پژوهشگاه
فضای مجازی

دفتر خاکستری ۵۰

پاسخ سریع
فروردین ۱۴۰۵

گوشی‌های هوشمند با سیستم عامل سفارشی بدون برنامک‌های گوگل

پاسخ به سوال مطرح شده از سوی معاونت امور اقتصادی و تنظیم مقررات


بسم الله الرحمن

گوشی‌های هوشمند با سیستم عامل سفارشی

بدون برنامک‌های گوگل

پاسخ به سوالات مطرح شده از کمیسیون تنظیم مقررات

دفتر خاکستری (Quick Answer) **شمارهٔ پنجاهم**

گردآورنده: امیرپویا باقری

تمام حقوق مادی و معنوی این اثر متعلق به پژوهشگاه فضای مجازی است و استفاده از آن تنها با ذکر منبع مجاز است.
همچنین محتوای منتشرشده در این گزارش بیانگر دیدگاه رسمی مرکز ملی فضای مجازی نیست.

نشانی: تهران، سعادت آباد، خیابان علامه شمالی، کوچه هجدهم غربی، پلاک ۱۷
تلفن: ۲۲۰۷۳۰۳۱-۰۲۱
کد پستی: ۱۹۹۷۹۸۷۶۲۹

مقدمه

وابستگی گسترده گوشی‌های هوشمند به اکوسیستم گوگل، به‌ویژه در سیستم‌عامل اندروید، طی یک دهه گذشته به یکی از موضوعات مهم در حوزه حکمرانی دیجیتال، امنیت ملی و استقلال فناوری کشورها تبدیل شده است. برخی دولت‌ها تلاش کرده‌اند با محدودسازی یا جایگزینی سرویس‌های گوگل، کنترل بیشتری بر داده‌ها، زیرساخت‌های ارتباطی و سیاست‌های امنیتی خود اعمال کنند، در حالی که برخی دیگر رویکرد تعامل و تنظیم‌گری را ترجیح داده‌اند. این گزارش با تمرکز بر بررسی تجربیات چهار کشور چین، روسیه، هند و کره جنوبی، در بخش نخست به بررسی چرایی، شیوه‌ها، چالش‌ها و نتایج محدود کردن یا مدیریت سرویس‌های گوگل در این کشورها می‌پردازد. در بخش دوم، نگاهی به سیاست‌ها و محدودیت‌های اعمال‌شده بر استفاده از اندروید و سرویس‌های وابسته به گوگل در میان مقامات دولتی، نظامی و امنیتی این کشورها خواهیم داشت. هدف، ترسیم تصویری واقع‌گرایانه از نسبت میان امنیت، حاکمیت دیجیتال و وابستگی به پلتفرم‌های جهانی است؛ نه در قالبی آرمانی و رویایی، بلکه بر پایه تجربه‌های عملی و قابل مقایسه.

بیان مسئله:

بررسی تجربیات این کشورها نشان می‌دهد که دولت‌ها در مواجهه با سرویس‌های گوگل عموماً یکی از این دو رویکرد را برگزیده‌اند. **محدودسازی ساختاری و جایگزینی اکوسیستم**، و **تنظیم‌گری و کنترل حقوقی بدون محدودیت کامل (بعضا همراه با محدودیت‌های جزیی)**. چین شاخص‌ترین نمونه رویکرد نخست است؛ کشوری که با تکیه بر ملاحظات امنیت ملی، کنترل اطلاعات و توسعه اکوسیستم بومی، دسترسی به سرویس‌های گوگل را به‌صورت کامل مسدود کرد و هم‌زمان با سرمایه‌گذاری سنگین، جایگزین‌های داخلی را به سطحی رساند که پاسخ‌گوی نیاز بازار داخلی باشند. در مقابل، کشورهایی مانند روسیه، هند و کره جنوبی مسیرهای

متفاوت‌تری را برگزیده‌اند. روسیه اگرچه محدودیت‌ها و فشارهای حقوقی و فنی قابل توجهی بر گوگل اعمال کرده، اما به دلیل وابستگی اجتماعی و اقتصادی کاربران و نبود جایگزین‌های فراگیر و مناسب، از فیلتر کامل و سراسری پرهیز کرده و محدودیت‌های جزیی همراه با فشارهای قانونی و تنظیمی را دنبال می‌کند. هند نیز به‌جای حذف سرویس‌های گوگل، تمرکز خود را بر تنظیم‌گری بازار، اعمال قوانین رقابتی و تلاش‌های محدود برای ایجاد گزینه‌های بومی گذاشته است؛ رویکردی که بیش از آنکه محدودیت‌گرا باشد امنیت‌محور و توسعه‌طلب است. کره جنوبی نیز با وجود حساسیت‌های امنیتی بالا، به‌ویژه در حوزه داده‌های راهبردی (مانند نقشه‌های هوایی)، ترجیح داده است از طریق قوانین سخت‌گیرانه حریم خصوصی و محدودسازی موردی (مانند داده‌های نقشه) حاکمیت خود را اعمال کند، بدون آنکه پیوندش با اکوسیستم جهانی فناوری قطع شود. این تفاوت رویکردها نشان می‌دهد که سیاست‌گذاری در قبال گوگل بیش از آنکه یک نسخه واحد داشته باشد، بازتابی از اولویت‌ها و واقعیت‌های امنیتی، اقتصادی و اجتماعی هر کشور است. در ادامه به صورت مجزا به بررسی رویکرد اختصاصی و تجربیات هر کشور خواهیم پرداخت.

چین: محدودسازی ساختاری و جایگزینی اکوسیستم گوگل

رویکرد و نگاه کلان چین

نگاه چین به سرویس‌های گوگل را نمی‌توان صرفاً در قالب «فیلترینگ اینترنت» توضیح داد؛ این رویکرد بخشی از یک چارچوب کلان‌تر در سیاست داخلی و خارجی چین است. از دید سیاست‌گذاران چینی، فضای مجازی امتداد قلمرو ملی است و دولت باید همان سطح از کنترل، قانون‌گذاری و اعمال حاکمیت را که بر زمین، دریا و هوا دارد، بر اینترنت نیز اعمال کند. این نگاه از اوایل دهه ۲۰۰۰ در اسناد رسمی حزب کمونیست چین شکل گرفت و در دوران ریاست‌جمهوری شی جین‌پینگ به یکی از ستون‌های سیاست حکمرانی تبدیل شد.[۱][۲]

در این چارچوب، شرکت‌هایی مانند گوگل صرفاً ارائه‌دهنده خدمات فناوری تلقی نمی‌شوند، بلکه بازیگرانی هستند که می‌توانند بر جریان اطلاعات، افکار عمومی، داده‌های شهروندان و حتی ثبات سیاسی تأثیر بگذارند. بنابراین، سیاست چین از ابتدا بر «ادغام کنترل اطلاعات، امنیت ملی و توسعه صنعتی» استوار بوده است؛ ترکیبی که به‌طور طبیعی به سمت حذف یا به حاشیه‌راندن پلتفرم‌های خارجی غیرقابل‌کنترل سوق پیدا می‌کند، نه تنظیم‌گری حداقلی یا هم‌زیستی بلندمدت با آن‌ها.

انتخاب مسیر حذف ساختاری سرویس‌های گوگل نتیجۀ هم‌زمان چند عامل سیاسی، نهادی و اجتماعی است. نخست، نظام سیاسی چین که بر کنترل متمرکز و ثبات بلندمدت تأکید دارد، فضای مجازی را یکی از اصلی‌ترین میدان‌های تهدید بالقوه می‌داند؛ تجربه اعتراضات، تحولات سیاسی جهانی و نقش شبکه‌های دیجیتال در بسیج اجتماعی، این حساسیت را تشدید کرده است[۳].

دوم، چین از نظر ظرفیت فنی و اقتصادی در موقعیتی قرار داشت که می‌توانست هزینه جدایی از اکوسیستم جهانی را تا حدی جبران کند: بازار داخلی چندصد میلیونی، نیروی انسانی گسترده، زنجیره تأمین سخت‌افزاری مستقل و شرکت‌های فناوری بومی که توان رشد و توسعۀ سریع داشتند.

عامل سوم، نگاه راهبردی چین به استقلال فناوری است. از دید پکن، وابستگی عمیق به

زیرساخت‌های دیجیتال آمریکایی، در بلندمدت یک آسیب‌پذیری ژئوپلیتیک محسوب می‌شود؛ آسیبی که می‌تواند در شرایط تنش یا تحریم به اهرم فشار تبدیل شود. حذف سرویس‌های گوگل، در این معنا، نه یک تصمیم صرفاً داخلی بلکه بخشی از سیاست کاهش وابستگی ساختاری به فناوری غربی بوده است [۴]. در نهایت، چین به دلیل ساختار اجتماعی و رسانه‌ای خاص خود، با هزینه سیاسی کمتری نسبت به بسیاری از کشورها توانست این گذار را مدیریت کند.

هزینه‌ها و الزامات پیاده‌سازی

اجرای این سیاست هزینه‌بر و زمان‌بر بوده است. بر اساس برآوردهای منتشرشده در گزارش‌های تحلیلی، چین طی بیش از یک دهه ده‌ها میلیارد دلار به‌صورت مستقیم و غیرمستقیم در توسعه زیرساخت‌های کنترل اینترنت، حمایت از شرکت‌های بومی و ایجاد جایگزین‌های داخلی سرمایه‌گذاری کرده است [۵]. تنها توسعه و نگه‌داری زیرساخت‌های فنی مرتبط با «فایروال بزرگ[۱]» شامل سامانه‌های فیلترینگ، بازرسی عمیق بسته‌ها (DPI)[۲] و تحلیل ترافیک، پروژه‌ای چندساله و پرهزینه بوده که از اوایل دهه ۲۰۰۰ آغاز شده و همچنان در حال به‌روزرسانی است [۶].

علاوه بر هزینه مالی، چین بهای دیگری نیز پرداخت کرده است: کاهش دسترسی مستقیم به دانش، ابزارها و پلتفرم‌های جهانی در کوتاه‌مدت، کند شدن تعاملات علمی و فناورانه بین‌المللی، و تحمیل هزینه تطبیق به کسب‌وکارها و توسعه‌دهندگان داخلی. با این حال، سیاست‌گذاران چینی این هزینه‌ها را «سرمایه‌گذاری راهبردی بلندمدت» تلقی کرده‌اند، نه زیان خالص.

تاریخچه اجرا و روند عملیاتی

حذف سرویس‌های گوگل در چین یک اقدام ناگهانی نبوده است. تنش میان گوگل و دولت چین از اواخر دهه ۲۰۰۰ آغاز شد و در سال ۲۰۱۰، با توقف سرویس جست‌وجوی گوگل به زبان چینی و انتقال آن به هنگ‌کنگ، وارد مرحله‌ای جدید شد [۷]. پس از آن، دسترسی به سرویس‌هایی مانند Gmail،

---

۱. Great FIrewall

۲. Deep Packet Inspection

Google Maps، Google Drive و Google Play به‌صورت تدریجی و در مقاطع مختلف محدود و مسدود شد. این روند هم‌زمان با تقویت زیرساخت‌های فیلترینگ و رشد جایگزین‌های داخلی پیش رفت، به‌گونه‌ای که حذف سرویس‌های گوگل با خلأ کامل خدمات برای کاربران همراه نشد.

خط زمانی محدودشدن سرویس های گوگل در چین:

- ۲۰۰۹—۲۰۱۰: مسدودسازی سرویس‌هایی مانند Gmail، Google Search و Google Maps
- ۲۰۱۰ به بعد: خروج تدریجی گوگل از بازار چین و توقف توسعه رسمی محصولات آن

دهه ۲۰۱۰: تثبیت فایروال بزرگ و تکمیل زیرساخت‌های فیلترینگ

دهه ۲۰۲۰: بلوغ اکوسیستم بومی و کاهش وابستگی کاربران به سرویس‌های خارجی

زیرساخت‌های اعمال سیاست

اعمال این رویکرد متکی بر مجموعه‌ای از زیرساخت‌های فنی، حقوقی و نهادی بوده است، از جمله:

- فایروال بزرگ برای فیلترینگ دامنه، IP و ترافیک رمزنگاری‌شده
- استفاده گسترده از DPI برای شناسایی و قطع ترافیک سرویس‌های خاص
- نظام مجوزدهی سخت‌گیرانه برای فعالیت شرکت‌های خارجی فناوری
- قوانین الزام‌آور ذخیره‌سازی داده در داخل کشور
- هم‌افزایی میان نهادهای امنیتی، رگولاتوری و شرکت‌های مخابراتی

- اکوسیستم سخت‌افزاری و نرم‌افزاری بومی (گوشی، اپ‌استور، پرداخت، نقشه)

این ترکیب باعث شده فیلترینگ نه صرفاً در سطح وب‌سایت، بلکه در سطح معماری شبکه اعمال شود[۶][۸].

سطح فیلترینگ و استثناها

دسترسی عمومی شهروندان به سرویس های گوگل عملاً مسدود است. با این حال، استثناهایی وجود دارد:

- نمایندگی‌های دیپلماتیک خارجی، شرکت‌های چندملیتی، برخی دانشگاه‌ها و مراکز تحقیقاتی بین‌المللی
- این دسترسی‌ها معمولاً از طریق شبکه‌های اختصاصی، خطوط اجاره‌ای بین‌المللی یا VPN های مجاز دولتی فراهم می‌شود
- حتی در این موارد، دسترسی کامل و بدون محدودیت نیست و ممکن است تحت نظارت یا ثبت ترافیک قرار داشته باشد[۹]

این الگو نشان می‌دهد که چین به‌جای «ممنوعیت مطلق»، از تفکیک دسترسی بر اساس نقش و کارکرد نهادی استفاده می‌کند.

جایگزین‌ها و ارزیابی کیفیت آن‌ها

خدمات گوگل	جایگزین چینی
Google Search	Baidu
Gmail	QQ Mail / NetEase
Google Maps	Amap / Baidu Maps
Google Play	AppGallery / Mi Store
YouTube	Youku / Tencent Video
Google Drive	Baidu Cloud

از نظر کیفیت، این سرویس‌ها در پاسخ به نیازهای داخلی، مانند پرداخت، مسیریابی، خرید آنلاین و مصرف محتوای بومی، بسیار کارآمد و رقابتی هستند. با این حال، ضعف‌هایی نیز وجود دارد:

- جست‌وجوی بین‌المللی محدودتر و سانسورشده‌تر
- نبود یکپارچگی کامل با ابزارها و استانداردهای جهانی توسعه نرم‌افزار
- چالش در تعاملات فرامرزی، به‌ویژه برای کاربران حرفه‌ای، پژوهشگران و کسب‌وکارهای بین‌المللی [۱۰]

چالش‌های باقی‌مانده برای کاربران

فیلترکامل سرویس های گوگل پیامدهایی داشته که هنوز به طور کامل برطرف نشده اند:

- دشواری دسترسی مستقیم به منابع علمی، فنی و دانشگاهی جهانی
- افزایش هزینه و پیچیدگی تعاملات بین‌المللی برای کسب‌وکارها
- وابستگی کاربران حرفه‌ای به راه‌حل‌های غیررسمی برای دسترسی به ابزارهای جهانی
- فاصله گرفتن تدریجی اکوسیستم دیجیتال چین از استانداردهای غالب جهانی

دور زدن محدودیت‌ها

بر اساس برآوردهای مؤسسات پژوهشی، بین **۵ تا ۱۰ درصد کاربران اینترنت در چین** به‌طور مقطعی از ابزارهای دور زدن محدودیت‌ها استفاده می‌کنند [۱۱]. روش‌های رایج شامل:

- VPN های غیرمجاز

- پراکسی‌ها و تونل‌های رمزنگاری‌شده
- شبکه‌های شرکتی یا دانشگاهی

این دسترسی‌ها عمدتاً برای استفاده از جستجوی گوگل و یوتیوب، شبکه‌های اجتماعی جهانی و منابع علمی به کار می‌رود، اما با ریسک‌های حقوقی و فنی همراه است.

جمع‌بندی

تجربه چین نشان می‌دهد که اجرای سیاست حذف کامل سرویس‌های گوگل تنها در شرایطی ممکن است که سه عامل هم‌زمان وجود داشته باشد: **اراده سیاسی پایدار، زیرساخت فنی پیشرفته و اکوسیستم بومی توانمند.** این رویکرد توانسته وابستگی راهبردی چین به پلتفرم‌های خارجی را به‌طور چشمگیری کاهش دهد و کنترل دولت بر فضای مجازی را تثبیت کند، اما در مقابل، هزینه‌هایی مانند محدود شدن تعاملات جهانی، کاهش دسترسی آزاد به اطلاعات و ایجاد شکاف میان اکوسیستم دیجیتال چین و جهان را نیز به همراه داشته است. چین این هزینه‌ها را آگاهانه پذیرفته و آن‌ها را بخشی از بهای استقلال دیجیتال خود می‌داند؛ انتخابی که لزوماً برای همهٔ جوامع و دولت‌ها قابل تکرار نیست.

روسیه: تنظیم‌گری سخت‌گیرانه، فشار تدریجی و حاکمیت دیجیتال بدون مسدودی کامل

رویکرد و نگاه کلان روسیه

برخلاف چین که به‌دنبال حذف ساختاری و جایگزینی کامل اکوسیستم خارجی است، روسیه مسیر کنترل تدریجی، اعمال فشار حقوقی و فنی، و حفظ دسترسی محدود اما مشروط را برگزیده است. اسناد و اظهارات رسمی نهادهایی مانند Roskomnadzor و شورای امنیت روسیه نشان می‌دهد که هدف اصلی، نه قطع کامل ارتباط دیجیتال با جهان، بلکه کاهش قدرت اثرگذاری سیاسی، رسانه‌ای و اقتصادی شرکت‌های خارجی بر جامعه روسیه است [۱۲] [۱۳].

این نگاه ریشه در تجربه اعتراضات داخلی، نقش شبکه‌های اجتماعی در بسیج سیاسی، و تشدید تقابل ژئوپلیتیکی روسیه با ایالات متحده و اتحادیه اروپا دارد. از منظر سیاست‌گذاران روسی، شرکت‌هایی مانند گوگل نه بازیگران خنثی بازار، بلکه بخشی از زیرساخت نفوذ نرم غرب محسوب می‌شوند؛ با این حال، وابستگی عمیق جامعه، اقتصاد دیجیتال و حتی دولت به برخی خدمات جهانی باعث شده سیاست «قطع کامل» پرهزینه و پرریسک تلقی شود.

سوم، سیاست‌گذاران روسی پس از حمله به اکراین در سال ۲۰۲۲ دریافتند که تحریم‌ها و خروج خودخواستهٔ شرکت‌های غربی، به‌تنهایی می‌تواند بخشی از هدف «کاهش وابستگی» را محقق کند؛ بنابراین تمرکز دولت بر قانون‌گذاری الزام‌آور، جریمه، کاهش کیفیت خدمات (throttling) و حمایت از جایگزین‌های داخلی قرار گرفت، نه مسدودسازی ناگهانی و سراسری [۱۵]. این رویکرد همچنین امکان مانور سیاسی و بازگشت‌پذیری بیشتری نسبت به مدل چین فراهم می‌کند.

هزینه‌ها و الزامات پیاده‌سازی

برآورد دقیق هزینه‌ها دشوار است، اما گزارش‌های تحلیلی می‌توانند تصویر نسبتا روشنی برای ما ایجاد کنند. بر اساس تحلیل CSIS (Center for Strategic and International Studies) و Atlantic Council،

روسیه بین سال‌های ۲۰۱۴ تا ۲۰۲۵ حداقل ۱۰ تا ۱۵ میلیارد دلار صرف توسعه زیرساخت‌های نظارتی، فیلترینگ، DPI، مراکز داده داخلی و حمایت از پلتفرم‌های بومی کرده است [۱۶][۱۷].
به طور مشخص:

- توسعه و استقرار تجهیزات **DPI** در شبکه اپراتورها، که از ۲۰۱۹ اجباری شد، میلیاردها روبل هزینه در برداشته و بخشی از آن به اپراتورها تحمیل شده است [۱۸].

- ایجاد و توسعه پلتفرم‌هایی مانند RuStore، VK Video و RuTube از طریق یارانه دولتی و حمایت مستقیم وزارت مخابرات و توسعه دیجیتال انجام شده است؛ تنها VK Group در بین سال‌های ۲۰۲۲ و ۲۰۲۴ بیش از ۱.۵ میلیارد دلار کمک مستقیم و غیرمستقیم دولتی دریافت کرده است [۱۹].

تاریخچه اجرا و روند عملیاتی

کنترل سرویس های گوگل و پلتفرم های غربی در روسیه تدریجی اما پیوسته بوده است و پس از ۲۰۲۲ شتاب گرفته است:

- ۲۰۱۵—۲۰۱۹: تصویب قوانین ذخیره‌سازی داده در داخل روسیه؛ آغاز فشار حقوقی بر گوگل و اپل

- ۲۰۲۱: جریمه‌های سنگین گوگل به دلیل «محتوای غیرقانونی»

- مارس ۲۰۲۲: مسدودسازی کامل Facebook و Instagram پس از قرارگرفتن Meta در فهرست «سازمان‌های افراطی» [۲۰]

- ۲۰۲۲—۲۰۲۳: اعمال محدودیت سرعت (throttling) بر یوتیوب (نه مسدودسازی کامل) [۲۱]

- ۲۰۲۳: ممنوعیت استفاده از Google ID و Apple ID برای احراز هویت در بسیاری از خدمات دیجیتال روسی [۲۲]
- ۲۰۲۴—۲۰۲۵: افزایش فشار فنی بر VPNها و حذف گسترده آن‌ها از فروشگاه‌های اپلیکیشن [۲۳]

زیرساخت‌های اعمال سیاست محدودسازی

زیرساخت حکمرانی دیجیتال روسیه ترکیبی از ابزارهای فنی و حقوقی است:

- DPI در سطح اپراتورها
- کنترل DNS و مسیریابی
- قوانین هویت دیجیتال مبتنی بر خدمات دولتی (Gosuslugi)
- الزام فروشگاه‌های اپلیکیشن به پیش‌نصب نرم‌افزارهای روسی
- شبکه‌های اختصاصی برای نهادهای دولتی و حساس

این معماری امکان کاهش کیفیت، اختلال هدفمند و نظارت گسترده را بدون قطع کامل فراهم می‌کند [۱۸] [۲۴].

سطح فیلترینگ و وضعیت سرویس‌ها (۲۰۲۶)

- **Instagram / Facebook** کاملاً مسدود
- **Twitter (X)** دسترسی ناپایدار، اختلال گسترده
- **YouTube** مسدود نیست، اما با کاهش سرعت، اختلال در ویدئوهای HD و فشار سیاسی مداوم روبه‌روست [۲۱]

- **Google Search / Gmail** در دسترس، اما تحت فشار حقوقی و جریمه
- **Google Play** فعال، ولی با الزام نصب RuStore و محدودیت برای برخی اپ‌ها

Aurora OS سیستم‌عامل سازمانی روسیه

Aurora OS سیستم‌عاملی مبتنی بر **Sailfish OS** (سیستم‌عامل موبایلی متن‌باز و توسعه یافته توسط Jolla) است که توسط شرکت **Open Mobile Platform** توسعه یافته و بر امنیت، مدیریت متمرکز و استفاده سازمانی تمرکز دارد. این سیستم‌عامل:

- به‌طور پیش‌فرض فاقد خدمات و اپلیکیشن‌های گوگل است
- از رمزنگاری سرتاسری، MDM[۳] و کنترل سیاست‌های امنیتی پشتیبانی می‌کند
- برای مصرف‌کنندهٔ سازمانی و دولتی توسعه پیدا کرده است.

بر اساس گزارش وزارت توسعه دیجیتال روسیه و تحلیل IDC روسیه، تا پایان ۲۰۲۵ حدود **۳۰۰ تا ۵۰۰ هزار دستگاه** مبتنی بر Aurora OS در نهادهای دولتی، شرکت‌های دولتی و زیرساخت‌های حساس استفاده شده‌اند [۲۵][۲۶]. این عدد نشان‌دهنده **موفقیت محدود در حوزه دولتی** است. البته باید تاکید داشت که این سیستم‌عامل از ابتدا تنها برای استفاده سازمانی توسعه پیدا کرده است و احتمال موفقیت آن، حتی در این سطح، در بازار و مصرف عمومی بسیار پایین است.

---

۳. Mobile Device Management

جایگزین‌های خدمات گوگل در روسیه

خدمات گوگل	جایگزین روسی / سطح جایگزینی
Google Search	Yandex Search
Gmail	Yandex.Mail / Mail.ru
Google Play	RuStore
Google Maps	۲GIS / Yandex Maps
YouTube	RuTube / VK Video
Google Drive	Yandex.Disk / Domestic cloud

نقاط قوت: این جایگزین‌ها برای نیازهای عمومی داخلی مناسب‌اند و با قوانین دولت روسیه سازگار هستند.

نقاط ضعف: کمبود تعامل و همگام‌سازی جهانی، کیفیت پایین‌تر در جست‌وجوی بین‌المللی، و نبود استانداردهای جهانی توسعه‌دهندگان باعث محدودیت در پذیرش فرامرزی شده است.

چالش‌های باقی‌مانده برای کاربران

- **دسترسی به منابع جهانی:** بسیاری از سایت‌ها، اپلیکیشن‌ها و ابزارهای آموزشی، علمی و تجاری جهانی به‌صورت مستقیم قابل دسترسی نیستند.
- **وابستگی به ابزارهای دورزدن:** کاربران برای دسترسی به برخی خدمات نیاز به VPN و پراکسی دارند که این ابزارها نیز علیرغم تلاش دولت برای حذف و محدود کردن، همچنان در سطح گسترده‌ای استفاده می‌شوند.
- **پیامدهای حقوقی:** قوانین جدید، از جمله جرم‌انگاری جست‌وجوی محتوای «افراطی» حتی از طریق VPN، باعث افزایش ریسک استفاده کاربران از چنین ابزارهایی شده است.

دور زدن محدودیت‌ها و استفاده از VPN

بـر اسـاس گزارش‌هـای Levada Center،Meduza و Top۱۰VPN, بیـن ۳۰ تـا ۴۰ درصـد کاربـران اینترنـت روسـیه در سـال‌های ۲۰۲۴—۲۰۲۵ حداقـل به‌صـورت مقطعـی از VPN اسـتفاده کرده‌انـد [۲۷][۲۸]. اسـتفاده اصلی روسی‌ها از VPN، دسترسی به اینسـتاگرام، یوتیـوب، رسـانه‌های مسـتقل و اسـتفاده از خدمات گوگل بـدون محدودیت بـوده اسـت. بـا این حـال، اسـتفاده از VPN با ریسـک حقوقی، اختلال و مسدودسـازی‌های مسـتمر همـراه اسـت.

جمع‌بندی

تجربـه روسـیه نشـان می‌دهـد کـه سیاسـت تنظیـم‌گری سـخت‌گیرانه بـدون حـذف کامـل می‌توانـد کـنترل دولـت بـر فضـای دیجیتـال را افزایش دهـد، بدون آنکه شـوک اجتماعی مشـابه مـدل چین ایجاد کنـد. ایـن رویکـرد در کاهـش نفـوذ رسـانه‌ای پلتفرم‌های خارجی و تقویت بازیگران داخلی تـا حدی موفق بـوده، امـا بـه بهـای کاهـش کیفیـت دسترسـی، افزایـش نارضایتی کاربـران و وابسـتگی گسـترده بـه VPN هـا. تحلیل‌گـران غربـی ایـن مـدل را «حاکمیـت دیجیتـال ناقـص» توصیـف می‌کننـد: مدلـی کـه کـنترل را افزایش داده، اما هنوز نتوانسـته جایگزین‌های کاملاً رقابتی و پایدار برای اکوسیسـتم جهانی ایجاد کند [۱۶] [۲۹].

هند: چالش‌های استقلال دیجیتال و تلاش‌های برای بومی‌سازی

رویکرد و نگاه کلان هند

هند در مواجهه با پلتفرم‌های فناوری بزرگ مانند گوگل، رویکردی تنظیم‌گری مبتنی بر بازار، حاکمیت داده و رقابت‌محور اتخاذ کرده است. این رویکرد ریشه در باور سیاست‌گذاران هندی دارد که فناوری‌های جهانی برای رقابت اقتصادی، دسترسی به اطلاعات و رشد استارت‌آپی ضروری‌اند و در عین حال باید با قوانین سخت‌گیرانه حریم خصوصی، رقابت عادلانه و حفاظت از داده‌های شهروندان سازگار شوند. [۳۰] [۳۱]

بنا به دیدگاه تحلیل‌گران مرکز تحقیقاتی Carnegie Endowment، هند تلاش کرده کنترل فضای دیجیتال را از طریق ساخت نهادهای قوی، قوانین حریم خصوصی و فشار بر روی خدمات خاص اعمال کند، بدون اینکه دسترسی عمومی به اکوسیستم فناوری جهانی را مسدود کند، زیرا حذف این خدمات می‌توانست هزینه‌های شدید اجتماعی و اقتصادی ایجاد نماید.

اولین دلیل اتخاذ این نگاه در هند، تمایل به حفظ ارتباط با اقتصاد جهانی فناوری است. با جمعیت بیش از یک میلیارد نفر و بازار موبایل فعال، هند نمی‌تواند از خدماتی مانند گوگل سرچ، جی‌میل و گوگل پلی چشم‌پوشی کند؛ چراکه این خدمات بخش جدایی‌ناپذیر کسب‌وکارهای آنلاین، آموزش، ارتباطات حرفه‌ای و تجارت الکترونیک هستند [۳۲]. دوم، دولت هند با نگاهی به ارتباط میان داده، نهادهای مالی و توسعه اقتصاد دیجیتال، قوانین سخت‌گیرانه حریم خصوصی و رقابت (شامل

موانع رفتار انحصاری) را تقویت کرده است تا شرکت‌های بزرگ فناوری «در چارچوب قوانین بازار هند» عمل کنند، نه اینکه از ورود به بازار سردرگم شوند یا کلا قید بازار هند را بزنند. تحلیل‌های Brookings Institution نشان داده‌اند که این رویکرد کمک می‌کند هند از ظرفیت‌های فناوری جهانی بهره ببرد و در عین حال از تجربه نهادهای خارجی در انفجار اقتصادی دیجیتال عقب نماند[۳۳].

عامل سوم، ساختار نهادی قوی در هند است که به دولت این امکان را می‌دهد تا با قوانین و مقررات، حضور شرکت‌های بزرگ فناوری را تنظیم کند بدون آنکه مجبور شود به فیلترینگ یا انسداد گسترده روی آورد. این ساختار نهادی، ترکیبی از دستگاه‌های نظارتی مثل سازمان رگولاتوری مخابرات هند (TRAI)، سازمان ملی تحول هند (NITI Aayog)، وزارت الکترونیک و فناوری اطلاعات و دادگاه‌های قضایی بوده که با همکاری هم مسیر سیاست‌گذاری مستقل دیجیتال را تقویت کرده‌اند.[۳۰][۳۴] تجربهٔ مهمی که باید به آن توجه داشت آخرین تلاش دولت برای الزام نصب اپلیکیشن‌های دولتی روی گوشی‌های اندرویدی بود، از جمله اپ‌هایی با هدف ارائه خدمات عمومی یا امنیتی. برجسته‌ترین نمونه در این زمینه، دستور نصب اجباری اپ «Sanchar Saathi» بود که دولت قصد داشت آن را به‌صورت پیش‌فرض روی تمامی گوشی‌های عرضه‌شده در کشور نصب و حذف‌ناپذیر کند. این اپ با هدف ارائه خدمات شناسایی و امنیت ملی معرفی شد اما بلافاصله با واکنش شدید عمومی، رسانه‌ای و حقوقی مواجه شد؛ کارشناسان حریم خصوصی، جامعه مدنی و فعالان دیجیتال معتقد بودند که چنین الزاماتی حقوق فردی، حریم خصوصی و انتخاب مصرف‌کننده را تضعیف می‌کند. در نهایت، قانون‌گذاران و قضات عالی کشور به‌طور موقت یا دائمی اجرای این اجباری را متوقف کردند، دولت را مجبور کردند به سمت روش‌های اختیاری، شفاف و مبتنی بر رضایت کاربر برود. این تجربه نشان داد که در هند، حتی اگر دولت بتواند ابزارهای اجرایی برای اعمال دسترسی سخت‌افزاری یا نرم‌افزاری ایجاد کند، آمادگی اجتماعی، نظارت قانونی و حساسیت به حریم خصوصی می‌تواند مانع از پیاده‌سازی کامل چنین سیاست‌هایی شود، موضوعی که در صورت تلاش برای محدود کردن یا جایگزینی سرویس‌های گوگل نیز باید مورد توجه قرار گیرد.

هزینه‌ها و الزامات پیاده‌سازی

تخمین هزینه‌ها در کاربرد این مدل پیچیده است و دولت هند هیچگاه به صورت رسمی در این مورد اظهارنظر نکرده است. با این حال، بر اساس گزارش KPMG India، هند بین سال‌های ۲۰۱۸ تا ۲۰۲۵ حدود ۲ تا ۳ میلیارد دلار را به توسعه چارچوب‌های قانونی حفظ حریم خصوصی، اجرای آن و حمایت از پروژه‌های بومی اختصاص داده است [۳۵]. این هزینه شامل خدمات مشاوره، آموزش اپراتورها برای انطباق با قوانین جدید، سرمایه‌گذاری در سازمان‌های ناظر و پروژه‌های آزمایشی است اما هیچ سرمایه‌گذاری مستقیمی روی زیرساخت‌های فیلترینگ یا حذف کامل خدمات خارجی وجود نداشته است.

برخی تحلیل‌ها نیز اشاره کرده‌اند که حذف کامل خدمات گوگل می‌توانست هزینه‌ای بیش از ۴۰ تا ۵۰ میلیارد دلار برای اقتصاد دیجیتال هند در طول پنج سال به دنبال داشته باشد، به دلایلی مانند افت بهره‌وری، دسترسی به بازار جهانی، کاهش سرمایه‌گذاری خارجی و پیامدهای آموزشی و تجاری [۳۶].

تاریخچه اجرا و روند عملیاتی

حرکت هند به سمت تنظیم‌گری مستقل در فضای دیجیتال نیز روندی تدریجی داشته است:

- ۲۰۱۶: پیشنهادات اولیه درباره قوانین حریم خصوصی داده‌ها
- ۲۰۱۸: قانون حفاظت از داده‌های شخصی در دستور کار وزارت الکترونیک قرار گرفت
- ۲۰۲۰: آغاز الزامات شفافیت برای شرکت‌های فناوری خارجی
- ۲۰۲۲: دستورالعمل‌های جدید □□□□ برای انطباق با رقابت عادلانه
- ۲۰۲۳–۲۰۲۵: فشار بر روی نحوه دسترسی به سرویس‌های خارجی، به همراه

تشدید جرایم بر نقض قوانین داده

زیرساخت‌های اعمال سیاست

زیرساخت سیاست‌گذاری دیجیتال هند شامل موارد زیر است:

- قوانین حریم خصوصی داده‌ها که شرکت‌ها باید داده را در چارچوب مشخص جمع‌آوری و ذخیره کنند
- الزامات شفافیت برای الگوریتم‌ها و سرویس‌های شخص ثالث
- نظارت حقوقی قوی از طریق دادگاه‌های دادگستری و مراجع نظارتی
- بسترهای حکومتی برای سیاست‌گذاری مثل NITI Aayog و شورای عالی فناوری اطلاعات

این چارچوب باعث شده خدمات خارجی بدون فیلترینگ یا مسدودیت‌های سخت‌گیرانه به فعالیت خود ادامه دهند، اما همزمان تحت نظارت و گزارش‌دهی شدید به نهادهای نظارتی قرار گیرند.

وضعیت فیلترینگ و محدودیت‌ها (۲۰۲۶)

در هند برخلاف چین یا روسیه، هیچ سرویس فناوری بزرگی به‌طور کلی مسدود نشده است. خدمات گوگل همچنان در دسترس مستقیم کاربران قرار دارد. با این حال، عبارت‌ها و خدمات خاصی که نقض قوانین حریم خصوصی تلقی شوند ممکن است برای مدتی تحت بررسی قرار گیرند، یا تنظیمات مرتبط با جمع‌آوری داده‌ها مجبور به تغییر شوند [۳۷].

BharOS: تلاش هند برای کاهش وابستگی به خدمات گوگل

BharOS (Bharat Operating System) یک تلاش بومی برای ایجاد سیستم‌عاملی مستقل از خدمات

گـوگل اسـت کـه بر پایـه Android Open Source Project (AOSP) و بـا مشـارکت بخـش آکادمیـک و خصوصـی توسـعه یافتـه اسـت [۳۸][۳۹]. اهـداف اصلـی آن عبارتنـد از:

- حذف ماژول‌های خدمات گوگل
- افزایش کنترل حریم خصوصی
- ارائه بسترامن برای توسعه‌دهندگان محلی

از نظر فنی BharOS قابلیت پشتیبانی از فروشگاه‌های اپ اختصاصی به نام PASS[۴] را دارد که امکان توزیع اپ‌ها بدون وابستگی به گوگل پلی را فراهم می‌کند. با این حال، تا اواخر ۲۰۲۵ تنها ۵۰۰۰ تا ۲۰۰۰۰ دستگاه آزمایشی با این سیستم‌عامل فعال شده‌اند و عرضه گسترده به بازار مصرف‌کننده عمومی هنوز شکل نگرفته است [۴۰][۴۱]. این تعداد نسبتاً اندک نشان می‌دهد که BharOS اکنون در مرحله آزمایشی یا مصرف محدود شرکتی/آزمایشی قرار دارد.

با وجود علاقۀ سیاست‌گذاران هندی به BharOS، ارزیابی‌های کارشناسی نشان می‌دهد که هند در کوتاه‌مدت توان توسعه یک سیستم‌عامل عاری از سرویس‌های گوگل در میان عموم مردم را ندارد. دلیل اصلی این محدودیت، نه فقدان توان فنی پایه، بلکه وابستگی عمیق اکوسیستم موبایل هند به اندروید است. بیش از ۹۵ درصد گوشی‌های هوشمند فعال در هند مبتنی بر اندروید هستند و بخش عمده تجربه کاربری، از پرداخت دیجیتال گرفته تا آموزش، حمل‌ونقل و سلامت، به اپلیکیشن‌هایی وابسته است که به‌طور مستقیم یا غیرمستقیم به خدمات گوگل متکی‌اند [۴۴]. برخلاف برخی گمانه‌زنی‌ها، اسناد رسمی و اظهارات مقامات وزارت الکترونیک و فناوری اطلاعات هند نشان می‌دهد که BharOS به‌عنوان جایگزین اندروید برای عموم مردم تعریف نشده است. بلکه دولت آن را یک پلتفرم راهبردی اختصاصی می‌داند که کاربرد اصلی آن در سه حوزه است:

۱. نهادهای دولتی حساس

۴. Private Application Store Services

۲. بخش‌های نظامی، امنیتی و زیرساخت‌های حیاتی

۳. سازمان‌ها و شرکت‌هایی با نیاز امنیتی بالا

بر اساس گزارش The Economic Times و Hindu BusinessLine، برنامه دولت تا سال ۲۰۲۷ تمرکز بر استفاده محدود اما پایدار BharOS در دستگاه‌های دولتی و پروژه‌های سازمانی است، و نه جایگزینی آن با اندروید در بازار مصرف‌کنندگان عمومی [۴۸][۴۹]. حتی در حوزه‌های مطرح شده نیز BharOS بیشتر به‌عنوان گزینه مکمل امن مطرح است تا یک جایگزین کامل؛ به این معنا که بسیاری از نهادها همچنان از اندروید یا iOS برای کاربری عمومی و از BharOS برای کاربردهای خاص استفاده خواهند کرد.

این چشم‌انداز نشان می‌دهد که هند برخلاف چین، به دنبال ساخت یک اکوسیستم موازی کامل نیست، بلکه می‌خواهد در مواقع حساس، گزینه‌ای مستقل و بومی در اختیار داشته باشد [۵۰].

دور زدن محدودیت‌ها

از آنجا که هیچ فیلترینگ عمومی اصلی وجود ندارد، دور زدن محدودیت‌ها مانند استفاده از VPN برای راهکارهای عمومی ضرورت ندارد. بر اساس گزارش Top۱۰VPN، درصد استفاده از VPN در میان کاربران هندی بین ۱۵ تا ۲۵ درصد است، اما معمولاً به دلایل مربوط به حفظ حریم خصوصی، تماشای محتواهای منطقه‌ای و امنیت شبکه‌های عمومی انجام می‌شود [۴۳].

جمع‌بندی

BharOS بیش از آنکه نماد «جدایی از گوگل» باشد، ابزار چانه‌زنی راهبردی و بیمه امنیتی دولت هند است. تجربهٔ ناموفق نصب پیش‌فرض و اجباری اپ‌های دولتی به هند آموخته که حذف یا محدودسازی شدید سرویس‌های جهانی بدون آماده‌سازی اجتماعی و فنی، پرهزینه و ناپایدار است. بنابراین، مسیر هند نه حذف گوگل، بلکه کاهش وابستگی در حوزه‌های حساس، افزایش قدرت تنظیم‌گری و حفظ انعطاف راهبردی است؛ مسیری که به احتمال زیاد در آینده نیز ادامه خواهد یافت.

کره‌جنوبی: تنظیم‌گری سخت‌گیرانه بدون حذف اکوسیستم گوگل

رویکرد و نگاه کلان

کره‌جنوبی رویکردی **کاملاً متمایز از چین و روسیه** در قبال خدمات گوگل و اندروید اتخاذ کرده است. سیاست کلان سئول نه بر حذف یا فیلترینگ خدمات گوگل، بلکه بر **تنظیم‌گری شدید، اعمال حاکمیت رقابتی و محدودسازی رفتارهای انحصارگرایانه** این شرکت‌ها است. این رویکرد ریشه در ترکیب خاصی از سیاست صنعتی کره، ساختار اقتصاد دیجیتال، و جایگاه این کشور در نظام بین‌الملل دارد.

تحلیل‌های منتشرشده در **Brookings Institution** و **Financial Times** نشان می‌دهد که کره‌جنوبی گوگل را نه تهدیدی امنیتی به سبک چین، و نه ابزار نفوذ ژئوپلیتیک به سبک نگاه روسیه، بلکه **بازیگری اقتصادی با قدرت بازار فوق العاده** تلقی می‌کند که باید مهار شود، بدون آنکه مزایای اتصال به اکوسیستم جهانی فناوری قربانی شود.[۵۱][۵۲]

انتخاب مسیر تنظیم‌گری به‌جای حذف، نتیجه چند عامل هم‌زمان است. نخست، **وابستگی عمیق اقتصاد دیجیتال کره‌جنوبی به بازارهای جهانی**؛ شرکت‌هایی مانند Samsung، LG، Naver و Kakao خود بازیگران بین‌المللی‌اند و حذف گوگل می‌توانست به اقدام متقابل یا بی‌ثباتی اکوسیستم منجر شود. دوم، **ظرفیت نهادی و حقوقی بالای دولت کره** در اعمال قانون رقابت و تنظیم‌گری پلتفرم‌ها، که نیاز به ابزارهای سخت مانند فیلترینگ را کاهش داده است.

سوم، نگاه کره‌جنوبی به «حکمرانی فضای مجازی» مبتنی بر **قانون، شفافیت و رقابت** است نه

کنترل زیرساختی. برخلاف چین، دولت کره نه زیرساخت فنی برای فیلترینگ سراسری دارد و نه اجماع سیاسی-اجتماعی برای چنین مداخله‌ای. در عوض، از ابزارهایی مانند قانون ضدانحصار، جریمه‌های سنگین و الزام به تغییر رفتار تجاری استفاده می‌کند[۵۳].

یکی از نمونه‌های شاخص تنظیم‌گری کره‌جنوبی در قبال گوگل، محدودسازی داده‌های دقیق مکانی در سرویس نقشه گوگل است. دولت کره‌جنوبی از اوایل دهه ۲۰۱۰ به‌دلیل ملاحظات امنیت ملی، به گوگل اجازه خروج داده‌های نقشه‌های با دقت بالا، به‌ویژه اطلاعات مرتبط با تأسیسات نظامی و زیرساخت‌های حیاتی، را نداده است. در نتیجه، نسخه کره‌ای نقشه گوگل سال‌ها با دقت کمتر و قابلیت‌های محدودتر نسبت به رقبای بومی مانند Naver Maps و Kakao Maps ارائه شده، بدون آنکه خود سرویس به‌طور کامل مسدود شود. به عبارتی کره‌جنوبی به‌جای حذف پلتفرم خارجی، از ابزارهای حقوقی و حاکمیتی برای کنترل لایه‌های حساس داده استفاده کرده است. این رویکرد، نمونه‌ای عملی از «حکمرانی داده‌محور» است که در آن دولت بدون قطع ارتباط با اکوسیستم جهانی، حاکمیت خود را بر داده‌های راهبردی حفظ می‌کند.

هزینه‌ها و الزامات پیاده‌سازی این رویکرد

اجرای تنظیم‌گری سخت‌گیرانه هزینه‌های مستقیم زیرساختی سنگینی نداشته، اما **هزینه‌های حقوقی، نهادی و سیاسی قابل‌توجهی** برای دولت کره ایجاد کرده است. بر اساس گزارش Korea Fair Trade Commission (KFTC) و تحلیل‌های رویتر، هزینه تقویت نهادهای تنظیم‌گر و تیم‌های تخصصی حقوق رقابت دیجیتال، طبق برآورد رسانه‌های اقتصادی کره، **صدها میلیون دلار در یک دهه** بوده است. در مقابل، جریمه‌های اعمال‌شده به گوگل و اپل به‌تنهایی **بیش از ۳۰۰ میلیون دلار** برآورد می‌شود. [۵۴] [۵۵]

به عبارتی کره جنوبی به جای سرمایه‌گذاری‌های زیرساختی، **در مسیر افزایش ظرفیت حکمرانی و استمرار حقوقی** هزینه کرده است.

تاریخ اجرا و روند عملیاتی

رویکردکره‌جنوبی تدریجی، مرحله‌به‌مرحله ومبتنی برقانون‌گذاری بوده‌است:

- **۲۰۱۱—۲۰۱۳**: آغاز تحقیقات ضدانحصار دربارۀ اندروید و گوگل سرچ
- **۲۰۱۶**: جریمه گوگل به دلیل محدودسازی تولیدکنندگان گوشی
- **۲۰۲۰**: تشدید بررسی رفتارهای انحصاری درگوگل پلی
- **۲۰۲۱**: تصویب قانون تاریخی موسوم به **Anti-Google Law** (اصلاح قانون کسب‌وکارهای مخابراتی)
- **۲۰۲۲—۲۰۲۴:** الزام گوگل و اپل به آزاد کردن سیستم‌های پرداخت جایگزین
- **۲۰۲۵—۲۰۲۶**: ادامه نظارت بر اجرای قانون و بررسی اثرات رقابتی آن [۵۶][۵۷]

سطح محدودسازی و وضعیت سرویس‌های گوگل (۲۰۲۶)

درکره‌جنوبی تمامی خدمات گوگل با رعایت قوانین کشور (مانند آزاد بودن پرداخت‌های جایگزین) فعال هستند. هیچ نهاد یا مقامی دسترسی ویژه یا استثنایی ندارد، زیرا **اصلاً فیلترینگی وجود ندارد.**

جایگزین‌های خدمات گوگل درکره جنوبی

کره‌جنوبی برخلاف چین، خدمات داخلی را به اجبار جایگزین خدمات گوگل نکرده، اما پلتفرم‌های قدرتمند داخلی دارد:

خدمات گوگل	جایگزین کره‌ای
Google Search	Naver
Google Maps	Kakao Maps / Naver Maps
YouTube	AfreecaTV(SOOP)
Google Play	One Store

نقاط قوت:

- کیفیت بالا در نیازهای داخلی
- رقابت واقعی با گوگل در برخی حوزه‌ها

نقاط ضعف:

- ناتوانی در بازار جهانی
- وابستگی به اندروید و iOS

چالش‌های دولت کره جنوبی در حکمرانی فضای مجازی

- وابستگی ساختاری به اندروید به‌عنوان سیستم‌عامل
- فشار لابی شرکت‌های فناوری آمریکا
- دشواری اجرای مؤثر قوانین بدون ایجاد هزینه برای توسعه‌دهندگان
- محدود بودن اثر تنظیم‌گری به بازار داخلی

جمع‌بندی

تجربه کره‌جنوبی نشان می‌دهد که **کنترل گوگل لزوماً به معنای حذف گوگل نیست.** این کشور با تکیه بر نهادهای قوی، قانون رقابت و قدرت بازار داخلی، موفق شده بدون فیلترینگ یا قطع

سرویس، بخشی از رفتارهای انحصاری گوگل را مهار کند. در عین حال، این مدل تنها در کشورهایی قابل پیاده‌سازی است که **ظرفیت حقوقی، استقلال قضایی و قدرت اقتصادی بالا** دارند. کره‌جنوبی نمونه‌ای از «حکمرانی تنظیم‌گرانۀ پیشرفته» است.

ملاحظات، ضرورت‌ها و محدودیت‌های استفاده از گوشی‌های اندرویدی در میان مقامات کشوری و امنیتی رده بالا

۱. مقدمه

گوشی‌های هوشمند طی یک دهه گذشته از ابزارهای صرفاً ارتباطی به زیرساخت‌های چندمنظوره پردازش، ذخیره و انتقال داده تبدیل شده‌اند. برای مقامات کشوری و امنیتی، به‌ویژه در سطوح بالادستی، این تحول به‌معنای شکل‌گیری یک «نقطه تمرکز ریسک» است؛ نقطه‌ای که هم‌زمان محل تلاقی ارتباطات شخصی، کاری، تصمیم‌سازی، جابه‌جایی فیزیکی و تعاملات نهادی است. در چنین شرایطی، سیاست‌گذاری درباره استفاده از گوشی‌های هوشمند، دیگر یک موضوع اداری یا انضباطی ساده نیست، بلکه بخشی از معماری کلان امنیت ملی محسوب می‌شود. [۶۰]

در میان سیستم‌عامل‌های موبایل، اندروید به‌دلیل ماهیت باز، تنوع شدید تولیدکنندگان، وابستگی به زنجیره تأمین پیچیده و اکوسیستم نرم‌افزاری گسترده، جایگاه ویژه‌ای در مباحث امنیتی پیدا کرده است. بسیاری از کشورها، حتی بدون اعلام ممنوعیت‌های صریح، در سال‌های اخیر به سمت اعمال محدودیت‌های عملیاتی، تفکیک سطح دسترسی و کنترل نهادی بر استفاده از گوشی‌های اندرویدی برای مقامات حساس حرکت کرده‌اند [۶۱]. در ادامه به بررسی ابعاد این مسئله و مقایسه الگوهای منتخب بین‌المللی می‌پردازیم.

۲. بیان مسئله

مسئله اصلی این گزارش، ریسک استفاده از گوشی‌های اندرویدی توسط مقامات کشوری و امنیتی رده بالا و نحوه مواجهه دولت‌ها با این ریسک است. این ریسک، ماهیتی یکنواخت ندارد و به‌شدت به سطح مقام، نوع مأموریت، میزان دسترسی به اطلاعات حساس و محیط عملیاتی وابسته است. برای مقامات عادی دولتی، ریسک استفاده از اندروید عمدتاً در سطح نشت اطلاعات اداری، دسترسی غیرمجاز به ایمیل‌ها و پیام‌های رد و بدل شده و سوءاستفاده از داده‌های سازمانی تعریف می‌شود. این ریسک‌ها معمولاً با ابزارهایی مانند مدیریت دستگاه همراه (MDM) و سیاست‌های امنیت اطلاعات قابل کنترل هستند [۶۲]. اما در سطح مقامات بالادستی، گوشی هوشمند به مخزنی از داده‌های بسیار حساس تبدیل می‌شود: الگوهای ارتباطی، شبکه روابط غیررسمی، اطلاعات مکانی، زمان‌بندی جلسات، و حتی سرنخ‌هایی از فرآیند تصمیم‌سازی.

در مورد مقامات نظامی و امنیتی، ریسک از سطح اطلاعاتی فراتر می‌رود و وارد حوزه‌های عملیاتی و راهبردی می‌شود. نفوذ یا بهره‌برداری از یک گوشی اندرویدی می‌تواند به شناسایی زنجیره فرماندهی، الگوهای جابه‌جایی، یا حتی مختل‌سازی تصمیم‌گیری در شرایط بحرانی منجر شود [۶۳].

اندروید نسبت به گوشی های ساده یا حتی برخی سیستم عامل های بسته تر، خطر پذیری بالاتری دارد، زیرا:

- معماری آن اجازه نصب اپلیکیشن از منابع متنوع را می‌دهد؛
- به‌روزرسانی‌های امنیتی به‌شدت وابسته به تولیدکننده و اپراتور است؛
- سطح دسترسی اپ‌ها به اجزای سیستم در بسیاری از پیاده‌سازی‌ها گسترده‌تر است؛
- و زنجیره تأمین سخت‌افزار و نرم‌افزار آن به‌طور کامل تحت کنترل یک نهاد واحد نیست [۶۴].

۳. تهدیدشناسی استفاده از اندروید برای مقامات کشوری و امنیتی رده بالا

۳.۱ تهدیدات فنی

از منظر فنی، گوشی اندرویدی یک سیستم‌عامل کامل با کرنل[۵]، سرویس‌های پس‌زمینه، API ها و لایه‌های متعدد نرم‌افزاری است. هر یک از این لایه‌ها می‌تواند محل بروز آسیب‌پذیری باشد. گزارش‌های امنیتی سال‌های اخیر نشان می‌دهد که فاصله زمانی بین کشف آسیب‌پذیری‌های بحرانی اندروید و برطرف شدن آن‌ها روی دستگاه‌های واقعی، به‌ویژه خارج از اکوسیستم گوشی‌های پرچم‌دار، می‌تواند بسیار طولانی باشد [۶۵].

برای مقامات بالادستی، این تأخیر به‌معنای قرارگرفتن طولانی‌مدت در معرض حملات روز صفر، بدافزارهای پیشرفته و جاسوس‌افزارهای دولتی است. نمونه‌هایی مانند Pegasus یا Predator نشان داده‌اند که نفوذ به گوشی‌های اندرویدی، حتی بدون تعامل کاربر، کاملاً امکان‌پذیر است و می‌تواند به کنترل کامل دستگاه منجر شود [۶۶].

۳.۲ تهدیدات اطلاعاتی

گوشی اندرویدی صرفاً ابزار انتقال پیام یا تماس نیست؛ بلکه یک پایگاه داده پویا از زندگی دیجیتال مقام مسئول است. داده‌های مکانی، تاریخچه تماس‌ها، متادیتای پیام‌رسان‌ها، فایل‌های ذخیره‌شده و حتی داده‌های سنسورها می‌توانند برای تحلیل‌های اطلاعاتی بسیار ارزشمند باشند [۶۷].

در سطح مقامات بالادستی، این داده‌ها امکان پروفایل‌سازی رفتاری و شبکه‌ای را برای بازیگران خارجی یا داخلی فراهم می‌کند. حتی در صورت رمزنگاری محتوای پیام‌ها، متادیتا همچنان می‌تواند الگوهای ارتباطی حساس را آشکار کند. بسیاری از نهادهای امنیتی، این نوع نشت غیرمستقیم اطلاعات را از خطرناک‌ترین ابعاد استفاده از گوشی‌های هوشمند می‌دانند [۶۸].

---

۵. Kernel

۳.۳ تهدیدات رفتاری و انسانی

بخش قابل‌توجهی از ریسک اندروید نه از ضعف فنی، بلکه از رفتار انسانی ناشی می‌شود. نصب اپلیکیشن‌های عمومی، استفاده هم‌زمان از گوشی برای امور شخصی و کاری، اتصال به شبکه‌های ناامن و بی‌توجهی به تنظیمات حریم خصوصی، همگی ریسک‌های انباشته ایجاد می‌کنند [۶۹].

برای مقامات ارشد، این مسئله پیچیده‌تر است؛ زیرا فشار کاری، تعاملات گسترده و اعتماد بیش‌ازحد به ابزارهای روزمره می‌تواند منجر به کاهش حساسیت امنیتی شود. بسیاری از پروتکل‌های بین‌المللی دقیقاً به همین دلیل بر تفکیک گوشی کاری و شخصی تأکید دارند [۷۰].

۳.۴ تهدیدات سیاسی—راهبردی

در سطح کلان، استفاده از اندروید توسط مقامات حساس، بخشی از مسئله وابستگی فناورانه است. اکوسیستم اندروید به شرکت‌ها، زیرساخت‌ها و سیاست‌های فرامرزی گره خورده است. این وابستگی می‌تواند در شرایط تنش سیاسی یا تحریم، به اهرم فشار یا نقطه آسیب‌پذیری راهبردی تبدیل شود [۷۱].

برخی کشورها این مسئله را نه صرفاً یک خطر فنی، بلکه بخشی از رقابت ژئوپلیتیک در فضای سایبری می‌دانند. از این منظر، کنترل یا محدودسازی استفاده از اندروید در سطوح بالادستی، اقدامی پیشگیرانه برای حفظ استقلال تصمیم‌سازی تلقی می‌شود [۷۲].

۴. الگوهای بین‌المللی: قوانین و پروتکل‌های استفاده از گوشی‌های هوشمند در سطوح دولتی و امنیتی

۴.۱ آمریکا

چارچوب کلی سیاست

ایالات متحده رویکردی مبتنی بر **مدیریت ریسک، تفکیک سطح دسترسی و استانداردسازی فنی** دارد و برخلاف برخی کشورها، به سمت ممنوعیت صریح سیستم‌عامل خاصی (از جمله اندروید) نرفته است. سیاست آمریکا بر این پیش‌فرض استوار است که تهدید اصلی سیستم‌عامل‌هایی مثل اندروید نیستند، بلکه **نحوه پیکربندی، مدیریت و استفاده از گوشی هوشمند** در سطوح مختلف حاکمیتی است. روند سیاستی آمریکا نشان می‌دهد که تمرکز اصلی بر **کنترل نرم‌افزاری، مدیریت مرکزی دستگاه (MDM) و آموزش رفتاری کاربران ارشد** است، نه حذف یک پلتفرم. این رویکرد ناشی از تنوع بالای نهادها و هزینه سیاسی و اجرایی ممنوعیت مطلق است [۷۴].

تفاوت سطح مقامات و نهادها

در سطوح پایین‌تر دولت فدرال، استفاده از گوشی‌های هوشمند شخصی (از جمله اندروید) در قالب سیاست‌های BYOD (Bring your own device) مجاز است، مشروط به اجرای کنترل‌های امنیتی پایه. یعنی کارمندان فدرال سطح پایین می‌توانند از گوشی شخصی خود برای کارهای دولتی استفاده

کنند اما باید تاییدیه‌ها و آموزش‌های امنیتی لازم را از مسئولین IT بگیرند، با این حال دسترسی به اطلاعات محرمانه و طبقه‌بندی شده با این دستگاه‌ها ممنوع است. در بعضی موارد هم لازم است نرم‌افزارهای امنیتی مورد تایید یا MDM بر روی این دستگاه‌ها نصب شود. اما برای مقامات ارشد، مسئولان سیاست خارجی، امنیت ملی، دفاع و اطلاعات، قواعد کاملاً متفاوتی اعمال می‌شود. در این سطوح:

- استفاده از **گوشی‌های دولتی مدیریت‌شده (Government-Furnished Equipment)** ترجیح داده می‌شود؛
- دسترسی به اطلاعات طبقه‌بندی‌شده از طریق موبایل عملاً ممنوع است؛
- و گوشی شخصی نباید به سامانه‌های حساس متصل شود [۷۴].

توصیه‌های اصلی دولت آمریکا بر موارد زیر است:

تفکیک کامل گوشی کاری و شخصی؛

محدودسازی نصب اپلیکیشن‌ها از طریق لیست سفید؛

و استفاده از پیام‌رسان‌های تأییدشده سازمانی دارد. پیام‌رسان‌های عمومی حتی اگر رمزنگاری سرتاسری داشته باشند، برای ارتباطات رسمی یا حساس توصیه نمی‌شوند، زیرا متادیتا و مدیریت سرورها خارج از کنترل دولت است [۷۵].

۴.۲ اسرائیل

چارچوب کلی سیاست

اسرائیل یکی از صریح‌ترین و متمرکزترین رویکردها را در میان کشورهای بررسی‌شده دارد. نگاه نهادهای امنیتی و نظامی اسرائیل به گوشی هوشمند، نه به‌عنوان ابزار شخصی، بلکه به‌عنوان **نقطه نفوذ عملیاتی بالقوه** است [۷۷].

بینش اسرائیل مبتنی بر **کاهش سطح حمله**[۶] است. سیاست این کشور نشان می‌دهد که در سطوح بسیار حساس، **سادگی، کنترل‌پذیری و یکپارچگی پلتفرم** بر آزادی انتخاب کاربر اولویت دارد [۷۹].

تفاوت سطح مقامات و نهادها

در نهادهای غیرنظامی، محدودیت‌ها بیشتر توصیه‌ای و نهادی است. اما در نیروهای دفاعی اسرائیل (IDF) و نهادهای اطلاعاتی:

- برای افسران ارشد، استفاده از برخی مدل‌ها یا سیستم‌عامل‌ها (به‌ویژه اندروید) محدود یا ممنوع شده است؛
- استانداردسازی روی پلتفرم‌هایی با چرخه به‌روزرسانی کنترل‌پذیرتر (مانند iOS) دنبال می‌شود؛
- و در بسیاری از موقعیت‌های عملیاتی، حمل هر نوع گوشی هوشمند ممنوع است [۷۸].

پیام‌رسان‌ها و اپ‌ها

پیام‌رسان‌های عمومی، حتی داخلی، در سطوح بالای نظامی تنها در شرایط بسیار کنترل‌شده مجازند. ارتباطات رسمی باید از کانال‌های رمزنگاری‌شده اختصاصی استفاده کنند. نصب اپلیکیشن‌های غیرضروری روی گوشی کاری عملاً ممنوع است.

۴.۳ چین

چارچوب کلی سیاست

چین ممنوعیت رسمی و اعلام‌شده‌ای برای اندروید ندارد، اما سیاست آن در قالب یک چارچوب

---

۶. **Attack Surface Reduction**

کلان‌تر تعریف می‌شود، **حاکمیت سایبری و کنترل زنجیره داده و فناوری.** در این چارچوب، گوشی هوشمند صرفاً یکی از اجزای اکوسیستم اطلاعاتی است [۸۰]. روند سیاستی چین نشان‌دهنده حرکت مستمر به سمت **خودکفایی دیجیتال و کنترل سخت‌گیرانه داده** است. در این نگاه، اندروید نه به‌خاطر ذاتش، بلکه به‌دلیل وابستگی به اکوسیستم خارجی، یک ریسک بالقوه محسوب می‌شود [۸۲].

تفاوت سطح مقامات و نهادها

در سطوح عادی دولتی، استفاده از گوشی‌های هوشمند خارجی رایج است. اما در نهادهای امنیتی، حزبی و تصمیم‌ساز:

- استفاده از گوشی‌ها و اپلیکیشن‌های خارجی به‌شدت محدود می‌شود؛
- کنترل نهادی بر نرم‌افزار، ترافیک داده و به‌روزرسانی‌ها اعمال می‌شود؛
- و در بسیاری موارد، استفاده از دستگاه‌ها و اپ‌های بومی ترجیح داده می‌شود [۸۱].

پیام‌رسان‌ها، اپ‌ها و بومی‌سازی

چین یکی از معدود کشورهایی است که اکوسیستم کامل پیام‌رسان و اپ بومی در اختیار دارد. پیام‌رسان‌های داخلی، تحت نظارت کامل، جایگزین گزینه‌های خارجی شده‌اند. این سیاست مستقیماً به کاهش ریسک نشت داده و نفوذ خارجی مرتبط است.

۴.۴ روسیه

چارچوب کلی سیاست

روسیه تمرکز خود را نه بر سیستم عامل، بلکه بر **کنترل ارتباطات، پیام‌رسان‌ها و جریان داده**

گذاشته است. سیاست‌های این کشور پس از ۲۰۱۴ و تشدید تحریم‌ها، رنگ‌وبوی راهبردی‌تری گرفته‌اند [۸۳]. بینش روسیه بر **حاکمیت دیجیتال و کاهش وابستگی نرم‌افزاری** استوار است. اندروید به‌خودی‌خود ممنوع نیست، اما محیط استفاده از آن به‌شدت کنترل می‌شود [۸۵].

تفاوت سطح مقامات و نهادها

برای مقامات عادی، استفاده از گوشی هوشمند محدودیت خاصی ندارد. اما برای نهادهای امنیتی و دولتی حساس:

استفاده از پیام‌رسان‌های خارجی یا اپ‌های خارج از کنترل دولت محدود یا ممنوع می‌شود؛

ارتباطات رسمی باید از بسترهای داخلی عبور کند؛

و در برخی موارد، گوشی‌های خاص با سیستم عامل و نرم‌افزار سفارشی استفاده می‌شود (AuroraOS). [۸۳]

پیام‌رسان‌ها و اپ‌ها

تمرکز روسیه بر جایگزینی پیام‌رسان‌های خارجی با نمونه‌های داخلی است. سیاست این کشور بیشتر نرم‌افزارمحور است تا سخت‌افزارمحور.

۴.۵ کره جنوبی

چارچوب کلی سیاست

کره جنوبی رویکردی **محیط‌محور و عملیاتی** دارد. سیاست‌ها بیشتر ناظر به «کجا» و «در چه شرایطی» گوشی هوشمند استفاده می‌شود، نه اینکه «چه سیستم‌عاملی» دارد [۸۶]. رویکرد کره جنوبی نشان می‌دهد که **کنترل فیزیکی و محیطی** هنوز یکی از مؤثرترین ابزارهای کاهش ریسک موبایل در نهادهای حساس است [۸۷].

تفاوت سطح مقامات و نهادها

در محیط‌های نظامی، اطلاعاتی و تحقیقاتی حساس:

- حمل گوشی هوشمند، اعم از اندروید یا iOS ممنوع یا محدود است؛
- در محیط‌های غیرحساس، محدودیت‌ها کاهش می‌یابد؛
- و برای مقامات ارشد، توصیه‌های رفتاری و امنیتی سخت‌گیرانه‌تری اعمال می‌شود.

پیام‌رسان‌ها و اپ‌ها

تمرکز بر جلوگیری از نشت اطلاعات محیطی (عکس، صدا، موقعیت) است. پیام‌رسان‌ها موضوع ثانویه محسوب می‌شوند.

۴.۶ ترکیه

چارچوب کلی سیاست

ترکیه ممنوعیت مستقیمی برای اندروید ندارد، اما در سال‌های اخیر چارچوب‌های امنیت سایبری خود را تقویت کرده است. تمرکز سیاستی بر **حفاظت از داده‌های دولتی و ارتباطات رسمی** است [۸۸]. سیاست ترکیه را می‌توان **میانه‌رو و تدریجی** دانست؛ بدون ممنوعیت سیستم‌عامل، اما با افزایش کنترل نرم‌افزاری و نهادی [۸۹].

تفاوت سطح مقامات و نهادها

در نهادهای امنیتی و نظامی:

- استفاده از پیام‌رسان‌های عمومی برای امور کاری محدود می‌شود؛
- توصیه به استفاده از بسترهای داخلی افزایش یافته است؛
- و تفکیک گوشی کاری و شخصی مورد تأکید قرار گرفته است.

۵. مقایسه تطبیقی کشورها در قبال استفاده از گوشی‌های اندروید توسط مقامات دولتی و نظامی

کشور	ممنوعیت‌یا محدودیت استفاده‌از اندروید	تمرکز سیاستی اصلی	منابع تهدید اصلی‌از دید کشور	تفکیک توصیه‌ها بر اساس سطح مقام‌ونهاد	تأکید بر موبایل، سیستم‌عامل یا اپ‌بومی	تمرکز امنیتی غالب
آمریکا	ممنوعیت صریح ندارد؛ محدودیت شدید در سطوح بالا	مدیریت ریسک، کنترل MDM، استانداردسازی	جاسوسی سایبری، نفوذ نرم‌افزاری، نشت متادیتا	بله؛ تمایز روشن بین کارکنان عادی، مقامات ارشد و نهادهای امنیتی	تأکید محدود؛ استفاده از ابزارهای سازمانی امن	نرم‌افزار، مدیریت دستگاه (MDM)، رفتار کاربر
اسرائیل	بله، در برخی نهادهای نظامی و برای افسران ارشد	کاهش سطح حمله و استانداردسازی پلتفرم	نفوذ عملیاتی، جاسوس‌افزار دولتی، شنود هدفمند	بسیار شدید؛ هرچه سطح بالاتر، محدودیت سخت‌تر	تمرکز بر انتخاب پلتفرم مشخص (غیربومی اما کنترل‌پذیر مانند iOS)	سیستم‌عامل + سیاست استفاده
چین	ممنوعیت رسمی ندارد؛ محدودیت نهادی گسترده	حاکمیت داده و خودکفایی فناوری	وابستگی فناورانه، نشت داده به خارج، نفوذ اطلاعاتی	بله؛ تفاوت معنادار بین سطوح حزبی، امنیتی و اداری	بسیار پررنگ؛ اپ‌ها و پلتفرم‌های بومی	نرم‌افزار + زنجیره داده
روسیه	ممنوعیت سیستم‌عامل ندارد؛ محدودیت ارتباطی	کنترل ارتباطات و پیام‌رسان‌ها	نفوذ اطلاعاتی، وابستگی نرم‌افزاری خارجی	بله؛ تمرکز بر نهادهای امنیتی و دولتی حساس	پررنگ در پیام‌رسان و نرم‌افزار، کمتر در سخت‌افزار	نرم‌افزار و زیرساخت ارتباطی
کره‌جنوبی	ممنوعیت اندروید ندارد؛ محدودیت محیط‌محور	حفاظت از محیط‌های حساس	نشت محیطی اطلاعات (تصویر، صدا، موقعیت)	بله؛ تفاوت شدید بین محیط نظامی و غیرنظامی	تأکید کم؛ تمرکز بر منع استفاده نه بومی‌سازی	کنترل فیزیکی و محیط عملیاتی
ترکیه	ممنوعیت صریح ندارد	امنیت ارتباطات دولتی و داده‌ها	نشت اطلاعات، سوءاستفاده از پیام‌رسان‌ها	بله؛ شدت توصیه‌ها با سطح مسئولیت افزایش می‌یابد	متوسط؛ گرایش به ابزارها و بسترهای داخلی	نرم‌افزار و سیاست نهادی

منابع

1.Xi Jinping, Cyber Sovereignty and Internet Governance, China Cyberspace Administration publications

2.Council on Foreign Relations, “China’s Digital Authoritarianism”

3.Freedom House, Freedom on the Net: China

4.Brookings Institution, “China’s Push for Indigenous Innovation”

5.McKinsey Global Institute, Digital China: Powering the Economy to Global Competitiveness

6.Harvard Kennedy School, Mapping China’s Great Firewall

7.Reuters, “Google stops censoring search results in China”

8.Open Technology Fund, “Measuring Internet Filtering in China”

9.Financial Times, “How multinationals access the internet in China”

10.MIT Technology Review, “Inside China’s parallel digital universe”

11.Citizen Lab, University of Toronto, Circumvention and VPN Use in China

12.Reuters – Russia tightens control over foreign tech platforms

13.Financial Times – Russia’s digital sovereignty strategy

14.Carnegie Endowment – Russia’s Internet Control Dilemma

15.Brookings Institution – Sanctions and Russia’s Tech Decoupling

16.CSIS – Digital Authoritarianism in Russia

17.Atlantic Council – Russia’s Sovereign Internet Project

18.Freedom House – Freedom on the Net: Russia

19.Bloomberg – Russia Funnels Billions into Domestic Tech Firms

20.Reuters – Russia bans Meta platforms

21.BBC – Why Russia hasn’t blocked YouTube

22.Alrud Law Firm – Russia bans foreign authentication systems

23.The Guardian – Russia’s war on VPNs

24.OECD – Internet Governance in Russia

25.IDC Russia – Aurora OS deployment report

26.Ministry of Digital Development of Russia – Official statements

27.Levada Center – Internet and VPN usage in Russia

28.Top10VPN – Russia VPN usage surge

29.MIT Technology Review – Russia’s controlled internet future

30.Carnegie Endowment – India’s Digital Sovereignty Strategy

31.Financial Times – India navigates digital governance

32.Bloomberg – India’s tech market and Google

33.Brookings Institution – Global tech and competition in India

34.Reuters – India’s digital rules update

35.KPMG India – Tech investment and digital policy report

36.Economic Times – Cost analysis of de-Googlefication

37.Hindustan Times – Digital policy and content regulation

38.LiveMint – What is BharOS?

39.Economic Times – BharOS rollout progress

40.TelecomTalk – BharOS device count

41.TechCrunch – Challenges for BharOS adoption

42.TRAI policy documents – Algorithm transparency guidelines

43.Top10VPN – VPN usage statistics India

44.Counterpoint Research – India Smartphone Ecosystem Dependency Analysis

45.GSMA – Mobile Operating Systems and Emerging Markets

46.BBC – India’s COVID apps and privacy debate

47.Observer Research Foundation – Digital Governance and State Power in India

48.The Economic Times – BharOS and India’s sovereign tech ambitions

49.Hindu BusinessLine – Government’s plans for BharOS clarified

50.Brookings Institution – India’s pragmatic path to digital sovereignty

51.Brookings Institution – Platform regulation in South Korea

52.Financial Times – South Korea takes on Big Tech

53.OECD – Digital competition policy: Korea case study

54.Reuters – South Korea fines Google over Android practices

55.Korea Fair Trade Commission – Official enforcement reports

56.BBC – South Korea’s anti-Google law explained

57.The Verge – How Korea forced Google to change Play Store rules

58.European Commission – Global coordination on platform regulation

59.Nikkei Asia – Naver, Kakao and Korea’s digital sovereignty

60.CISA – Mobile Communications Best Practice Guidance

61.OECD – Digital Security Risk Management

62.NSA – Mobile Device Best Practices

63. RAND Corporation – Cyber Risks to Military Operations

64.NIST – Security Considerations for Mobile Devices

65.Google Project Zero – Android Vulnerability Reports

66. Citizen Lab – Pegasus and Mobile Spyware Reports

67.ENISA – Threat Landscape for Mobile Devices

68. MIT Technology Review – Metadata and Surveillance

69. Harvard Kennedy School – Human Factors in Cybersecurity

70. UK NCSC – Mobile Device Guidance for Senior Officials

71. Council on Foreign Relations – Technology and Geopolitics

72. CSIS – Cyber Power and National Security

73.CISA – Mobile Communications Security Guidance

74.NSA – Mobile Device Best Practices

75.NIST – Mobile Device Security

76.GAO – Federal Mobile Device Management

77.IDF / Israeli Security Doctrine analyses

78.Jerusalem Post – Military mobile restrictions

79. RAND – Attack Surface Reduction

80.Cyberspace Administration of China

81. MERICS – China digital governance

82.CSIS – China tech sovereignty

83.Carnegie Endowment – Russia digital sovereignty

84.Roskomnadzor policy analyses

85.OECD – Russia cyber governance

86.South Korean Ministry of Defense statements

87.Yonhap – Military security policies

88.Turkish National Cyber Security Strategy

89.SETA – Turkey cyber policy analysis

QUICK
ANSWER

دفترهای خاکستری

این دفترها برای پاسخ علمی سریع، مختصر و دقیق به مسئله‌ها و نیازهایی تهیه و تولید می شود که در حین فعالیت مرکز ملی فضای مجازی و سایر دستگاه ها پیش آمده و به بررسی دقیق و در عین حال سریع نیاز دارند.



پژوهشگاه
فضای مجازی