommunikationsmodell in solchen Fällen schlicht zum Kommunikationspartner.

2.2.1 Steganographie

Bestimmte Aspekte dieser Gegenmaßnahme haben wir bereits erwähnt, als wir das Problem der Uneindeutigkeit digitaler Daten behandelt haben. Steganographie bezeichnet allgemein das Verstecken von Daten in anderen Daten. Beispiele dafür, wie dies unter Ausnutzung verschiedener Intepretierungen eines einzigen Bitmusters geschehen kann, finden sich in Abschnitt 1.2.

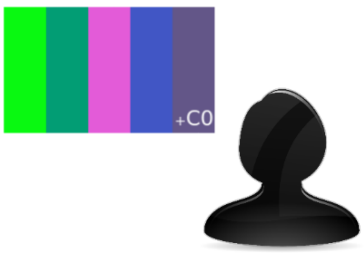

Abb. 8: Steganographie

Steganographie ist jedoch ein allgemeineres Konzept[WIKI-2013e]. Sehr gut geeignet zum Verstecken von Informationen sind beispielsweise Datensätze, die von Natur aus Rauschen – d.h. jede Art kleinster zufälliger Ungenauigkeiten enthalten. Neben dem Bereich der Audiodaten, aus dem der Begriff „Rauschen“ entstammt, betrifft dies auch Bilder, insbesondere Fotografien. Auf Grund unvermeidbarer technischer Ungenauigkeiten der in Kameras verwendeten Bildsensoren ist jedes Pixel eines Bildes immer ganz leicht fehlerhaft – gehen wir von Graustufenbildern aus, bedeutet das, entweder minimal zu hell oder minimal zu dunkel. Je schlechter die Lichtverhältnisse bei der Aufnahme, desto stärker ist dieses Rauschen.

Abb. 9: Steganographie in Bilddateien
links: Container – rechts: Geheimbild

Die Tatsache, dass kleinste Ungenauigkeiten in digitalen Daten also in manchen Anwendungsbereichen akzeptiert und erwartet werden, kann man sich zu Nutze machen, indem man geheime Informationen in diesen vermeintlichen Ungenauigkeiten codiert.

Abbildung 9 zeigt ein Beispiel für diese Art von Steganographie. In dem linken Bild (zwei Bäume) ist das rechte (Katzenbild) unsichtbar versteckt. Digitale Farbbilder werden – vorbehaltlich einer eventuellen Kompression – gespeichert, indem zu jedem Pixel drei Byte, also drei Werte zwischen 0 und 255 abgelegt werden, die für den jeweiligen Rot-, Grün- und Blauanteil des Bildes stehen. Missbraucht man nun die niederwertigsten zwei Bits jedes dieser Bytes für versteckte Daten, bedeutet das für das Ursprungsbild lediglich, dass die einzelnen Farbwerte zwischen 0 und 255 um bis zu vier Zähler falsch sein können. Dies entspricht einer Abweichung vom Originalbild von unter 1,6% und fällt daher mit bloßem Auge in aller Regel nicht auf.

Bei Wahl eines geeigneten Bildes – wie des ohnehin qualitativ schlechten Baumfotos in der Abbildung – bewegt man sich hier gar im Bereich des ohnehin enthaltenen natürlichen Rauschens.

In diesem Beispiel wurden die zwei niederwertigsten Bits genutzt, um ein weiteres, unkomprimiertes Bild zu speichern. Da, wie erläutert, nur zwei Bit jedes RGB-Farbwertes für die geheimen Daten abgezwackt wurden, führt dies zu den sichtbaren Farbungenauigkeiten des versteckten Katzenbilds.

Schwerer detektierbar als das naive Verstecken eines unkomprimierten Bildes ist die Verwendung geheimer Daten, die aufgrund ihrer Codierung eine ähnliche statistische Verteilung aufweisen wie das zu erwartende Rauschen des verwendeten Containers (also in unserem Beispiel des Baum-Bilds). Möchte man keine passende Codierung speziell für den verwendeten Container erzeugen, eignen sich auch komprimierte und/oder verschlüsselte Daten recht gut, da sie – ähnlich wie Rauschen – eine hohe Entropie, eine hohe „Zufälligkeit" aufweisen. Diese entsprechend dabei der (Gleich-)Verteilung des sogenannten „weißen" Rauschens.

Mit Steganographie lassen sich unsere Angriffsszenarien 2 und 3 umgehen. Sofern es gelingt, den Zensor über deren Einsatz an sich im Dunklen zu lassen, lässt sich gar schon der Versuch von Zensurmaßnahmen vermeiden.

Wesentlicher Nachteil dieser Methode ist – neben dem hohen Aufwand – dass es nicht mehr möglich ist, ein nicht-eingeweihtes Publikum mit der Veröffentlichung zu erreichen.

2.2.2 Nutzung von Dienstleistern außerhalb des Zensur-Einflussbereichs

Unsere Angriffsszenarien 2 und 3 basieren darauf, dass der Zensor Einflussmöglichkeiten auf verwendete Dienstleister, wie beispielsweise Webhoster, besitzt. Nichts liegt also näher, als auf Dienstleister auszuweichen, bei denen eben dies nicht der Fall ist. Im Falle staatlicher Zensur meint dies im Wesentlichen Dienstleister im Ausland.

Natürlich birgt auch diese Methode Risiken. Zum Einen kann der Zensor den Zugang zu derartigen Dienstleistern einfach blockieren (unser Angriffsszenario 4). Im kommenden Abschnitt stellen wir eine Gegenmaßnahme hierzu vor.

Abb. 10: Ausländische Dienstleister

Zum Anderen kann derartiges Verhalten den Zensor dazu bewegen, alternativ direkte Repression gegen die Kommunikatorin einzusetzen (unser Angriffsszenario 5). Um dies zu vermeiden, wird die Kommunikatorin daran interessiert sein, ihre Identität geheim zu halten. Sie möchte **anonym** publizieren.

Kommunikation über das Internet ist grundsätzlich zurückverfolgbar. Wie Anonymität gegen dieses Problem gesichert werden kann, behandeln wir ab dem nächsten Abschnitt.

Wird der fremde Dienstleister von der Kommunikatorin bezahlt, ist der Zahlungsvorgang eine weitere Gefahr für ihre Anonymität. Als anonymes Zahlungsmittel sind beispielsweise Prepaid-Karten einsetzbar. Diese Karten können gegen den Wert ihres Guthabens an vielen verschiedenen Verkaufsstellen wie z.B. Tankstellen erworben und bar bezahlt werden. Mittels einer auf jeder Karte angebrachten eindeutigen Nummer kann nun auf der Webseite eines Dienstleisters, der die entsprechende Prepaid-Karte akzeptiert, bezahlt werden. Eine in diesem Zusammenhang bekannt gewordene Marke ist die „paysafecard“.

Auch die kryptografische Onlinewährung Bitcoin kann unter Umständen hierzu verwendet werden. Grundsätzlich ist Bitcoin nur **pseudonym**, jedoch nicht anonym. Ein Benutzer wird in Bitcoin durch eine eindeutige Identifikationsnummer repräsentiert. Jede Transaktion in Bitcoin wird archiviert und ist einschließlich der beteiligten Identifikationsnummern für immer öffentlich einsehbar.

Pseudonymität bedeutet, dass der Benutzer nicht gezwungen ist, diese Bitcoin-Identität mit seiner realen zusammenzuführen. Es ist jedoch sehr schwierig,

Bitcoins für reales Geld zu erwerben oder wieder zu verkaufen, ohne dass es dabei zu genau dieser Zusammenführbarkeit kommt. Der Einsatz von Bitcoin wird in vielen Fällen das Problem des anonymen Zahlungssystems also nur auf das Problem des anonymen Bitcoinerwerbs verschieben.

2.2.3 Proxy-Server

Als Proxy – von lateinisch *proximus*, der Nächste[WIKI-2013f] – versteht man einen Server, der Anfragen im Auftrag des Benutzers weiterleitet. Anstatt sich direkt mit einem bestimmten Dienst zu verbinden, kann die Benutzerin also einen Proxyserver bitten, die Verbindung in ihrem Namen aufzubauen.

Proxy-Server werden im Internet völlig unabhängig von der Thematik der Zensur mit großer Verbreitung eingesetzt. So dienen beispielsweise sogenannte *Caching Proxies* der Performanceoptimierung, indem sie Antworten auf sehr häufige Anfragen selbst vorhalten und so der eigentlich den Dienst zur Verfügung stellende Server mit deutlich weniger Anfragen belastet wird.

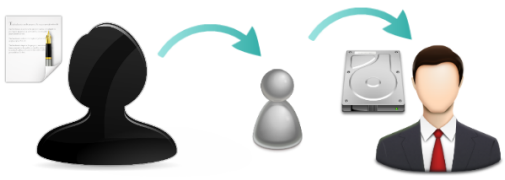

Abb. 11: Verwendung eines Proxys

Im Bereich der Zensur-Gegenmaßnahmen können mit Proxyservern zwei unabhängige Ziele erreicht werden. Zum einen sind sie als Gegenmaßnahme zu Angriffsszenario 4 nutzbar, also zum Umgehen von **Dienstsperren**. Wie in Abschnitt 2.1.4 beschrieben, hat ein Zensor meist nur die Möglichkeit, Sperren für bestimmte Teilnetze des Internets durchzusetzen, so etwa für einen Staat. Bedient sich die Kommunikatorin eines Proxyservers in einem anderen Teilnetz, ist sie von den Sperrmaßnahmen nicht mehr betroffen.

Zum Anderen sind Proxyserver zur Verschleierung der eigenen Identität, also zum Erreichen von **Anonymität** nutzbar. Überwacht beispielsweise der Zensor die Internetverbindung der Kommunikatorin oder des Dienstleisters oder überwacht der Dienstleister selbst die Inhalte seiner Kunden zum Zweck der Repression, kann die Kommunikatorin so unerkannt bleiben.

Bei einer normalen Kommunikation im Internet sind beiden Seiten die Identitäten der Kommunikationspartner bekannt. Datenpakete im Internet enthalten in ihrem Paketkopf Felder für die IP-Adressen des Absenders und des Empfängers. Mit Hilfe des jeweiligen Internet Service Providers kann in aller Regel die physische Identität des Benutzers einer bestimmten IP-Adresse in Erfahrung gebracht werden.

Es ist dabei auch in der Regel nicht möglich, falsche Adressdaten anzugeben. Stimmt die Empfängeradresse nicht, ist trivial, dass das Datenpaket nicht mehr zugestellt werden kann. Stimmt die Absenderadresse nicht – dies bezeichnet man als *IP Spoofing* – kann der Empfänger nicht antworten. Bestimmte im Internet sehr häufig verwendete Protokolle (z.B. TCP auf Grund des sogenannten Drei-Wege-Handshakes) sind dabei auch dann auf eine gültige Absenderadresse angewiesen, wenn die Benutzerin an sich auf eine Antwortmöglichkeit verzichten könnte. Auch werden Datenpakete mit gefälschter Absenderadresse nach entsprechenden Empfehlungen von immer mehr Internet Service Providern ausgefiltert[NSA-2005].

Frei verfügbare Proxyserver sind in großer Zahl im Internet zu finden. Eine kurze Anfrage an die jeweils bevorzugte Suchmaschine ergibt zahlreiche Indexseiten mit hunderten, nach verschiedenen Kriterien filterbaren Einträgen. Daneben kann die Kommunikatorin natürlich auch selbst einen Proxyserver außerhalb des Zugriffsbereichs des Zensors betreiben oder eine vertrauenswürdige Kontaktperson oder entsprechende Organisation hierum bitten.

Wichtig ist zur Umgehung eventueller Abhörmaßnahmen, dass die Kommunikation zwischen Kommunikatorin und Proxy verschlüsselt erfolgt. Die Kommunikation zwischen Proxy und Dienstleister kann dagegen im Klartext erfolgen.

Bei der Verwendung von Proxyservern zur Erlangung von Anonymität sind einige Fallstricke zu beachten. Nicht jeder Proxyserver anonymisiert die Benutzerin. Wie Eingangs erwähnt, ist die Verschleierung der Benutzeridentität für viele Proxyserver überhaupt nicht Einsatzzweck. Bei Proxies für das Protokoll HTTP – also das Besuchen von Webseiten – ist es dabei nicht unüblich, dass der Proxy die Original-Absenderadresse der weitergeleiteten Anfrage schlicht anhängt[WIKI-2013g].

Verzeichnisse frei verfügbarer Proxyserver erlauben oft das Filtern nach diesem Kriterium. Testet man den zu verwendenden Proxyserver jedoch nicht selbst auf dieses Merkmal, besteht selbstverständlich die Gefahr fehlerhafter oder veralteter Angaben im Index.

Schließlich steht und fällt die Eignung eines Proxyservers zur Anonymisierung mit dessen Vertrauenswürdigkeit. Gibt der Proxy-Betreiber Verbindungsdaten an den Zensor weiter, kann dieser die weitergeleiteteten Anfragen wieder ihrem ursprünglichen Absender zuordnen. Zensoren könnten auch selbst Proxyserver unter falschem Namen und dem Versprechen der Anonymisierung betreiben, um an die Daten ihrer Gegner zu gelangen. Schließlich reicht es auch aus, wenn ein eigentlich vertrauenswürdiger Proxy durch einen Angriff des Zensors komprimittiert wird. Derartige Sicherheitslücken sind nie auszuschließen.

Die Benutzung von Proxyservern ist also riskant, da der Proxy einen **Single Point of Failure** darstellt: Ist seine Sicherheit gebrochen, verliert die Schutzmaßnahme sofort ihre Wirksamkeit.

Eine Weiterentwicklung des Prinzips der Proxyserver zur Anonymisierung stellen wir im folgenden Abschnitt vor.

2.3 Anonyme Netze

In Abschnitt 2.2 haben wir vergleichsweise primitive, weitgehend manuell zu besorgende Gegenmaßnahmen gegen Zensurversuche beschrieben. Hier geht es nun um Systeme, die versuchen, alle Schritte zur Erlangung starker Anonymität automatisiert auszuführen.

Bei anonymen Netzen handelt es sich um bestimmte Overlay-Netzwerke – eine Art spezielle Benutzergruppen – wobei die Kommunikation innerhalb des Overlay-Netzwerkes durch eine spezielle, bei jedem Nutzer installierte Anonymisierungssoftware gesteuert wird.

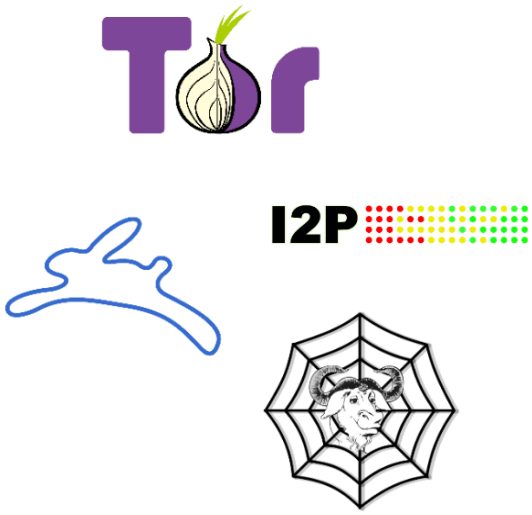

Abb. 12: Vier anonyme Netze

Abbildung 12 zeigt von oben nach unten beispielhaft die Logos vier bekannter anonymer Netze: The Onion Router (TOR), Invisible Internet Project (I2P), Freenet und GNUnet.

TOR und I2P sind dabei als direkte Weiterentwicklungen des Proxy-Prinzips zu betrachten. Bei Freenet und GNUnet basiert das Sicherheitsmodell relevant auf anderen Prinzipien[4].

Ein weiteres wichtiges Unterscheidungsmerkmal verschiedener anonymer Netze ist, ob sie nur zur anonymen Kommunikation unter den Netzteilnehmern nutzbar sind oder ob auch Verbindungen nach „außen“ möglich sind – also zu Diensten, die nicht am jeweiligen anonymen Netzwerk teilnehmen. Von den hier genannten vier Netzwerken erlauben drei aus technischen und prinzipiellen Erwägungen nur interne Verbindungen.

4 Hier ist insbesondere ein weiterentwickeltes Ameisenprinzip („egal, welchen wahllos komplizierten Weg eine Anfrage durch das Netz nimmt – die Antwort nimmt den gleichen“) zu nennen.

2.3.1 TOR

Auf die Ausnahme, TOR, möchten wir nun genauer eingehen[DIN-2004]. Wir beziehen uns dabei für den Rest dieses Abschnitts stets auf den Fall der Kommunikation mit einem Dienstleister, der nicht Teil von TOR ist[5]. Viele der folgenden Ausführungen sind mit dem Fall der Kommunikation mit Diensten innerhalb des TOR-Netzes als auch mit der Funktionsweise von I2P vergleichbar.

Eine mit TOR anonymisierte Verbindung kann die Benutzerin herstellen, indem sie die TOR-Software lokal startet und in konventionellen Anwendungsprogrammen, z.B. einem Browser, ihren eigenen Rechner als Proxyserver einträgt. Hierzu wird in TOR standardmäßig Port 9050 verwendet.

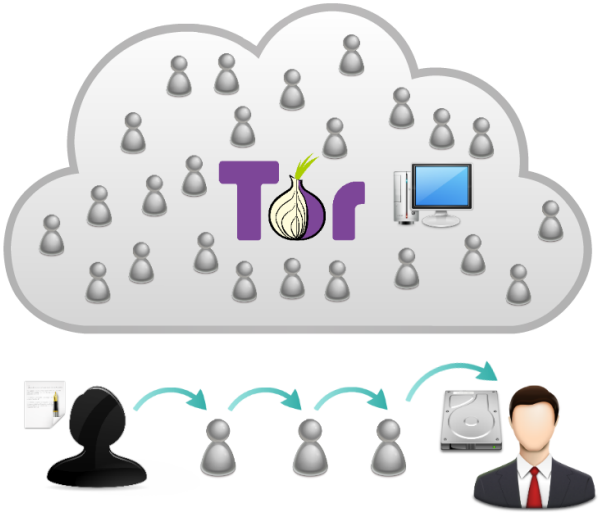

Abb. 13: Das TOR-Kommunikationsmodell

Wie bereits in Abschnitt 2.2.3 beschrieben, stellt die Verwendung eines einzelnen Proxyservers einen Single Point of Failure und damit ein relevantes Risiko dar. Wird eine Verbindung über nur einen Proxy zwischen der Benutzerin und ihrem Kommunikationspartner hergestellt, kennt dieser Proxy alle nötigen Daten, um die anonymisierte Anfrage mit der physischen Identität der Benutzerin zusammenzuführen. Wird die Sicherheit dieses einen Proxys durch den Zensor kompromittiert, ist die Anonymisierung gebrochen.

Das Problem der Kompromittierung einzelner Proxies verschärft sich in TOR dadurch, dass die verschiedenen Proxy-Server innerhalb des Netzwerks durch Freiwillige zur Verfügung gestellt werden. Damit ist es auch einem Angreifer mit recht geringem Aufwand möglich, bösartige Proxy-Server in das Netz einzubringen.

5 Das Gegenstück, Dienste innerhalb des anonymen Netzwerks, wird im TOR-Jargon als *hidden service* bezeichnet.

Die Auswahl der Proxies erfolgt in TOR bei jeder Einwahl ins anonyme Netz (sowie anschließend in regelmäßigen Abständen) nach dem Zufallsprinzip. Würde TOR in jeder Verbindung nur einen einzigen Proxy zur Anonymisierung verwenden, wäre für den Fall, dass der Angreifer genau einen bösartigen Proxy in das System eingebracht hat, die Erfolgswahrscheinlichkeit des Angriffs bei jeder Einwahl 1/n, wobei n für die Gesamtzahl der verfügbaren Proxies im Netzwerk steht. Infiziert der Angreifer das Netz mit mehreren bösartigen Servern, steigt die Erfolgswahrscheinlichkeit des Angriffs um („nur“) einen konstanten Faktor. Man spricht daher davon, dass ein solcher Angriff **lineare Komplexität** besitzt bzw. in der Klasse **O(n)** liegt.

TOR strebt, wie viele anonyme Netze, dagegen mindestens eine **quadratische Komplexität** aller Angriffe, und damit quadratische Sicherheit an. Man schreibt, Angriffe auf TOR sollen mindestens in der Klasse **$O(n^2)$** liegen. In Abschnitt 2.3.2 werden wir darauf eingehen, dass dieses Ziel nicht vollständig erreicht wurde.

Zu diesem Zweck setzt TOR eine Kette aus drei Proxies[6] ein. Die Benutzerin sendet die zu übermittelnden Daten also an den ersten Proxy, der sich damit in der Proxykette am nähesten an der Benutzerin, „innen“, befindet. Dieser Proxy leitet die Nutzdaten an den zweiten, „mittleren“ Proxy weiter, der sie wiederum an den letzten, „äußeren“ sendet. Dieser übermittelt die Daten schließlich an ihr Ziel – den eigentlichen Kommunikationspartner der Benutzerin.

Somit trägt der innere Proxy nur Wissen über die Identität der Benutzerin und der äußere nur Wissen über den aktuellen Kommunikationspartner. Damit wurden diese beiden nur gemeinsam nützlichen Geheimnisse auseinandergezogen. Der mittlere Proxy dient der Trennung der beiden Geheimnisträger[7].

6 TOR verwendet statt Proxy die Bezeichnung Onion Router (OR) und bezeichnet mit Onion Proxy (OP) die von allen Netzteilnehmern eingesetzte Software. Die Länge der Proxykette ist variabel; drei ist Standardwert und nahezu ausschließlich verwendet.

2.3.2 Sicherheitserwägungen zu TOR

Der quadratische Angriff

Das von TOR gewünschte Ziel quadratischer Sicherheit ist von Anfang an kein besonders hohes. In der Kryptologie geht man davon aus, dass Sicherheit erreicht ist, wenn ein erfolgreicher Angriff den Aufwand von mindestens 2^{80} Operationen erfordert[BRA-2010]. Unterschiedliche Komplexität der einzelnen Operationen ist dabei kein vorrangiger Faktor: Um den Faktor tausend schwerere Operationen entsprechen lediglich einer Erhöhung des Exponenten um etwa 10, um den Faktor eine Million schwerere einer Erhöhung um etwa 20.

Als eine „Operation" bezeichnen wir in diesem Zusammenhang die Bildung einer Proxykette durch die Benutzerin per zufälliger Auswahl von drei Proxies. Gehen wir davon aus, dass im gesamten TOR-Netzwerk nur zwei kompromittierte Proxies existieren. Der Angriff ist erfolgreich, wenn zufällig sowohl die Position des inneren als auch die des äußeren Proxies mit diesen kompromittierten Servern besetzt wird.

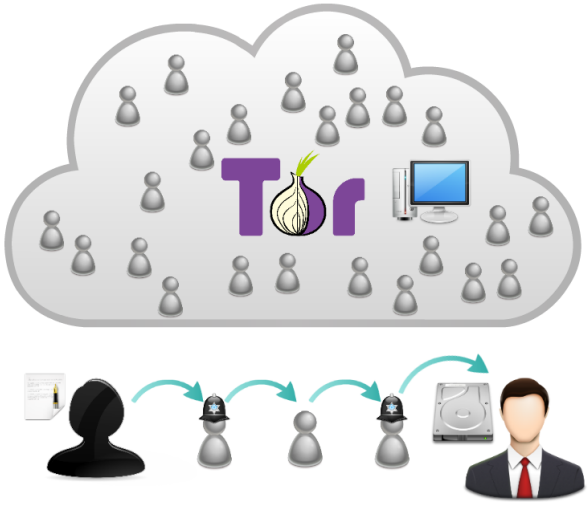

Abb. 14: Der quadratische Angriff

Untersuchen wir zunächst, ob dieser Angriff tatsächlich eine invers quadratische Erfolgschance hat. Die Wahrscheinlichkeit, dass bei der Zufallsauswahl der innere Proxy mit einem der beiden kompromittierten besetzt wird, beträgt 2/n, wobei n wieder für die Gesamtzahl der verfügbaren Proxyserver steht. Wenn dies eintritt,

7 Der mittlere Proxy verhindert primär, dass ein bösartiger Kommunikationspartner, der mit linearem Aufwand den inneren Proxy in einer Verbindung kompromittiert hat, anhand einer gemeinsamen Verbindung (von ihm selbst sowie vom inneren Proxy zum äußeren Proxy) die Identität der Benutzerin mit der aktuellen Verbindung verbinden kann. Dadurch wäre die Anonymität mit nur einem komprimittierten Proxy gebrochen gebrochen.

beträgt die Wahrscheinlichkeit, dass nun[8] noch der äußere Proxy durch den verbliebenen komprimittierten besetzt wird, 1/n.

Die Gesamtwahrscheinlichkeit für den zufälligen Eintritt einer kompromittierten Proxyketten ist das Produkt dieser beiden Teilwahrscheinlichkeiten:

$$P = \frac{2}{n} * \frac{1}{n} = \frac{2}{n^2}$$

Es handelt sich also tatsächlich um die angestrebte invers quadratische Wahrscheinlichkeit.

Es ist nun zu erwarten, dass im Durchschnitt alle $\frac{n^2}{2}$ Fälle genau dieses Ereignis eintritt, da $\frac{n^2}{2} * \frac{2}{n^2} = 1$. Der tatsächlich erwartete Angriffsaufwand in durchschnittlicher Zahl benötigter Operationen hängt von n, der Anzahl der verfügbaren Proxyserver im Netz ab. Derzeit (Juli 2013) beträgt diese gut 4000[9]. Für den Angriff sind also „nur“ $\frac{4000^2}{2} = 8\,000\,000 \approx 2^{23}$ Operationen nötig.

Ein solches System würde in der Kryptologie schon lange als gebrochen angesehen werden.

---

8 Voraussetzung ist im Fall von genau zwei kompromittierten Proxyservern natürlich, dass als mittlerer Proxy keiner dieser beiden gewählt wird. Die Wahrscheinlichkeit hierfür beträgt nahezu 100% – (n-2)/(n-1). Zudem müsste für die nun folgende Teilwahrscheinlichkeit der Nenner (n-2) lauten, da die beiden bereits gewählten Proxies ja nicht mehr zur Verfügung stehen. Tatsächlich ist der Nenner in der Praxis meist noch etwas kleiner, da auch Proxyserver, die nach eigener Angabe der gleichen Organisation wie einer der beiden bereits gewählten angehören, von der Wahl ausgeschlossen werden. Dagegen vergrößert sich die Angriffswahrscheinlichkeit dadurdh, dass der Angreifer durch Verbindungskorrelation alternativ die Möglichkeit hat, entweder den inneren und den mittleren oder den mittleren und den äußeren Proxy zu korrumpieren. Im Interesse einer klareren Darstellung vernachlässigen wir all diese Feinheiten in der Berechnung.

9 Im Toleranzrahen – vermutlich auf Grund unterschiedlicher Aktualisierungszeiträume – ähnliche Werte: 4027 [TOR-2013] sowie 4109 und 4076 [TNS-2013].

Nun trifft dieses Problem TOR besonders schwer, da TOR im Gegensatz zu den meisten anderen Netzen nicht von jedem Benutzer verlangt, gleichzeitig durch Leistung von Proxydiensten zur Anonymisierung beizutragen. Damit bleibt das „n“ in TOR vergleichsweise klein. Aber auch für eine utopische Serverzahl von einer Million erhalten wir lediglich eine Anfgriffskomplexität von etwa 2^{39}, für eine vollkommen unrealistische von einer Milliarde etwa 2^{59}. Die quadratische Skalierung der Angriffskomplexität zur Netzgröße reicht also nicht aus.

Der Directory-Server

Das TOR-Netzwerk besitzt einen Single Point of Failure. Um festzustellen, welche Proxyserver im Netzwerk zur Verfügung stehen, ruft die Software diese Information von einem sogenannten *Directory Server* ab. Gelingt es dem Angreifer, in diesen Server einzudringen, kann er veranlassen, dass den Benutzern nur noch seine korrupten Proxyserver gemeldet werden. In diesem Fall hat er alle Proxyketten dieser Benutzer sicher gebrochen.

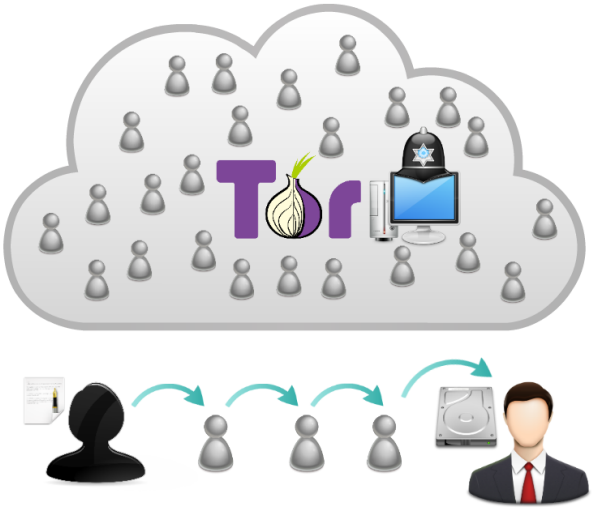

Abb. 15: Angriff auf Directory Server

Der Angriff wird dadurch erschwert, dass es tatsächlich nicht nur einen, sondern mehrere Directory Server im TOR-Netzwerk gibt. Diese Zahl ist jedoch überschaubar: Ursprünglich waren es drei[DIN-2004], inzwischen sind es neun[TOR-2013]. Spätestens, wenn der Angreifer fünf Directory Server übernommen hat, besitzt er jedoch Kontrolle über das gesamte TOR-Netzwerk, da seine Directory Server im internen Abstimmungsprozess die Mehrheit besitzen. Dieser Angriff skaliert nicht mit der Netzgröße. Er hat also **kontante Kosten**, befindet sich in der Komplexitätsklasse **O(1)**.

Im Jahre 2010 wurde schon einmal ein erfolgreicher Einbruch in zwei der damals sieben Directory Server bekannt. Nach Angaben des TOR-Projekts haben die Angreifer jedoch keine Versuche unternommen, das TOR-Netzwerk zu stören. Vermutlich war ihnen gar nicht bewusst, welch sensible Maschinen sie in ihre Gewalt gebracht hatten. Stattdessen haben sie die mit reichlich Bandbreite ausgestatteten Server für Angriffe auf andere Ziele im Internet benutzt[HEI-2010][DIN-2010].

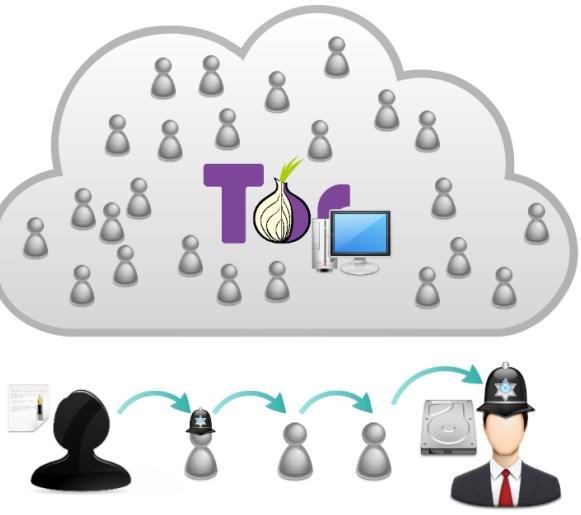

Abb. 16: Angriff durch zeitliche Lokalität

Zeitliche Lokalität

TOR ist ein anonymes Netz niedriger Latenz. Das heißt, Datenübertragungen werden mit so wenig Verzögerung wie möglich durch die Proxykette zum Ziel übertragen. Für den Fall eines bös-artigen Kommunikationspartners ergibt sich hieraus eine Angriffsmöglichkeit mit **linearer Komplexität**, also ein Angriff in **O(n)**.

Wie zu Beginn dieses Abschnitts beschrieben, besitzt der Angriff, nur den inneren Proxy zu komprimittieren, eine lineare Komplexität. Auf Grund der niedrigen Latenz des Systems kann ein bösartiger Kommunikationspartner nun feststellen, dass mit minimalem zeitlichen Unterschied zunächst eine (unlesbare, da verschlüsselte) Nachricht seinen korrupten Proxserver passiert und anschließend eine Nachricht bei ihm eingeht.

Durch diese Nahezu-Gleichzeitigkeit kann er ungeachtet der Verschlüsselung die von der Benutzerin an den inneren Proxy geschickte Nachricht als diejenige identifizieren, die ihn schließlich erreicht hat. Er kennt damit die Identität der Kommunikatorin und kann, so die Nachricht unerwünschte Inhalte enthält, nun Repressionsmaßnahmen einleiten.

Diese Schwachstelle war den Erfindern von TOR bereits seit Beginn bekannt[DIN-2004].

Neben diesem Angriff über die zeitliche Lokalität sind weitere analoge Angriffe möglich, beispielsweise über sogenannte Trafficmuster.

Praktische Relevanz

Die genannten Angriffsmöglichkeiten auf TOR stellen eine reale Gefahr für Personen dar, die unerwünschte Inhalte publizieren. Insbesondere der Angriff über zeitliche Lokalität aber auch der naive quadratische Angriff haben eine akzeptable Erfolgschance. Hierbei ist zu beachten, dass der Angreifer bei regelmäßiger TOR-Nutzung der Benutzerin auch regelmäßig weitere Chancen zum Angriff erhält.

Dennoch ist bisher kein Fall öffentlich bekannt geworden, bei dem tatsächlich durch Angriff auf TOR als System Identitäten von Benutzern offengelegt wurden.

Praktisch durchgeführt wurde dagegen zum Beispiel ein Angriff, in dem den zu deanonymisierenden Personen durch Täuschung manipulierte TOR-Software untergeschoben wurde, die schlicht das Nutzerverhalten dokumentiert hat[ARS-2011].

3 Beispiele von Zensurmaßnahmen aus der Praxis

In diesem Kapitel möchten wir anhand verschiedener, ausgewählter Beispiele zeigen, welche Formen Zensur haben kann. Alle Beispiele sind aktuell in dem Sinne, dass die Maßnahmen entweder derzeit andauern oder nicht länger als drei Jahre zurückliegen.

Alle genannten Beispiele erfüllen unsere Definition von Zensur, wie wir sie in Abschnitt 1.1 dargestellt haben. Die Auswahl der Beispiele soll auch zeigen, dass das übliche Verständnis von Zensur im westlich-demokratischen Kulturkreis und speziell in Deutschland – einem dort extrem negativ konnotierten Begriff – nicht immer dieser Definition entspricht.

Wir versuchen, alle diese Beispiele neutral gegeneinander darzustellen und keine ethisch-moralische Interpretation zu implizieren, ob diese nun jeweils als „richtige" oder „schlimme", legitime oder abzulehnende Zensur zu sehen sind oder nicht.

3.1 Arabischer Frühling

Der Begriff *arabischer Frühling* „bezeichnet eine im Dezember 2010 beginnende Serie von Protesten, Aufständen und Revolutionen in der arabischen Welt, welche sich, beginnend mit der Revolution in Tunesien, in etlichen Staaten im Nahen Osten (Maschrek/Arabische Halbinsel) und in Nordafrika (Maghreb) gegen die dort autoritär herrschenden Regime und die politischen und sozialen Strukturen dieser Länder richten."[WIKI-2013j]

Im Folgenden möchten wir kurz auf die Revolutionen in Tunesien und Ägypten eingehen. Die Rolle des Internets in diesen Ereignissen ist umstritten. Während westliche Medien gerne den griffigen Begriff der „Facebook-Revolution" wählen, betonen andere, wie der deutsch-ägyptische Blogger Philip Rizk, die klassische Rolle der Straße. Das Schlagwort dagegen sei „totaler Schwachsinn"[TEL-2012].

Doch wenngleich „Facebook-Revolution“ sicherlich die politischen und sozio-ökonomischen Hintergründe vernachlässigt und auch außer Acht lässt, dass zumindest die Revolutionen in Tunesien und Ägypten nicht ohne die Unterstützung des Militärs möglich gewesen wären, so hat das Internet dennoch von Beginn an eine entscheidende Rolle gespielt. Social-Media-Plattformen wie Youtube, Twitter und natürlich Facebook waren anfänglich die wichtigsten Medien zur Mobilisierung der Bevölkerung und dienten später auch der Übermittlung von Informationen und Bildmaterial an ausländische Medien. Insbesondere der private Nachrichtensender *Al Jazeera* mit Sitz im Emirat Katar wurde mit Hilfe dieser Quellen als „Revolutions-TV“ bekannt und füllte damit die Lücke, die die zensierten staatsinternen Fernsehsender hinterließen.[BPB-2011]

Die Reaktionen ließen nicht lange auf sich warten. Sowohl Tunesiens Regime unter Präsident Ben Ali als auch die ägyptische Führung von Präsident Mubarak wählten unter Anderem Maßnahmen nach Szenario 4 unseres Modells (Abschnitt 2.1), die Sperrung von Diensten. In Tunesien wurden so die Webseiten von Al-Jazeera, Amnesty International, Wikileaks, den Videoportalen YouTube und Daily Motion sowie zeitweise Facebook staatlich blockiert. Statt der gewünschten Seiten erschien dann die HTTP-Fehlermeldung 404, „Page not found“[BPB-2011]. Offenbar wurden Anfragen also auf einen unkonfigurierten Webserver umgeleitet.

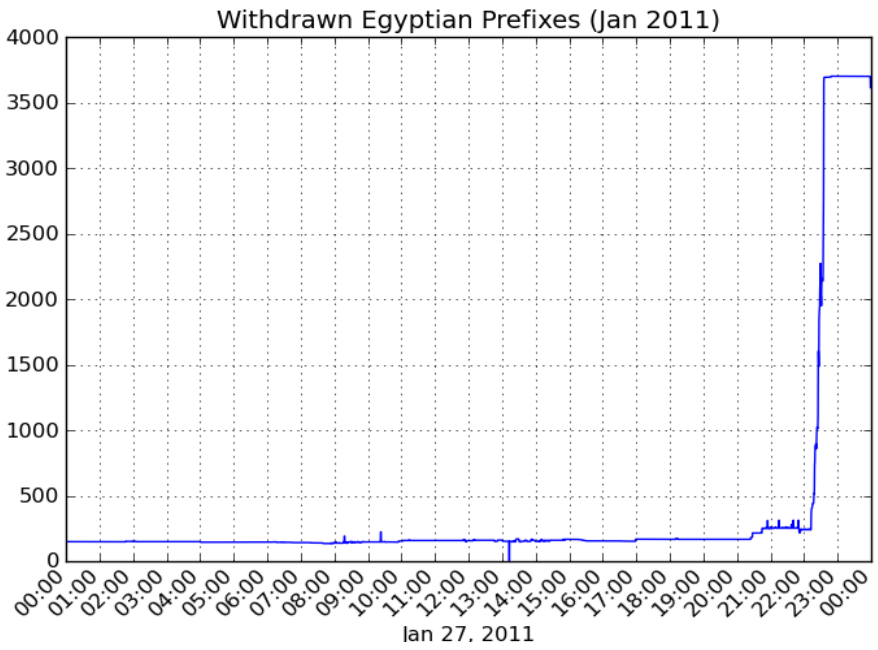

Abb. 17: Abtrennung des ägyptischen Internets

Ägypten schrieb mit einer wesentlich drastischeren Aktion Internetgeschichte. Am 27. Januar 2011 gegen 22:30 Uhr UTC kappten die vier großen ägyptischen Internet Service Provider sämtliche internationalen Verbindungen. Über 3500 BGP-Routen (zu BGP vgl. Abschnitt 2.1.4) wurden zurückgezogen[REN-2011].

Bei diesen Aktionen handelt es sich um klassische Fälle von Dienstsperren, wie unser Modell sie beschreibt. Sie haben auch deren übliche Schwachstelle: Auch der Machtbereich dieser beiden Zensoren endete an den Staatsgrenzen und betraf somit nur einen kleinen Teilbereich des Internets. Wichtigste Gegenmaßnahme der betroffenen Nutzerinnen und Nutzer war das Ausweichen auf ausländische Dienstleister (Gegenmaßnahme 2 unseres Modells aus Abschnitt 2.2).

So verbreiteten Aktivisten etwa die Telefonnummern verschiedener Einwahlknoten ausländischer Internet Service Provider, über die unbeschränkter Netzzugang möglich war[SPI-2011]. Über diese Kanäle war weiter der Upload von Informationen und Bildmaterial auf ebenfalls außerhalb des Zensureinflusses stehende Server möglich, das über ausländische Massenmedien – besonders prominent wie schon erwähnt Al Jazeera – auch wieder ins Land zurückfloss[BPB-2011].

3.2 Volksrepubliken China und Nordkorea

Die Volksrepublik China ist für ihren rigorosen Umgang mit politischen Dissidenten bekannt. Besondere Aufmerksamkeit erhielt dieser Umstand 2010, als dem chinesischen Schriftsteller, Menschenrechtler und Mitautor des Bürgerrechts-Manifests *Charta 08* der Friedensnobelpreis verliehen wurde[SHE-2010]. Liu Xiaobo konnte den Preis nicht entgegennehmen, da er sich bis heute im Gefängnis befindet[WIKI-2013k].

Die chinesische Führung reagierte empört auf die Verleihung. Die Regierung bestellte den norwegischen Botschafter ein und übergab eine Protestnote. Die Ehefrau des Systemkritikers wurde unter Hausarrest gestellt, so dass auch sie nicht an der Verleihung teilnehmen konnte[WIKI-2013k].

Im Sinne unseres Modells aus Abschnitt 2.1 lässt sich dies als Maßnahme der Kategorie 5 beschreiben, wenngleich das Vorgehen zunächst nichts mit dem Internet zu tun hat.

Dieser Fall dient uns jedoch als Beispiel, um auf die Eigenheiten des chinesischen Internetzensursystems hinzuweisen, das gerne in Anlehnung an die Chinesische Mauer (englisch „Great Wall of China“) als „Great Firewall of China“ bezeichnet wird. Das offiziell als *Projekt Goldener Schild* bezeichnete System wurde ab 1998 entwickelt und ist seit 2003 im Einsatz. Neben selektiven Dienstsperren auf DNS- wie auch IP-Basis (Szenario 4 unseres Modells aus Abschnitt 2.1) werden übermittelte Inhalte auf dem Transportweg, unabhängig von einem konkreten Dienstleister, auf unerwünschte Inhalte untersucht.

Diese sogenannte *Deep Packet Inspection*[10] dient der Umsetzung einer automatischen Vorzensur (Kategorie 3 unseres Modells) sowie möglicherweise auch der direkten Repression gegen die Absender. Besonders hervor sticht hierbei, dass der Goldene Schild nach Erkennung solch unerwünschter Datenpakete die beanstandete Verbindung automatisch trennt und für eine Zeitspanne von bis zu 30 Minuten keinen neuen Verbindungsaufbau zulässt[WIKI-2013l].

Dieses Verhalten ließ sich zum Zeitpunkt der Drucklegung reproduzieren, indem man beispielsweise auf der Website der staatlichen Nachrichtenagentur Xinhua, http://www.news.cn/english, nach 刘晓波 (Liu Xiaobo) sucht.

Dieses Verhalten wurde unregelmäßigen Tests zufolge, die wir in den letzten Jahren durchgeführt haben, im zweiten Halbjahr 2012 und ersten Halbjahr 2013 stark reduziert. Waren bis dahin auf allen von uns getesteten Seiten derartige Sperren für eine Vielzahl von Schlüsselwörtern geschaltet – von chinesischen Dissidenten über die religiöse Gruppe *Falun Gong* bis hin zu Informationen zum Rückzug des

10 Der unabhängig etablierte Begriff betont, dass anders als auf dem Transportweg üblich, nicht nur Absenderadresse, Empfängeradresse und andere Kopf-Informationen der einzelnen Datenpakete sondern auch deren Inhalt zur Entscheidung über Weiterleitung oder Löschung des Pakets herangezogen werden.

Unternehmens Google aus der Volksrepublik – ist dies nun nur noch für wenige Begriffe und auf deutlich weniger Websites feststellbar. Auch sind in der Regel nur noch chinesische Ausdrücke und nicht deren lateinische Umschrift von dieser Art der Zensur betroffen. Auf der Website der größten chinesische Suchmaschine, *baidu.com*, sind kaum noch derartige Sperren zu finden. Stattdessen erhält man bei Eingabe der vormals komplett geblockten Begriffe nun eine baidu-eigene Meldung, die auf die Entfernung einiger Ergebnisse aus rechtlichen Gründen hinweist[11]

In der Volksrepublik Nordkorea ist für die allermeisten Personen schlicht kein Anschluss ans weltweite Internet möglich. Stattdessen betreibt das Land unter dem Namen *Kwangmyong* ein nationales Intranet. Hier stehen vor allem Informationen nordkoreanischer Behörden und Forschungseinrichtungen und einiger weniger Unternehmen zur Verfügung; auch ein Dienst ähnlich der eMail wird bereitgestellt. Zudem werden ausgewählte Websites aus dem Internet durch die zuständigen Stellen heruntergeladen, durch die Zensur geprüft und anschließend in Kwangmyong republiziert[WIKI-2013m].

Der Zugang zum weltweiten Internet ist auf bestimmte Regierungsmitarbeiter sowie ausgewählte Privatpersonen beschränkt. Letzteres betrifft im Wesentlichen ausländische Unternehmer. So berichtete die Tageszeitung taz 2010 vom deutschen Internetunternehmer Volker Elösser, der in Nordkorea das Unternehmen Nosotek gegründet hat. „Als Ausländer darf ich in meiner Privatwohnung einen Telefon- und einen Internetanschluss mit Zugang zum weltweiten Netz haben, mein Büro aber darf es nicht“, so Elösser in der taz. Das sorge für reichlich Probleme im geschäftlichen eMail-Verkehr. Das Blatt berichtet: „Auf seinem Computer zu Hause lädt er jeden Morgen früh die E-Mails herunter, bevor er ins Geschäft fährt. Sein Internetanschluss kostet 250 Euro monatlich.“[TAZ-2010].

11 Wortlaut laut automatischer Übersetzung durch den Google-Übersetzer: „According to relevant laws, regulations and policies, some search results have not been displayed.“.
Originalwortlaut: „根据相关法律法规和政策，部分搜索结果未予显示。”

3.3 Private Zensur in der westlichen Welt

Nicht nur Staaten haben ein Interesse daran, ihnen unliebsame Informationsübermittlungen zu unterbinden. Als Beispiel für derartige Maßnahmen durch Private, insbesondere auch private Unternehmen, sind die Durchsetzung des Marken- und Urheberrechts zu nennen. Auf letzteres und die zur Sicherung des geistigen Eigentums konkret eingesetzten Mittel gehen wir in diesem Abschnitt genauer ein. Das Urheberrecht erweist sich als besonders gutes Beispiel, da es Anwendungsfälle für alle fünf Szenarien unseres Modells aus Abschnitt 2.1 liefert.

In Deutschland verbietet § 15 UrhG insbesondere das Kopieren und die Übermittlung urheberrechtlich geschützter Werke, wenn hierfür keine besondere Genehmigung vorliegt. Für den Fall der Zuwiderhandlung droht das Gesetz dem Verletzer unter Anderem Ersatz entfallener Lizensierungseinnahmen (§ 97), Geldstrafe oder Freiheisstrafe bis zu drei Jahren (§ 106) sowie in bestimmten Fällen Vernichtung der zum Kopieren verwendeten Computer und anderer Geräte (§ 98) an. Obwohl geistiges Eigentum primär ein Recht Privater und das Urheberrecht daher Zivilrecht ist, nimmt hier also auch der Staat durch strafrechtliche Bestimmungen (§ 106) maßgeblich an dem Zensurgebilde teil.

In den USA sind die gleichen Taten durch 17 USC[12] § 106 verboten. Angedroht werden hier insbesondere Ersatz entgangener Einnahmen (§ 504) sowie in bestimmten Fällen Freiheitsstrafe bis zu zehn Jahren (17 USC § 506 in Vereinigung mit 18 USC § 2319).

Das Urheberrecht versucht also primär, durch direkte Einflussnahme und Bedrohung potenzieller Verletzer unliebsame Veröffentlichungen zu verhindern. Es handelt sich also zunächst um Maßnahmen nach Szenario 1 und ggf. eskalierend 5 unseres Modells aus Abschnitt 2.1.

12 Übliche Schreibweise für 17. Buch des gesammelten amerikanischen Bundesrechts (United States Code).

Auch Vorgaben an Dienstleister, also Kategorie 2 unseres Modells, kommen hierbei zum Einsatz. § 10 TMG legt fest, dass Dienstleister wie Hostingunternehmen für über ihre Dienste begangene Urheberrechtsverletzungen verantwortlich sind, wenn sie derartige Daten nicht unverzüglich löschen, sobald sie von ihnen Kenntnis erlangen.

Das US-amerikanische Recht bestimmt gleiches in 17 USC §512(c). Ein Rechteinhaber kann also jederzeit direkt vom Dienstleister die Entfernung unerwünschter Inhalte verlangen und hat dabei stets rechtliche Druckmittel auf seiner Seite. Eine derartige Aufforderung ist im amerikanischen Recht genauer formalisiert[13] und wird umgangssprachlich als „DMCA Takedown Notice“[14] bekannt.

Ein Beispiel für automatisierte Vorzensur – Szenario 3 unseres Modells – liefert das Unternehmen YouTube LLC. Im Rahmen seines Programms „Content ID“ unterhält es eine Liste urheberrechtlich geschützter Werke, zu der die jeweiligen Rechteinhaber beitragen. Jedes Video, das auf Youtube hochgeladen wird, wird auf Ähnlichkeit mit diesen Werken überprüft. Wird hierbei zum Beispiel festgestellt, dass das Video urheberrechtlich geschützte Musik eines teilnehmenden Rechteinhabers enthält, wird eine Aktion entsprechend den Vorgaben des Rechteinhabers ausgewählt. Derzeit haben diese die Möglichkeit, die Veröffentlichung nur zu registrieren, der Veröffentlichung automatisch eigene Werbeeinblendungen hinzuzufügen oder die Veröffentlichung zu unterbinden[YOU-2013].

In Abschnitt 2.1.4 stellten wir im Zusammenhang mit DNS-basierten Sperren des Zugangs zu bestimmten Diensten fest, dass ein Zensor in der Regel nur in der Lage ist, derartige Maßnahmen in ganz beschränkten Teilen des Internets vorzunehmen, da er keinen Zugang zu den autoritativen DNS-Servern hat.

13 17 USC §512(c)(3)(A)

14 Der Digital Millenium Copyright Act (DMCA) ist ein Änderungsgesetz aus dem Jahre 1998. Es enthält wesentliche Änderungen und Ergänzungen des in Buch 17 des amerikanischen Bundesrechts (United States Code) geregelten Urheberrechts.

Ebenfalls in Zusammenhang mit dem Urheberrecht zeigten US-amerikanische Behörden 2012 bei der Stillegung des One-Click-Hosters *Megaupload* (einer Maßnahme nach Szenario 4 unseres Modells), dass diese Einschränkung auf sie nicht zutrifft.

Neben verschiedenen weiteren Maßnahmen veranlassten die zuständigen Stellen eine Umleitung aller Anfragen an die Domain megaupload.com an einen eigenen Dienst, der lediglich über die Beschlagnahmung der Domain informiert[WIKI-2013h]. Wie Abbildung 18 zeigt, gingen die Vorwürde hier jedoch über bloße Urheberrechtsverletzung hinaus.

Abb. 18: Beschlagnahmungsnachricht

Eingriffe in das weltweite Domain Name System sind für amerikanische Behörden leichter als für Stellen anderen Staaten möglich, da das US-Handelsministerium die Aufsicht über die DNS-Rootzone ausübt[WIKI-2013i].

Die Rootzone ist die Basis aller Domains und ist – beschränkt nur durch eingesetztes Caching – an jeder DNS-Namensauflösung beteiligt. Für weitere Informationen zum Domain Name System und seiner Manipulierbarkeit, siehe Abschnitt 2.1.4.

3.4 Deutschland

In Abschnitt 3.3 sind wir auf Aspekte des Urheberrechts eingegangen. Nachdem wir dort bereits einen besonderen Blick auf die Situation in Deutschland geworfen haben, möchten wir diesen nun verallgemeinern.

Bewusst keinen Bezug nehmen werden wir dabei auf zwei besondere Debatten der letzten Jahre, Vorratsdatenspeicherung und Zugangserschwerungsgesetz, da sie aktuell nicht mehr Teil der Rechtslage sind. Unter Vorratsdatenspeicherung verstand man die in ihrer bisherigen Form für verfassungswidrig und nichtig erklärte[BVG-2010] Pflicht von Telekommunikationsdienstleistern, sämtliche Verbindungsdaten ihrer Nutzer für einen Zeitraum von sechs Monaten zu speichern und berechtigten staatlichen Stellen auf Aufforderung zur Verfügung zu stellen. Das durch den Bundestag wieder aufgehobene Zugangserschwerungsgesetz verpflichtete Telekommunikationsdienstleister, den Zugang zu sämtlichen auf einer geheimen Liste aufgeführten Dienste zu sperren[ZEG-2010].

Nach deutschem Rechtsverständnis stellt Zensur einen Eingriff in die Grundrechte der Meinungsfreiheit, Rezipientenfreiheit und ggf. Pressefreiheit dar. Diese Rechte garantiert das Grundgesetz in Art. 5 Abs. 1:

> »*Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.*«

Durch ihren Verfassungsrang und als Teil des unveräußerlichen Grundrechtekatalogs[15] kommt diesen Garantien eine extrem hohe Bedeutung zu. Im folgenden möchten wir in diesem Abschnitt darauf eingehen, in wie weit in Deutschland dennoch Zensurmaßnahmen im Sinne unserer Definition in Abschnitt 1.1 stattfinden.

15 Sogenannte „Ewigkeitsklausel" Art. 79 Abs. 3 GG: „Eine Änderung dieses Grundgesetzes, durch welche (...) die in den Artikeln 1 und 20 niedergelegten Grundsätze berührt werden, ist unzulässig."

Durch unsere Betrachtungen zum Urheberrecht haben wir hier schon wichtige Aspekte vorweggenommen. Zu Art. 5 Abs. 1 des Grundgesetzes sind drei fundamentale Einschränkungen zu beachten. Hier ist zunächst zunächst zu sehen, dass die Grundrechte grundsätzlich nur den Staat und seine Organe binden. Private sind grundsätzlich nicht zur Gewährleistung der Grundrechte verpflichtet[16].

Als weitere fundamentale Abweichung zu unserer Definition ist der Begriff der Zensur im Sinne des Grundgesetzes ausschließlich als Vorzensur zu verstehen. Das absolute Verbot „Eine Zensur findet nicht statt" hat für Maßnahmen der Nachzensur keinerlei Bedeutung[BOK-2013a].

Schließlich enthält Art. 5 GG in Absatz zwei selbst ganz wesentliche Einschränkungen der zunächst garantierten Grundrechte:

> »*Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.*«

Die zunächst auf Verfassungsrang garantieren Rechte können also tatsächlich durch einfaches Gesetz eingeschränkt werden. Wir gehen nun zunächst auf einige besonders relevante Bestimmungen des Strafrechts ein, die nach unserem Modell aus Abschnitt 2.1 Maßnahmen der Kategorie 1 darstellen.

§§ 186 - 187 des Strafgesetzbuches (Üble Nachrede und Verleumdung) verbieten zum Schutz der persönlichen Ehre bestimmte Tatsachenbehauptungen über einen Dritten. Der Tatbestand der Verleumdung ist dabei als besonders schwerer Fall der üblen Nachrede zu verstehen, der mit höherer Strafe – bis zu fünf Jahren Freiheitsentzug – bedroht ist. Wir konzentrieren uns daher auf den „Basistatbestand" der üblen Nachrede.

16 Art. 1 Abs. 3 GG: „Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht."

»*Wer in Beziehung auf einen anderen eine Tatsache behauptet oder verbreitet, welche denselben verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen geeignet ist, wird, wenn nicht diese Tatsache erweislich wahr ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Tat öffentlich oder durch Verbreiten von Schriften (§ 11 Abs. 3) begangen ist, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.*«

– § 186 StGB

Verboten können neben Lügen also auch wahre Behauptungen sein, sofern der Verbreiter nicht in der Lage ist, sie zu beweisen.

Während nach diesen Vorschriften nur die Freiheit der Behauptung von Tatsachen eingeschränkt wird, verbietet § 185 StGB (Beleidigung) unter bestimmten Umständen auch Meinungsäußerungen.

»*Die Beleidigung wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Beleidigung mittels einer Tätlichkeit begangen wird, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.*«

Verbotene Meinungsäußerungen sind dabei „Werturteile, durch die der Täter seine eigene Missachtung kundgibt“[BOK-2013b].

Weitere Vorschriften des Strafrechts, die nach unserer Definition aus Abschnitt 1.1 als Zensur bezeichnet werden müssen, beinhalten das Verbot des Aufrufs zu Straftaten.

»*Wer öffentlich, in einer Versammlung oder durch Verbreiten von Schriften zu einer rechtswidrigen Tat auffordert, wird wie ein Anstifter bestraft. Bleibt die Aufforderung ohne Erfolg, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.*«

– § 111 StGB

Einem Anstifter wiederum droht § 26 StGB die gleiche Strafe wie dem Täter selbst an. Das Verbot des Aufrufs zu Straftaten beinhaltet auch das Verbot zu nach anderen Vorschriften, u.A. den in diesem Abschnitt vorgestellten, verbotenen Äußerungen und Datenübertragungen aufzurufen.

Unter Androhung von bis zu zehn Jahren Gefängnis in den schlimmsten Fällen verbietet das StGB in § 184a/b/c bestimmte Formen von Pornographie. Verboten sind insbesondere jede Verbreitung von gewalt- und tierpornographischen Daten, im Falle kinder- und jugendpornographischer Daten auch deren bloßer Besitz.

Hinaus über die eigentliche Ermächtigung des Art. 5 Abs. 2 GG, Zensurmaßnahmen durch allgemeine Gesetze zu schaffen, geht das Verbot der Billigung des Nationalsozialismus.

> »*Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer öffentlich oder in einer Versammlung den öffentlichen Frieden in einer die Würde der Opfer verletzenden Weise dadurch stört, dass er die nationalsozialistische Gewalt- und Willkürherrschaft billigt, verherrlicht oder rechtfertigt.*«
>
> – § 130 Abs. 4 StGB

Obgleich es sich nicht um ein *allgemeines* Gesetz handelt – verboten sind hier vielmehr ganz konkrete Inhalte, die als Meinung geäußert werden können – hat das Bundesverfassungsgericht diese Bestimmung unter Berufung auf eine besondere historische Dimension bestätigt[BVG-2009].

Im Rahmen unserer Definition von Zensur muss zum Schluss noch die allgemeine zivilrechtliche Schadenersatzpflicht genannt werden.

> »*Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.*«
>
> – § 823 BGB

Es handelt sich hierbei um die allgemeinere Form eines Anspruchs, den wir in Abschnitt 3.3 bereits in Bezug auf das Urheberrecht kennegelernt haben. Eingeschlossen sind hier insbesondere Äußerungen, die geeignet sind, einem Geschäftsbetrieb zu schaden. Der hierdurch Geschädigte kann den Ersatz entgangener Einnahmen verlangen.

Bei Tatsachenbehauptungen kommt es hier ähnlich dem Straftatbestand der üblen Nachrede in der Praxis ebenfalls nicht darauf an, ob die getätigte Äußerung der Wahrheit entspricht oder nicht. Vielmehr ist auch hier entscheidend, ob die Behauptung auch beweisbar ist.

Ein Beispiel hierfür wäre die Behauptung eines Restaurantgastes, er habe in der Küche Schaben gesehen. Diese Behauptung unzureichender hygienischer Zustände ist geschäftsschädigend. Kann der Gast sie nicht beweisen, muss er mit einer Verurteilung zu Schadenersatz rechnen.

4 Fazit

Zensur ist ein in demokratischen Gesellschaften geächtetes Konzept[BPB-2013]. Demokratische Staaten wie Deutschland rechtfertigen von ihnen durchgeführte Maßnahmen, die im Sinne unserer Definition dennoch Zensur darstellen – in der Sprache des Grundgesetzes sind dies Einschränkungen der Grundrechte auf Meinungs-, Rezipienten- und Pressefreiheit – stets mit dem Schutz Anderer vor Verletzung ihrer Rechte, hinter die die genannten Grundrechte in diesen speziellen Fällen zurücktreten müssen.

All diese Rechte sind Ausprägungen eines Regelwerks, nach dem unsere Gesellschaft organisiert ist (vergleiche die Begriffsdefinition „Gesellschaft“ aus Abschnitt 1.1). Man kann bis hierher also bejahen, dass Zensur dem Schutz der Gesellschaft vor Verletzung ihrer Grundlagen dient und damit tatsächlich deren Wohl.

Um einen neutralen Standpunkt zu wahren, ist es jedoch wichtig, Konzepte gleich welcher Art nicht einfach als gegeben anzunehmen. Hierzu gehören auch die eingangs genannten Rechte des Einzelnen, die in demokratischen Staaten Rechtfertigung für Zensurmaßnahmen darstellen. Solche Rechte sind Teil des Aufbaus einer Gesellschaft zu dem Zeitpunkt, zu dem diese Rechte existieren. Auch jedes ethisch-moralische System bis hin zu grundlegenden Errungenschaften wie den allgemeinen Menschenrechten ist Teil des kulturellen Schatzes und damit des Status Quo einer Gesellschaft.

Zu diesem Status Quo gehören auch Aspekte wie Machtverteilung, praktizierte Arten von Entscheidungsfindungen und Stellung des Einzelnen in der Gesellschaft. Wie unsere Beispiele in Kapitel 3 gezeigt haben, trifft der in den Rechtssystemen westlich-demokratischer Staaten verbreitete Zensurbegriff dabei besonders auf Länder zu, die in den drei letztgenannten Aspekten völlig anders agieren; in denen vor Allem die Stellung des Einzelnen in Bezug zur Stellung der jeweiligen Führung stark, teilweise bis zur Unkenntlichkeit zurücktritt.

Zensurmaßnahmen dienen stets dem Erhalt des Status Quo und damit dem Schutz vor Veränderung. Dies ergibt sich trivial daraus, dass nur derjenige, der eine entsprechende tatsächliche Macht besitzt, derartige Maßnahmen überhaupt durchsetzen kann.

Sie dienen damit letztlich dem Schutz einer bestimmten Gesellschaft vor existenzbedrohenden Gefahren. Da die Stellung des Einzelnen Frage der jeweiligen Gesellschaftsordnung ist, sagt dies noch nichts darüber aus, ob Zensur auch dem Wohl des einzelnen Menschen dient.

Die Frage, ob Zensur dem Wohle der Gesellschaft als solchen dient, ist also nichts anderes als eine besondere Ausprägung der völlig subjektiven Frage, in welcher Gesellschaft wir leben möchten. In Gesellschaften, die sich die Freiheit des Einzelnen als Leitsatz gegeben haben, sagt das Maß an Zensur zudem etwas darüber aus, wie viel dieser Freiheit sich die jeweilige Gesellschaft tatsächlich zutraut.

Anhang A. Abkürzungsverzeichnis

Abb.	Abbildung
ASCII	American Standard Code for Information Interchange
RGB	Rot-Grün-Blau-Farbsystem
DNS	Domain Name System
IP	Internetprotokoll, auch kurz für IP-Adresse
BGP	Border Gateway Protocol
TOR	The Onion Router
I2P	Invisible Internet Project
UTC	Universal Time, Coordonné Koordinierte Weltzeit
USC	United States Code
DMCA	Digital Millenium Copyright Act
GG	Grundgesetz
StGB	Strafgesetzbuch
UrhG	Urheberrechtsgesetz
TMG	Telemediengesetz
Art.	Artikel
Abs.	Absatz

Anhang B. Quellenverzeichnis

WIKI-2013 a Wikipedia: *Zensur (Informationskontrolle)*. http://de.wikipedia.org/w/index.php?title=Zensur_(Informationskontrolle)&oldid=120516851, abgerufen 28.07.2013.

b Wikipedia: *DeCSS*. http://en.wikipedia.org/w/index.php?title=DeCSS&oldid=558932497, abgerufen 28.07.2013.

c Wikipedia: *Illegal Prime.* http://en.wikipedia.org/w/index.php?title=Illegal_prime&oldid=549543374, abgerufen 28.07.2013.

d Wikipedia: *AACS encryption key controversy*. http://en.wikipedia.org/w/index.php?title=AACS_encryption_key_controversy&oldid=552750829, abgerufen 28.07.2013.

e Wikipedia: *Steganographie*. http://de.wikipedia.org/w/index.php?title=Steganographie&oldid=119936517, abgerufen 29.07.2013.

f Wikipedia: *Proxy (Rechnernetz).* http://de.wikipedia.org/w/index.php?title=Proxy_(Rechnernetz)&oldid=120269392, abgerufen 29.07.2013.

g Wikipedia: *X-Forwarded-For*. http://en.wikipedia.org/w/index.php?title=X-Forwarded-For&oldid=563040890, abgerufen 29.07.2013.

h Wikipedia: *Megaupload*. http://en.wikipedia.org/w/index.php?title=Megaupload&oldid=563316826, abgerufen 30.07.2013.

i Wikipedia: *DNS root zone*. http://en.wikipedia.org/w/index.php?title=DNS_root_zone&oldid=559380152, abgerufen 30.07.2013.

WIKI-2013 j Wikipedia: *Arabischer Frühling*. http://de.wikipedia.org/w/index.php?title=Arabischer_Fr%C3%BChling&oldid=121093207, abgerufen 31.07.2013.

k Wikipedia: *Liu Xiaobo*. http://de.wikipedia.org/w/index.php?title=Liu_Xiaobo&oldid=119194072, abgerufen 31.07.2013.

l Wikipedia: *Internet censorship in the People's Republic of China*. http://en.wikipedia.org/w/index.php?title=Internet_censorship_in_the_People%27s_Republic_of_China&oldid=566380574, abgerufen 31.07.2013.

m Wikipedia: *Kwangmyong*. http://en.wikipedia.org/w/index.php?title=Kwangmyong_(network)&oldid=565672180, abgerufen 31.07.2013.

DUD-2013 Duden online: *Zensur, die*. http://www.duden.de/rechtschreibung/Zensur, abgerufen 28.07.2013.

BPB-2011 El Difraoui, Asiem: *„Die Rolle der neuen Medien im Arabischen Frühling".* In: Dossier *Arabischer Frühling*, Bundeszentrale für Politische Bildung, Bonn, 2011. http://www.bpb.de/internationales/afrika/arabischer-fruehling/52420/die-rolle-der-neuen-medien?p=all, abgerufen 21.07.2013.

BPB-2013 „Politiklexikon" der Bundeszentrale für Politische Bildung: *Zensur.* http://www.bpb.de/wissen/KZM09M, abgerufen 28.07.2013. Dort zitiert aus: Schubert, Klaus; Klein, Martina: *Das Politiklexikon*. 5., aktualisierte Auflage. Dietz, Bonn, 2011.

HIL-1997 Hillmann, Karl-Heinz: *Gesellschaft*. In: Soziologielexikon, 3. überarbeitete und erweiterte Auflage. R. Oldenbourg, München, 1997. S. 215.

WIPO-1996 *WIPO Copyright Treaty*. Weltorganisation für geistiges Eigentum, Genf, 20.12.1996. Online verfügbar unter http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html, abgerufen 28.07.2013.

WIPO-2013 Kein Titel: Übersicht über Beitrittsdaten der Staaten zum WIPO-Urherberrechtsabkommen. Online verfügbar unter http://www.wipo.int/export/sites/www/treaties/en/documents/pdf/wct.pdf, abgerufen 28.07.2013.
Weltorganisation für geistiges Eigentum, Genf.

CAR-2001 Phil Carmody: *The world's first illegal prime number?* http://fatphil.org/maths/illegal1.html, abgerufen 28.07.2013

CAR-2010 Phil Carmody: *Curriculum Vitæ Summary.* http://fatphil.org/me/cvsum_nov2010.html, abgerufen 28.07.2013

YOU-2013 YouTube, LLC: *How Content ID works.* https://support.google.com/youtube/answer/2797370?hl=en&ref_topic=2778545, abgerufen 28.07.2013.

NSA-2005 Vanessa Antoine et. al.: *Router Security Configuration Guide*. National Security Agency, Ft. Meade, 2005. S. 40. Online verfügbar unter: http://www.nsa.gov/ia/_files/routers/C4-040R-02.pdf, abgerufen 29.07.2013.

PRO-2013 Statistik des Proxyverzeichnisses Proxy-listen.de (wahllose Probe aus verfügbaren Listendiensten). http://www.proxy-listen.de, abgerufen 29.07.2013.

DIN-2004 Dingledine, Roger; Mathewson, Nick; Syverson, Paul: *TOR: The Second-Generation Onion Router*. In: Proceedings of the 13th conference on USENIX Security Symposium, Volume 13, USENIX Association, Berkeley, S. 21. Online verfügbar unter: https://www.usenix.org/legacy/event/sec04/tech/full_papers/dingledine/dingledine.pdf, abgerufen 30.07.2013.

TOR-2013 Statistiken über den aktuellen Stand des TOR-Netzwerks: *Tor Metrics Portal: Consensus Health*, https://metrics.torproject.org/consensus-health.html, abgerufen 30.07.2013.

TNS-2013 Kowalski, Joseph B.: Software *Tor Network Status,* Werte der Installationen auf http://torstatus.info sowie http://torstatus.blutmagie.de, abgerufen 30.07.2013.

BRA-2010 Braun, Michael: Lehrveranstaltung *Kryptologie.* Hochschule Darmstadt, Sommersemester 2010

HEI-2010 Bachfeld, Daniel: *Server des Tor-Projekts gehackt*. Heise, Hannover. http://www.heise.de/security/meldung/Server-des-Tor-Projekts-gehackt-910931.html, abgerufen 30.07.2013.

DIN-2010 Dingledine, Roger: *Tor Project infrastructure updates in response to security breach*. Mail vom 20.01.2010 an die Mailingliste or-talk. Online verfügbar unter http://archives.seul.org/or/talk/Jan-2010/msg00161.html, abgerufen 30.07.2013.

ARS-2011 Sean Gallagher: *Anonymous collects, publishes IP addresses of alleged pedophiles*. Ars Tecnica. http://arstechnica.com/business/2011/11/anonymous-collects-publishes-ip-addresses-of-alleged-pedophiles, abgerufen 30.07.2013.

TEL-2012 Kaul, Christa Tamara: *Facebook-Revolution in Ägypten? - Totaler Schwachsinn!*, in: *Telepolis,* Heise, 2012. http://www.heise.de/tp/blogs/6/151200, abgerufen 31.07.2013,

REN-2011 Cowie, Jim: *Egypt Leaves the Internet*. Renesys Blog, 2011. http://www.renesys.com/2011/01/egypt-leaves-the-internet, abgerufen 31.07.2013.

SPI-2011 Reißmann, Ole; Rosenbach, Marcel: *Revolutionshilfe aus Berlin*. In: Der Spiegel, 2011, Nr. 44. Online verfügbar unter http://www.spiegel.de/spiegel/a-791039.html, abgerufen 31.07.2013.

SHE-2010 Shetty, Salil: *Ein leerer Stuhl als Symbol*. In: *Süddeutsche.de*, 2010. http://www.sueddeutsche.de/politik/nobelpreis-fuer-liu-xiaobo-das-symbol-des-leeren-stuhls-1.1034535, abgerufen 31.07.2013.

TAZ-2010 Lietsch, Julia: *IT-Firma ohne Internet*. taz.de, 2010. http://www.taz.de/!112354/, abgerufen 31.07.2013.

USC *United States Code*, Bundesrecht der Vereinigten Staaten von Amerika. Online verfügbar unter http://www.law.cornell.edu/uscode/text, abgerufen 30.07.2013.

DMCA US-amerikanischer *Digital Millenium Copyright Act*, 1998. Online verfügbar unter http://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf, abgerufen 30.07.2013

GG *Grundgesetz für die Bundesrepublik Deutschland,* online verfügbar unter http://www.gesetze-im-internet.de/gg, abgerufen 30.07.2013.

StGB Deutsches *Strafgesetzbuch*, online verfügbar unter http://www.gesetze-im-internet.de/stgb, abgerufen 30.07.2013.

UrhG Deutsches *Gesetz über Urheberrecht und verwandte Schutzrechte,* online verfügbar unter http://www.gesetze-im-internet.de/urhg, abgerufen 30.07.2013.

TMG Deutsches *Telemediengesetz*, online verfügbar unter http://www.gesetze-im-internet.de/tmg, abgerufen 30.07.2013.

ZEG-2010 Ehemaliges deutsches *Gesetz zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen*. Bundesgesetzblatt I Jahrgang 10 Nr. 6, S. 78 ff. Online verfügbar unter: http://www2.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl110s0078.pdf, abgerufen 31.07.2013.

BOK-2013 a Schemmer: *Beck'scher Online-Kommentar GG*. 15. Edition 18, Beck, München, 2003. Art. 5 Rn 114. Online (Paywall) verfügbar unter: http://beck-online.beck.de/?vpath=bibdata/komm/BeckOK_VerfR_18/GG/cont/BeckOK.GG.a5.gll%2Ehtm, abgerufen 31.07.2013.

BOK-2013 b Valerius: *Beck'scher Online-Kommentar StGB.* Edition 22, Beck, München, 2013. §185. Online (Paywall) verfügbar unter: http://beck-online.beck.de/?vpath=bibdata/komm/BeckOK_StR_22/StGB/cont/beckok.StGB.p185.htm, abgerufen 31.07.2013.

BVG-2009 Bundesverfassungsgerichtsurteil 1 BvR 2150/08 vom 4.11.2009, online verfügbar unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20091104_1bvr215008.html, abgerufen 31.07.2013.

BVG-2010 Bundesverfassungsgerichtsurteil 1 BvR 256/08 vom 2.3.2010, online verfügbar unter http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.htmlabgerufen 31.07.2013.

Anhang C. Abbildungsverzeichnis

Leerseite.

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

fbi
FACHBEREICH INFORMATIK