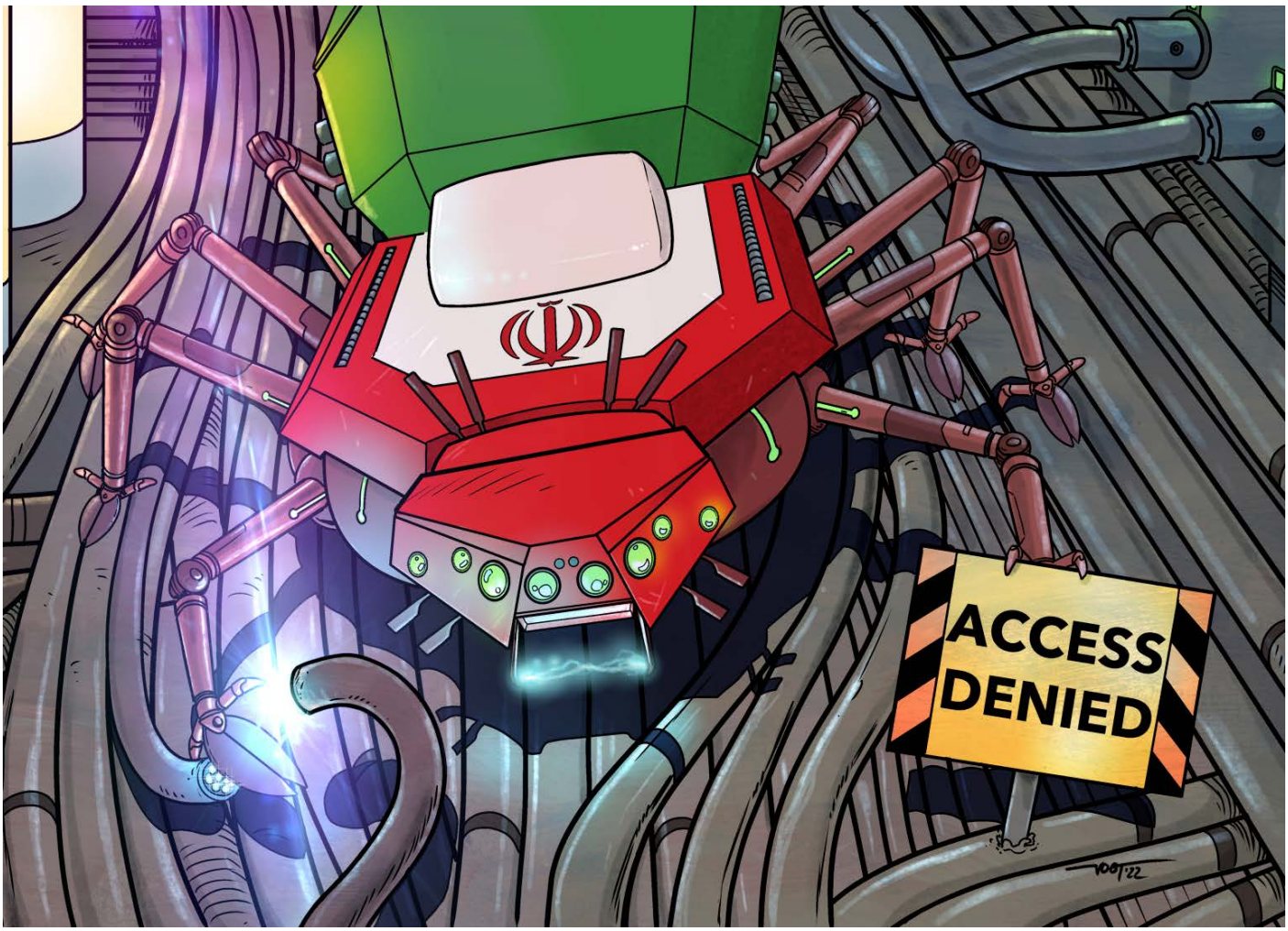


Bild: Michael Vogt

Im Überwachungsnetz

Wie das iranische Regime IT und Netzkontrolle gegen die Proteste nutzt

Nicht nur die IP-Infrastruktur und Mobilfunknetze, auch viele iranische IT-Firmen sind staatlich kompromittiert. Paradoxerweise halfen die US-Sanktionen dabei, Überwachungsstrukturen auszubauen. Diese nutzt der Staatsapparat nun, um die Proteste kleinzuhalten.

Von Marcus Michaelsen und Maryam Mirza

Nik Yousefi meldete Anfang Oktober in seinem bislang letzten Tweet: „Gestern haben sie meine Wohnung gestürmt." Kurz zuvor hatte der in Teheran lebende Filmemacher auf Instagram ein Video zur Unterstützung der landesweiten Proteste gegen die iranische Regierung veröffentlicht, das sich in den sozialen Medien rasant verbreitete. Dann war er untergetaucht, um einer drohenden Verhaftung zu entgehen. Nachdem die Beamten ihn nicht aufgefunden hatten, seien sie direkt zum Haus seiner Freunde gefahren, so Yousefi. An deren Adresse konnten sie nur über den Lieferdienst Snap Food gelangt sein, bei dem er einmal Essen dorthin bestellt habe.

Wenig später wurde Nik Yousefi aufgegriffen und sitzt seitdem im berüchtigten Evin-Gefängnis in der iranischen Hauptstadt Teheran ein. Und er ist längst nicht der einzige Dissident, dem Regime-Agenten mithilfe der Daten von Snap Food nachspürten. Seit mehr als drei Monaten unternimmt die iranische Regierung viel, um die Protestbewegung zu unterdrücken – und das Internet ist sowohl für die Protestierenden als auch für das Regime zu einem entscheidenden Werkzeug geworden.

Auslöser der Unruhen war der Tod der 22-jährigen Jina Mahsa Amini. Die junge Frau aus der kurdischen Provinzstadt Saqqez wurde am 13. September 2022 während einer Besuchsreise in Teheran von der Sittenpolizei festgenommen, weil ihr Kopftuch angeblich nicht korrekt saß. In der Haft hat man sie geschlagen. Sie starb drei Tage später an ihren Verletzungen.

Die Proteste gegen das brutale Vorgehen der Sittenpolizei und den offiziellen Kopftuchzwang erfassten schnell das ganze Land. Auf den Straßen entlädt sich bis heute eine lang aufgestaute Wut über staatliche Misswirtschaft, die Diktatur und die Stellung von Frauen in der Gesellschaft. Und die Regierung schlägt brutal zurück. Menschenrechtsorganisationen geben bislang fast 500 getötete Protestierende und über 18.000 Inhaftierte an (Stand Mitte Dezember 2022).

Die Start-ups und der Staat

Im Bestreben nach umfassender Kontrolle hat der Sicherheitsapparat selbst alltägliche Internetanwendungen im Visier. Gehackte E-Mails, die Aktivisten des Anonymous-Kollektivs im Oktober ins Netz stellten, zeigen, dass auch bekannte iranische Internetfirmen mit dem Regime kooperieren. Die Mails geben einen Einblick in die Korrespondenz der IT-Unternehmen mit der obersten Zensurbehörde des Landes.

Der frühere Start-up-Unternehmer Arash Zad ist von der Authentizität der Dokumente überzeugt. Ihm zufolge haben einige Firmen weitaus mehr als notwendig mit der Behörde kooperiert – um sich gut zu stellen oder um Konkurrenten zu schädigen. Der Betreiber eines Online-Bezahldienstes etwa habe die Zensoren auf eine Domain des Exilsenders Manoto TV aufmerksam gemacht, über die Iraner den Journalisten Fotos und Videos zukommen lassen konnten. „Das war eines der scheußlichsten Dinge, auf die ich in diesen Mails gestoßen bin“, erklärt Zad im Gespräch mit c’t.

Iranische Start-ups haben lange Jahre davon profitiert, dass es keine internationale Konkurrenz gab. Denn bereits seit 1979 existieren US-Sanktionen gegen Iran. Da sie großen Technologiekonzernen den Zugang zum iranischen Markt versperrten, entstanden viele lokale Klon-Produkte. Mit großem Erfolg ersetzt etwa Cafe Bazaar seit 2011 de facto den Play Store von Google. Als Kopie des Amazon-Konzepts dominiert Digikala den Onlinehandel.

Kurz währende Hoffnung

Das Atomabkommen von 2015 ließ Hoffnung auf eine Entspannung der Beziehungen Irans zu Europa und den USA aufkeimen. Nun interessierte sich auch das Ausland für diesen rapide wachsenden Markt. Im Juni 2015 sollte die iBRIDGE-Konferenz in Berlin aufstrebende iranische Talente mit internationalen Investoren zusammenbringen. So erwarb eine niederländische Firma Beteiligungen an Cafe Bazaar. Und auch die Berliner Rocket-Internet-Gruppe, die in Konzerne wie United Internet und Alibaba investiert ist, streckte ihre Fühler nach Iran aus.

Der Traum von einem Silicon Valley des Mittleren Ostens zerplatzte allerdings schnell. Im September 2015 setzten die Revolutionsgarden Arash Zad fest, der damals zu den Pionieren der iranischen Tech-Szene zählte. Nur wenige Stunden nach seiner Verhaftung wurden seine E-Mail-Konten für eine Phishing-Kampagne genutzt, die sich gegen iranische Techies im In- und Ausland richtete. Wegen „Kontakten zu regimefeindlichen Gruppen“ musste Arash Zad für mehr als zwei Jahre ins Gefängnis, davon verbrachte er fünf Monate in einer Einzelzelle. Das war ein klares Signal: Der iranische Sicherheitsapparat würde nicht tatenlos dabei zusehen, wie ein international vernetzter IT-Sektor aufblüht.

Im Januar 2020 ergriffen die Revolutionsgarden den recht bekannten Softwareingenieur Behdad Esfahbod, der in Kanada für Facebook arbeitete und seine Familie in Teheran besuchen wollte. In der Isolationshaft wollten sie ihn dazu zwingen, iranische Aktivisten im Ausland auszuspionieren, die daran arbeiteten, die iranische Internetzensur zu umgehen. Auch im Zuge der derzeitigen Proteste hat das Regime mehrere Tech-Experten verhaftet, darunter den prominenten Pro-

c't kompakt

- Die US-Sanktionen haben begünstigt, dass eine isolierte iranische IT-Infrastruktur entstand, die unter staatlicher Überwachung und Kontrolle steht.
- Das Regime kann sowohl Mobilfunknetze als auch internationale IP-Verbindungen nach Belieben blockieren – auch begrenzt auf einzelne Regionen in Iran.
- Twitter und VPNs spielen eine große Rolle, um die globale Aufmerksamkeit für die Proteste gegen das Regime aufrechtzuerhalten.

Bild: ibridges.org

Als die USA 2015 ihre Sanktionen gegen Iran lockerten, entstand auf Start-up-Konferenzen wie der iBRIDGE in Berlin die Hoffnung auf ein Silicon Valley im Mittleren Osten.

Bild: Arash Zad

Arash Zad, einst Pionier der iranischen Start-up-Szene, wurde von den Revolutionsgarden festgesetzt und landete für zwei Jahre im Gefängnis.

grammierer Amiremad Mirmirani, bekannt als Jadi. Er hatte in seinem Podcast die mittlerweile von der Europäischen Union sanktionierte iranische Firma Arvan Cloud für ihren Beitrag zur staatlichen Internetzensur kritisiert.

Um unter Irans autoritärem Regime zu bestehen, bleibe den Internetfirmen oft gar keine andere Wahl als zu kooperieren, erklärt Amin Sabeti, Gründer des Computer Emergency Response Team in Farsi (CERTFA). Dies ist eine Organisation, die sich auf erste Hilfe bei Cyberattacken staatsnaher Hacker spezialisiert hat. „Wenn ein Staatsanwalt wissen will, wer wann ein Taxi genommen hat oder die Revolutionsgarden bei denen im Büro stehen und Zugriff auf Nutzerdaten verlangen – bei wem wollen sie sich beschweren? Wie sollen sie Widerstand leisten?“

Die Betreiber der beliebten Navigationsapp Balad zogen Ende Oktober die Konsequenz. Unter den aktuellen Bedingungen sei es ihnen nicht mehr möglich, die Rechte ihrer Nutzer zu schützen, verkündeten sie auf Instagram. Deshalb wollten sie ihren Dienst in den nächsten Monaten einstellen, Mitarbeiter würden versetzt oder entlassen.

Werden iranische Internetnutzer nach den jüngsten Erkenntnissen zur staatlichen Überwachung ihr Verhalten ändern? Arash Zad ist skeptisch. „Vielleicht sind einige jetzt vorsichtiger bei der Nutzung dieser Apps, immerhin könnten ihre Freiheit oder ihr Leben auf dem Spiel stehen. Aber es ist auch ein Markt mit vielen Monopolen – für viele Dienstleistungen gibt es nur einen Anbieter. Die meisten Leute haben sich an diese bequemen Services gewöhnt.“

Nationales Internet

Wie nur wenige andere Länder greift Iran in die Netzarchitektur ein, um innerhalb seiner Landesgrenzen größtmögliche Kontrolle über Datentransfers und Kommunikation zu erlangen. Die Weichen für den Ausbau eines „nationalen Internet“ stellte das Regime nach den Protesten gegen die Manipulation der Präsidentschaftswahlen im Jahr 2009.

Schon damals mobilisierte sich eine Opposition über soziale Netzwerke und erzielte internationale Aufmerksamkeit. Westliche Medien betitelten die Demonstrationszüge in den iranischen Städten als „Twitter-Revolution“. Ein Jahr später, unter dem Eindruck der Aufstände des Arabischen Frühlings, beschrieb die damalige US-Außenministerin Hillary Clinton das Internet in einer viel beachteten Rede als Waffe im Kampf gegen Diktatoren. Sie versprach Unterstützung für Netzaktivisten auf der ganzen Welt.

Zugleich wurden die iranischen Atomanlagen zum Ziel eines der ersten internationalen Cyberangriffe gegen eine kritische Infrastruktur. Mit dem Schadprogramm Stuxnet wollten die USA und Israel die Nuklearanreicherung sabotieren. Für das Regime in Teheran wurde das Internet damit zu einem strategischen Schlachtfeld.

Das Ziel war klar: Man wollte ein Netz, das leicht zu überwachen und zugleich resilient gegenüber Angriffen von außen bleibt. Bis 2020 wurden die Anbindungen zum globalen Internet auf wenige Knotenpunkte reduziert. Experten gehen davon aus, dass inzwischen fast alle Verbindungen über die Telecommunication Infrastructure Company laufen, die direkt dem IT-Ministerium untersteht und zudem von Funktionären des Sicherheitsapparats beaufsichtigt wird. Parallel dazu hat der Staat die Zahl der Netzwerke im Land ausgebaut. Im Vergleich zu den Nachbarländern erreicht Iran eine hohe Konnektivität innerhalb seiner Landesgrenzen und will so dem nationalen Netz Stabilität geben.

Staatlich geförderte Anwendungen wie der Messenger Soroush und die Super-App Rubika sollen globale Plattformen ersetzen. Rubika ist über ein Geflecht staatsnaher Firmen mit einem durch die Revolutionsgarden kontrollierten Konsortium verbunden. Das chinesische Vorbild WeChat lässt grüßen. 2021 tauchten plötzlich auf Rubikas Instagram-Klon die Profile prominenter iranischer Sportler, Schauspieler und Influencer auf. Die Originalprofile waren zuvor ohne deren Wissen bei Instagram gelöscht worden.

Werkzeuge der Repression

Im November 2019 zeigte das Regime erstmals, dass es mittlerweile totale Kontrolle über die Infrastruktur hat. Aus Wut über die drastische Erhöhung der Benzinpreise gingen Menschen im ganzen Land auf die Straße. Die Proteste wendeten sich schnell gegen auch gegen die Regime-Elite hinter Revolutionsführer Ali Khamenei. Die Reaktion folgte prompt: Innerhalb eines Nachmittags schalteten alle großen Internetprovider ihre Netzwerke ab. Fünf

Bild: dpa

Trotz staatlicher Kommunikationsblockaden dauern die Proteste in Teheran und vielen anderen Städten des Landes an.

Tage lang war Iran von der Welt abgeschnitten. Für die in London ansässige Organisation Netblocks, die weltweit Internetsperren dokumentiert, war diese Blockade aufgrund des Ausmaßes und der technischen Komplexität der bislang schwerwiegendste Shutdown ihrer Messungen.

Erst als die Provider das Land allmählich wieder ans globale Netz anschlossen, traten die Zeugnisse der staatlichen Gewalt zutage. Amnesty International konnte auf Basis von Handyvideos und Fotos mehr als dreihundert Männer, Frauen und Kinder identifizieren, die während der Proteste von Regimekräften getötet wurden. Schätzungen zufolge liegt die tatsächliche Zahl aber bei bis zu 1500 Todesopfern.

Als im September 2022 die Proteste über den Tod von Jina Amini ausbrachen, hatte das Regime also bereits Erfahrungen gesammelt. Schnell ordnete der Nationale Sicherheitsrat die Blockade von WhatsApp und Instagram an, den letzten noch zugänglichen internationalen Plattformen. Selbst Onlinespiele mit Chat-Funktion wurden gesperrt, um Regimekritikern keine Nischen zu bieten. Ein landesweiter Shutdown aber blieb bislang aus, weil die Regierung wirtschaftliche Schäden fürchtet. Stattdessen arbeitet man mit zeitlich und regional begrenzten Sperrungen.

Ein vom Open Observatory of Network Interference (OONI) und Partnerorganisationen veröffentlichter Report dokumentiert für die ersten Wochen der Proteste „digitale Ausgangssperren“: Von Nachmittag bis Mitternacht unterbrachen die drei größten Mobilfunkanbieter ihre Dienste. Die Nutzer verloren die Verbindung zum mobilen Datenverkehr, der für viele Iraner der einzige Zugang zum Internet ist. Dies sollte die Kommunikation der Protestler auf den Straßen erschweren.

Das Regime nutzt Deep Packet Inspection, um VPN-Verbindungen in den Datenströmen zu erkennen und zu blocken. Auch drosselt es die Geschwindigkeit der Datenübertragung. Dadurch können Aktivisten kaum noch Fotos und Videos versenden. „Das ist wie ein Wasserhahn, aus dem nur noch ein paar Tropfen kommen. Man kann zwar behaupten, dass es einen Wasseranschluss gibt, aber in Wirklichkeit nützt der Hahn niemandem etwas“, umschreibt Amin Sabeti vom CERTFA diese Situation.

Am stärksten von der Zensur betroffen sind die Provinzen Kurdistan und Belutschistan, wo das Regime ungleich härter gegen die protestierende Bevölkerung vorgeht. Die von ethnischen und religiösen Minderheiten bewohnten Regionen werden seit jeher stark vom Staat diskriminiert. In den kurdischen Städten seien die Verbindungen oft tagelang unterbrochen, berichtet Kaveh Ghoreishi, ein kurdisch-iranischer Journalist, der in Berlin lebt: „Mitunter nutzen Aktivisten SIM-Karten aus den benachbarten kurdischen Provinzen im Irak, um die Internetzensur zu umgehen. Aber diese Verbindungen werden von der iranischen Regierung mit Störsendern unterbrochen.“

Das Onlinemagazin The Intercept berichtete im Oktober auf Basis geleakter Dokumente von einem Überwachungsprogramm, das der iranischen Regierung umfassende Kontrolle über den Mobilfunk gibt. Das System könne Verbindungen ausspähen, manipulieren und gezielt unterbrechen. Zudem erlaube es den Behörden, Nutzer aus den schnelleren 3G- und 4G-Netzen zu veralteten 2G-Verbindungen zu zwingen. Dort sind viele Funktionen heutiger Smartphones nicht nutzbar und Daten lassen sich leichter abschnorcheln.

Inwieweit Iran für dieses Programm Unterstützung aus dem Ausland erhalten hat, ist nach einer ersten Auswertung der Dokumente noch nicht klar. Kooperationen im IT-Bereich bestehen mit Russland und China. Vor allem China hilft mit Technologie und Know-how bei Internetzensur und digitaler Überwachung. Die chinesische Firma Tiandy hat Iran kürzlich ein Kamerasystem mit Gesichtserkennungssoftware verkauft, das die Aufgaben der Sittenpolizei bei der Durchsetzung der Kleidungsvorschriften übernehmen könnte.

Kampf um Aufmerksamkeit

Nach der bitteren Erfahrung vom November 2019 wissen iranische Aktivisten, wie wichtig es ist, das weltweite Interesse an ihrem Widerstand aufrechtzuerhalten.

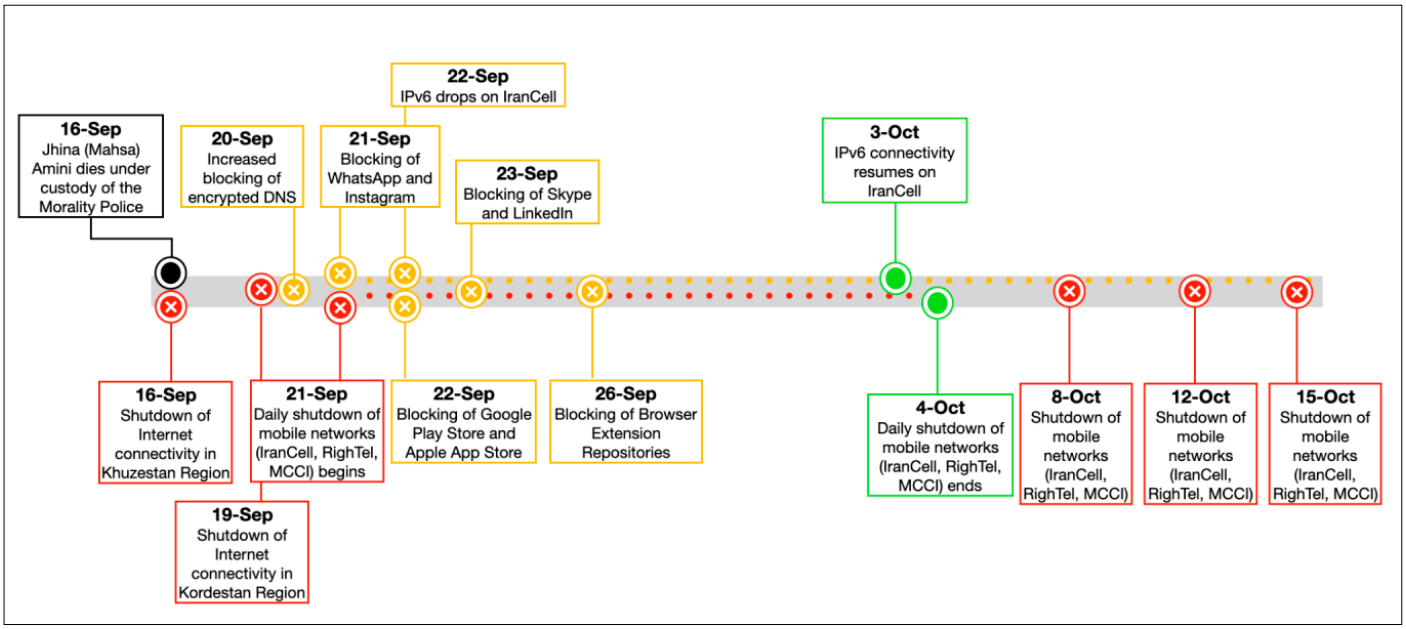
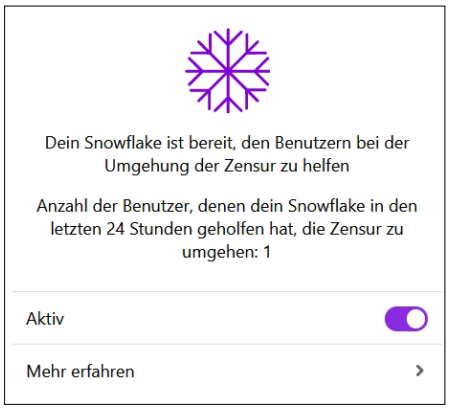


Bild: Open Observatory of Network Interference (OONI)

Das Open Observatory of Network Interference (OONI) hat staatliche Netzeingriffe in den ersten vier Wochen des Protests zusammengetragen.



Mit dem Browser-Add-on Snowflake stellt man einen Proxy ins Tor-Netz bereit und kann live verfolgen, ob er genutzt wird.

Gelingt es der Regierung, eine totale Kommunikationssperre durchzusetzen und den Kontakt zur internationalen Öffentlichkeit zu unterbrechen, können die Revolutionsgarden noch hemmungsloser gegen die Bevölkerung vorgehen. Unter hohem Risiko nehmen deshalb Aktivisten noch immer Videos auf und schicken sie außer Landes.

Die Übernahme von Twitter durch Elon Musk im Oktober traf die iranische Protestbewegung daher zum falschen Zeitpunkt. Über Twitter können Nachrichten aus Iran unmittelbar internationale Journalisten und Politiker erreichen. Nichtregierungsorganisationen nutzen das auf der Plattform verbreitete Videomaterial zur Dokumentation von Menschenrechtsvergehen. Während westliche Nutzer – auch viele Medienschaffende – in den ersten Tagen nach Musks Übernahme in Scharen zu alternativen Angeboten wie Mastodon wechselten, bleibt iranischen Journalisten und Aktivisten dieser Ausweg versperrt, wollen sie wertvolle Reichweite behalten.

Mahsa Alimardani von der britischen Nichtregierungsorganisation (NGO) Article 19 weist auf neue Sicherheitslücken hin, die durch den Verkauf von Twitter entstehen. Die für Menschenrechte und Sicherheit zuständigen Teams der Plattform hätten aufgrund jahrelanger Bemühungen von NGOs Erfahrung beim Umgang mit Nutzern aus autoritären Ländern gesammelt: „Wann immer eine Aktivistin verhaftet wurde, haben diese Teams schnell deren Accounts gesichert.“ Das sei wichtig, um den Missbrauch der Konten zu verhindern und kritische Daten zu schützen. Viele dieser Mitarbeiter sind nun von Musk entlassen worden. „Die privaten Admins bei Mastodon wissen gar nicht, wie man solche Risikogruppen schützen muss“, erklärt Alimardani.

Nur wenige Tage nach Ausbruch der Proteste tat die US-Regierung endlich das, was Internetaktivisten schon seit Jahren gefordert hatten: Washington lockerte die Sanktionen, die Iranern die Angebote US-amerikanischer Technologiekonzerne verwehrt hatten. Mit dem üblichen Aplomb kündigte Elon Musk sofort an, seinen Satelliten-Internetdienst Starlink für Iran freizuschalten. Tatsächlich sind mittlerweile einige Empfangsgeräte ins Land gelangt. Diese bergen jedoch auch Risiken, da die Sicherheitsdienste deren Nutzer möglicherweise lokalisieren können.

Hilfe erwünscht

Weitaus hilfreicher wäre es, leistungsstarke VPNs bereitzustellen, da sind sich viele Internetaktivisten einig. Anwendungen wie Psiphon und Tor verzeichnen in den letzten Monaten steigende Nutzerzahlen in Iran. Beide tunneln den Datenverkehr über ein Netzwerk von Computern und helfen so, Blockaden zu umgehen und die Anonymität im Netz zu bewahren [1]. Das Tor-Projekt bietet die Browser-Erweiterung Snowflake an, einen Proxy, mit dem auch Nutzer in Deutschland über ihren heimischen Computer Menschen aus Iran schnell Zugang zum Tor-Netzwerk geben können.

Journalistinnen wie Gilda Sahebi retweeten Informationen aus Iran und steigern damit die Aufmerksamkeit für die Protestbewegung.

Der Leiter der Community-Arbeit bei Tor, Gustavo Gus, berichtet, dass nach anfänglichem großen Erfolg Snowflake im Oktober plötzlich für iranische Nutzer des Tor-Proxys Orbot blockiert war. Mit Orbot lassen sich die Apps auf Android-Smartphones über Tor schützen. Es habe zwei Wochen gedauert, bis man eine Lösung entwickeln konnte: „Unter den Bedingungen von Zensur und Überwachung ist es sehr schwer, mit Nutzern in Iran zu kommunizieren. Wir brauchen immer Feedback von Leuten, die unsere Anpassungen testen. Viele Kanäle aber sind blockiert.“

Die große Nachfrage aus Iran habe das Team an den Rand seiner Kräfte gebracht. „Es ist, als ob man in einer Küche arbeitet, auf einmal kommen viel mehr Gäste und wollen Essen“, erzählt Gustavo. Tor bräuchte mehr Freiwillige, die auf ihren Servern einen eigenständigen Proxy für Snowflake installieren, der mehr Bandbreite bietet als Privatzugänge, und die Kapazität des Netzwerks erhöht.

Stefan Leibfarth, der für den Chaos Computer Club in Stuttgart einen Exit-Node für Tor betreibt, betont, dass Freiwillige in Deutschland einen wesentlichen Anteil der benötigten Server und Bandbreite für den gesamten Service stellen. Dieses Engagement sei meist rein ehrenamtlich. „Dafür wünschen wir uns mehr öffentliche Aufmerksamkeit und Anerkennung“, sagt Leibfarth. Eine direkte staatliche Finanzierung sieht er skeptisch, hält aber eine breite Förderung durch verschiedene Geldgeber für wünschenswert.

Um das iranische System der Überwachung und Internetkontrolle zu schwächen, müssten letztlich alle Unternehmen, die in irgendeiner Form darin involviert sind, Konsequenzen spüren, denkt der frühere Start-up-Pionier Arash Zad. Ob dies tatsächlich geschieht, ist derzeit ungewiss, denn noch sind die Folgen der Protestbewegung für das Regime und die Gesellschaft Irans nicht abzusehen. *(hob@ct.de)* c't

Literatur

[1] Ronald Eikenberg, Freies Internet für freie Bürger, Wie Surfer Netzsperren und Zensur umgehen, c't 8/2022, S. 14

Erwähnte Dokumentationen: ***ct.de/y6ep***