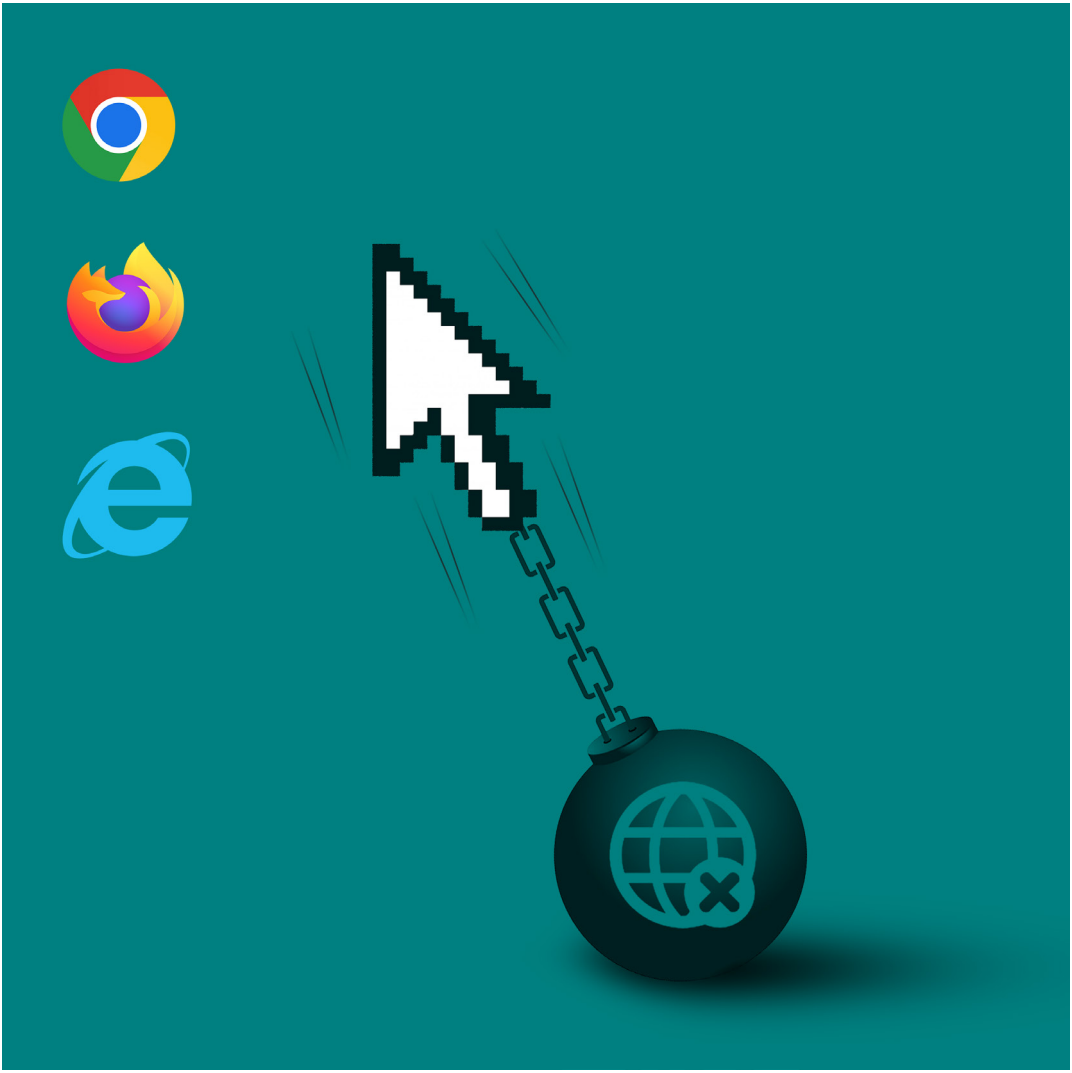

خاموشی اینترنت در ایران

نگاهی به نقض حقوق بشر در ایران

توانا
TAVAANA

خاموشی اینترنت در ایران

نگاهی به نقض حقوق بشر در ایران

توانا
TAVAANA
آموزشکده آنلاین
برای جامعه مدنی ایران
e-collaborative
for civic education

www.tavaana.org

پروژهٔ

e-collaborative
for civic education

www.eciviced.org

خاموشی اینترنت در ایران

نگاهی به نقض حقوق بشر در ایران

ناشر: E-Collaborative for Civic Education

زمستان ۱۴۰۲

---

e-collaborative
for civic education

ECCE (E-Collaborative Civic Education) یک سازمان غیرانتفاعی در ایالات متحده آمریکا تحت 501c3 است که از فناوری اطلاعات و ارتباطات برای آموزش و ارتقای سطح شهروندی و زندگی سیاسی دموکراتیک استفاده می‌کند.

ما به عنوان بنیان‌گذاران و مدیران این سازمان اشتیاق عمیق مشترکی داریم که شکل‌دهنده ایده‌های جوامع باز است. همچنین برای ما، شهروند، دانش شهروندی، مسئولیت و وظیفه شهروندی یک فرد در محافظت از جامعه سیاسی دموکراتیک پایه و اساس کار است؛ همان‌طور که حقوق عام بشر که هر شهروندی باید از آن‌ها برخوردار باشد، اساسی و بنیادی هستند. ECCE دموکراسی را تنها نظام سیاسی قادر به تأمین طیف کاملی از آزادی‌های شهروندی و سیاسی برای تک‌تک شهروندان و امنیت، برابری و عدالت می‌داند. ما دموکراسی را مجموعه‌ای از ارزش‌ها، نهادها و فرایندها می‌دانیم که مبشر صلح، توسعه، تحمل و مدارا، تکثرگرایی و جوامعی شایسته‌سالار است که به کرامت انسانی و دستاوردهای انسانی ارج می‌گذارند.

ما پروژه اصلی ECCE یعنی «آموزشکده توانا: آموزشکده مجازی برای جامعه مدنی ایران» را در سال ۲۰۱۰ تاسیس کردیم. آموزشکده توانا در ارائه منابع و آموزش در دنیای مجازی در ایران، یک نهاد پیشرو است. توانا با ارائه دوره‌های آموزشی زنده در حین حفظ امنیت و با ناشناس‌ماندن دانشجویان، به یک جامعه آموزشی قابل اعتماد برای دانشجویان در سراسر کشور تبدیل شده است. این دروس در موضوعاتی متنوع مانند نهادهای دموکراتیک، امنیت دیجیتال، حقوق زنان، وب‌نویسی، جدایی دین و دولت و توانایی‌های رهبری ارائه می‌شوند. آموزشکده توانا آموزش زنده دروس و سمینارهای مجازی را با برنامه‌هایی مثل مطالعات موردی در جنبش‌های اجتماعی و گذارهای دموکراتیک، مصاحبه با کنشگران و روشنفکران، دستورالعمل‌های خودآموز، کتابخانه مطالب توصیفی، ابزارهای کمکی و راهنمایی برای آموزشگران ایرانی و حمایت مداوم و ارائه مشاوره آموزشی برای دانشجویان تکمیل کرده است.

تلاش ما برای توسعه توانایی‌های آموزشکده توانا متوجه گردآوردن بهترین متفکران ایران و صداهای حذف‌شده است. به همین ترتیب، به دنبال انتشار و ارتقای آثار مکتوب روشنفکران ایرانی هستیم که ایده‌های آنان در جمهوری اسلامی ممنوع شده است.

یکی از نقاط تمرکز تلاش توانا، ترجمه متون کلاسیک دموکراسی و مقالات معاصر در این باره و نیز ترجمه آثار مرتبط با جامعه مدنی، حقوق بشر، حاکمیت قانون، روزنامه‌نگاری، کنشگری و فناوری اطلاعات و ارتباطات است. امید ما این است که این متون بتواند سهمی در غنای فردی هم‌وطنان ایرانی و برساختن نهادهای دموکراتیک و جامعه‌ای باز در ایران داشته باشد.

سپاسگزار بازتاب نظرات و پیشنهادهای شما!

فهرست

مقدمه

قطع اینترنت در هر کشوری توسط حکومت حاکم بر آن کشور به منظور پنهان‌سازی شدت نقض حقوق بشر در آن کشور صورت می‌گیرد. حکومت‌های ناقض حقوق بشر، چون جمهوری اسلامی، برای قطع ارتباطات آنلاین شهروندان خود با سراسر دنیا و جلوگیری از انتشار اخبار درگیری‌های سیاسی، به دفعات و به شیوه‌های گوناگون دست به قطع اینترنت زده‌اند و می‌زنند.

در واقع قطع اینترنت توسط حکومت‌هایی چون جمهوری اسلامی، یک فضای امن برای آنان فراهم می‌کند تا بتوانند اقدامات فاحش ناقض حقوق بشر را به آسودگی و پنهان از انظار جامعه جهانی انجام دهند. بدیهی است که این اقدام، حکومت‌ها را به استبداد نزدیک‌تر و از پاسخ‌گویی دورتر می‌کند. این در حالی است که وظیفه‌ی بنیادین حکومت‌ها پاسداری از حقوق اولیه شهروندان و پاسخگویی در قبال آن است نه اینکه هم این حقوق را نقض کنند و هم از پاسخگویی اجتناب کنند.

ما در این کتابچه به صورت خلاصه قطع اینترنت توسط جمهوری اسلامی را بررسی می‌کنیم و خشونت صورت‌گرفته در خلال قطعی اینترنت را نیز از نظر خواهیم گذراند.

قطع اینترنت یعنی چه؟

«قطع اینترنت» شامل مجموعه گسترده‌ای از انواع مداخله‌ها و محدودیت‌ها در ارتباطات و فناوری‌های پایه‌ای است. این موارد می‌تواند از طریق مکانیزم و راه‌های مختلفی انجام شود؛ از آسیب‌زدن به زیرساخت‌های اساسی ارتباطی و غیرفعال‌کردن آن گرفته تا مداخله در اطلاعات مسیریابی، دستکاری در سیستم نام دامنه‌ها، پیاده‌سازی یا الزام استفاده از مکانیزم‌های فیلترینگ یا DPI عمیق و کاهش سرعت پهنای باند.

روش‌های فنی که در هر قطع اینترنت انجام می‌شود، بسته به نوع زیرساخت ارتباطی محلی، درجه مرکزیت یا کنترل حکومت بر آن زیرساخت و تاثیری که قطع اینترنت روی یک منطقه جغرافیایی خاص و محدوده خدمات ارتباطی دارد، متفاوت است. برخی از روش‌های قطع اینترنت سخت‌تر قابل تشخیص و اثبات هستند یا در معرض بازرسی و نظارت خارجی قرار ندارند؛ مسئله‌ای که دست حکومت‌ها را برای کنترل ارتباطات شهروندان بازتر می‌کند و آن‌ها با خیال راحت به کار خود ادامه می‌دهند.

تعریف‌های مختلفی از قطع اینترنت وجود دارد که بر اساس آن گروه‌های مختلف، هدف‌های مختلفی را دنبال می‌کنند. این اقدامات که مشخصا توسط حکومت یا به نیابت از حکومت برای قصد مشخصی صورت می‌گیرد، دسترسی به سیستم‌های ارتباطی آنلاین را به طور عمدی مختل می‌کند.

قطع اینترنت در حقیقت مجموعه اختلالاتی است که در سیستم‌های الکترونیکی

ارتباطی اصلی ایجاد می‌شود تا ارتباط شهروندان برای انتشار اطلاعات قطع شود و به طور کلی جریان اطلاعات از سوی حکومت کنترل شود.

قطع اینترنت و نقض حقوق بشر

خاموشی اینترنت یا محدودسازی دسترسی شهروندان به آن، تاثیرات مخرب بسیاری دارد. از جمله به‌شدت آزادی بیان و دسترسی به اطلاعات را محدود و حقوق شهروندان را نقض می‌کند. حقوقی مانند حق شرکت در تجمعات و حق شرکت در امور عمومی از جمله انتخابات آزاد و منصفانه.

علاوه بر این، خاموشی اینترنت تاثیراتی منفی بر حقوق اقتصادی، اجتماعی و فرهنگی افراد دارد. می‌تواند کار و روش زندگی افراد را بر هم بزند و منجر به این شود که افراد نتوانند کسب درآمد و تجارت کنند یا دسترسی شهروندان به منابع آنلاین آموزشی را محدود کند. همچنین از دسترسی به خدمات بهداشتی، درمانی و دیگر خدمات ضروری جلوگیری می‌کند و تاثیرات منفی بر سلامت روحی و روانی افراد می‌گذارد.

حکومت‌ها با این کار توانایی افراد را در برگزاری تجمعات و تشکیل اجتماعات در زمینه‌های مختلف محدود می‌کنند و امنیت و رفاه آن‌ها را مستقیما به خطر می‌اندازند.

مجموع این مشکلات به‌ویژه به شهروندانی که در مناطق کم‌تر توسعه‌یافته زندگی می‌کنند و به زیرساخت‌های ارتباطی ضعیفی دسترسی دارند، آسیب می‌زند.

قطع اینترنت به همین ترتیب می‌تواند موجب افزایش درصد خطراتی چون نشر اطلاعات غلط، انتشار شایعات و افزایش ناامنی در مناطقی شود که در معرض آسیب‌هی ناشی از بحران‌های امنیتی قرار دارند. به علاوه در برخی موارد، قطع اینترنت عامل

پنهان‌کردن اسناد و مدارک جنایات جنگی و نقض حقوق بشر می‌شود که در نتیجه‌ی آن شکاف میان حکومت و مردم افزایش پیدا می‌کند.

در ایران نیز جمهوری اسلامی با قطع اینترنت در شرایطی چون اعتراضات سراسری، انتخابات، بحران‌های امنیتی و اضطرابات اجتماعی ناشی از سیاست‌های خود، حقوق بشر را به‌شدت نقض می‌کند.

تاریخچه قطعی اینترنت در ایران

مقامات جمهوری اسلامی از سال‌ها پیش از اجرای طرح «شبکه ملی اطلاعات»، با استفاده از تدابیر به ظاهر قانونی و سیاست‌های خود، اقدام به کنترل بسترهای ارتباط اینترنتی و زیرساخت‌های مخابراتی در مواقع بحرانی کرده‌اند. تشکیل «شورای عالی فضای مجازی» و توسعه «شبکه ملی اطلاعات» (NIN) یکی از این اقدامات است.

شبکه ملی اطلاعات، یک شبکه داخلی و حکومتی است که شامل پلتفرمی برای به‌اشتراک‌گذاری ویدیو، موتور جستجو، نرم‌افزارهای پیام‌رسان، سرویس ایمیل و نرم‌افزارهای تجارت الکترونیک محلی می‌شود.

جمهوری اسلامی با بستن اینترنت به روی شهروندان هم‌زمان با اعتراضات و تجمعات سراسری، فشار را بر آن‌ها بیش‌تر می‌کند. از برجسته‌ترین نمونه‌های قطع اینترنت توسط حکومت می‌توان به قطع کامل اینترنت در سراسر کشور هم‌زمان با اعتراضات سراسری شهروندان علیه افزایش قیمت بنزین در ۲۵ آبان ۱۳۹۸(۱۶ نوامبر ۲۰۱۹) اشاره کرد؛ اعتراضاتی که به گزارش خبرگزاری رویترز، به نقل از سه تن از مقامات جمهوری اسلامی، حدود ۱۵۰۰ نفر در جریان آن به دست نیروهای سرکوبگر حکومت کشته شدند. از این میان سازمان حقوق بشری عفو بین‌الملل هویت ۳۰۴ نفر از کشته‌شدگان را احراز و اسناد آن را منتشر کرد.

نمونه دیگر، قطع اینترنت در استان سیستان‌وبلوچستان در پی تجمعات اعتراضی

شهروندان علیه کشتار ۱۰ شهروند توسط نیروهای امنیتی در بهمن ۱۳۹۹ است.

در شهریور ۱۴۰۱ (سپتامبر ۲۰۲۲) نیز گونه‌ای جدید از قطع اینترنت در ایران آغاز شد؛ ۲۵ شهریور مهسا (ژینا) امینی به دلیل آنچه «عدم رعایت حجاب مناسب» از سوی حکومت عنوان می‌شود، توسط «پلیس امنیت اخلاقی» بازداشت و بر اثر ضرب‌وشتم کشته شد. این اتفاق اعتراضات بسیاری را در سراسر کشور به دنبال داشت. اعتراضاتی که در ریشه در نارضایتی‌های بلندمدت از سیاست‌ها و رفتارهای غیرانسانی حکومت داشت که شامل رفتارهای زن‌ستیزانه‌ی آن نیز می‌شد. پیرو چنین رخدادی و با سراسری‌شدن خیزش در کشور، اینترنت با استفاده از تکنیک‌های پیشرفته‌ای قطع شد که به برخی از آن‌ها اشاره می‌کنیم.

- اخلال شدید در سرویس‌های تلفن همراه؛ شامل شرکت‌های ارتباطات همراه ایران، رایتل، ایرانسل و مبین‌نت
- قطع اینترنت منطقه‌ای و اعمال محدودیت بر آن؛ به عنوان نمونه در استان‌های کردستان، خوزستان و سیستان‌وبلوچستان
- مسدودکردن پروتکل‌های انتقال داده‌های وب با امنیت بالا
- مسدودکردن سیستم‌های رمزگذاری‌شده نام دامنه (DNS)
- مسدودکردن آخرین پلتفرم‌های رسانه‌های اجتماعی در دسترس در ایران، از جمله «اینستاگرام»، «واتس‌اپ»، «لینکدین» و «اسکایپ»
- مسدودکردن «اپ‌استور» و «گوگل‌پلی» و محدودکردن دانلود برنامه‌های VPN

این اختلالات اینترنت، کار را برای ایرانیان دشوارتر کرده و آن‌ها را در به‌اشتراک‌گذاری شواهدی از سرکوب اعتراضات صلح‌آمیز توسط نیروهای سرکوب محدودتر کرده و همچنین امنیت فعالیت‌های آن‌ها را با مشکلات بیشتری مواجه کرده است. جمهوری اسلامی همچنین پیش از این خدمات اینترنتی ناامن خود را نیز گسترانده بود که به صورت کلان در قالب پروژه «شبکه ملی اطلاعات» تعریف می‌شوند؛ مانند پلتفرم «آپارات»، نسخه داخلی یوتیوب در ایران و نیز پلتفرم «روبیکا». در هر دو فضای مورد ذکر، جمهوری اسلامی دخالت و نظارت دارد.

با این حال، در میانه مهرماه ۱۴۰۱، محدودیت شبانه‌روزی از اپراتورهای شبکه همراه برداشته شد، اما اپ‌استورها، اپلیکیشن‌ها و پلتفرم‌های رسانه‌ها و شبکه‌های اجتماعی

همچنان مسدود هستند.

البته که جدای از این محدودیت‌ها اینترنتی بایستی به این نکته اشاره کرد که قتل مهسا امینی به‌تنهایی نقض جدی حقوق شخصی او محسوب می‌شود؛ حقوقی چون حق آزادی و امنیت شخصی، حق آزادی از شکنجه و برخورد غیرانسانی، حق دادگاهی عادلانه و حق زندگی.

بر اساس آخرین گزارش سازمان حقوق بشر ایران در فروردین ۱۴۰۲ نیروهای امنیتی طی خیزش انقلابی سال ۱۴۰۱ در ۲۳ استان کشور، ۵۳۷ تن را به قتل رسانده‌اند که دست‌کم ۴۸ تن از کشته‌شدگان زن و ۶۸ تن کودک (زیر ۱۸ سال) بوده‌اند.

سازمان حقوق بشری عفو بین‌الملل نیز شواهد فراوانی از شکنجه، بدرفتاری و خشونت جنسی علیه معترضان توسط نیروهای امنیتی را مستند کرده است. رفتار جمهوری اسلامی توسط جامعه بین‌المللی به عنوان مصداقی از نقض تعهدات بین‌المللی حقوق بشری محکوم شده است و بسیاری از دولت‌ها و ائتلاف‌ها از مقامات جمهوری اسلامی خواسته‌اند که خشونت را متوقف کنند و دسترسی کامل به اینترنت را بازگردانند.

قطعی اینترنت از سال ۱۳۹۴ به بعد، بنا موارد مختلفی از جمله اعتراضات، انتخابات و جلوگیری از نفوذ هکرها چندین بار در ایران رخ داده است.

مروری بر تاریخچه مختصر قطعی اینترنت در ایران

- شهریور ۱۴۰۱: در پی قتل مهسا امینی و در جریان انقلاب ملی ۱۴۰۱ ایران
- اسفند ۱۳۹۹: قطع اینترنت در استان سیستان‌وبلوچستان پس از کشتار ۱۰شهروند توسط نیروهای امنیتی
- آبان ۱۳۹۸: پس از اعتراضات گسترده در سراسر کشور به دلیل افزایش قیمت بنزین، جمهوری اسلامی اینترنت به طور گسترده قطع شد.
- دی ۱۳۹۶: در پی اعتراضات به اوضاع نابسامان اقتصاد، اینترنت در برخی مناطق قطع شد
- آبان ۱۳۹۶: در طول اعتراضات علیه ناکارآمدی حکومت، اینترنت در برخی مناطق کشور قطع شد
- اردیبهشت ۱۳۹۶: در طول انتخابات ریاست جمهوری، حکومت، اینترنت را با هدف

کاستن از فعالیت هکرها به صورت جزئی قطع کرد

- آبان ۱۳۹۴: پس از انفجار در بخشی از تهران، اینترنت به طور گسترده قطع شد
- تیر ۱۳۹۱: در طول مذاکرات هسته‌ای با غرب، مقامات، اینترنت را به صورت جزئی قطع کردند
- خرداد ۱۳۸۸: در طول اعتراضات گسترده مردم ایران به نتایج انتخابات ریاست جمهوری، اینترنت در برخی مناطق قطع شد

جمهوری اسلامی در چه شرایطی اینترنت را قطع می‌کند؟

بسیاری از حکومت‌ها که تصمیم به اجرای قطع اینترنت می‌گیرند، آن را به عنوان حرکتی لازم در راستای کنترل حکومت بر رسانه‌ها، روزنامه‌نگاری و فضاهای مدنی در نظر می‌گیرند. کشورهایی با حکومت‌های خودکامه‌ای که پیش از گسترش فناوری اینترنت هم سابقه بلندمدتی در کنترل اطلاعات بر اساس مصالح خود داشته‌اند، در مواقع بحرانی به قطع‌کردن اینترنت روی می‌آورند. در چنین شرایطی است که فناوری‌هایی که در دولت‌های دموکراتیک در راستای بهینه‌سازی خدمات اینترنتی به کار می‌روند به عنوان نمونه در ایرانِ تحت کنترل جمهوری اسلامی به صورت نادرست و بیش‌تر برای مختل‌کردن یا مداخله در ارتباطات اینترنتی استفاده می‌شوند؛ به ویژه که در استفاده از این فناوری‌ها در کشورهایی چون ایران تعادلی وجود ندارد و قوانین تعادل‌بخش و سودمندی در استفاده از آنان نیز وجود ندارد. به عنوان نمونه، این در مورد فناوری «بررسی بسته‌های عمیق» (deep packet inspection) نیز مشاهده می‌شود، به این معنا که محتوای بسته‌های داده، هنگام عبور از یک نقطه، بازرسی و بررسی می‌شوند. این روش در کشورهای دموکراتیک برای تشخیص سوءاستفاده از کودکان همراه با چندین مرحله کنترل و تعادل استفاده می‌شود، اما در حکومت‌های استبدادی مانند جمهوری اسلامی، به عنوان روشی برای جلوگیری از دسترسی کاربران به سایت‌ها و خدمات اینترنتی حاوی

سخنان سیاسی-انتقادی در مخالفت با حکومت به کار می‌رود.

در جمهوری اسلامی، بیش‌ترین احتمال قطعی اینترنت زمانی است که حکومت با تجمعات و اعتراضات مردمی خیابانی روبه‌رو می‌شود و احتمال شکست خود را مقابل آن بالا می‌بیند. همچنین در شرایطی که اعتراضات درباره‌ی مسائل اجتماعی و سیاسی از جمله بیکاری، فساد و نارضایتی‌های مربوط به امور داخلی کشور، در فضای مجازی جلوه گسترده‌ای پیدا کند، باز هم ممکن است به این روش روی آورد. بنابراین حکومت از قطع اینترنت می‌تواند به عنوان یک ابزار برای محدودکردن دسترسی به اطلاعات و برای جلوگیری از افشای نقض حقوق بشر در ایران استفاده کند.

سازمان‌های مدنی و حقوق بشری برای مبارزه با قطع اینترنت در ایران چه باید کنند؟

۱- اطلاع‌رسانی به نهادهای بین‌المللی: سازمان‌های مدنی برای جلب توجه جهانی به قطع اینترنت در ایران، می‌توانند به ارائه اطلاعات دقیق و صحیح به نهادهای بین‌المللی در زمینه قطع اینترنت و نقض حقوق بشر بپردازند.

۲- فشار بر جمهوری اسلامی با امضای توافقنامه‌های بین‌المللی: دولت‌ها و سازمان‌های بین‌المللی می‌توانند از طریق سیاست فشار، نظارت بر جمهوری اسلامی را افزایش دهند و آن را مجبور به پاسخگویی کنند؛ به ویژه که جمهوری اسلامی بسیاری از این توافقنامه‌های بین‌المللی در حمایت از حقوق بشر و آزادی‌های اساسی را امضا کرده است ولی از اجرای آن تن می‌زند.

۳- ایجاد فشار از طریق رسانه‌ها: رسانه‌ها می‌توانند برای جلب توجه عمومی به این موضوع تلاش کنند و اطلاعات دقیق و صحیح در زمینه قطع اینترنت و تخلفات حقوق بشر در ایران منتشر کنند.

۴- ارائه ابزارهای ضروری ارتباطی به شهروندان ایرانی: سازمان‌های مدنی و دولت‌ها

می‌توانند به صورت مستقیم به مردم ایران ابزارهای امنیتی و ابزارهای ارتباطی مانند VPN ارائه کنند تا بتوانند با قطع اینترنت مقابله کنند.

۵- ارتباط با سازمان‌های داخلی: سازمان‌های مدنی و دولت‌ها می‌توانند با سازمان‌های فعال داخل ایران در ارتباط باشند و برای مقابله با قطع اینترنت و تخلفات حقوق بشری با آن‌ها همکاری کنند.

حکومت‌ها چگونه اینترنت را قطع و منابع را فیلتر می‌کنند؟

در جمهوری اسلامی، قطع دسترسی به اینترنت به گونه‌های مختلف صورت می‌گیرد؛ از جمله استفاده از فیلترینگ برای سانسور محتوا، فیلترینگ DNS برای دسترسی به سایت‌های خارجی، قطع کلی اینترنت و قطع دسترسی به شبکه‌های اجتماعی و پیام‌رسان‌ها. به علاوه در برخی موارد، سرعت اینترنت به‌شدت محدود می‌شود به طوری که دسترسی به برخی از سایت‌ها و خدمات آنلاین برای کاربران دشوار و ناممکن می‌شود.

عموما قطع اینترنت توسط حکومت‌ها به صورت قطع کلی اینترنت یا با مسدودکردن شبکه‌های اجتماعی انجام می‌شود. یکی دیگر از تاکتیک‌ها، محدودکردن سرعت اینترنت است؛ به گونه‌ای که سرعت اینترنت آن‌قدر محدود شود که هرگونه ارتباط غیر متنی، مانند پخش زنده فیلم از تظاهرات - و فعالیت‌هایی از این دست - غیرممکن شود.

سرویس‌دهندگان اینترنت (ISP)[1] برای اجرای محدودیت‌ها - پس از درخواست حکومت‌ها - از روش‌های زیر استفاده می‌کنند:

قطع شبکه

سازمان‌های حکومتی از روش‌هایی مانند اجبار آی.اس.پی‌ها و شرکت‌های موبایل به

1. Internet Service Provider.

خاموش‌کردن مدارهای شبکه ارتباطات کشور برای مسدودکردن دسترسی به اینترنت استفاده می‌کنند.

حکومت‌هایی که کنترل کاملی بر شبکه کشور خود دارند، ممکن است همچنین «دکمه خاموش‌کننده اینترنت» نصب کنند. سازمان ملل متحد استفاده از چنین مکانیزمی برای خاموشی فضای اینترنتی را محکوم کرده است.

اختلال و تغییرات در پروتکل BGP

BGP یا Border Gateway Protocol یکی از اصلی‌ترین پروتکل‌های استفاده‌شده در شبکه‌های اینترنت است که برای انتقال بسته‌های داده بین شبکه‌ها استفاده می‌شود.

تغییرات در پروتکل BGP می‌تواند موجب ایجاد مشکلاتی چون تغییر مسیر بسته‌های داده شود که در برخی موارد می‌تواند به اختلال در ارتباطات اینترنتی منجر شود.

در ایران، چندین بار در گذشته تغییراتی در پروتکل BGP رخ داده که موجب اختلال در ارتباطات اینترنتی شده است. این نوع اختلالات و تغییرات در پروتکل BGP برای کاربران اینترنتی در ایران موجب مشکلاتی مانند عدم دسترسی به سایت‌های مورد نظر یا کاهش سرعت ارتباطات می‌شود.

مسدودکردن آدرس آی.پی

وب‌سایت‌ها و برنامه‌ها برای میزبانی محتوای خود از سرورهای وب استفاده می‌کنند که هر یک از آن‌ها یک آدرس آی.پی منحصربه‌فرد دارد. این آدرس عددی منحصربه‌فرد است و به دستگاه‌ها اجازه می‌دهد که یکدیگر را پیدا کرده و با یکدیگر ارتباط برقرار کنند.

سرویس‌دهنده‌های اینترنت می‌توانند لیستی از آدرس‌های IP را (همراه با خدماتی که برای مسدودسازی مدنظر دارند) ایجاد کنند و سپس تمام ترافیک اینترنت «به آن» یا «از آن» آدرس‌ها را مسدود کنند. از آنجایی که چندین وب‌سایت و خدمات می‌توانند روی یک آدرس آی.پی مشترک منتشر شوند، این روش از سانسور اینترنتی معمولا موجب می‌شود که دایره‌ی مسدودسازی عملا فراتر از آن هدف اولیه برود و موجب دردسرهای بیشتر برای کاربران اینترنت شود.

فیلترینگ DNS

فیلترینگ DNS شبیه به مسدودسازی IP عمل می‌کند؛ اما دقیق‌تر است به این دلیل که به جای آدرس آی.پی، به Domain Name (نام دامنه) حمله می‌کند. برای نمونه در xyz.com، نام دامنه‌ها در یک پایگاه داده‌ی توزیع‌شده در چندین سرور DNS ذخیره می‌شوند. مرورگرها به دستگاه‌های واسطه به نام DNS resolver نیاز دارند تا برای آدرس‌های URL[1] مشخص، در این پایگاه‌های داده جستجو کنند و آدرس مقصد مورد نظر را بازیابی کنند. ارائه‌دهندگان اینترنت امکان دستکاری در این DNS resolver را دارند تا برای برخی جستجوهای DNS، اطلاعات نادرستی بازگردانده شود، مانند عدم وجود twitter.com. در این صورت کاربران معمولا به جای بارگذاری صفحه وب یا برنامه، با یک صفحه خطا مواجه می‌شوند.

استفاده از DPI

DPI به بررسی محتوای کامل بسته‌های داده‌ای که ترافیک اینترنتی را تشکیل می‌دهند، می‌پردازد تا امکان مسدودکردن محتوا یا برنامه‌های خاصی را فراهم کند. دی.پی.ای، دستگاه‌هایی هستند که بین کاربران و در کل اینترنت به عنوان میان‌جعبه‌ها شناخته می‌شوند و نقش مهمی در فیلترینگ اینترنت داشته‌اند؛ مانند فیلترینگ در چین. شرکت‌هایی مانند Huawei و Allot تولیدکنندگان دستگاه‌های DPI هستند.

DPI همچنین در کاهش سرعت برای نوع خاصی از ترافیک مانند ویدئو یا Voice Over Internet Protocol) VOIP) بسیار مؤثر است.

این روش موجب شده است که وی.پی.ان‌هایی که در چین کار می‌کنند، می‌بایست حتما از تکنولوژی‌هایی مانند تاریک‌سازی ترافیک استفاده کنند تا بتوانند امکان تاثیر DPI را بلاموضوع کنند.

مسدودکردن پروتکل

حکومت‌ها می‌توانند از این روش برای مسدودکردن خدمات پیام‌رسان‌های فوری مانند

1. Uniform Resource Locator.

پیام‌رسان تلگرام یا ایمیل استفاده کنند تا از ارتباط مردم جلوگیری کنند.

راه‌حل‌هایی برای دورزدن فیلترینگ و مقابله با جدایی کامل از دنیای دیجیتال

متاسفانه در صورت قطعی کامل اینترنت، امکان دسترسی به اینترنت به هیچ شکلی وجود ندارد. با این حال، هنوز راه‌حل‌هایی برای جلوگیری از جدایی کامل از دنیای دیجیتال وجود دارند.

تحریم شبکه اجتماعی و مسدودکردن محتوای آنلاین از اشکال رایج در سانسور اینترنت هستند که با استفاده از ابزارهای مناسب قابل دورزدن هستند. در ادامه به بررسی برخی از مهم‌ترین ابزارها برای دورزدن محدودیت اینترنتی می‌پردازیم:

VPN و فیلترشکن‌ها

یک وی.پی.ان با رمزنگاری اتصال اینترنت کاربر و تغییر آدرس آی.پی او عمل می‌کند، مگر اینکه ارائه‌دهنده خدمات اینترنت قادر باشد تمام آدرس‌های آی.پی مورد استفاده توسط سرویس وی.پی.ان را مسدود یا ترافیک آن را شناسایی و مسدود کند. در غیر این صورت یک وی.پی.ان به کاربر امکان دسترسی آسان به سایت‌ها و برنامه‌هایی را می‌دهد که با استفاده از فیلترینگ IP و DNS مسدود شده‌اند.

حکومت‌ها در زمان قطع شبکه‌های اجتماعی، اغلب تلاش می‌کنند برنامه‌های VPN را نیز مسدود کنند. بنابراین برای هر شخصی که تحت سلطه این رژیم‌ها زندگی می‌کند،

مهم است که پیش از وقوع قطع اینترنت، یک VPN معتبر و قابل اعتماد که در کشورش کار می‌کند را دانلود کند.

قطع‌کنندگان اینترنت، در برخی مواقع برای قطع شبکه اینترنت نیز از مسدودکردن پروتکل استفاده می‌کنند تا از استفاده از وی.پی.ان برای دورزدن قطعی اینترنت جلوگیری کنند. اما آن دسته از سرویس‌های وی.پی.ان که از تکنیک‌های پنهان‌سازی استفاده می‌کنند، همچنان کار خواهند کرد.

پس از کشته‌شدن مهسا امینی توسط پلیس جمهوری اسلامی و آغاز گسترده اعتراضات مردمی، فشار حکومت برای محدودکردن دسترسی آزاد به اینترنت بیش‌تر و بیش‌تر شد، تا جایی که استفاده از ابزارهای بسیاری را مسدود کرد و تا مدت‌ها هم بسیاری از ابزارهای رفع فیلترینگ مسدود بودند. همچنان نیز بسیاری از وی.پی.ان‌ها کار نمی‌کنند و کاربران زیادی با مشکلات جدی برای دسترسی آزاد به منابع و اپلیکیشن‌ها روبه‌رو هستند.

شبکه Tor

تور یک سیستم رایگان است که منبع آن باز و قابل دسترسی است که برای امکان ارتباط ناشناس در وب طراحی شده است. نام این سیستم از نام پروژه اصلی The Onion Router گرفته شده است. تور مانند VPN، فعالیت شما را رمزنگاری می‌کند و آدرس آی.پی‌تان را پنهان می‌کند. این قابلیت، کاربران را قادر می‌کند به سرویس‌های آنلاین مسدودشده دسترسی پیدا کنند.

برای یک فعال مدنی-سیاسی یا عقیدتی در حکومتی که دست به سانسور گسترده و شدید می‌زند، ناشناس‌بودنِ کامل - که توسط تور فراهم می‌شود - ارزش تضمین سرعت و قابلیت استفاده بالایی دارد.

پیام‌رسان سیگنال (Signal)

زمانی که حکومت‌ها شبکه‌های اجتماعی را مسدود می‌کنند، معمولا پیام‌رسان‌ها شرایط بدتری را تجربه می‌کنند. این اختلالات موجب می‌شود که در کشورهایی که پیام‌رسان‌ها تنها روش قابل اعتماد ارتباطات شخصی هستند، دچار اختلال شوند و ارتباطات بین افراد

سخت و دشوار شود.

پیام‌رسان سیگنال یکی از ابزارهای امن ارتباطی است که دارای مزیت امنیتی بیش‌تری نسبت به سایر پلتفرم‌های پیام‌رسان است. برای استفاده از آن حتما اطمینان حاصل کنید که شما و هر کسی که ممکن است در طول قطعی اینترنت، بخواهید با آن‌ها تماس بگیرید، سیگنال را در دستگاه خود نصب کرده باشند.

شبکه‌های Bluetooth Mesh Networks

در زمان اعتراضات مردمی، وقتی حکومت‌ها به طور کامل اینترنت را قطع می‌کنند، افراد می‌توانند از پیام‌رسان‌های آفلاین برای ارتباط استفاده کنند. این برنامه‌ها شبکه‌های Peer-to-peer محلی ایجاد می‌کنند که در آن برای تبادل پیام‌ها و داده‌ها از بلوتوث به جای اینترنت استفاده می‌شود.

Sneakernet

اصطلاح اسنیکرنت به حرکات انسانی برای انتقال اطلاعات بین افرادی گفته می‌شود که همگی تحت تاثیر قطعی اینترنت هستند. حتی می‌تواند به قاچاق اطلاعات درباره اتفاقات کشور نیز اشاره داشته باشد.

برای این کار، اطلاعات مهم و حساس را روی درایوهای USB و یا هارد دیسک خارجی دانلود و ذخیره می‌کنند و سپس آن را به کسی که قرار است به محل گیرنده سفر کند، می‌سپارند. ایده‌آل این است فایل‌ها در این روش حتما رمزگذاری شوند.

هزینه‌های قطعی اینترنت

ردیاب هزینه‌های قطعی اینترنت ۲۰۲۳، نشان می‌دهد که تا آوریل ۲۰۲۳ بیش از ۲۰ کشور در سراسر جهان با قطعی اینترنت مواجه شده‌اند. بر اساس یافته‌های این ردیاب، هزینه کلی این قطعی‌ها بیش از ۹۰۰ میلیون دلار آمریکا تخمین زده شده است.

قطعی اینترنت در این کشورها در اغلب موارد به دلیل اعتراضات و اعتصابات عمومی، انتخابات، فشارهای سیاسی یا درگیری‌های نظامی اتفاق افتاده است. این قطعی‌ها موجب اختلال در اقتصاد، آسیب به پایه‌های حقوق بشر، تخریب زیرساخت‌های فنی و ازبین‌رفتن شغل‌های بسیاری شده است.

Rank	Country	Total Cost	Duration (Hrs)	Internet Users Affected	Peaceful Protest	Free & Fair Elections	Press Freedom
1	Ethiopia	$110.2 million	1,224	29.8 million	✗		
2	Myanmar	$42.7 million	3,120	23.7 million	✗	✗	✗
3	Iraq	$35.7 million	64	20.6 million			
4	India	$33.5 million	240	9.9 million	✗		
5	Turkey	$5.8 million	12	70 million			
6	Iran	$1.4 million	32	26.4 million	✗		
7	Mauritania	$0.9 million	10	1.7 million			
8	Suriname	$0.1 million	12	0.4 million	✗		

همان‌گونه که در جدول بالا می‌بینند، هزینه‌های قطعی اینترنت برای حکومت در ایران کم نیست ولی ترجیح جمهوری اسلامی سرکوب و جلوگیری از انتشار آزاد اطلاعات است.

منابع

- «گزارش ۲۰۰ روزه از سرکوب اعتراضات سراسری»، سازمان حقوق بشر ایران، ۱۵ فروردین ۱۴۰۲.
- «قطع اینترنت»، دویچه وله فارسی.
- "How Iran Is Using the Protests to Block More Open Internet Access", Sophie Bushwick; The Scientific American; October 13, 2022.
- "A Web of Impunity: The killings Iran's shutdown hid"; Amnesty.
- "Shutdown Monitor: What is Happening in Sistan and Baluchestan?"; Filter Watch; February 26, 2021.
- "We are risking death: Iranians on Mahsa Amini protests"; The Guardian; September 23, 2022.
- "Iran protests reach 19 cities despite internet disruption"; Jon Gambrell; PBS; October 12, 2022.
- "Tactics of repression :How Iran is trying to stop Mahsa Amini protests"; Joyce Sohyun Lee, Stefanie Le, Atthar, Mirza & Bebash Dehghanpisheh; The Washington Post; October 5, 2022.
- "Technical multi-stakeholder report in Internet shutdowns"; OONI, IODA, M-Lab, Cloudflare, Kentik, Censored Planet, ISOC, Article19, OONI; November 29, 2022.
- "Iran blocks social media, app stores and encrypted DNS amid

Mahsa Amini protests"; Simone Basso, Maria Xynou, Arturo Filastò and Amanda Meng; OONI; November 29, 2022.

- "Suppressing Dissent: The Rise of the Internet Curfew"; Doug Madory and Peter Micek; Kentik; November 16, 2022.
- "Iran protests: Government uses internet 'kill-switch' as tech savvy youth continue to evade digital censorship"; Sanya Burgess; Sky News; October 18, 2022.
- "Hacked Documents: How Iran Can Track And Control Protesters' Phones"; Sam Biddle, Murtaza Hussain; The Intercept; October 28, 2022.
- "Whatever it takes›: Iran crackdown killed 1,500"; Reuters; December 24, 2019.
- "Iran's Internet Blackouts Are Part of a Global Menace"; Yasmin Green; WIRED; October 19, 2022.
- "Cost of Internet Shutdowns"; Samuel Woodhams, Simon Migliano; Top10VPN; April 24, 2023.