# Internetzensur: Methoden und deren Beobachtung

Gerhard Hagerer
Betreuer: Lukas Schwaighofer
Seminar Future Internet WS2012/2013
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: gerhard.hagerer@in.tum.de

## ZUSAMMENFASSUNG

In der vorliegenden Arbeit geht es um Internetzensur im Sinne von Internetausfällen, wie sie auf Anordnung von den Regierungen in Ägypten und Libyen zu Beginn des Jahres 2011 im Zusammenhang mit den dort auftretenden Revolutionen passierten. Im Referenzpaper [1] wurden diese durch BGP-Routenaktualisierungen und unangeforderten Datenverkehr (*Internet Background Radiation*) in Darknets durch Network Telescopes mit Erfolg beobachtet. Dabei konnten zwei Abschaltmethoden unterschieden werden: der Einsatz von Paketfiltern sowie Techniken, die dem Abtrennen ganzer Teilnetze des Internets (*autonome Systeme*) gleichkommen. Diese Themen werden in ihrer Theorie ausführlich allgemeinverständlich erklärt, um im Anschluss daran die Internetausfälle der Revolutionen in Ägypten und Libyen technisch analysieren zu können.

## Schlüsselwörter

Ausfälle, Verbindungsabbruch, Zensur, Darknet, Network Telescope, Internet Background Radiation

## 1 Einführung

In der heutigen Zeit wird uns zunehmend bewusst, welche gesellschaftlichen und politischen Konsequenzen moderne Technologien wie das Internet haben. Soziale Netzwerke wie Facebook und Twitter ermöglichen vielen Menschen weltweit eine einfache, schnelle und starke Vernetzung miteinander. Dadurch ist es besser als jemals zuvor möglich, sich mit anderen online zu organisieren und auszutauschen. Diese moderne Entwicklung widerspricht dem Interesse von totalitären Regierungen, welche freie Meinungsäußerung und das Versammlungsrecht in ihren Ländern zu unterdrücken versuchen. Somit machen diese das freie Internet zum Feind und versuchen dieses einzuschränken. Dies wird mit den Mitteln der modernen Zensurtechnologie zu erreichen gesucht: entweder werden regierungskritische digitale Inhalte von höchster Instanz blockiert und können nicht heruntergeladen werden oder Internetbenutzern wird der Zugang zum Internet gänzlich verwehrt. Was in der Onlinewelt allerdings passiert, wenn eine ganze Bevölkerung sich gegen ihre eigene Regierung zusammenschließt, konnte am Anfang des Jahres 2011 im Zuge des arabischen Frühlings beobachtet werden: Ägypten und Libyen erlitten vollständige, von den dortigen Regierungen veranlasste Internetausfälle, was weltweit sichtbare Veränderungen im Internet auslöste, sowohl in Routingtabellen von BGP-Routern als auch in der Grundlast des Datenverkehrs [2] [3]. Es kann insofern von einer globalen digitalen Erschütterung gesprochen werden, wie sie bis zu diesem Zeitpunkt noch nie vorgekommen ist. Es dauerte nicht lang, bis Regional Internet Registries und Network Telescopes entprechende Daten veröffentlichten, die alsbald zum Objekt von Forschungen über die Beobachtung von Internetausfällen wurden. In diesem Zusammenhang ist insbesondere das Paper "Analysis of Country-wide Internet Outages Caused by Censorship" [1] zu erwähnen, welches besagte Ereignisse in Ägypten und Libyen zum Forschungsgegenstand hat. Die vorliegende Arbeit nimmt im Wesentlichen auf dieses Bezug, um die in den beiden Ländern angewendeten Internetabschaltungen technisch zu analysieren. Folgende Technologien sind dafür relevant und also solche Gegenstand genauerer Betrachtung:

- das Internet als Verbund von vielen autonomen Systemen (Kapitel 2)
- das Border Gateway Protocol (*BGP*) als wichtigstes Element zur Wegefindung im Internet zwischen autonomen Systemen (Kapitel 3)
  - BGP-Withdrawals als Folge von Internetausfällen
  - Geolocation Datenbanken, Regional Internet Registries und Network Telescopes als Datenquellen, um Internetausfälle zu beobachten
- Paketfilter als weiteres Werkzeug, um Internetzensur umzusetzen (Kapitel 4)

Diese Punkte werden ergänzt durch Kapitel 5, in welchem die in den Revolutionen angefallenen Daten analysiert werden, um anhand davon die vorher erklärte Theorie zur Zensur und zu Internetabschaltungen zu veranschaulichen.

## 2 Begriffe und Funktionsweise des Internets

Um die verschiedenen Möglichkeiten der beabsichtigten Internetabschaltung bzw. -zensur verstehen zu können, ist es erforderlich, die Funktionsweise, die Organisationsform und entsprechende Fachbegriffe des Internets zu kennen. Diese Dinge werden in diesem Kapitel erläutert.

### 2.1 Internet und autonome Systeme

Das Internet ist ein großes, dezentral organisiertes Computernetzwerk bestehend aus vielen kleineren Netzwerken, genannt autonome Systeme (engl. autonomous Systems, Abkürzung: *ASs*). Ein Internet-Service-Provider (Abkürzung: *ISP*), eventuell auch eine Universität oder eine größere Firma, stellt seinen Endkunden einen Zugang zum eigenen Netzwerk beziehungsweise AS zur Verfügung. Dieses ist mit


doi: 10.2312/NET-2013-02-1_01

mindestens einem anderen autonomen System anderer ISPs verbunden. Es besteht zwischen zwei beliebigen ASs immer eine Verbindung, entweder direkt oder indirekt über mehrere andere AS. Folglich existiert zwischen allen Endkunden immer mindestens eine Route. Das resultierende Netz wird Internet genannt. [4]

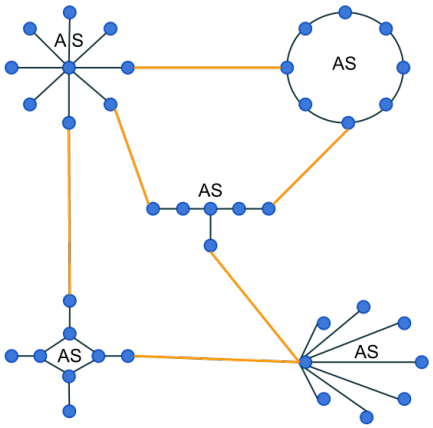


**Abbildung 1: Schematische Darstellung von autonomen Systemen (ASs)**

## 2.2 Routing

Wie auf Abbildung 1 ersichtlich besteht ein AS aus zwei Arten von vermittelnden Knotenpunkten (*Routern*): Welche mit Verbindungen nach außen und innen (für die vorliegende Arbeit genannt *Exterior Gateways*) und welche mit ausschließlich inneren Verbindungen. Exterior Gateways stellen die Schnittstellen eines AS zu anderen ASs und damit zum Rest der Welt dar. Somit sind diese Knotenpunkte für die globale externe Routenfindung zuständig. Die anderen dagegen dienen nur der internen Routenfindung innerhalb eines AS. Dementsprechend wird im Allgemeinen zwischen zwei Routingprotokollfamilien unterschieden: *Exterior Gateway Protocols* und *Interior Gateway Protocols*. Ersterer Protokollart ist das Border Gateway Protocol (*BGP*) zuzuordnen, welches als weltweiter Standard Anwendung im Internet findet. BGP wird in Unterkapitel 3.1 erläutert. [4] [5]

## 2.3 IP-Vergabe und Regional Internet Registries

Ein ISP beantragt für seine ASs jeweils IP-Adressbereiche und eine global eindeutige Nummer (*AS-Nummern*) bei der auf dem jeweiligen Kontinent zuständigen Regional Internet Registry (*RIR*) (diese bekommt diese Daten wiederum von der IANA zugewiesen, siehe dafür [6]) - die Zuständigkeiten der RIRs sind auf Abbildung 2 zu erkennen. Anschließend kann er die IP-Adressen an seine Endkunden weitergeben. Diese gehen damit ins Internet, um Daten weltweit zu senden und zu empfangen. Die AS-Nummern sind zwischen den verschiedenen ASs für die eindeutige Identifikation bei der Routenfindung der Daten (*Routing*) notwendig. Im Speziellen wird darauf im Unterkapitel 3.1 eingegangen. [5] [7]


**Abbildung 2: Weltweite Zuständigkeiten von Regional Internet Registries (RIRs) [7]**

# 3 BGP

In diesem Kapitel soll die externe Routenfindung genauer betrachtet werden, um zu sehen, wie das BGP-Routing im Internet zwischen den verschiedenen ASs funktioniert (Unterkapitel 3.1). Dabei wird auch erläutert, durch welche Eingriffe hier Internetzensur im Sinne von gezielten Internetabschaltungen ermöglicht wird (Unterkapitel 3.2). Zudem wird auf zwei Methoden für die externe Messung solcher Ereignisse (mittels Steuerungsdaten und Nutzdaten) eingegangen. Beispiele für die beschriebenen Zensurmaßnahmen finden sich im Kapitel 5. Alle diese Themen gehen, soweit nicht anders vermerkt, zurück auf eine wissenschaftliche Arbeit zum Thema Internetausfälle und ihre Beobachtbarkeit [1].

## 3.1 Funktionsweise von BGP-Routing

Im Internet sind die am BGP-Routing teilnehmenden Router die Exterior Gateways der ASs. Diese speichern in ihren Routingtabellen Einträge ab, welche alle möglichen Routen zum jeweiligen *IP-Adressraum*, der seinerseits eine Menge von IP-Adressen umfasst, enthalten. Diese Routen sind als Vektoren von AS-Nummern der ASs gegeben, die als vermittelnde Knotenpunkte auf dem Weg zum IP-Zieladressraum liegen.

Ein neues AS macht sich mittels dessen Exterior Gateway (auch *BGP-Router* genannt) im Internet global bekannt, indem es anderen ASs seine Existenz bekanntgibt (*BGP-Announcement*). Es übermittelt an benachbarte ASs (bzw. deren BGP-Router) im Wesentlichen folgende Informationen: seinen IP-Adressraum, seine AS-Nummer und alle durch ihn erreichbaren IP-Adressräume einschließlich der dazugehörigen AS-Routenvektoren (*UPDATE*-Nachricht). Die benachrichtigten BGP-Router ergänzen ihre Routingtabellen um die neuen IP-Adressräume und benachrichtigen selber wiederum ihre externen Nachbarn über die neuen Routeninformationen (*UPDATE*-Nachricht) und so fort, bis alle BGP-Router des Internets mit der neuen Information versorgt sind. Damit ist ein neuer IP-Adressraum von überall auf der Welt her ansprechbar.

Um den Online-Status gegenseitig zu überprüfen, teilen sich benachbarte BGP-Router diesen in regelmäßigen Zeitabständen durch KEEPALIVE-Nachrichten mit. Wenn die Zeitspanne zwischen zwei KEEPALIVE-Nachrichten von einem BGP-Router zu lang wird, so gilt dessen AS bzw. IP-Adressraum vom benachbarten Router aus betrachtet zunächst als nicht mehr erreichbar und der darauf verweisende


doi: 10.2312/NET-2013-02-1_01

Eintrag wird aus der BGP-Routingtabelle gestrichen (*BGP-Withdrawal*). Es kann danach jedoch wieder zu einem BGP-Announcement kommen, sofern es eine andere noch bestehende Verbindung zum AS gibt. Diese Verbindung kann gegebenenfalls indirekt über andere BGP-Router und ASs laufen - Abbildung 1 liefert eine Veranschaulichung für mehrere mögliche Routen zwischen verschiedenen ASs. Derartige Änderungen, wie das Löschen oder das Modifizieren von Einträgen, werden wiederum im Internet mittels UPDATE-Nachrichten verbreitet. [8]

## 3.2 BGP-Withdrawals und Internetzensur

BGP-Withdrawals können z.B. durch eine Trennung des BGP-Routers vom Netz durch Ziehen des Netzwerkkabels oder durch entsprechende Änderungen der Konfiguration des jeweiligen BGP-Routers ausgelöst werden. In der Folge ist das mit den BGP-Routern assoziierte AS und der entsprechende IP-Adressraum vom Internet abgetrennt. Das bedeutet, dass alle zugehörigen Endnutzer (Clients wie Server) andere Endnutzer außerhalb des ASs nicht kontaktieren bzw. nicht von ihnen kontaktiert werden können. Es gibt keine Möglichkeit, diese Internetsperre zu umgehen, wie das beispielsweise bei Paketfiltermechanismen denkbar wäre. Allerdings kann es sein, dass Teilnehmer innerhalb des ASs noch untereinander kommunizieren können, sofern den Routern innerhalb des AS noch normal funktionieren. Somit ist es möglich, gezielt ganze Gruppen von Endnutzern vom Internet abzukoppeln. Insofern kann diesbezüglich nicht nur von einem Internetzensur-, sondern auch von einem Internetabschaltungs- bzw. Internetausfallmechanismus gesprochen werden.

## 3.3 Globale Messbarkeit von BGP-Withdrawals

Es stellt sich die Frage, ob es Möglichkeiten gibt von außerhalb zeitnah herauszufinden, wo auf der Welt derartige Internetabschaltungen stattfinden. Dies ist insbesondere dann interessant, wenn großflächige Internetausfälle mit historischen Ereignissen wie Revolutionen oder Bürgerkriegen in Zusammenhang stehen. Das Vorgehen von Regierungen gegen die eigene Bevölkerung würde damit online global beobachtbar.

In den folgenden Unterkapiteln wird eine Methode zur Eingrenzung des zu überwachenden IP-Adressbereichs und zwei Messmethoden für die Überwachung von BGP-Withdrawals vorgestellt. Letztere sind in zwei Kategorien unterteilbar. Einerseits können BGP-UPDATE-Nachrichten an gut vernetzten BGP-Routern daraufhin analysiert werden, ob und welche BGP-Withdrawals darin sichtbar werden. Diese Art von Analyse bezieht sich nur auf Routingdaten, welche als solche ausschließlich zwischen BGP-Routern ausgetauscht werden (Steuerebene, engl. *Control Plane*). Andererseits können normale Pakete, sprich Nutzdaten, beim Empfänger beobachtet werden. Hat dieser die Pakete vorher nicht angefordert spricht man von unangefordertem Datenverkehr. Die kontinuierliche Analyse der Quell-IP-Adressen dieser Daten in einem entsprechend großem Maßstab mittels Network Telescopes machen BGP-Withdrawals sichtbar, wenn derartige Messungen über einen gewissen Zeitraum hinweg durchgeführt werden. BGP-Router dienen dabei weder als Sender noch als Empfänger für diese Art von Daten, sondern leiten diese nur weiter (Nutzdatenebene, engl. *Data Plane*). [9]

### 3.3.1 Ortung von BGP-Withdrawals

Um genaue Aussagen über Internetausfälle in einer bestimmten Region auf der Welt zu machen, ist es notwendig, den beobachteten IP-Bereich darauf einzuschränken. Dadurch wird eine weniger aufwändige und weitaus solidere Messung von BGP-Withdrawals möglich.
Die fünf RIRs (siehe Abbildung 2) stellen auf ihren Webseiten die Informationen darüber zur Verfügung, welchem Land welches AS bzw. welche AS-Nummer zugewiesen ist. Dabei muss sich ein AS nicht zwangsweise komplett im entsprechenden Land befinden, genauso wie ASs aus anderen Ländern Endnutzern im beobachteten Land Internet zur Verfügung stellen können. Jedoch fallen in vielen Ländern diese Ungenauigkeiten bei den Messungen kaum auf. Somit verfälschen sie nicht die Aussagen über plötzliche große Ausfälle vor Ort, wie in den angeführten Beispielen (Kapitel 5) zu beobachten ist.
Ist bekannt, welche ASs im zu beobachteten Land liegen, liefern öffentlich zugängliche Datenbankabfragen der RIRs über die AS-Nummern die IP-Adressbereiche, die diesen zugeordnet sind. Infolgedessen ist der IP-Bereich für ein Land für jedermann verfügbar, sofern kleinere Unwägbarkeiten ignoriert werden.
Darüberhinaus bieten kommerzielle Anbieter eigene Geolocation-Datenbanken an, welche zur Überprüfung herangezogen werden können. Beispiele hierfür werden in Unterkapitel 5.1 gegeben.

### 3.3.2 Messbarkeit der Routingdaten

Es soll nun vorgestellt werden, welche Datenquellen für die Routingdaten zur Verfügung stehen, welche Arten von Daten dies sind und welche Aussagen bezüglich BGP Withdrawals daraus ableitbar sind.

Wie zu Beginn dieses Kapitels bereits erwähnt, sind bei den Routingdaten die UPDATE-Nachrichten, die zwischen den BGP-Routern versendet werden, von Interesse. Ein Blick in diese Nachrichten gibt Aufschluss darüber, welche Veränderungen (Announcements und Withdrawals) in der jeweiligen Routingtabelle stattgefunden haben. Diese Nachrichten werden im Internet innerhalb der Control Plane zwischen durch Announcements bekanntgegebenen BGP-Routern ausgetauscht und in deren Routingtabellen diesen abgespeichert. Hierbei sei darauf hingewiesen, dass die Routingtabellen von BGP-Routern in Bezug auf die verschieden zugewiesenen IP-Adressräume vollständig, eindeutig und damit in der Tat sehr groß sind.

Es kann ein Ziel sein, zeitliche Verzögerungen zwischen BGP-Announcements/-Withdrawals und deren Bekanntwerden bei entfernteren BGP-Routern gering zu halten. Ist dies der Fall, so erscheint es sinnvoll, einen gut vernetzten BGP-Router für das Speichern der UPDATE-Nachrichten zu verwenden. Dies hat eine geringere Anzahl Hops zwischen Ziel und Empfänger zur Folge und damit auch geringere Latenzzeiten.

In der Praxis sind vor allem Forschungseinrichtungen sowie die RIRs an den besagten BGP-Daten interessiert. Die Daten werden benutzt, um BGP-Phänomene zu erforschen und das BGP weiterzuentwickeln. Besagte Einrichtungen stellen entsprechende Rohdatensätze zum Download bereit sowie weitere Tools, z.B. zur Analyse und Visualisierung. Es wird im Kapitel 5 auf konkrete Beispieldatenbanken hingewiesen.


doi: 10.2312/NET-2013-02-1_01

### 3.3.3 *Messbarkeit von Nutzdaten*

Im Gegensatz zu Routingdaten, die nur zwischen BGP-Routern ausgetauscht werden, machen Nutzdaten den eigentlichen Datenverkehr zwischen Endnutzern aus. Es werden Pakete zwischen zwei Rechnern, Sender und Empfänger, übertragen. Beide besitzen eine eindeutige IP-Adresse, um das Routing hin (Anfrage) und zurück (Antwort) zu ermöglichen. Das Fälschen der Absenderadresse nennt sich *IP-Spoofing* (siehe Abbildung 3). Die Folge davon ist eine Antwort des Empfängers hin zu einer anderen IP-Adresse als der des ursprünglichen Senders. Die dadurch im Internet verursachten Daten werden *Internet Background Radiation (IBR)* genannt [10]. Die IBR bildet eine gewisse kontinuierliche überall vorhandene Grundlast im globalen Datenverkehr und kann somit als eine Art Grundrauschen im Internet verstanden werden.

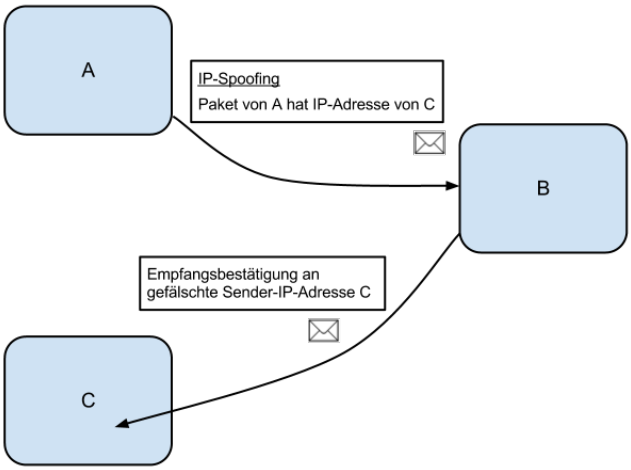


**Abbildung 3: Darstellung von IP-Spoofing. Die Quell-IP-Adresse eines Pakets wird gefälscht. Die Bestätigung geht an einen anderen Sender.**

Es gibt mehrere Ursachen für IBR:

- ***DoS-Attacken***
  Diese kommen zustande, indem gezielt eine sehr große Menge von Anfragen an Computersysteme gesendet werden [11] mit dem Ziel, diese unter Überlast zusammenbrechen zu lassen. Hat jede dieser Anfragen aufgrund von Spoofing eine gefälschte IP-Adresse, wie dies bei DoS-Attacken tatsächlich Anwendung findet (siehe z.B. [1] Kapitel 5.1.3), wird die Antwort an diese gesendet und damit IBR erzeugt. Dadurch tritt spontan für begrenzte Zeit eine große Menge IBR auf (auch *backscatter-traffic* genannt).
- **Scannen von IP-Adressräumen**
  Um herauszufinden, ob sich hinter einer beliebigen IP-Adresse ein Empfänger befindet, wird an diese eine Anfrage gestellt (z.B. via Ping). Bei Durchführung in großem Stil mit vielen IP-Adressen ist eine entsprechende Menge von IBR die Konsequenz. Insbesondere Würmer wie der *Conficker-Wurm* verfahren auf diese Art und Weise, wodurch neue Opfer aufgefunden und infiziert werden. Die Verbreitung des Conficker-Wurms ist groß genug, dass dieser global ein kontinuierliches Maß an IBR erzeugt (siehe [1] Kapitel 4.3). Diese Art von eigentlich unerwünschtem Datenverkehr erweist sich ironischerweise bei IBR-Messungen als besonders hilfreich.
- **Fehlerhafte oder schlechte Netzwerkkonfigurationen**
  Durch fehlerhafte Einstellungen, z.B. falsche IP-Einstellungen von DNS-Servern oder fehlerhafte Firmware bzw. schlechte Konfigurationen von Routern, die wiederum falsche IP-Zuweisungen zur Folge haben, kommt ebenso IBR auf.

Wird die IBR, die aus bestimmten IP-Adressbereichen stammt, z.B. denen eines Landes, über eine gewisse Zeit hinweg kontinuierlich aufgezeichnet, so weisen starke plötzliche Abnahmen von IBR auf Internetausfälle oder -abtrennungen zu den entsprechenden Zeitpunkten hin.

Die Werkzeuge für die Aufzeichnung von IBR sind sogenannte *Network Telescopes*. Diese benutzen IP-Adressräume, die keinen Rechnern zugewiesen sind (*Darknets*), um die daran adressierten Pakete und deren Quell-IP-Adresse aufzuzeichnen. Auch wenn diese Adressräume nur einen sehr kleinen Bruchteil des gesamten Internets ausmachen können, so konnte in Experimenten herausgefunden werden, dass Internetausfälle sich in IBR-Messungen innerhalb von Darknets via Network Telescopes deutlich niederschlagen (siehe [1] Kapitel 5). In der Konsequenz sind Internetabtrennungen über Nutzdatenanalyse in Darknets global und zu jeder Zeit sichtbar, wobei insbesondere Würmern eine Schlüsselrolle zukommt. Dies wird in den Beispielen dieser Arbeit (Kapitel 5) gezeigt werden.

## 4 Paketfilter

Auch wenn BGP-Withdrawals kein triviales Themengebiet sind, sind diese doch leicht durch Ziehen des Netzwerksteckers zu erzeugen. Der Effekt mag für Regierungen interessant sein, um schnell und unkompliziert eine ganze Bevölkerung vom Internet abzutrennen. Allerdings lässt sich mittels dieser Methode nicht beliebig nach Quell-IP-Adresse differenzieren, so dass schnell ein ganzer IP-Adressblock, aber nicht spezielle IP-Adressen vom Internet abgetrennt werden können. Insofern ist eine spezifischere Auswahl an Institutionen, die in einem Land besser online bleiben, nicht ohne weiteres möglich: wichtige Unternehmen, Banken, Stadtwerke und viele weitere sind auf das Funktionieren einer modernen Kommunikationsinfrastruktur angewiesen, um ein Land nicht vollends im Chaos versinken zu lassen. Ein weiteres Manko der der BGP-Withdrawals ist zudem die fehlende Möglichkeit, lediglich den Zugriff auf bestimme Bereiche des globalen Internets zu verhindern. In Anbetracht der wachsenden Rolle von sozialen Netzwerken wie Facebook und Twitter zwecks Nachrichtenaustausch und Demonstrationsorganisation erscheint eine entsprechende Restriktion des Zugriffs auf derartige Plattformen für totalitäre Regierungen ebenso als attraktiv [12]. Dafür sind Paketfilter das geeignete Mittel, deren Funktionsweise im Folgenden kurz dargelegt wird.

### 4.1 Funktionsweise

Das Ziel eines Paketfilters ist es, den in Form von Paketen in und aus einem Netzwerk kommenden Datenverkehr nach bestimmten Kriterien - z.B. Quell- und Ziel-IP-Adresse - zu filtern. Dies wird durch eine Software realisiert, die als Teil einer Firewall auf Routern oder anderen Netzwerkgeräten


doi: 10.2312/NET-2013-02-1_01

zum Einsatz kommt. Dabei wird in Filterregeln definiert, welche Pakete durchgelassen und welche verworfen werden. Dafür wird jedes eintreffende Paket vom Filter geöffnet und dessen Inhalt auf die angegebenen Kriterien überprüft. [13]

## 4.2 Einsatzmöglichkeiten

Solche Systeme werden standardmäßig in sehr vielen Netzwerken benutzt und dienen in erster Linie der Sicherheit, da dadurch unerwünschter Zugriff von außen ins eigene Netz unterbunden werden kann. Erweiterte Paketfilter können ebenso als Kinderschutz zu Hause eingesetzt werden, indem nicht nur nach Quell- oder Zieladresse von Seiten mit jugendgefährdenden Inhalten, sondern auch nach Inhalt selbst, z.B. bestimmten Stichworten, gefiltert wird. Nach unter anderem genau diesem Prinzip funktionieren auch sehr große Zensurinfrastrukturen wie beispielsweise in China [14]. In dieser Arbeit wird in Unterkapitel 5.3 im Zusammenhang mit der Revolution in Libyen auf eine weitere Anwendung eines Paketfilters eingegangen.

# 5 Beispiele

Innerhalb dieses Unterkapitels werden nun Beispiele dargelegt, die zeigen sollen, wie sich Internetausfälle praktisch in Routing- und Nutzdaten bemerkbar gemacht haben. Es werden zwei historische Ereignisse angeführt: die Revolutionen in Ägypten und Libyen. Beide fanden im Jahre 2011 im Zuge des arabischen Frühlings statt. Bei beiden Ereignissen wurde auf Anlass der damaligen Regierungen das Internet abgeschaltet (siehe dazu auch Unterkapitel 3.2). In welchen Datenquellen sich die hieraus resultierten BGP-Withdrawals niedergeschlagen haben ist Bestandteil von Unterkapitel 5.1. Im Anschluss daran werden die Daten für jedes Land analysiert - siehe Ägypten (Unterkapitel 5.2)) und Libyen (Unterkapitel 5.3).

## 5.1 Datenquellen

Um Routing- und Nutzdaten aus bestimmten Ländern beobachten zu können, müssen die den Ländern zugewiesenen IP-Adressräume herausgefunden werden (siehe Ortung von BGP-Withdrawals (Unterkapitel 3.3.1)).

### 5.1.1 *Ortung*

Da sowohl Libyen als auch Ägypten in Afrika liegen, ist somit AfriNIC [15] die zuständige RIR. Dessen Datenbanken geben Aufschluss über die ASs, welche im jeweiligen Land liegen. Zusätzlich sind diese Länderzuweisungen durch weitere unabhängige *Geolocation Datenbanken* überprüfbar, wie zum Beispiel die von MaxMind [16]. In den vorliegenden Beispielen waren die Unterschiede dieser beiden Datenbanken allerdings klein und haben für die in dieser Arbeit gemachten Beobachtungen keine Relevanz (für genaueres siehe [1], Kapitel 4.1.1).

### 5.1.2 *Routingdaten*

Die Datenquellen für BGP-UPDATES, welche weltweite Informationen von BGP-Withdrawals enthalten, werden einerseits von der University of Oregon respektive dessen RouteViews Projekt [17], andererseits von RIPE NCC bzw. RIPEstat zur Verfügung gestellt [18]. RIPE NCC stellt zudem für die bei beiden Ereignissen gemachten BGP-Beobachtungen separate Webseiten mit Daten und Analysen parat [2] [3]. Die Kombination dieser beiden Datenbanken - RouteViews und RIPE NCC - ergibt die Grundlage der analysierten BGP-UPDATES (siehe [1], Kapitel 4.1.2).

### 5.1.3 *Nutzdaten*

Für die Aufzeichnung von IBR (siehe Unterkapitel 3.3.3) in den folgenden Beispielen wird auf die Daten vom UCSD Network Telscope des Internetverbunds CAIDA [19] (Cooperative Association for Internet Data Analysis) zurückgegriffen. Das davon beobachtete Darknet macht 1/256tel des gesamten IPv4-Adressraums aus (siehe [1], Kapitel 4.3). Dieser Adressraum mag sehr klein im Verhältnis zum gesamten Internetadressraum erscheinen. Es zeigt sich jedoch in den betrachteten IBR-Messungen, dass die Internetausfälle darin eindeutig sichtbar werden.

## 5.2 Revolution Ägypten

Die Revolution Ägyptens vollzog sich in den Anfangsmonaten des Jahres 2011. Sie wurde von großen Unruhen und Protesten im Land begleitet, welche vor allem über soziale Netzwerke wie Facebook organisiert wurden [20]. Infolgedessen ging die ägyptische Regierung massiv gegen die eigene Bevölkerung vor [21]: beinahe das ganze Land wurde am 27.01.2011 kurz vor Mitternacht vom Internet abgetrennt. Nur wenige wichtige Institute, wie z.B. die ägyptische Börse, blieben von außerhalb des Landes erreichbar. Dieses Ereignis ist von historischer Bedeutung, da es die erste beabsichtigte Abtrennung eines ganzen Landes vom Internet war [22].

### 5.2.1 *Analyse der Routingdaten*

Erste kleinere Anzeichen für den Verlust von IPv4-Internetrouten nach Ägypten, sprich BGP-Withdrawals, wurden ab 20:30 Uhr UTC von den BGP-Datenquellen aufgezeichnet (siehe Abbildung 4). Nach wenigen sehr kleinen Withdrawals wurden die meisten ägyptischen IPv4-Adressen auf einen Schlag zwischen 22:15 Uhr und 22:40 Uhr von außen unerreichbar. Die neueren - und standardmäßig von den meisten Nutzern nicht verwendeten - IPv6-Adressen waren jedoch davon unberührt und blieben damit während des gesamten Ausfalls online.

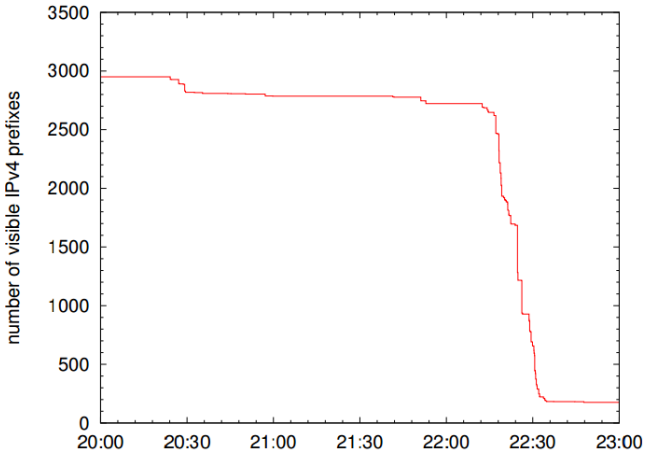


**Abbildung 4: Darstellung der BGP-Withdrawals im Zuge der Internettrennung von Ägypten am 27.1.2011** [1]


doi: 10.2312/NET-2013-02-1_01

Der Internetausfall hielt an bis zum 2.2.2011 am Morgen (siehe Abbildung 5). Die ersten vorher getrennten IPv4-Adressen waren ab 9:30 Uhr wieder verfügbar. Um 10:00 Uhr war fast das ganze Land wieder online, bis um 11:45 Uhr wurde die ursprüngliche Konnektivität vollständig wiederhergestellt.
Anhang der Abnahme der erreichbaren IPv4-Adressen lässt sich feststellen, dass das Offline- und Onlineschalten Ägyptens nicht viel Zeit beanspruchte und jeweils innerhalb einer halben Stunde fast vollständig vollzogen wurde.

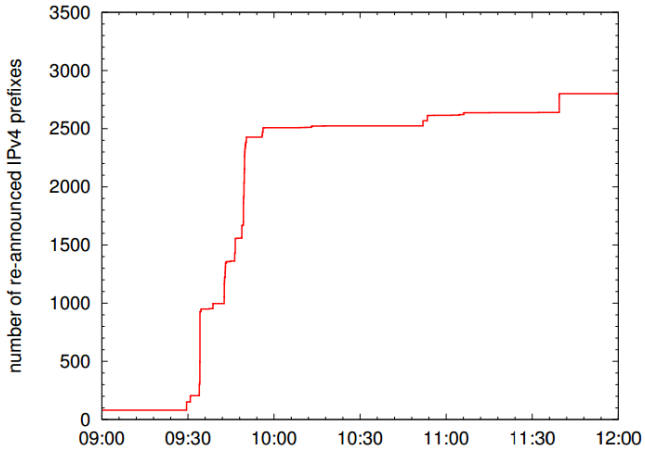


**Abbildung 5: Darstellung der BGP-Announcements der Internettrennung in Ägypten am 2.2.2011 [1]**

### 5.2.2 *Analyse der Nutzdaten*

Es wurde bereits in Unterkapitel 3.3.3 erklärt, inwieweit plötzliche Schwankungen in den Nutzdaten, genauer gesagt in der IBR, aus beobachteten IP-Adressbereichen auf BGP-Withdrawals hinweisen. Abbildung 6 ist ein Diagramm, welches die von CAIDAs Network Telescope gemessene IBR aus Ägyptens IP-Adressräumen über die Zeit des Internetausfalls hinweg kontinuierlich darstellt.

Bei dessen Betrachtung fallen die sinus-artigen Datenverkehrsschwankungen auf, die auf wechselhafte Benutzung des Internets bei Tag und bei Nacht hinweisen. Darüberhinaus ist ein deutliches Abnehmen der IBR offensichtlich, beginnend kurz vor dem 28.1.2011 und anhaltend bis zum 2.2.2011. Diese Zeitspanne entspricht der in den vorigen BGP-Veränderungen beschriebenen Offlinezeit Ägyptens. Somit ist dies ein deutlicher Hinweis dafür, dass IBR-Messungen in Darknets via Network Telescopes Aufschluss über Internetausfälle geben können. Dies ist im Gegensatz zur Messung der BGP-Routingdaten eine in diesem Maßstab erstmals gemachte Beobachtung, was als besondere Leistung des Papers "Analysis of Country-wide Internet Outages Caused by Censorship" [1] hervorzuheben ist. Das verdeutlicht, wie viel IBR aus einem relativ kleinem Adressraum ins gesamte Internet verteilt wird. Eine sehr kleine Teilmenge - rund 1/256tel, die Größe des überwachten Darknets - dieser extrem gestreuten Daten reicht vollkommen aus, um stichhaltige Aussagen über Interneterschütterungen weltweit machen zu können. Besonders interessant ist hierbei die Differenzierung der Datensorten, aus welchen die IBR besteht.

Wie aus Abbildung 7 hervorgeht, kommt die IBR während des Internetausfalls ausschließlich von mit dem Conficker-

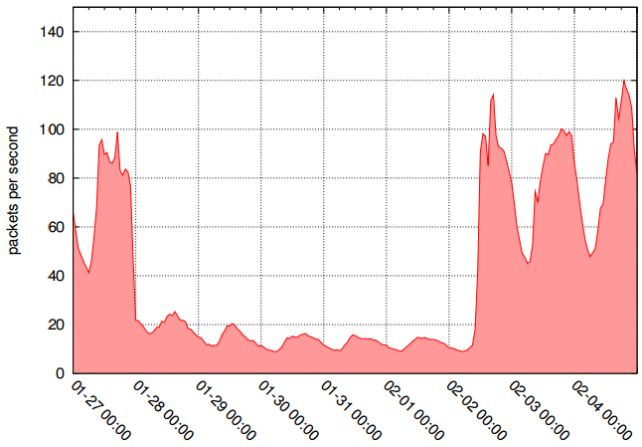


**Abbildung 6: Die während der Internettrennung aufgezeichnete IBR aus Ägypten [1]**

Wurm infizierten Rechnern, welche nicht durch die Regierung vom Internet getrennt wurden. Hier wird einem besonders stark vor Augen geführt, wie groß die Datenbelastung fürs Internet durch den Conficker-Wurm ist. Sogar ein kleiner Bruchteil des ägyptischen Internets ist so stark mit dem Wurm durchsetzt, dass dieser global aus verhältnismäßig kleinen Darknets heraus messbar ist.
Der Backscatter-Traffic befindet sich fast ununterbrochen auf 0-Niveau mit kurzen, aber sehr ausschlagenden Ausnahmen vom 2. bis 4.2.2011. Dies weist auf DoS-Attacken hin, die während der ägyptischen Revolution gegen das Regime ausgeführt wurden. Diese Attacken stehen in Zusammenhang mit Ankündigungen der Hackergruppe Anonymous, welche in einem kurz vorher veröffentlichten Brief derartige Attacken ankündigte [23].
Alle weiteren Internetdaten (subsumiert unter "other") sinken auf ein verhältnismäßig sehr kleines Niveau ab.

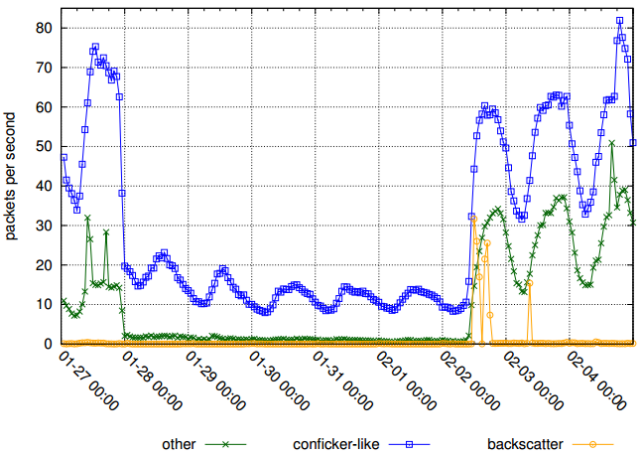


**Abbildung 7: Differenzierung der IBR nach Datenverkehr durch Conficker, Backscatter und anderen Ursachen [1]**


doi: 10.2312/NET-2013-02-1_01

## 5.3 Revolution Libyen

In Libyen begannen erste Proteste mit dem Aufkeimen der ägyptischen Revolution. Die Proteste steigerten sich zunehmends, bis sich am 16.2.2011 ein Bürgerkrieg zwischen der Regierung und oppositionellen Gruppen ankündigte [12]. In der Folge koppelte die Regierung am 18.2.2011 fast ganz Libyen über Nacht vom Internet ab. Dies wurde ein weiteres Mal in der darauf folgenden Nacht wiederholt. Darüberhinaus wurde fortan von erschwertem Zugang zu sozialen Medien wie Facebook und Twitter berichtet [12]. Am 2.3.2011 startete eine weitere Offensive der Regierung [24]. Infolgedessen kam es zu Luftangriffen gegen die Opposition und am 3.3.2011 zu einem weiteren Internetshutdown, der diesmal knapp 4 Tage anhielt. [1]

Im Beispiel von Libyen ist der zweite und der dritte Internetausfall von anderer technischer Natur als der aus Ägypten.

### 5.3.1 *Analyse der Routingdaten*

Da für den dritten Ausfall keine BGP-Routingdaten angefallen sind, werden nur die ersten beiden anhand der BGP-Withdrawals in Abbildung 8 dargestellt. Diese sind in der Abbildung differenziert nach den ASs, in welchen IP-Adressen zurückgezogen wurden. Für die Analysen in dieser Arbeit wird nur das landesweit grösste AS (LyStateAS) betrachtet.

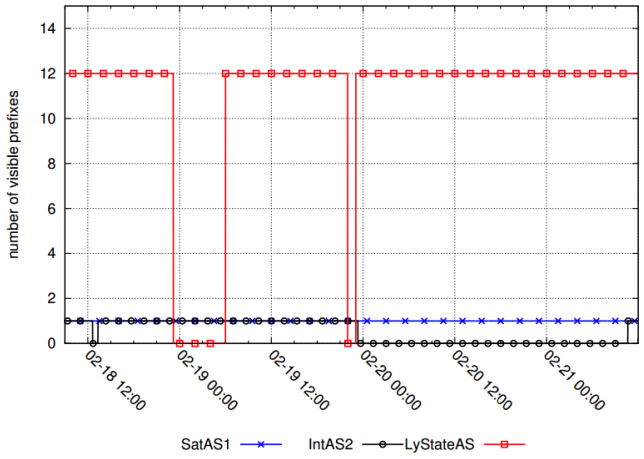


**Abbildung 8: BGP-Withdrawals vom 18. und 19.2.2011, differenziert nach drei libyschen ASs. SatAS1 versorgt Libyen via Satellit mit Internet.** [1]

Ersichtlich sind die Ausfälle, die jeweils am 18. und 19.2.2011 kurz vor Mitternacht beginnen, anhand der Anzahl der erreichbaren IPv4-Adressräume. Waren beim ersten die IP-Adressen ca. sechs Stunden entzogen, so war dies beim zweiten nur ungefähr eine Stunde der Fall. Die BGP-Withdrawals und -Announcements der IP-Adressräume passierten jeweils auf einen Schlag.

### 5.3.2 *Analyse der Nutzdaten*

Eine Analyse der vom Network Telescope gemessenen IBR (siehe Abbildung 9) des gleichen Zeitraums zeigt ein vollständigeres Bild.

Beide Ausfälle sind hier durch die beiden größeren Lücken im Datenverkehr zu erkennen. Während die hier betrachtete

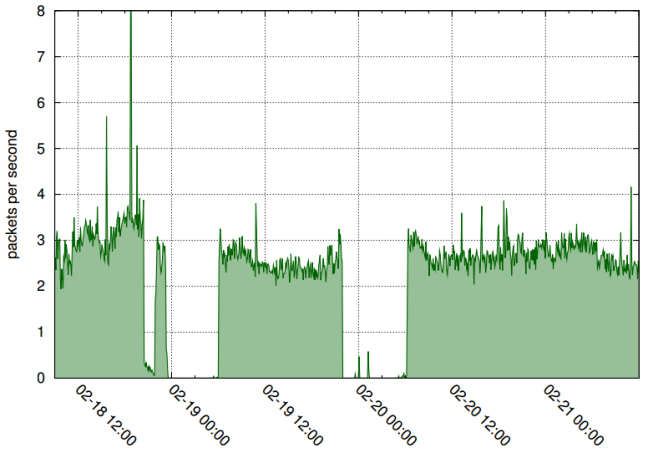


**Abbildung 9: IBR aus Libyen, aufgezeichnet vom 18. bis 21.2.2011. Die zwei großen Lücken spiegeln die zwei Internetausfälle wieder.** [1]

Dauer des ersten Ausfalls der aus Abbildung 8 entspricht, liegt die Sache beim zweiten anders.

Dessen Dauer beträgt in Abbildung 9 ca. 8 Stunden, was um ein Vielfaches länger ist, als es die vorher betrachteten BGP-Routingdaten in Abbildung 8 vermuten ließen. Zudem entspricht diese längere Zeitspanne der tatsächlichen Offlinezeit. Das bedeutet, dass eine weitere Zensurmaßnahme jenseits von BGP-Withdrawals zum Einsatz gekommen sein muss, wenn der Datenverkehr selbst nach dem Wiederherstellen der BGP-Routen gleichermaßen reduziert blieb.

Dies weist auf den Einsatz eines Paketfilters (siehe dafür Kapitel 4) hin, welcher kurz nach dem Entzug der BGP-Routen installiert und aktiviert worden ist. Er kommt an der Stelle zur Geltung, wo die BGP-Routen wiederhergestellt werden - Abbildung 8, 20.2. kurz vor 00:00 Uhr - und ist fortan für den Internetausfall - wie in Abbildung 9 ab 00:00 Uhr ersichtlich - verantwortlich. Was seine Funktionsweise angeht, so verwirft er alle ein- und ausgehenden Pakete. Die Folge ist, dass die Endnutzer, welche normalerweise über den entsprechenden Router online gehen, über diesen keine Pakete ins Internet verschicken oder von dort empfangen können. Der Effekt ist für den Endnutzer nicht ohne Weiteres von einem BGP-Withdrawal zu unterscheiden. Nur in den hier abgebildeten Messungen ist der Unterschied durch den Vergleich der BGP-Routingdaten mit der IBR sichtbar.

### 5.3.3 *Anmerkungen*

Es sei der Vollständigkeit halber auf zwei Details verwiesen:

- Die mediale Berichterstattung erwähnte schon vor den Internetabschaltungen einen erschwerten Zugriff auf soziale Netzwerke [12]. Dies ist ein Hinweis auf weitere Paketfilter, die bereits vorher zum Einsatz kamen und deren Filterregeln entsprechende Webseiten blockierten.
- Beim dritten Internetausfall Libyens kommt annähernd derselbe Paketfilter wie beim zweiten zum Einsatz, BGP-Withdrawals finden dort allerdings nicht statt. Für Details wird auf das Referenzpaper verwiesen (siehe [1], Kapitel 5.2).


doi: 10.2312/NET-2013-02-1_01

## 6 Schluss

Es wurden im Zusammenhang mit Zensur zwei Internetausfallarten sowie Methoden zu deren Beobachtung beschrieben. Dabei wurde gezeigt, dass sich Ausfälle, die BGP-Withdrawals zur Folge haben, von Ausfällen, die durch Paketfiltermechanismen zustande kommen, unterscheiden. Erstere kommen einem Abtrennen des Internetkabels an BGP-Routern gleich und sind global durch Änderungen in den BGP-Routingtabellen zu beobachten. Beide hingegen können von Network Telescopes bemerkt werden, da die IBR in Darknets durch beide Ausfallarten sichtbar abnimmt. Dem Conficker-Wurm, der ein erhebliches Datenvolumen im Internet verursacht, kommt hierbei eine besondere Bedeutung zu. Durch die unterschiedlichen Messergebnisse auf der BGP-Steuerungsebene ist es möglich beide Ausfallarten voneinander zu unterscheiden.
Darüberhinaus hat das Beispiel Libyens gezeigt, dass mit zunehmender Erfahrung der Zensoren Paketfilter bevorzugt eingesetzt werden. Dies ist auf die Filterregeln zurückzuführen, welche eine feinere Anpassung der Zensur und des Ausfalls ermöglichen. In die Zukunft projiziert bedeutet dies, dass bei derartigen Ereignissen keine BGP-Withdrawals mehr zu erwarten sind und die Beobachtung derartiger Online-Erschütterungen über Network Telescopes erfolgen müssen, wie dies im Referenzpapier das erste Mal in der Form durchgeführt wurde [1].

## Literatur


[1] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, A. Pescapé, "Analysis of Country-wide Internet Outages Caused by Censorship", ACM

[2] RIPEstat - Egyptian Internet Outage. https://stat.ripe.net/events/egypt. Abgerufen am 24.9.2012

[3] Unsolicited Internet Traffic from Lybia - RIPE Labs. https://labs.ripe.net/Members/emileaben/unsolicited-internet-traffic-from-libya. Abgerufen am 24.9.2012

[4] RFC 1930 - Guidelines for creation, selection, and registration of an Autonomous System (AS). IETF. Network Working Group. March 1996. http://tools.ietf.org/html/rfc1930. Abgerufen am 29.10.2012

[5] RFC 1771 - A Border Gateway Protocol 4 (BGP–4). IETF. Network Working Group. March 1995. http://tools.ietf.org/html/rfc1771. Abgerufen am 29.10.2012

[6] IANA - Autonomous System (AS) Numbers. http://www.iana.org/assignments/as-numbers/as-numbers.xml. Abgerufen am 29.10.2012

[7] IANA - Number Resources. http://www.iana.org/numbers. Abgerufen am 29.10.2012

[8] RFC 4271 - A Border Gateway Protocol. IETF. Network Working Group. January 2006. http://tools.ietf.org/html/rfc4271. Abgerufen am 29.10.2012

[9] RFC 3746 - Forwarding and Control Element Separation (ForCES) Framework. IETF. Network Working Group. April 2004. ftp://ftp.rfc-editor.org/in-notes/rfc3746.txt. Abgerufen am 29.10.2012

[10] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, L. Peterson. Characteristics of Internet background radiation. In Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, IMC '04, Seiten 27–40, New York, NY, USA, 2004. ACM.

[11] Internet Denial-of-Service Considerations. IETF. Network Working Group. November 2006. http://tools.ietf.org/html/rfc4732. Abgerufen am 29.10.2012

[12] Aufstände in Arabien - Gaddafi kappt Facebook und Twitter. 19.02.2011. rom/dpa/Reuters/dapd. http://www.spiegel.de/politik/ausland/aufstaende-in-arabien-gaddafi-kappt-facebook-und-twitter-a-746597.html. Abgerufen am 24.9.2012

[13] Network Layer Firewall. WanRedundancy.org. http://www.wanredundancy.org/resources/firewall/network-layer-firewall. Abgerufen am 24.9.2012

[14] Bericht: Computer sollen in China nur noch mit Filtersoftware verkauft werden. Andreas Wilkens. 08.06.2009. heise online. http://www.heise.de/newsticker/meldung/Bericht-Computer-sollen-in-China-nur-noch-mit-Filtersoftware-verkauft-werden-179181.html. Abgerufen am 24.9.2012

[15] AfriNIC (Regional Internet Registry für Afrika). http://www.afrinic.net/en/services/whois-query. Abgerufen am 24.9.2012

[16] MaxMind. MaxMind GeoLite Country: Open Source IP Address to Country Database. http://www.maxmind.com/app/geolitecountry. Abgerufen am 24.9.2012

[17] University of Oregon. University of Oregon Route Views project. http://www.routeviews.org. Abgerufen am 24.9.2012

[18] RIPE NCC: Routing Information Service (RIS). http://www.ripe.net/data-tools/stats/ris/routing-information-service. Abgerufen am 24.9.2012

[19] UCSD Network Telescope http://www.caida.org/projects/network_telescope/. Abgerufen am 24.9.2012

[20] Lena Jakat. Sueddeutsche.de - 31.01.2011 - Krise in Ägypten - Die Kinder des 6. April und der Tag der Entscheidung. http://www.sueddeutsche.de/politik/krise-in-aegypten-die-kinder-des-april-rufen-zum-protest-1.1053426. Abgerufen am 24.9.2012

[21] Sueddeutsche.de - 28.01.2011. http://www.sueddeutsche.de/politik/massenproteste-in-aegypten-angekuendigt-tag-des-zorns-beginnt-mit-festnahmen-1.1052282. Abgerufen am 24.9.2012

[22] Ägypten ist offline und ohne Mobilfunk [4. Update]. heise online. 28.01.2011. http://www.heise.de/newsticker/meldung/Aegypten-ist-offline-und-ohne-Mobilfunk-4-Update-1179102.html. Abgerufen am 24.9.2012

[23] OPERATION EGYPT - ANONYMOUS PRESSE-MITTEILUNG. AnonNews.org. 26.01.2011. 27.01.2011. http://anonnews.org/?p=press&a=item&i=299. Abgerufen am 24.9.2012




doi: 10.2312/NET-2013-02-1_01

[24] Libyan Islamists seize arms, take hostages. 2012 AFP. 21.02.2011. http://news.smh.com.au/breaking-news-world/libyan-islamists-seize-arms-take-hostages-20110221-1b19c.html. Abgerufen am 24.9.2012


doi: 10.2312/NET-2013-02-1_01