NAHER OSTEN/NORDAFRIKA 05.02.2026 | Fereidoon Bashar & Mani Mostofi & Hanna Voss

Mörderischer Blackout

Als das Netz verstummte, begann das Töten. Irans digitaler Autoritarismus wirkt über Grenzen hinweg – was macht Europa?

Am 8. Januar 2026, als Millionen Iraner auf den Straßen protestierten, veranlasste das islamische Regime eine Internetabschaltung von beispiellosem Ausmaß und zuvor nie gesehener technischer Komplexität. Die Kommunikationssperre war nahezu vollständig und unterbrach den internationalen Zugang, die inländische Netzwerkkonnektivität, mobile Daten und Festnetzdienste. Unter dem Schutz des umfassendsten Kommunikationsblackouts in der Geschichte des Landes entfesselten die iranischen Sicherheitskräfte eine blutige Welle staatlich sanktionierter Gewalt.

Die Weltöffentlichkeit hat das volle Ausmaß der Ereignisse der letzten Wochen immer noch nicht erfasst. Die *Human Rights Activists News Agency* (HRANA) hat bestätigt, dass bis zum 2. Februar über 6 400 Demonstranten und Passanten getötet wurden, darunter 146 Kinder. Diese Zahlen steigen weiter; mehr als 11 200 bekannte Fälle werden noch untersucht. Die Behörden nahmen mindestens 42 000 Demonstranten und Aktivisten fest, darunter 325 Kinder. Anwälte, Aktivisten, Journalisten und normale Bürger werden weiterhin inhaftiert oder getötet. Es gibt Hinweise auf Kopfschüsse und das Verschwinden von verwundeten Demonstranten in Krankenhäusern – zugleich ist der größte Teil des Landes weiterhin von der Außenwelt abgeschnitten.

Seit über einem Jahrzehnt gibt die Islamische Republik Milliarden Euro für ein Internet aus, das auf Überwachung, Zensur und zentralisierte Kontrolle ausgelegt ist.

Die Internetsperre der Islamischen Republik hat nicht nur die Iraner zum Schweigen gebracht. Sie hat die darauf folgende staatliche Gewalt ermöglicht. Seit über einem Jahrzehnt gibt die Islamische Republik Milliarden Euro für ein Internet aus, das nicht auf Offenheit, sondern auf Überwachung, Zensur und zentralisierte Kontrolle ausgelegt ist. Das von iranischen Politikern als *National Information Network* (NIN) bezeichnete System wurde von Chinas *Great Firewall* inspiriert und bewusst

durch öffentlich-private Partnerschaften entwickelt, um dem Staat die entscheidende Kontrolle über Internetzugang und Telekommunikation zu geben. Infolgedessen sind Millionen von Websites im Iran gesperrt, darunter Plattformen wie Instagram und Telegram. Irans Bürger werden für grundlegende Dienste wie Bildung, Zahlungen und Bankgeschäfte auf inländische Anwendungen wie Rubika verwiesen, die mit Überwachungsfunktionen ausgestattet sind.

Diese Kontrolle ist strukturell angelegt. Das iranische Inlandsnetzwerk ist nur über zwei von der Regierung kontrollierte Gateways mit dem globalen Internet verbunden. Die Behörden können daher die internationale Konnektivität drosseln oder unterbrechen und zugleich begrenzte interne Dienste aufrechterhalten. Das *National Information Network* (NIN) wird mit Sicherheitstools wie *Deep Packet Inspection* kombiniert, Mobilfunknetze werden landesweit manipuliert und der verschlüsselte Datenverkehr wird gezielt gestört. Das System ermöglicht dem Staat, die Gesellschaft mit bemerkenswerter Präzision zu isolieren, wodurch wirtschaftliche Auswirkungen minimiert werden und gleichzeitig maximale politische Kontrolle möglich ist.

Mit dieser Infrastruktur schaltet die Islamische Republik das Internet routinemäßig ab, wenn es sich in der Krise wähnt, ob bei Protestbewegungen, bei Wahlen oder im Kriegsfall. Der Blackout im Januar 2026 zeigt, worauf dieses System logisch hinausläuft. Ein System, das täglich zur Filterung von Informationen und zur Überwachung der Bürger eingesetzt wird, wurde zu einem Instrument der Massengewalt. Denn durch die Unterbrechung der Kommunikation wurden Demonstranten isoliert, Journalisten zum Schweigen gebracht und Beweise unterdrückt. Dadurch wurden Bedingungen geschaffen, unter denen die Sicherheitskräfte nahezu straffrei handeln konnten. Wie der UN-Sonderberichterstatter für Menschenrechte im Iran gewarnt hat, könnten die daraus resultierenden Missbräuche Verbrechen gegen die Menschlichkeit darstellen. Für Europa sollte klar sein: Digitaler Autoritarismus ist tödlich.

Er ist auch transnational. Das iranische Modell der digitalen Unterdrückung ist kein isolierter Einzelfall. Autoritäre Regierungen beobachten sich gegenseitig genau und tauschen Technologien, Strategien und Erfahrungen aus. China exportiert seine Zensurinfrastruktur ins Ausland, und Iran und Russland tauschen sich über ihr Know-how zu Abschaltungen, Überwachung und

Informationsmanipulation aus. Jede erfolgreiche Anwendung digitaler Unterdrückungssysteme verschiebt die Grenzen dessen, was getan werden kann, ohne dass es zu nennenswerten internationalen Konsequenzen kommt.

Digitale autoritäre Praktiken, die sich einmal als wirksam erwiesen haben, breiten sich aus.

Dies stellt eine wachsende Bedrohung für die europäischen Demokratien und ihre Sicherheit dar. Digitale autoritäre Praktiken, die sich einmal als wirksam erwiesen haben, bleiben nicht auf weit entfernte Krisensituationen beschränkt. Sie breiten sich aus. Beispielsweise setzt Iran koordinierte Desinformationsnetzwerke ein und führt Einmischungsoperationen im Ausland durch, die darauf abzielen, politische Debatten in den Ländern Europas zu beeinflussen. Auch grenzüberschreitende Maßnahmen zur Cyber-Repression nehmen zu; sogar deutsche Mitglieder des Europäischen Parlaments sind zur Zielscheibe von Hacking-Kampagnen geworden, die vom iranischen Staat gefördert werden. Digitale Isolation und staatliche Kontrolle über die Kommunikation werden zu Instrumenten staatlicher Gewalt und daher führen diese Praktiken zunehmend zu Instabilität weit über die Grenzen des Iran hinaus.

Die Iraner leben seit langem mit Zensur und sind zu Experten für ihre Umgehung geworden. Jeder Iraner weiß, wie man virtuelle private Netzwerke (VPNs) nutzt, um staatliche Kontrollen zu umgehen, und viele bevorzugen verschlüsselte Messaging-Apps gegenüber den von der Regierung geförderten Plattformen. Wenn es Internet-Sperren gibt, entstehen informelle „Helfer-Communities“, die Ad-hoc-Infrastrukturen einsetzen, um Tools wie DeltaChat zu nutzen und sich womöglich über abgegrenzte Netzwerke von Starlink-Terminals zu verbinden. Diese Communities entstehen nicht spontan. Sie basieren auf Vertrauen, das über Jahre hinweg dadurch gewachsen ist, dass technisches Wissen getauscht wurde und Community-Fähigkeiten aufgebaut wurden.

Lokale Gemeinschaften im Iran und anderswo sind auf Technologien und Ressourcen angewiesen, die von einem globalen Netzwerk von Aktivisten für Internetfreiheit und digitale Rechte entwickelt wurden. Diese Gemeinschaft – bestehend aus zivilgesellschaftlichen Organisationen, Computerfachleuten, Forschern und kleinen

Unternehmen – entwickelt Anti-Zensur-Tools und Technologien zum Schutz der Privatsphäre, die autoritäre digitale Taktiken ausbremsen können. Ihre Bemühungen sind für den Schutz der Zivilbevölkerung, für unabhängige Berichterstattung und für die Frühwarnung vor Massengräueltaten von entscheidender Bedeutung. Doch dieses Ökosystem leidet unter chronischer Unterfinanzierung und ist zunehmend staatlicher Repression ausgesetzt, und das gerade zu einer Zeit, wo die Nutzung solcher Tools zwingend notwendig ist.

Digitale Autoritäre können nicht alle Kanäle gleichzeitig blockieren.

Die Unterstützung derjenigen, die sich gegen digitalen Autoritarismus wehren, erfordert eine ganzheitliche, auf verschiedene Interessengruppen ausgerichtete Strategie, deren Schwerpunkt auf Resilienz durch Vielfalt liegt. Das bedeutet, in ein breites Portfolio jeweils unvollkommener, aber sich ergänzender Tools zu investieren: dezentrale Messaging-Anwendungen, anpassungsfähigere VPN-Technologien, Tech-Support für digitale Sicherheit, Satellitenkonnektivität und nachhaltiger Aufbau von technischen Kapazitäten in den Communities. Digitale Autoritäre können nicht alle Kanäle gleichzeitig blockieren. Ein diversifizierter Ansatz erhöht die Kosten der Zensur exponentiell und zwingt Regime dazu, immer mehr politisches und finanzielles Kapital aufzuwenden, um die Kontrolle aufrechtzuerhalten.

Deutschland und die Europäische Union befinden sich in einer guten Position, um zu handeln. Über Besorgniserklärungen hinaus sollte Europa eine kohärente Strategie für digitale Rechte entwickeln, die eine nachhaltige Unterstützung für die Technologien und Gemeinschaften institutionell verankert, damit Menschen unter repressiven Bedingungen miteinander in Verbindung bleiben können. Dazu gehören die Finanzierung der Wartung bestehender Tools, die Stärkung der Gemeinschaften, die diese Technologien in der Praxis nutzbar machen, und die Unterstützung der Forschung zu neuen Zensurtechniken.

Die Internetsperre im Iran und die durch sie ermöglichten Morde waren eine Tragödie für die Bevölkerung Irans. Sie sollten auch Europa als Warnung dienen.



Fereidoon Bashar
Berlin

Fereidoon Bashar ist Geschäftsführer von *ASL19*, einer Technologie- und Exilmedienorganisation, die sich dem Kampf gegen digitalen Autoritarismus verschrieben hat. Er arbeitet daran, Bedrohungen für die Zivilgesellschaft im Iran zu bekämpfen, indem er gemeinsam mit und für verschiedene Gemeinschaften Lösungen entwirft und entwickelt.



Mani Mostofi

Mani Mostofi ist Jurist, Völkerrechtsexperte und Menschenrechtsaktivist mit langjähriger Erfahrung in der internationalen Menschenrechtsarbeit. Er leitete unter anderem *Advocacy*- und Forschungsprojekte bei UN-nahen Initiativen sowie bei *Human Rights Watch* und ist heute Direktor von *Miaan*.



Hanna Voss
Beirut

Hanna Voss war Redakteurin für die *taz am Wochenende* und ist nun im Auslandsbüro der Friedrich-Ebert-Stiftung in Beirut tätig.