

Äthiopien: Telefon- und Internetüberwachung beschneidet Rechte

Äthiopien: Telefon- und Internetüberwachung beschneidet Rechte
Mit ausländischer Technologie wird Opposition in In- und Ausland bespitzelt
Äthiopiens Regierung verwendet ausländische Technologie, um die Verwendung von Telefonen und des Internets durch oppositionelle Aktivisten und Journalisten im In- und Ausland umfassend zu überwachen, so Human Rights Watch in einem heute veröffentlichten Bericht. In dem 100-seitigen Bericht "They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia" wird detailliert dargelegt, welche Technologie Äthiopiens Regierung in mehreren Ländern erworben hat und dazu nutzt, die Überwachung vermeintlicher Oppositionspolitiker im eigenen Land und im Ausland zu erleichtern. Mit ihren Überwachungspraktiken verstößt die Regierung gegen das Recht auf freie Meinungsäußerung, Vereinigungsfreiheit und Informationsfreiheit. Durch den staatlichen Telekommunikationskonzern Ethio Telecom kontrolliert die Regierung sämtliche Mobilfunk- und Internetdienstleistungen des Landes, was eine missbräuchliche Überwachung erleichtert.
"Äthiopiens Regierung nutzt ihre Kontrolle über das Telekommunikationssystem dazu, abweichende Stimmen mundtot zu machen", so Arvind Ganesan, Direktor der Abteilung Wirtschaft und Menschenrechte von Human Rights Watch. "Die ausländischen Firmen, deren Produkte und Dienstleistungen Äthiopiens illegale Überwachungsaktivitäten erleichtern, laufen Gefahr, sich zu Komplizen bei Menschenrechtsverstößen zu machen." Für den Bericht wurden zwischen September 2012 und Februar 2014 in Äthiopien und zehn weiteren Ländern über 100 Gespräche mit Missbrauchsopfern und ehemaligen Nachrichtendienstmitarbeitern geführt. Weil der Staat das Monopol über das gesamte Telekommunikationssystem hält, können Äthiopiens Nachrichtendienste praktisch unbegrenzt auf die Anruferdaten aller Telefonnutzer des Landes zugreifen. Ohne den Rechtsweg einzuschlagen oder sich Kontrollen zu unterwerfen, zeichnen die Dienste regelmäßig und problemlos Telefonate auf. Die Aufzeichnungen von Telefonaten mit Familienangehörigen und Freunden - speziell solcher mit ausländischen Telefonnummern - werden häufig bei entwürdigenden Befragungen eingesetzt. Willkürlich Verhafteten wird dort vorgeworfen, verbotenen Organisationen anzugehören. Während friedlicher Proteste wurden Mobilfunknetze abgeschaltet, die Standorte von Demonstranten wurden mithilfe von Informationen aus ihren Mobiltelefonen bestimmt.
"Sie haben mich verhaftet und mir alles gezeigt", sagte ein ehemaliges Oppositionsmitglied Human Rights Watch. "Sie hatten eine Liste mit all meinen Telefonaten, und sie spielten mir ein Gespräch vor, das ich mit meinem Bruder geführt hatte. Sie haben mich verhaftet, weil wir am Telefon über Politik gesprochen hatten. Es war mein allererstes Telefon und ich dachte, ich könnte endlich frei reden." Die Regierung hat den Zugang zu Informationen eingeschränkt, indem sie Websites blockierte, die politische Ereignisse in Äthiopien unabhängig oder kritisch analysieren. 2013 führten Human Rights Watch und Citizen Lab, ein auf Internetsicherheit und Menschenrechte spezialisiertes Forschungszentrum der Universität Toronto, in Äthiopien einen Feldversuch durch. Dabei stellte sich heraus, dass Äthiopien weiterhin die Websites von Oppositionsgruppen, Medienunternehmen und Bloggern blockiert. In einem Land, in dem unabhängige Medien nur eine sehr geringe Rolle spielen, ist der Zugang zu derartigen Informationen von besonderer Wichtigkeit. Bei der Überwachung der Mobilfunkkanäle haben Äthiopiens Behörden wiederholt die ethnische Gruppe der Oromo ins Visier genommen. Mithilfe aufgezeichneter Telefongespräche wurden Inhaftierte zu dem Geständnis gezwungen, Mitglied verbotener Gruppen zu sein, etwa der Oromo-Befreiungsfront, die mehr Autonomie für die Oromo anstrebt. Inhaftierte mussten Informationen über Mitglieder dieser Gruppen preisgeben. Bei Gerichtsverfahren auf Grundlage des äußerst problematischen Gesetzes zur Terrorismusbekämpfung wurden abgefangene E-Mails und Telefonate als Beweis vorgelegt, ohne dass davor eine richterliche Genehmigung eingeholt worden war. Darüber hinaus haben die Behörden Personen inhaftiert und befragt, die von ausländischen, möglicherweise nicht in den Ethio-Telecom-Datenbanken enthaltenen Nummern angerufen wurden. Das hat dazu geführt, dass speziell auf dem Land viele Äthiopier Angst haben, Anrufe ins Ausland zu führen oder von dort zu erhalten. Da viele Äthiopier im Ausland arbeiten, stellt dies ein sehr ernstes Problem dar. Die Technologie, die Äthiopien zur Überwachung des Telekommunikationsverkehrs einsetzt, stammt größtenteils von dem chinesischen Telekommunikationsausrüster ZTE, der mindestens seit dem Jahr 2000 in dem Land aktiv ist und von 2006 bis 2009 den Staat exklusiv belieferte. ZTE ist eine Größe in der afrikanischen wie auch der globalen Telekommunikationsbranche und spielt auch beim Ausbau des jungen äthiopischen Telekommunikationsnetzes eine zentrale Rolle. Auf Anfragen von Human Rights Watch, ob man etwas unternehme, um in Äthiopien Menschenrechtsverstöße durch unrechtmäßige Mobilfunküberwachung zu thematisieren und zu verhindern, hat ZTE nicht reagiert. Auch mehrere europäische Unternehmen haben Äthiopien mit moderner Überwachungstechnologie beliefert, die dazu verwendet wurde, im Ausland lebende Äthiopier ins Visier zu nehmen. Offenbar hat Äthiopien FinFisher erworben, eine Software des britisch-deutschen Unternehmens Gamma International, sowie Remote Control System des italienischen Anbieters Hacking Team. Mit diesen Programmen verschaffen sich Nachrichten- und Geheimdienste Zugang zu Daten, Informationen und Aktivitäten auf den befallenen Rechnern. Die Software kann Tastatureingaben und Passwörter aufzeichnen und ferngesteuert Webcam und Mikrofon einschalten, so dass der Computer praktisch zum Abhörgerät umfunktioniert wird. Von Äthiopiern, die in Großbritannien, den USA, Norwegen und der Schweiz leben, ist bekannt, dass ihre Rechner mit dieser Software infiziert wurden; in den USA und Großbritannien gab es deswegen Klagen wegen unerlaubten Abhörens. Ein per Skype geführtes Gespräch, das von infizierten Rechner eines Äthiopiers stammt, ist auf regierungsfreundlichen Websites aufgetaucht. Gamma hat nicht auf Anfragen von Human Rights Watch reagiert, ob man ernsthaft Maßnahmen ergriffen habe, damit diese Produkte nicht an Länder verkauft werden oder von ihnen genutzt werden, wenn deren Regierungen für Menschenrechtsverletzungen verantwortlich sind. Hacking Team hat gewisse Vorsichtsmaßnahmen ergriffen, die die missbräuchliche Nutzung seiner Produkte begrenzen soll, aber das Unternehmen hat nicht bestätigt, ob und in welcher Form diese Schritte beim Geschäft mit der äthiopischen Regierung zum Tragen kamen.
"Dass Äthiopien ausländische Technologie dazu nutzt, Mitglieder der Opposition im Ausland ins Visier zu nehmen, ist ein zutiefst beunruhigendes Beispiel für diesen weltweiten unregulierten Handel. Es entsteht die echte Gefahr von Missbrauch", sagte Ganesan. "Die Hersteller der Programme sollen unverzüglich Schritte gegen einen Missbrauch ihrer Produkte ergreifen. Dazu zählt auch die Prüfung, inwieweit diese Programme gegen im Ausland lebende Äthiopier zum Einsatz kamen und kommen und inwieweit bei der Nutzung in Äthiopien Menschenrechte berührt wurden." Solch wirkungsvolle Bespitzelungssoftware ist auf globaler Ebene praktisch völlig unreguliert, auf Landesebene gibt es nur unzureichende Kontrollen oder Ausfuhrbeschränkungen. 2013 legten Menschenrechtsgruppen Beschwerde bei der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ein. In der Beschwerde hieß es, Spyware-Technologie sei dazu genutzt worden, Aktivisten in Bahrain ins Visier zu nehmen. Citizen Lab hat Beweise dafür gefunden, dass diese Software in über 25 Ländern verwendet wurde. Der Schutz der Privatsphäre, Meinungsfreiheit, Informationsfreiheit und Vereinigungsfreiheit sind international geschützt und stehen auch in der Verfassung Äthiopiens. Doch gerichtliche und gesetzliche Mechanismen zum Schutz der Bürger vor unrechtmäßiger staatlicher Überwachung fehlen in Äthiopien oder werden ignoriert. Vertieft wird die Gefahr noch dadurch, dass in äthiopischen Strafanstalten Folter und andere Misshandlung politischer Gefangener weitverbreitet sind. Dass Äthiopien Überwachungstechnologie nicht noch umfassender einsetzt, könnte an fehlenden Kapazitäten und mangelndem Vertrauen innerhalb wichtiger Ministerien liegen, so Human Rights Watch. Mit zunehmenden Kapazitäten ist es jedoch durchaus möglich, dass die unrechtmäßige Überwachung von Mobilfunk- und E-Mail-Verkehr in Äthiopien noch deutlichere Formen annimmt. Viele Äthiopier haben das Gefühl, dass die Regierung alles überwacht. Das verschärft das Ausmaß der tatsächlichen Kontrolle und führt dazu, dass die Bürger sich in hohem Maße selbst zensieren und sich in Telekommunikationsnetzen zu vielen Themen gar nicht mehr offen äußern. Selbstzensur ist vor allem in den ländlichen Gebieten des Lands weit verbreitet, weil dort die Netzabdeckung und der Zugang zum Internet sehr stark eingeschränkt sind. Wichtigste Kontrollwerkzeuge der Regierung sind ein umfassendes Informantennetzwerk und gegenseitige Bespitzelung. Wie Human Rights Watch festgestellt hat, führt die Situation auf dem Land dazu, dass viele vom Land stammende Äthiopier Mobiltelefone und andere Telekommunikationstechnologie einfach als weiteres Instrument ansehen, das ihrer Überwachung dient. Äthiopiens Telekommunikationssystem wächst. Deshalb muss dringend Rechtsschutz gewährleistet sein und Mitarbeiter von Nachrichtendiensten dürfen nicht uneingeschränkt Zugriff auf die Privatkommunikation der Bürger haben", sagte Ganesan. "Bei der Einführung von Internet- und Mobilfunktechnologien sollte die Demokratie gefördert werden, es sollte die Verbreitung von Ideen und Meinungen und der Zugang zu Informationen erleichtert werden. Es darf jedoch nicht passieren, dass dadurch die Rechte der Menschen beschnitten werden."
Human Rights Watch Deutschland
Poststraße 4-5
10178 Berlin
Telefon: +49 (0)30 259306-0
Telefax: +49 (0)30 259306-29
Mail: berlin@hrw.org
URL: www.hrw.org/de

src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=560650" width="1" height="1">

Pressekontakt

Human Rights Watch Deutschland

10178 Berlin

hrw.org/de
berlin@hrw.org

Firmenkontakt

Human Rights Watch Deutschland

10178 Berlin

hrw.org/de
berlin@hrw.org

Weitere Informationen finden sich auf unserer Homepage