



Bundesamt
für Migration
und Flüchtlinge

Informationszentrum
Asyl und Migration



Länderkurzinformation Iran

Netzaktivitäten und Netzüberwachung

Stand: 07/2026

Urheberrechtsklausel

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrecht zugelassen ist, bedarf der vorherigen Zustimmung des Bundesamtes für Migration und Flüchtlinge. Dies gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen. Auszugsweiser Nachdruck und Vervielfältigung auch für innerbetriebliche Zwecke ist nur mit Quellenangabe und vorheriger Genehmigung des Bundesamtes gestattet.

Die Inhalte dürfen ohne gesonderte Einwilligung lediglich für den privaten, nicht kommerziellen Gebrauch sowie ausschließlich amtsinternen Gebrauch abgerufen, heruntergeladen, gespeichert und ausgedruckt werden, wenn alle urheberrechtlichen und anderen geschützten Hinweise ohne Änderung beachtet werden.

Copyright statement

This report/information is subject to copyright rules. Any kind of use of this report/information – in whole or in part – not expressly admitted by copyright laws requires prior approval by the Federal Office of Migration and Refugees (Bundesamt). This applies in particular to the reproduction, adaptation, translating, microfilming, or uploading of the report/information in electronic retrieval systems. Reprinting and reproduction of excerpts for internal use is only permitted with reference to the source and prior consent of the Bundesamt.

Use of the report/information may be made for private, non-commercial and internal use within an organisation without permission from the Bundesamt following copyright limitations.

Disclaimer

Die Information wurde gemäß der EUAA COI Report Methodology (2023) sowie den Qualitätsstandards des Bundesamtes für Migration und Flüchtlinge (2022) auf Grundlage sorgfältig ausgewählter und zuverlässiger Informationen innerhalb eines begrenzten Zeitrahmens erstellt. Alle zur Verfügung gestellten Informationen wurden mit größter Sorgfalt recherchiert, bewertet und aufbereitet. Alle Quellen werden genannt und nach wissenschaftlichen Standards zitiert.

Die vorliegende Ausarbeitung erhebt keinen Anspruch auf Vollständigkeit. Findet ein bestimmtes Ereignis, eine bestimmte Person oder Organisation keine Erwähnung, bedeutet dies nicht, dass ein solches Ereignis nicht stattgefunden hat oder die betreffende Person oder Organisation nicht existiert. Der Bericht/die Information erlaubt keine abschließende Bewertung darüber, ob ein individueller Antrag auf Asyl-, Flüchtlings- oder subsidiären Schutz berechtigt ist. Die benutzte Terminologie sollte nicht als Hinweis auf eine bestimmte Rechtsauffassung verstanden werden. Die Prüfung des Antrags auf Schutzgewährung muss durch den für die Fallbearbeitung zuständigen Mitarbeiter erfolgen. Die Veröffentlichung stellt keine politische Stellungnahme des Bundesamtes für Migration und Flüchtlinge dar.

Diese Ausarbeitung ist öffentlich.

Disclaimer

The information was written according to the „EUAA COI Report Methodology“ (2023) and the quality standards of the Federal Office for Migration and Refugees (Bundesamt) (2022). It was composed on the basis of carefully selected and reliable information within a limited time frame. All information provided has been researched, evaluated and analysed with utmost care within a limited time frame. All sources used are referenced and cited according to scientific standards.

This document does not pretend to be exhaustive. If a certain event, person or organization is not mentioned, this does not mean that the event has not taken place or that the person or organization does not exist. This document is not conclusive as to the merit of any particular claim to international protection or asylum. Terminology used should not be regarded as indication of a particular legal position. The examination of an application for international protection has to be carried out by the responsible case worker. The information (and views) set out in this document does/do not necessarily reflect the official opinion of the Bundesamt and makes/make no political statement whatsoever.

This document is public.

Inhaltsverzeichnis

1. Netzaktivitäten – Netzüberwachung.....	1
1.1 Akteure staatlicher Überwachung.....	1
1.2 Maßnahmen der Netzüberwachung	2
1.2.1 Abschaltung, Drosselung und Ausspähung des Datenverkehrs.....	2
1.2.2 Zensur.....	3
1.2.3 Blockade und Filterung	3
1.2.4 Cyberangriffe	4
1.2.5 Entwicklung des Nationalen Informationsnetzwerkes.....	5

1. Netzaktivitäten – Netzüberwachung

Ein erheblicher Anteil regierungskritischer Debatten in Iran findet im virtuellen Raum und über soziale Medien statt. Entsprechend strebt die iranische Regierung anhaltend nach Zensur und Überwachung des Internets und mobilen Datenverkehrs.¹ Netzaktivitäten besonders engagierter Personen, die Einfluss auf die öffentliche Meinung ausüben, können in den Blick staatlicher Kontrolle geraten. Zwar liegen kaum gesicherte Erkenntnisse darüber vor, inwieweit alltägliches Nutzerverhalten und Online-Aktivitäten überwacht werden. Jedoch werden staatliche Maßnahmen bereits seit mehreren Jahren vorangetrieben, um regierungsfeindliche Aktivitäten zu identifizieren und gegen diese vorzugehen.²

Da das Hauptaugenmerk des Sicherheitsapparates auf dem Schutz der islamischen Regierung liegt, sollen jegliche Aktivitäten identifiziert werden, die dessen Kontrolle und Autorität gefährden und untergraben könnten. Bestimmte Zielgruppen lassen sich hierbei schwer definieren.³ Im Fokus der Überwachung können Online- und Social-Media-Aktivitäten von Personen, Gruppen oder Medien stehen, die das politische und religiöse Gefüge anfeinden und in Frage stellen.⁴ Insbesondere diejenigen mit einer hohen Reichweite und Vernetzung (etwa auch aufgrund ihrer Profession, Kontakte, Bekanntheit) sowie entsprechend anzunehmendem Einfluss auf die Öffentlichkeit, darunter auch Iranerinnen und Iraner im Ausland.⁵

Einige dieser Aspekte sollen im Folgenden näher beleuchtet werden.

1.1 Akteure staatlicher Überwachung

Im Jahr 2012 richtete der mittlerweile verstorbene Revolutionsführer Ali Khamenei per Dekret den sog. Obersten Rat für den Cyberspace (engl. Supreme Council of Cyberspace, SCC) als übergeordnete Kontrollinstanz ein. Dieser hat 27 Mitglieder und entwickelt allgemeine Leitlinien für die Verwaltung des virtuellen Raumes. Auf deren Grundlage befindet ein Ausschuss darüber, was anstößige und somit illegale Online-Inhalte sind, die gefiltert oder gesperrt werden sollen.⁶ In dem Ausschuss sind Ministerien, Sicherheitsbehörden sowie die staatliche Rundfunkanstalt (IRIB) vertreten.⁷ Das Ministerium für Kultur und islamische Führung und das Ministerium für Informations- und Kommunikationstechnologie sind die wichtigsten Regulierungsbehörden für Online-Inhalte und haben die Kontrolle über den gesamten Datenverkehr inne.⁸

Zur Durchsetzung der entsprechenden politischen Leitlinien werden mehrere ausführende Behörden eingesetzt. Hierzu zählt v.a. die Polizei des Cyberspace und Informationsaustausches (pers.: FATA), die in den Jahren 2010/2011 als Untereinheit der Polizei geschaffen wurde.⁹ In deren Zuständigkeit liegen die Bekämpfung von Cyberkriminalität (wie etwa Finanzbetrug und Verletzungen der Privatsphäre), aber auch das Vorgehen gegen regimekritische Beiträge jeglicher Art im virtuellen Raum. Sie soll an der Überwachung, Einschüchterung und Verhaftung von Online-Aktivistinnen und Aktivisten beteiligt sein.

¹ AC, [Iranians on #SocialMedia](#), Atlantic Council, letzte Aktualisierung 15.12.2021.

² Anm.: als Ausgangspunkt gilt das Jahr 2009/10; LI, [Temanotat Iran, Internett og sosiale medier](#), Landinfo, letzte Aktualisierung 09.11.2022; Rferl, [Iran Accused Of Secretly Implementing Controversial Draft Internet Bill](#), Radio Free Europe/Radio Liberty, letzte Aktualisierung 09.09.2022; [A19, Tightening the Net: China's Infrastructure of Oppression in Iran, Article19, February 2026, 7](#).

³ Anm.: Landinfo nennt hierbei zu kurdischen Parteien zugehörige Personen und christliche Konvertiten (LI, [Temanotat Iran, Internett og sosiale medier](#), Landinfo, letzte Aktualisierung 09.11.2022, 53). Da diese Personengruppen jedoch nicht ausschließlich Netzaktivitäten betreiben, werden sie hier nicht hervorgehoben, sondern als mögliche Zielgruppen neben weiteren erachtet.

⁴ LI, [Temanotat Iran, Internett og sosiale medier](#), Landinfo, letzte Aktualisierung 09.11.2022, 34, 57.

⁵ Ebd.

⁶ LI, [Temanotat Iran, Internett og sosiale medier](#), Landinfo, letzte Aktualisierung 09.11.2022, 12-14.

⁷ engl.: Islamic Republic of Iran Broadcasting (Art. 175 d. Verf. verbietet privaten Rundfunk/TV; IRIB obliegt das Rundfunkmonopol)

⁸ USDOS, [2024 Country Reports on Human Rights Practices](#), U.S. Department of State, 13.08.2025.

⁹ LI, [Iran: Criminal procedures and documents](#), Landinfo, Office of the Commissioner General for Refugees and Stateless Persons, State Secretariat for Migration, December 2021, 20.

Einem Bericht des Menschenrechtsportals Filterwatch zufolge habe die FATA mit etwa 42.000 freiwilligen Helfern, die über gute digitale Fähigkeiten verfügen, eine breite soziale Basis.¹⁰ Zudem überschneiden sich ihre Zuständigkeiten teils mit den Aufgaben des an die IRGC angegliederten Zentrums zur Untersuchung organisierter Kriminalität (engl. CIOC).¹¹

Ebenfalls an Überwachungs- und Gegenmaßnahmen beteiligt sind Einheiten der Revolutionswächter (engl. IRGC), sowie des Informationsministeriums. Im weit ausdifferenzierten Sicherheitsapparat Irans übernehmen diese als Justizvollzugsbehörden, neben allgemeinen Polizeieinheiten, Aufgaben bei der Strafverfolgung.¹²

1.2 Maßnahmen der Netzüberwachung

1.2.1 Abschaltung, Drosselung und Ausspähung des Datenverkehrs

Anlässlich sozialer Unruhen und großer Demonstrationen reagiert die iranische Führung u.a. mit der vollständigen oder teilweisen Abschaltung und Filterung des Internets, wie im Rahmen der landesweiten Proteste zwischen 28.12.2025 und 13.01.2026.¹³ Hierbei wurde ab dem 08.01.2026 der Zugang zu in- und ausländischen Nachrichtenseiten, sozialen Medien und Kommunikationsplattformen, sowohl über Breitband- als auch Mobilfunknetze, zeitweise komplett abgeschaltet.¹⁴ Im Zuge der militärischen Auseinandersetzung Irans mit Israel und den USA ab 28.02.2026, kam es zu einer erneuten staatlich initiierten landesweiten Abschaltung des Internets. Die Internetblockade wurde erst ab 26.05.2026 nach einer durch Staatspräsident Masoud Pezeshkian erlassenen Anordnung wieder aufgehoben und gilt als die bisher am längsten aufrechterhaltene landesweite Internetsperre in Iran. Auch nach der Aufhebung wurde von anhaltenden Einschränkungen der Internetkonnektivität berichtet.¹⁵ In den Jahren 2021/22 wurde hingegen noch vermehrt von lokalen Drosselungen und örtlich begrenzten Abschaltungen berichtet, z.B. im Zusammenhang mit Protesten in der Provinz Khuzestan.¹⁶ Im Gegensatz zu Totalabschaltungen wie im Jahr 2026, wurden auch während der landesweiten Demonstrationen ab September 2022 lokale Abschaltungen (z.B. in Sanandaj, Provinz Kordestan) und Drosselungen, inklusive des mobilen Datenverkehrs, vorgenommen.¹⁷

Einem Bericht des aktivistischen Portals The Intercept zufolge nutzen iranische Behörden ein unter dem Namen SIAM bekanntes System, um mobile Netzverbindungen zu orten und die Datenübertragungsrate zu verlangsamen, aber auch die Verschlüsselung von Telefongesprächen zu knacken und Bewegungsprofile zu erstellen. Hierbei können per Fernbefehl die Nutzung von Mobiltelefonen verändert, gestört und überwacht werden.¹⁸

Dies erlaube auch Zugriffe auf persönliche Daten wie etwa Namen, Adresse und ID-Nummern von Besitzenden eines Mobiltelefons. Inwieweit dies von Behörden für personenbezogene Maßnahmen eingesetzt wird, bleibt unklar. In Einzelfällen wurde berichtet, dass Personen, die sich in geographischer Nähe von Demonstrationen aufhielten, Textnachrichten erhalten hätten, in deren Inhalt vor einer Teilnahme gewarnt worden sei.¹⁹

¹⁰ FW, [Iran's Cyber Police — 'Society-Based Policing' and the Rise of Peer Surveillance](#), Filterwatch, letzte Aktualisierung 18.02.2019.

¹¹ LI, [Iran: Criminal procedures and documents](#), Landinfo, Office of the Commissioner General for Refugees and Stateless Persons, State Secretariat for Migration, December 2021, 20.

¹² LI, [Temanotat Iran, Internett og sosiale medier](#), Landinfo, letzte Aktualisierung 09.11.2022, 16.

¹³ Reuters, [Nationwide internet blackout reported in Iran as protests persist](#), Reuters News Agency, letzte Aktualisierung 08.01.2026: NB, [Latest News #Iran](#), NetBlocks, letzte Aktualisierung 30.01.2026.

¹⁴ Ebd.

¹⁵ APN, [Iranians are back online after a monthslong shutdown but still face heavy restrictions](#), Associated Press News, letzte Aktualisierung 28.05.2026; Reuters, [Iran's president orders reopening of international internet access, state media reports](#), letzte Aktualisierung 25.05.2026.

¹⁶ DW Farsi, [قطع اینترنت در شهرهای خوزستان](#) [Internetausfälle und langsame Verbindungen in Städten der Chuzestan-Region], Deutsche Welle Farsi, letzte Aktualisierung 07.05.2022.

¹⁷ NB, [Internet disrupted in Iran amid protests over death of Mahsa Amini](#), NetBlocks, letzte Aktualisierung 19.09.2022; FW, [زن، زندگی، و](#) [Frauen, Leben und Internetausfälle: Netzwerkstatusbericht – September und Oktober 2022], Filterwatch, letzte Aktualisierung 17.10.2022; RF, [همزمان با اعتراضات سراسری در ایران](#) [Weitreichende Störungen des Mobinnet-Internets fallen mit landesweiten Protesten im Iran zusammen], Radio Farda, letzte Aktualisierung 25.09.2022.

¹⁸ TI, [Hacked Documents: How Iran can track and control protesters' phones](#), The Intercept, letzte Aktualisierung 28.10.2022.

¹⁹ Ebd.

1.2.2 Zensur

Die Überwachung des virtuellen Raumes findet auch in Form von Zensur statt. Die iranische Führung ist bemüht, Bürgerinnen und Bürger vor ausländischem, insbesondere westlichem Einfluss fernzuhalten und negative Berichterstattung über die Islamische Republik zu vermeiden. Hierdurch soll auch regierungsfeindlichen Aktivitäten vorgebeugt werden.²⁰ Laut Berichten der Menschenrechtsorganisation Freedom House sind beispielsweise Tageszeitungen und Zeitschriften anhaltender Zensur ausgesetzt und erhalten von den Behörden Warnungen hinsichtlich der Themenwahl und der Art der Berichterstattung.²¹ Zudem komme es zu Fällen von Selbstzensur unter Online-Berichterstattenden sowie bei gewöhnlichen Internetnutzenden.²²

Beispielsweise wurden im Rahmen der landesweiten Proteste im September 2022 Medienschaffende verhaftet, weil sie über den Tod der iranischen Kurdin Gina Mahsa Amini in sozialen Netzwerken berichtet hatten.²³ In dem Zusammenhang erging die Ankündigung durch das Innenministerium, dass Berichte, die im Widerspruch zur offiziellen [Anm.: regierungsnahen] Berichterstattung zu Aminis Tod stünden, strafrechtlich verfolgt werden würden.²⁴

1.2.3 Blockade und Filterung

Als weitere Maßnahme kann der Zugang zu bestimmten Webinhalten und Anwendungen verwehrt (blockiert) oder selektiv gewährt (gefiltert) werden. Verschiedene Technologien kommen hierbei zum Einsatz, u.a. ein zentrales Filtersystem, das eine Website innerhalb weniger Stunden im gesamten Netz sperren kann, aber auch Methoden zur Drosselung des Datenverkehrs (s.o.).²⁵

Websites und Internetdienste werden in Iran immer wieder zeitweise offiziell blockiert, darunter Facebook, Telegram, X (vormals Twitter)²⁶, Youtube, Signal, sowie Anwendungen wie Blogspot, Blogger, Wix und Wordpress. Häufig greifen Nutzende aber zur Umgehung von blockierten und gefilterten Inhalten auf verschlüsselte VPN-Anwendungen (Virtual Private Networks) zurück, die einen Zugriff ermöglichen, jedoch zum Teil mit hohen Kosten verbunden sind.²⁷ Der Zugang zu weiterhin häufig genutzten Diensten wie Instagram und WhatsApp wurde im Zuge von landesweiten Protestereignissen, wie etwa im Jahr 2022, zeitweise stark eingeschränkt oder gesperrt.²⁸ Im Dezember 2024 gab die Regierung bekannt, vorübergehend erfolgte Beschränkungen für WhatsApp und Google Play aufzuheben.²⁹ Im Juni 2025 wurden zuvor implementierte staatliche Blockaden von Instagram und WhatsApp wiederaufgehoben, sodass Zugriffe zumindest zeitweise ohne Umgehungssoftware möglich gewesen seien.³⁰

Blockaden bestehen weiterhin gegen Webauftritte internationaler Nachrichtenmedien, Menschenrechtsorganisationen, politisch-oppositionelle Inhalte sowie Webseiten ethnischer und religiöser Minderheiten, aber auch islamischer Strömungen die von der zwölferschiitischen Staatsreligion abweichen.³¹

²⁰ LI, [Temanotat Iran, Internett og sosiale medier](#), Landinfo, letzte Aktualisierung 09.11.2022, 30.

²¹ FH, [Freedom in the World 2025, Iran](#), Freedom House, 2025, D.

²² FH, [Freedom on the Net 2025, Iran](#), Freedom House, 2025, B.

²³ DW, [1000 Festnahmen nach Protesten im Iran](#), Deutsche Welle, letzte Aktualisierung 25.09.2022; BBC News, [Iran tries female journalists who reported on Mahsa Amini's death](#), British Broadcasting Corporation, letzte Aktualisierung 30.05.2023.

²⁴ RF, [«جان‌باختن مهسا امینی؛ معاون امنیتی وزارت کشور بجای گزارش «تهدید کرد» Innenministeriums „droht“, anstatt zu berichten](#)], Radio Farda, letzte Aktualisierung 28.09.2022

²⁵ FH, [Freedom on the Net 2025, Iran](#), Freedom House, 2025, B.

²⁶ Anm.: paradoxerweise nutzte die iranische Führung bisher neben Instagram auch Twitter, u.a. auch der Revolutionsführer Khamenei und weitere mit der Regierung verbundene Beamte und Einrichtungen. Dieses Vorgehen wurde z.T. durch ultrakonservative Parlamentsmitglieder verteidigt, siehe z.B.: IranInt, [Hardline Iran lawmaker defends unrestricted internet access for officials](#), Iran International, letzte Aktualisierung 07.11.2024.

²⁷ LI, [Temanotat Iran, Internett og sosiale medier](#), Landinfo, letzte Aktualisierung 09.11.2022, 52; Anm.: im Oktober 2024 sprach sich der amtierende Präsident Pezeshkian für eine Bekämpfung des Handels von VPNs aus. Ob und in welchem Ausmaß konkret Maßnahmen gegen eine VPN-Nutzung erfolgen, ist bisher unklar (siehe: IW, [Pezeshkian Targets VPNs Instead of Lifting Internet Filtering in Iran](#), Iranwire, letzte Aktualisierung 11.10.2024).

²⁸ LI, [Temanotat Iran, Internett og sosiale medier](#), Landinfo, letzte Aktualisierung 09.11.2022, 49; NB, [Internet disrupted in Iran amid protests over death of Mahsa Amini](#), NetBlocks, letzte Aktualisierung 19.09.2022.

²⁹ [AJ, Iran to lift ban on WhatsApp, Google Play, state media report, Al Jazeera, letzte Aktualisierung 24.12.2024](#)

³⁰ [IW, Iran Lifts Blocks on Instagram and WhatsApp After Two-Year Ban, Iranwire, letzte Aktualisierung 25.06.2025](#).

³¹ FH, <https://freedomhouse.org/country/iran/freedom-net/2025>, Freedom House, 2025.

Zur Umgehung von Filterungen und Blockaden wird primär auf die bereits erwähnte Nutzung von VPN und weitere technische Hilfsmittel zurückgegriffen. So ermöglichte beispielsweise die Nutzung der kostenfreien Applikation Conduit während der landesweiten Internetblockade im Jahr 2026 (siehe Punkt 1.2.1) in begrenztem Umfang auch Internetzugriffe von Iran aus.³² Zudem gewann die Verwendung von Starlink-Satelliten des US-Raumfahrtunternehmens SpaceX im Jahr 2026 zunehmend an Bedeutung für die Umgehung staatlicher Internetblockaden. Medienberichten zufolge wurde im Zuge der landesweiten Internetsperre vermehrt technische Ausrüstung hierfür nach Iran eingeschmuggelt. In diesem Zusammenhang wurde von mehreren Verhaftungen wegen des Kaufs und Verkaufs von Starlink-Terminals sowie von Beschlagnahmungen und möglichen Haftstrafen berichtet.³³ Der Internetzugriff über Starlink ist jedoch weiterhin nur als äußerst begrenzt zugängliche Option zu betrachten, da die Empfangsanlagen zunächst illegal auf dem Schwarzmarkt erworben werden müssen und preislich zwischen rd. 1.000 bis zu 2.000 EUR pro Stück gehandelt werden.³⁴ Laut Medienberichten waren bis zum Jahr 2024 ca. 6.000 bis 7.000 Geräte importiert worden. Über eine etwaige landesweit verbreitete Nutzung wurde hierbei jedoch nicht berichtet.³⁵ Im Januar 2026 seien im gesamten Staatsgebiet etwa 50.000 Empfangsgeräte vorhanden gewesen und das Unternehmen SpaceX habe den Zugang unterdessen ohne weitere Abonnement-Gebühren ermöglicht.³⁶

1.2.4 Cyberangriffe

Zunehmend verbreitet sind Cyberattacken, die sich gegen Netzwerk-Accounts und Benutzerkonten von als regierungsfeindlich erachteten Einzelpersonen oder Gruppen, wie Aktivistinnen und Aktivisten, Medienschaffende, Studierende, sowie systemkritische Kulturschaffende, richten können.³⁷

Einige Methoden die hierzu Anwendung finden sind u.a. die Verbreitung von Computerviren und Schadsoftware durch Infiltration von digitalen Netzwerken (z.B. über Fake-Profile auf sozialen Netzwerken³⁸), Phishing (hierbei werden Nutzende v.a. per Email dazu verleitet, Passwörter auf gefälschten Zugangsseiten und Anwendungen einzugeben) und Installation von Schad- und Spionagesoftware zur Sammlung aber auch Löschung von Daten, sowie zur Außerkraftsetzung von Anwendungen.³⁹

Das Webportal Filterwatch, das die Internetfreiheit in Iran untersucht, weist darauf hin, dass Nutzende selbst über Umgehungstools wie VPN-Verbindungen von solcher Schadsoftware beeinträchtigt werden könnten, da auch schädliche VPN-Dienste in Umlauf gebracht wurden.⁴⁰ Unklar bleibt, ob iranische Behörden auch Nachrichteninhalte auf verschlüsselten ausländischen Anwendungen überwachen können, oder sich ihr Zugriff auf die lokale Nutzung beschränkt. Landinfo Norwegen geht davon aus, dass die iranischen Behörden sich über Phishing-Angriffe auch Zugang zu Accounts und Endgeräten im Ausland verschaffen könnten.⁴¹

³² BBC Persian, [بزنند؟ دور را اینترنت فیلترینگ تا کرده کمک ایران داخل مردم به چطور و چیست کاندونیت](#) [What is Conduit and how has it helped people inside Iran bypass internet filtering?], British Broadcasting Corporation Persian, letzte Aktualisierung 01.02.2026.

³³ BBC Persian, [اینترنیت خاموشی بر غلبه برای ایران به استارلینک قاچاق](#) [Smuggling Starlink to Iran to overcome internet blackout], letzte Aktualisierung 04.05.2026; BAMF, Briefing Notes v. 30.03.2026, Bundesamt für Migration und Flüchtlinge, letzte Aktualisierung 30.03.2026; BAMF, Briefing Notes v. 13.04.2026, letzte Aktualisierung 13.04.2026, m.w.N.

³⁴ NTV, [Erste Starlink-Einheiten im Iran verfügbar](#), ntv Nachrichtenfernsehen, letzte Aktualisierung 17.10.2022.

³⁵ IW, [Iranians Defy Internet Restriction with Smuggled Starlink Devices](#), Iranwire, letzte Aktualisierung 10.09.2024.

³⁶ DPA, [Wie Starlink die iranische Internet-Blockade durchdringt](#), Deutsche Presseagentur, letzte Aktualisierung 16.01.2026;

³⁷ NYT, [Iranian Hackers Found Way Into Encrypted Apps](#), Researchers Say, The New York Times, letzte Aktualisierung 18.09.2020.

³⁸ Anm.: mutmaßlich sollten über provokante und regierungskritische Beiträge der Fake-Profile darauf entsprechend reagierende Personen ins Visier genommen werden; so soll der US-Konzern Meta (Facebook, Instagram, Whatsapp) bereits im Jahr 2021 ein Netzwerk von rd. 200 gefälschten Accounts auf Instagram und Facebook entfernt haben, das mutmaßlich mit dem Korps der Islamischen Revolutionsgarden (IRGC) in Verbindung gestanden habe (vgl. Meta, [September 2021 coordinated inauthentic behavior report](#), Meta Platforms Inc., letzte Aktualisierung 11.10.2021).

³⁹ FW, [Frauen, Leben, Freiheit: Eine Zusammenfassung zum Stand der digitalen Rechte während der Proteste](#), letzte Aktualisierung 27.01.2023.

⁴⁰ IW, [Iranians Defy Internet Restriction with Smuggled Starlink Devices](#), Iranwire, letzte Aktualisierung 10.09.2024; BD, EyeSpy - Iranian Spyware Delivered in VPN Installers, Bitdefender, letzte Aktualisierung 11.01.2023.

⁴¹ LI, [Temanotat Iran, Internett og sosiale medier](#), Landinfo, letzte Aktualisierung 09.11.2022, 38.

1.2.5 Entwicklung des Nationalen Informationsnetzwerkes

Ein langfristiges Ziel der Regierung besteht darin, ein sicheres und stabiles nationales Intranet separat vom weltweiten Netz zu etablieren. Offiziell soll dies der Eindämmung von ausländischen Cyberangriffen dienen und einer westlich-kulturellen Invasion entgegenwirken.⁴² Jedoch wird angenommen, dass auch stärkere Kontrolle über den inländischen Datenverkehr ausgeübt wird und der Einfluss internationaler Webinhalte in Iran nach chinesischem Vorbild wirksamer zensiert werden soll.⁴³

Zudem wird angestrebt, mit dem nationalen Netz dem durch umfassende Abschaltungen, Blockaden und Filterung verursachten erheblichen wirtschaftlichen Schaden und damit verbundenem Unmut in der Bevölkerung entgegenzuwirken.⁴⁴

Ein weiteres Ziel der iranischen Führung ist es, ausländische Internetdienste wie Messaging-Apps und soziale Netzwerke weitgehend durch heimische zu ersetzen. Verbunden mit Anreizen wie günstigeren inländischen Datentarifen soll die Zahl der Nutzer auf diesen Plattformen erhöht werden.⁴⁵ In der Bevölkerung stößt jedoch auch dies aus Angst vor staatlicher Kontrolle und mangelnder Privatsphäre auf Ablehnung.⁴⁶

Exklusive nationale Inhalte können wiederum Abschaltungen und Blockaden des weltweiten Netzes erleichtern, da sich inländische Websites und Apps – wie Bank-, Medien- und Regierungswebsites – weitgehend auf inländischen Servern befinden und somit selbst bei Abschaltung des internationalen Netzes verfügbar bleiben.⁴⁷

Laut einem Bericht des Menschenrechtsportals Filterwatch strebt die iranische Regierung weiterhin an, den Internetzugriff von einer öffentlichen Dienstleistung in ein staatlich gewährtes Privileg umzuwandeln. So solle ein Großteil der Bevölkerung bei Bedarf gezielt digital isoliert werden können, bei gleichzeitiger Aufrechterhaltung der Funktionalität von wirtschaftlich relevanten Online-Diensten.⁴⁸ Im Zusammenhang der landesweiten Internetsperre während der militärischen Auseinandersetzung Irans mit Israel und den USA ab 28.02.2026 wurde berichtet, dass iranische Behörden nur Regierungsmitgliedern und deren engen Vertrauten sowie einigen regierungsnahen Medienschaffenden Zugang zum weltweiten Internet über sogenannte weiße SIM-Karten gewährt hatten. Der Großteil der Bevölkerung sei auf die Nutzung des nationalen Internet beschränkt gewesen, abgesehen von den genannten illegalen Möglichkeiten eines Zugangs zum weltweiten Internet, wie z.B. VPN und Starlink (s.o.).⁴⁹

⁴² AC, [Iranians on #SocialMedia](#), Atlantic Council, letzte Aktualisierung 15.12.2021.

⁴³ A19, [Tightening the Net: China's Infrastructure of Oppression in Iran](#), Article19, February 2026, 8; CT, [Whatever it takes to end it, Iran's shift toward more oppressive governance](#), Critical Threats American Enterprise Institute, December 2021, 16-17.

⁴⁴ FW, [Exclusive Report: The Network Behind Iran's Internet Shutdown: From Engineering Disconnection to Profiting off Sanctions](#), Filterwatch, letzte Aktualisierung 03.02.2026; RF, [«است کرده مشکل دچار» را فولاد و لبنیات و دارو تولید ایران در اینترنت قطع](#) [Internetausfall im Iran beeinträchtigt die Produktion von Medikamenten, Milchprodukten und Stahl], letzte Aktualisierung 01.11.2022.

⁴⁵ FW, [Exclusive Report: The Network Behind Iran's Internet Shutdown: From Engineering Disconnection to Profiting off Sanctions](#), Filterwatch, letzte Aktualisierung 03.02.2026.

⁴⁶ Tejarat, [شوند؟ می‌هاخار جی، جایگزین داخلی‌های تلفن](#) [Werden inländische Plattformen ausländische ersetzen?], letzte Aktualisierung September 2022.

⁴⁷ AC, [Iranians on #SocialMedia](#), Atlantic Council, letzte Aktualisierung 15.12.2021.

⁴⁸ FW, [Exclusive Report: The Network Behind Iran's Internet Shutdown: From Engineering Disconnection to Profiting off Sanctions](#), Filterwatch, letzte Aktualisierung 03.02.2026.

⁴⁹ [BBC Persian](#), [۱۰۰۰ در اینترنت قطع ساعت](#) [One Thousand hours of internet outage in Iran; Internet hashtag becomes trending], British Broadcasting Corporation Persian, letzte Aktualisierung 10.04.2026.

Diesbezüglich wird in einem weiteren Bericht von Filterwatch auf ein von der iranischen Regierung angestrebtes Modell eines hybriden Internetshutdowns hingewiesen. Demnach gäbe es Hinweise darauf, dass die iranischen Behörden im Nachgang der landesweiten Internetsperre seit Mai 2026 ein gesteuertes hybrides Abschaltmodell anwendeten. Durch die Wiederöffnung internationaler Gateways und Datenverkehrsknotenpunkte sei genügend sichtbare Internetaktivität erzeugt worden, um automatisierten globalen Systemen zur Messung von Internetkonnektivitäten eine Wiederherstellung zu signalisieren und dadurch Behauptungen über eine Normalisierung zu untermauern. Gleichzeitig hätten verfügbare Daten gezeigt, dass die eigentlich verfügbare Bandbreite weiterhin stark eingeschränkt war, wodurch das tatsächliche Volumen des internationalen Datenverkehrs deutlich reduziert blieb. Dieses Modell hätte iranischen Behörden ermöglicht, vor dem Eindruck einer vermeintlich wiederhergestellten Konnektivität, die Kontrolle über den grenzüberschreitenden Internetzugang weitgehend aufrechtzuerhalten.⁵⁰ Mit Verweis auf eine im Mai 2026 im iranischen Staatsfernsehen geführte Diskussion von Regierungsmitgliedern über die Zukunft des iranischen Internets habe dieses Modell eine von der iranischen Regierung angestrebte Kontrolle, Verwaltung und Regulierung des Internets begünstigt.⁵¹ Diese Annahmen lassen sich nicht anhand weiterer Quellen bestätigen.

⁵⁰ [FW, The Illusion of Reconnection: Iran's New Hybrid Internet Shutdown Model, Filterwatch, letzte Aktualisierung 01.06.2026](#) (FW verweist auf eine Diskussion von Regierungsmitgliedern im iranischen Fernsehen)

⁵¹ Ebd.

Impressum

Herausgeber

Bundesamt für Migration und Flüchtlinge
90461 Nürnberg

ISSN

2943-7938

Stand

07/2026

Druck

Bundesamt für Migration und Flüchtlinge

Gestaltung

Bundesamt für Migration und Flüchtlinge

Bestellmöglichkeit

Referat Informationsvermittlung/Länder- und Rechtsdokumentation,
Bundesamt für Migration und Flüchtlinge, Nürnberg

E-Mail: informationsvermittlungsstelle@bamf.bund.de
<https://milo.bamf.de>

Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Bundestags-, Landtags- und Kommunalwahlen sowie für Wahlen zum Europäischen Parlament.

www.bamf.de