



اندیشکده فرهنگ و توسعه

یادداشت



نویسنده: ایرنه پوترانتو

منبع انتشار: کارنگی

تاریخ انتشار: مارس ۲۰۲۶

معماری سرکوب دیجیتال

پس از کودتای ۲۰۲۱ در میانمار، حکومت نظامی، اپراتورهای مخابراتی و ارائه دهندگان خدمات اینترنتی (ISP) در این کشور را مجبور به اجرای کنترل‌های اطلاعاتی، از جمله نصب فناوری نظارت و رهگیری در شبکه‌های خود، ارائه داده‌های کاربر به پلیس و مقامات نظامی و اجرای ثبت سیم کارت برای کاربران تلفن همراه کرد. تاکتیک‌های حکومت نظامی منجر به خروج Telenor، یک شرکت مخابراتی نروژی، و Ooredoo، یک شرکت مخابراتی قطری، از بازار میانمار در سال ۲۰۲۲ شد و آنها عملیات محلی خود را به نهادهای وابسته به ارتش فروختند. به طور خاص، Telenor Myanmar به یک شرکت لبنانی مرتبط با ارتش میانمار فروخته شد و این شرکت متعاقباً نام خود را به ATOM Myanmar تغییر داد. در همان زمان، Ooredoo Myanmar توسط شرکتی با روابط با چهره‌های مرتبط با ارتش خریداری شد و به U9 Myanmar تغییر نام داد. بخش مخابرات تحت سلطه ارتش در میانمار، سرکوب دیجیتال تحت حمایت دولت را از طریق قطعی‌های مکرر اینترنت (با حداقل هشتاد و پنج مورد قطعی در سال ۲۰۲۴)، و استفاده از ابزارهایی مانند «پهپادهای نظارتی، دستگاه‌های کرک آیفون و نرم‌افزارهای هک» برای سرکوب مقاومت ضد حکومت نظامی و نافرمانی مدنی، فعال و نهادینه کرده است. در ژانویه ۲۰۲۵، دستگاه سرکوب دیجیتال میانمار با تصویب یک قانون بحث‌برانگیز امنیت سایبری تقویت شد که به دولت توانایی بیشتری برای مسدود کردن وبسایت‌ها و نظارت بر کاربران اینترنت می‌دهد.

میانمار رویکردی مشابه روسیه و چین اتخاذ کرده است، جایی که قوانین و مقررات سختگیرانه اینترنت، اجبار دولتی بر ISPها را ممکن ساخته و کنترل‌های گسترده اطلاعات را تسهیل کرده است. به عنوان مثال، روسیه در سال ۲۰۱۹ قانون «اینترنت مستقل» را تصویب کرد که یک سیستم نام دامنه ملی (DNS) را ایجاد کرد که توسط Roskomnadzor، تنظیم‌کننده اینترنت روسیه، نگهداری می‌شود. DNS به عنوان دفترچه آدرس اینترنت عمل می‌کند و یک URL را به یک آدرس IP عددی تبدیل می‌کند. بنابراین، کنترل دولت بر DNS ملی به دولت اجازه می‌دهد تا دسترسی به برخی وبسایت‌ها را به طور کامل مسدود کند یا کاربران را به سایت‌های تحت تحریم دولت هدایت کند. دولت از ژانویه ۲۰۲۱ از همه ISPهای فعال در روسیه خواست که از DNS ملی استفاده کنند. بنابراین، قانون «اینترنت مستقل» دولت را قادر ساخته است تا هزاران وبسایت، از جمله سایت‌هایی که «میزبان مطالب انتقادی از مقامات یا تهاجم [اوکراین] هستند، و همچنین سایت‌های خبری بین‌المللی، وبسایت‌های جامعه مدنی و سایت‌های خبری اوکراینی» را مسدود کند.

ادبیات موجود در مورد سرکوب دیجیتال، کنترل‌های اطلاعاتی را در سطوح کاربرد و محتوا، از جمله فیلتر یا مسدود کردن محتوا و درخواست‌های دولتی به پلتفرم‌های رسانه‌های اجتماعی برای حذف محتوا، بررسی کرده است. با این حال، محققان به خوبی مطالعه نکرده‌اند که چگونه ISPهایی که زیرساخت‌های اساسی را ایجاد و/یا اداره می‌کنند، کنترل‌ها را اعمال می‌کنند. با توجه به نقش آنها به عنوان دروازه‌بانان دسترسی به اینترنت، درک شیوه‌های ISP و نظارت دولت بر آنها برای درک چگونگی عملکرد کنترل‌های اطلاعاتی در عمل ضروری است. این مقاله با تجزیه و تحلیل نقش ISPها در کنترل اطلاعات و بررسی مکانیسم‌هایی که سرکوب دیجیتال تحت هدایت دولت از طریق آنها در زیرساخت شبکه عمل می‌کند، به این شکاف می‌پردازد.

کنترل دولتی بر ارائه دهندگان خدمات اینترنتی: پیدایش و تکامل آن

در حوزه‌های قضایی که فقط ارائه‌دهندگان دولتی وجود دارند، دسترسی به اینترنت در برابر نظارت و دستکاری‌های دولتی بسیار آسیب‌پذیر است. به عنوان مثال، در چین، دولت زیرساخت‌های اینترنتی را از طریق برنامه‌ریزی گسترده و هماهنگ دولتی، همراه با تلاش برای تضمین کنترل مداوم دولت، ایجاد کرده است. اکثر زیرساخت‌های فیزیکی اینترنت چین، در مناطق شهری و روستایی، توسط شرکت‌های دولتی - یعنی China Telecom، China Unicom و China Mobile - ساخته و نگهداری می‌شوند که خدماتی مانند پهنای باند، اتصالات خط ثابت و داده‌های تلفن همراه را ارائه می‌دهند. مداخله شدید دولت، همراه با اعمال موانع قابل توجه بر سر راه فعالیت‌های نهادهای خارجی در این کشور، به این ارائه‌دهندگان دولتی اجازه داده است تا بر بازار اینترنت چین تسلط یابند. علاوه بر این، چین یک سیستم سانسور اینترنتی سراسری ایجاد و نگهداری کرده است که ترافیک اینترنتی ورودی و خروجی از شبکه‌های کشور را فیلتر می‌کند. این سیستم سانسور که به طور عامیانه به عنوان فایروال بزرگ



شناخته می‌شود، در سال 1998 توسط وزارت امنیت عمومی، تنها چهار سال پس از برقراری اتصال کاملاً کاربردی این کشور به اینترنت جهانی، راه‌اندازی شد.

اخیراً، در سال ۲۰۲۴، چین محدودیت‌های سرمایه‌گذاری خارجی را برای شرکت‌هایی که خدمات مخابراتی، از جمله دسترسی به اینترنت، ارائه می‌دهند، لغو کرد. با این حال، ISP های تازه تأسیس هنوز ملزم به استفاده از زیرساخت شبکه موجود تحت کنترل ارائه دهندگان دولتی و اخذ مجوز فعالیت از وزارت صنعت و فناوری اطلاعات (MIIT)، یکی از چندین نهاد چینی که سانسور آنلاین و آفلاین را اعمال می‌کنند، هستند. به عنوان بخشی از فرآیند صدور مجوز، MIIT تأیید می‌کند که ISP ها از قوانین سانسور محتوای آن پیروی کرده‌اند، با توجه به اینکه همه ISP های فعال در چین، صرف نظر از مالکیت، باید مسدود کردن و فیلتر کردن محتوا را اجرا کنند. به دلیل این الزامات سختگیرانه سانسور، فیلترینگ محتوای گسترده‌ای در کشور وجود دارد، از جمله در برابر «انتقاد از افراد، سیاست‌ها یا رویدادهایی که جزئی جدایی‌ناپذیر از سیستم تک حزبی در نظر گرفته می‌شوند»، که منجر به «نسخه‌ای بسیار کنترل شده، تحت نظارت و دستکاری شده» از اینترنت چین می‌شود. مورد چین نشان می‌دهد که تسلط دولت بر زیرساخت شبکه، که به اوایل تأسیس اینترنت برمی‌گردد، کنترل‌های مداوم اینترنت و نظارت گسترده بر کاربران اینترنت را تسهیل می‌کند.

در سایر حوزه‌های قضایی که ISP های خصوصی با ISP های دولتی همزیستی داشته‌اند، کنترل دولت بر زیرساخت‌های شبکه معمولاً به تدریج تکامل یافته است. این نوع تکامل در روسیه آشکار است، جایی که زیرساخت اینترنت آن، که در دوران شوروی ساخته شده بود، توسط سازمان‌های خصوصی و مؤسسات تحقیقاتی با مشارکت محدود دولت توسعه داده شد. روسیه برای اولین بار در سال ۱۹۹۰ از طریق یک شبکه رایانه‌ای که توسط RELCOM (ارتباطات قابل اعتماد) اداره می‌شد، به اینترنت جهانی متصل شد، که توسط گروهی از برنامه‌نویسان رایانه در مؤسسه کورچاتوف توسعه داده شده بود. تا اواسط دهه ۱۹۹۰، ISP های تجاری متعددی در روسیه وجود داشتند، مانند FidoNet، GlasNet، IASnet و Sovam Teleport که همگی توسط سازمان‌های خصوصی تأسیس شده بودند. تا اوایل دهه ۲۰۰۰، اینترنت روسیه (یا به اختصار "RuNet") در مقایسه با رسانه‌های سنتی، احتمالاً به دلیل نرخ پایین نفوذ اینترنت - یعنی در سال ۲۰۰۸، تنها ۱۴ درصد از جمعیت به اینترنت دسترسی داشتند - نظارت دولتی کمتری داشت. پایگاه کاربران RuNet متعاقباً در طول اعتراضات گسترده ۲۰۱۲-۲۰۱۱ به دلیل سوءظن به تقلب انتخاباتی گسترش یافت، موضوعی که تا حد زیادی توسط رسانه‌های سنتی روسیه نادیده گرفته می‌شد اما روزنامه‌نگاران و وبلاگ‌نویسان مستقل به طور فعال در فضای آنلاین درباره آن بحث می‌کردند. این افزایش بحث‌های سیاسی آنلاین در دهه ۲۰۱۰ باعث شد محققان از اینترنت به عنوان «حوزه عمومی جایگزین» روسیه یاد کنند.

قبل از سال ۲۰۱۲، RuNet عمدتاً از طریق چارچوب‌های قانونی عمومی و قوانین موجود در مورد رسانه‌های جمعی، ارتباطات و حفاظت از اطلاعات اداره می‌شد، نه از طریق قوانین خاص اینترنت یا فیلترینگ مستقیم اینترنت به سبک چین. با این حال، پس از سال ۲۰۱۲، روسیه چندین قانون سختگیرانه تصویب کرد که توانایی دولت را برای محدود کردن و سانسور گفتار آنلاین افزایش داد، که توسط تحلیلگران به عنوان "حمله برق‌آسای" علیه آزادی بیان آنلاین به رهبری دولت توصیف شد. به عنوان مثال، قانون فدرال شماره ۱۳۹-FZ سال ۲۰۱۲ و قانون فدرال شماره ۳۹۸-FZ سال ۲۰۱۳ به Roskomnadzor اختیار داد تا وبسایت‌ها را ممنوع کند و ISP ها را ملزم به رعایت دستورالعمل‌های مسدودسازی آن کند.

تا سال ۲۰۱۵، خانه آزادی (Freedom House) به دلیل اقدامات قابل توجه برای «افزایش کنترل بر فضای آنلاین، به ویژه پیش از بازی‌های المپیک سوچی»، روسیه را «غیرآزاد» ارزیابی کرده بود. در سال‌های بعد، روسیه با به کارگیری طیف وسیعی از ابزارهای قانونی و دخالت فنی در زیرساخت‌های اینترنت، مقررات اقتدارگرایانه خود بر اینترنت را تشدید کرده است. ۲۸ به عنوان مثال، روسیه از ارائه‌دهندگان خدمات اینترنتی (ISP) می‌خواهد سیستم‌های نظارتی موسوم به SORM (سیستم فعالیت‌های تحقیقاتی عملیاتی) را نصب کنند که شامل سخت‌افزار و نرم‌افزاری است که با هزینه اپراتور نصب می‌شود اما مستقیماً توسط سرویس امنیت فدرال فدراسیون روسیه (FSB)، آژانس اصلی اطلاعات و امنیت داخلی این کشور، کنترل می‌شود. SORM که ابتدا در سال ۱۹۹۵ برای شنود و نظارت بر تلفن معرفی شد، بعداً در سال ۱۹۹۸ (SORM-2) با اینترنت سازگار شد و در سال ۲۰۱۴ (SORM-3) گسترش یافت تا شامل جمع‌آوری فراداده‌ها و فایل‌های چندرسانه‌ای نیز باشد. دولت پس از تصویب قانون موسوم به یاروویا (در واقع مجموعه‌ای از دو لایحه فدرال روسیه، ۳۷۴-FZ و ۳۷۵-FZ) در سال ۲۰۱۶، عملکرد SORM را به طور قابل توجهی گسترش داد. این قانون، ارائه‌دهندگان خدمات اینترنتی و ارائه‌دهندگان خدمات مخابراتی را ملزم به ذخیره





یادداشت

محتوای تمام ارتباطات کاربران تا شش ماه و ابر داده‌ها را تا سه سال می‌کند. اصلاحیه‌ای در سال 2018 پس از انتقاد از سوی ارائه‌دهندگان خدمات اینترنتی، برخی از این الزامات را اصلاح کرد، مانند الزام ذخیره محتوای تمام ارتباطات (به عنوان مثال، تماس‌های صوتی، داده‌ها، تصاویر و پیام‌های متنی) تنها به مدت سی روز، اگرچه نگهداری ابر داده‌ها همچنان سه سال باقی ماند و ظرفیت ذخیره‌سازی سالانه 15 درصد افزایش یافت. تلاش‌های روسیه برای کنترل اینترنت فراتر از مرزهای آن نیز گسترش یافته است، به ویژه در سرزمین‌های اوکراین که پس از حمله 2022 اشغال کرده است. به عنوان مثال، در خرسون، روسیه اینترنت را قطع کرد و متعاقباً از طریق ارائه‌دهنده دولتی خود، روستلکام، اتصال را برقرار کرد تا این سرزمین را در زیر ساخت اینترنت روسیه ادغام کند. علاوه بر این، از ژانویه 2023، ارائه دهنندگان خدمات اینترنتی در سرزمین‌های موقتاً اشغال شده باید SORM را برای اهداف «رهگیری قانونی و ذخیره ابر داده‌های مشتریان خود» نصب کنند.

تجربیات چین و روسیه نشان می‌دهد که چگونه ترتیبات اولیه زیر ساخت شبکه - تسلط دولت در اینترنت چین در مقابل توسعه بخش خصوصی در اینترنت روسیه - به الگوهای متمایز کنترل فنی و مکانیسم‌هایی که امروزه نیز ادامه دارند، کمک کرده است. به عنوان مثال، اگرچه هر دو کشور توسط خانه آزادی به طور مشابه به عنوان "غیرآزاد" طبقه‌بندی می‌شوند، روسیه سیستم سانسور سراسری دولتی ندارد، در حالی که چین "فایروال بزرگ" خود را دارد. این تضاد اهمیت انتخاب‌های زیر ساختی تاریخی را نشان می‌دهد و فرضیات مربوط به اعمال یکسان کنترل‌های اطلاعاتی تحت هدایت دولت را به چالش می‌کشد. بنابراین، درک توسعه زیر ساخت اینترنت یک کشور برای درک چگونگی اعمال کنترل دولت‌ها بر فضاها و آنلاین بسیار مهم است، زیرا این معماری، امکان‌سنجی، روش‌ها و اثربخشی سرکوب دیجیتال را شکل می‌دهد.

کنترل‌های زیر ساختی و آزادی اینترنت

به عنوان بخشی از ابزار سرکوب دیجیتال خود، دولت‌ها می‌توانند با اعمال محدودیت‌هایی بر ارائه‌دهندگان دسترسی و حمل و نقل که ترافیک اینترنت را حمل می‌کنند، جریان اطلاعات آنلاین را محدود کنند. ارائه‌دهندگان دسترسی، خدمات اینترنتی را مستقیماً به مصرف‌کنندگان و مشاغل ارائه می‌دهند - نمونه‌های اصلی آمریکایی شامل AT&T، Comcast (Xfinity) و Verizon هستند. در مقابل، ارائه‌دهندگان حمل و نقل مانند Cogent و Lumen زیر ساخت‌های اساسی اینترنت را به شبکه‌های دیگر ارائه می‌دهند تا اینکه مستقیماً به کاربران خانگی خدمت‌رسانی کنند. از آنجایی که ارائه‌دهندگان حمل و نقل، چندین ارائه‌دهنده دسترسی را به هم متصل می‌کنند، کنترل دولت بر آنها منجر به مکانیسم کارآمدتری برای نظارت، فیلتر کردن یا دستکاری ترافیک اینترنت می‌شود. علاوه بر این، از آنجا که اکثر کاربران اینترنت از نحوه عملکرد یا تنظیم مقررات ارائه‌دهندگان حمل و نقل بی‌اطلاع هستند، دولت‌ها می‌توانند ارائه‌دهندگان حمل و نقل را مجبور به نظارت و سانسور کاربران اینترنت با خطر کمتر واکنش عمومی کنند.

با توجه به اهمیت ارائه دهنندگان خدمات ترانزیت، رژیم‌های استبدادی مانند چین، ازبکستان و امارات متحده عربی، اینترنت خود را طوری تنظیم و پیکربندی کرده‌اند که فقط ارائه دهنندگان خدمات اینترنتی دولتی به عنوان ارائه دهنندگان خدمات ترانزیت در حوزه قضایی آنها فعالیت کنند. ارائه دهنندگان دولتی از رژیم‌های استبدادی در سایر محیط‌های استبدادی نیز فعالیت داشته‌اند. به عنوان مثال، ارائه دهنندگان دولتی امارات متحده عربی خدمات اینترنتی را در گابن، موریتانی و مراکش نیز ارائه می‌دهند. این شبکه زیر ساختی استبدادی، سرکوب دیجیتال و کنترل اطلاعات فرامرزی را تسهیل می‌کند.

نظارت دقیق دولتی بر صنعت ISP در میانمار نیز مشهود است و منجر به نگرانی گروه‌های جامعه مدنی در مورد روابط و همکاری گسترده بین ISP‌ها و دولت شده است. به عنوان مثال، قبل از خروج آنها از میانمار، هم Ooredoo و هم Telenor با انتقادهایی در مورد رعایت سیاست‌های ناقض حقوق بشر مواجه شده بودند. پس از کودتای 2021، Ooredoo میانمار اظهار داشت که "متأسفانه" از دستورالعمل‌های دولت برای محدود کردن دسترسی به پهنای باند تلفن همراه و بی‌سیم پیروی کرده است. علاوه بر این، فعالان حقوق بشر استدلال کردند که همکاری Telenor میانمار با حکومت نظامی منجر به دستگیری یا اعدام رهبران دانشجویی و فعالان طرفدار دموکراسی شده است. در نتیجه، در دسامبر 2024، Justice For Myanmar و ICJ Norway شکایتی را علیه گروه Telenor که اکثریت آن متعلق به دولت نروژ است و مدیریت عملیات میانمار آن به پلیس نروژ ارائه کردند. در این شکایت، آنها ادعا کردند که شرکت تابعه Telenor در میانمار با "به اشتراک گذاشتن داده‌های حساس ترافیک





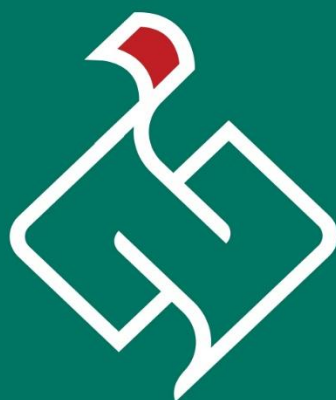
شبکه با حکومت نظامی و انتقال تجهیزات به اصطلاح شنود قانونی به یک شرکت مرتبط با ارتش میانمار "تحریم‌های نروژ را نقض کرده است.

علاوه بر این، ISP های میانمار، که اکنون مالکیت آنها با ارتش مرتبط است، به فناوری نظارت و فیلترینگ دست یافته‌اند که اقتدارگرایی فراملی را در این کشور بیشتر تقویت می‌کند. در ماه مه 2024، سازمان عدالت برای میانمار دریافت که حکومت نظامی «یک سیستم نظارت و سانسور وب جدید برای افزایش کنترل خود بر اینترنت» به دست آورده است، از جمله ابزارهای بازرسی عمیق بسته‌ها (DPI) برای نظارت و فیلتر کردن محتوا برای استفاده توسط ISP های خود. در ماه مه 2025، تحقیقات مشترک توسط Finance Uncovered و Myanmar Now به این نتیجه رسید که Frontiir، یک ISP مستقر در یانگون، تجهیزات Geedge را نصب کرده است که قادر به ردیابی فعالیت آنلاین کاربران، مسدود کردن وبسایت‌ها و جلوگیری از استفاده از شبکه‌های خصوصی مجازی (VPN) برای دور زدن سانسور آنلاین است. (Frontiir، یک ISP که 40 میلیون دلار بودجه توسعه از دولت‌های بریتانیا، نروژ و دانمارک در ازای سهام عدالت دریافت کرده است، این اتهامات را رد کرد.

دولت‌های اقتدارگرا در سراسر جهان به طور فزاینده‌ای از کنترل خود بر اپراتورهای شبکه، وضع مقررات سختگیرانه و فروش بین‌المللی فناوری‌های نظارتی و فیلترینگ برای افزایش قابلیت‌های سرکوب دیجیتال خود استفاده می‌کنند. نتیجه، تشدید چالش‌ها برای حفاظت از حقوق اساسی بشر و ثبات اینترنت جهانی باز و به هم پیوسته است. این تحولات، نیاز فوری به همکاری بین‌المللی برای تقویت چارچوب‌های حکومت دموکراتیک، مقابله با نفوذ دیجیتال اقتدارگرایان فراملی و حفظ آزادی اینترنت را برجسته می‌کند. اجرای اصول راهنمای سازمان ملل در مورد تجارت و حقوق بشر، که تصریح می‌کند شرکت‌ها مسئولیت احترام به حقوق بشر و انجام اقدامات لازم برای اطمینان از اینکه ابزارها و خدمات آنها در سرکوب دیجیتال همدست نیستند را بر عهده دارند، در مرکز این تلاش قرار دارد.

فعالان و دولت‌های دموکراتیک برای مقابله با این روندها چه کاری می‌توانند انجام دهند؟ حداقل، وقتی شرکت‌های مستقر در دموکراسی‌های لیبرال، مانند Telenor در نروژ، شرکت‌های تابعه خود را در کشورهای اقتدارگرا می‌فروشند، باید خریداران بالقوه را از نظر ارتباط با ناقضان حقوق بشر و نهادهای تحریم‌شده بررسی کنند. آنها همچنین باید گزارش‌های شفافیت در مورد چگونگی مطابقت چنین خروج‌ها یا فروش‌هایی با استانداردهای بین‌المللی حقوق بشر منتشر کنند (به عنوان مثال، با گنجاندن اصول راهنمای سازمان ملل در مورد تجارت و حقوق بشر در شرایط خرید). وقتی صحبت از بررسی مکان‌ها و عملیات ارائه‌دهندگان خدمات دولتی اقتدارگرا می‌شود، گروه‌های جامعه مدنی و محققان در موقعیت مناسبی برای انجام تحقیقات برای افشای خطرات نظارتی و تسهیل حمایت آگاهانه هستند. اما این فعالیت‌ها به منابع قابل توجهی نیاز دارند - پشتیبانی که دولت‌های دموکراتیک می‌توانند در ارائه آن کمک کنند. در نهایت، دموکراسی‌ها می‌توانند برنامه‌های سوادآموزی و امنیت دیجیتال را برای کاربران اینترنتی ساکن در حوزه‌های قضایی با شبکه‌هایی که توسط ISP های مرتبط با اقتدارگرا اداره می‌شوند، تأمین مالی کنند. بدون اقدام هماهنگ، دولت‌های اقتدارگرا و متحدان آنها به سوءاستفاده از شکاف‌های نظارتی و ایجاد همکاری‌های بیشتر برای صادرات قابلیت‌های نظارتی و سانسور و تثبیت سرکوب دیجیتال در سراسر جهان ادامه خواهند داد.





انديشكده فرهنگ و توسعه

 WWW.CDSTT.IR

 [CDSTT.IR](https://www.instagram.com/CDSTT.IR)

 [CDSTT](https://twitter.com/CDSTT)