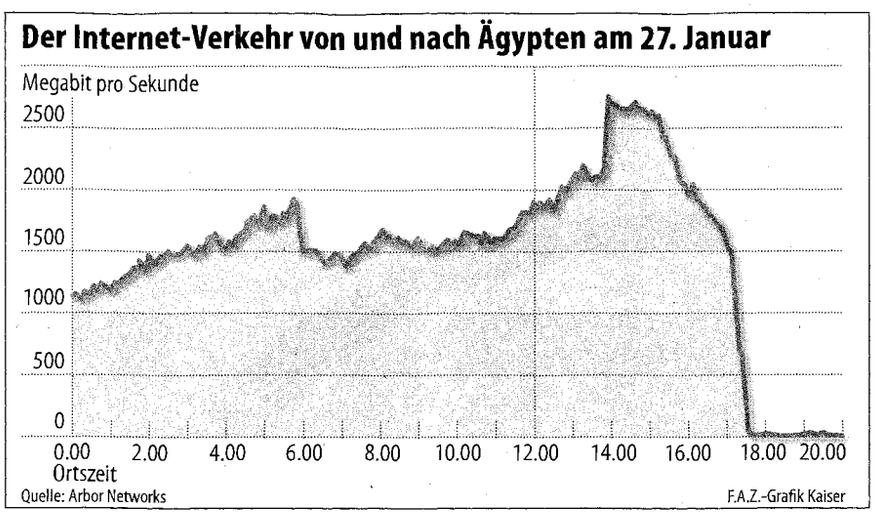
Faz, 8.2.2011

Wie Ägypten das Internet gezielt abschaltete

Mubaraks Cybertruppe kombiniert Filtersysteme mit Routing-Störung. Die Technik der Abschaltung hat die amerikanische Armee entwickelt.

Von Peter Welchering



Dann ging alles Schlag auf Schlag: *Am 27. Januar wurden 3200 Routen des ägyptischen Internets lahmgelegt, nur 300 blieben offen, wie diese Grafik zeigt.*

Tagelang waren die von Oppositionellen genutzten Server und Maildienste in Ägypten nicht erreichbar. Auch über Facebook, Twitter & Co. konnten die meisten Ägypter nicht mit Freunden und Bekannten im Ausland kommunizieren und sich auch nicht zu Demonstrationen verabreden. Die mit massiver Unterstützung der Vereinigten Staaten aufgebaute Cybertruppe des ägyptischen Präsidenten hat in technischer Hinsicht ganze Arbeit geleistet: Die Internetkommunikation der Opposition war abgeschaltet. Doch Regierungsserver, Kommunikationsverbindungen des staatlichen Fernsehens und die über Alexandria laufenden Transitdatenleitungen von Europa nach Asien waren von der Netzblockade ausgenommen.

Zunächst hatte die ägyptische Regierung noch mit einer ganz klassischen Methode versucht, soziale Netzwerke und Mailserver der Opposition zu blockieren: Sie sperrte die Weiterleitung über die Datenbanken mit den Internetprotokolladressen. Jeder Web-Server im Internet hat neben dem Server- oder Domain-Namen (etwa faz.net) auch eine IP-Adresse (für FAZ.net 193.227.146.10). Erst durch diese eindeutige IP-Adresse wird ein Server identifiziert.

Vom Domain Name System zur Netzsperre

Die Datenbanken des Domain Name System stellen nun eine logische Verbindung zwischen dem Domain-Namen und dieser IP-Adresse her. Bei einer Netzsperre wird diese Verbindung verhindert. Würde also zum Beispiel die Domain faz.net mit einer Netzsperre belegt, würde damit unterbunden, dass in der Datenbank des Domain Name System vom Domain-Namen faz.net auf die IP-Adresse 193.227.146.10 verwiesen wird. Der Server wäre über eine Anfrage an das Domain Name System nicht auffindbar. Allerdings kann solch ein Server mit Netzsperre direkt durch die Eingabe der IP-Adresse mit dem Browser aufgerufen werden. Und das haben die ägyptischen Oppositionellen auch gemacht, um diese von der Regierung verhängte Netzsperre zu umgehen.

Das aus Geheimdienstlern und Militärangehörigen bestehende Cyberteam der ägyptischen Regierung hatte sehr schnell erkannt, dass die verhängten Netzsperren großräumig umgangen wurden. Deshalb griff es zu einem bisher noch nicht eingesetzten Blockademittel, das die Cybertruppe der amerikanischen Armee vor zwölf Monaten entwickelt hatte: sogenannte Routenabschaltungen.

Die Netze der einzelnen Internetprovider tauschen ihre Daten über das sogenannte Border Gateway Protocol aus, eine Art globales Navigationssystem für das Internet. Dieses Routenprotokoll legt fest, wie die Daten von einem Provider-Netzwerk zum nächsten weitergereicht werden, bis sie ihren Empfänger erreicht haben. Die amerikanischen Spezialisten hatten nun vor einem Jahr ein halbes Dutzend unterschiedlicher Befehlssätze entwickelt, mit denen man die für die Weiterleitung von Daten über das Border Gateway Protocol (BGP) notwendigen Transport- und Routeninformationen löschen kann.

Ursprünglich sollten mit diesen BGP-Befehlssätzen während der Cyberwar-Übung des amerikanischen Heimatschutzministeriums im vergangenen Herbst einzelne Netzwerkrouten zwischen Providern in Kalifornien zu Testzwecken blockiert werden. Das an der Stabsrahmenübung beteiligte Computernotfallteam des Staates Kalifornien hatte jedoch Bedenken, dass eine solche Routenblockade außer Kontrolle geraten könnte. Deshalb wurden die BGP-Blockade-Befehlssätze während der Übung nicht eingesetzt.

Das Cyberteam der ägyptischen Regierung hat diese Befehlssätze genutzt, um die Weiterleitung von Daten zwischen den fünf ägyptischen Internetprovidern teilweise zu blockieren. Link Egypt, Vodafone, Telecom Egypt, Etisalat Misr und Noor Data Networks betrieben zirka 3500 dieser sogenannten BGP-Routen. Bei einem Großteil sind die Routeninformationen für den Datentransport in der Nacht vom 27. zum 28. Januar gelöscht worden. Betroffen waren nach inoffiziellen Schätzungen des amerikanischen Cybercommand etwa 3200 dieser Routen, nur 300 fest definierte blieben offen.

Damit erreichte Mubaraks Cybertruppe, dass sämtliche Regierungsserver, die Systeme der Börse und Banken und alle Knotenrechner für den Datentransit von Europa nach Asien uneingeschränkt arbeiten konnten, die Server von Facebook, Twitter und anderen sozialen Netzwerken aber genauso blockiert waren wie von oppositionellen Kreisen genutzte Mail- und Web-Server, auf denen Blogs bekannter Mubarak-Kritiker gehostet wurden.

In der Nacht zum 30. Januar gelang es ägyptischen Oppositionellen allerdings, E-Mails, Blog-Beiträge und kurze Handy-Videos über die noch verbliebenen Routen über soziale Netzwerke zu verbreiten. Die in Alexandria stationierte Cybertruppe wollte die noch offenen BGP-Routen deshalb auch noch sperren. Bei den Vorbereitungsarbeiten dafür stellte sich allerdings heraus, dass eine solche Totalblockade dann auch auf die Vermittlungsrechner des europäisch-asiatischen Kabelsystems übergreifen könnte, das auch gern als „digitaler Suezkanal" bezeichnet wird (F.A.Z. vom 31. Januar). Dieses System gilt als das Rückgrat des Internets zwischen Europa und Asien. Insgesamt sind unter Wasser rund 20 000 Kilometer Glasfaser verlegt, die von Marseille durchs Mittelmeer nach Alexandria führen, von dort weiter über Dubai bis nach Singapur. Ohne diese Internetverbindung über Alexandria nach Asien würde in der Buchhaltung von nicht wenigen deutschen Konzernen nicht mehr viel laufen.

Zahlreiche Kontierungen, Rechnungen und Zahlungsanweisungen werden nämlich von Dienstleistern in asiatischen Staaten, vornehmlich Indien, ausgeführt. Auch große Teile der von indischen Softwareentwicklern nach Europa gelieferten Computerprogramme werden über diesen digitalen Suezkanal befördert. Und nicht zuletzt die grafische Industrie in Deutschland ist von dieser Datenverbindung extrem abhängig, denn ein großer Teil der Bildbearbeitung für Prospekte, Kataloge und Werbeanzeigen findet in Asiens Großstädten statt.

Würde diese Datenautobahn von Europa nach Asien durch eine Totalblockade aller Netzwerkrouten in Ägypten gestört, wären internationale Proteste garantiert. Das wollte die Regierung Mubarak auf jeden Fall vermeiden. Gleichwohl wollte sie auch nicht hinnehmen, dass über die noch verbliebenen Netzwerkrouten Informationen ins Ausland gelangten. Deshalb wurde die Routenblockade am letzten Januarwochenende noch durch eine automatische Analyse der Datenpäckchen ergänzt.

Internationale Proteste wollte man vermeiden

Inzwischen hatte Mubaraks Cybertruppe nämlich einen recht genauen Überblick, an welche IP-Adressen Oppositionelle ihre Informationen schickten. Datenpäckchen mit dieser Zieladresse werden seitdem ausgefiltert. Das funktioniert allerdings nicht lückenlos. Denn einige soziale Netzwerke und Kurznachrichtendienste wie Twitter arbeiten mit unterschiedlichen IP-Adressen, die noch nicht alle vom ägyptischen Filtersystem erfasst sind. Außerdem haben Exil-Ägypter in Europa für einige Nachrichtenrouten sogenannte Sammelserver eingerichtet, die mit temporären IP-Adressen arbeiten, die ständig wechseln. Wohl auch deshalb konnte über den Kurznachrichtendienst Twitter ohne weitreichende Unterbrechungen aus Ägypten berichtet werden.