یادداشت

حق مردم برای دانستن

علیرضا دقیقی، وکیل پایه‌یک دادگستری: در عصر دیجیتال، اطلاعات نه‌تنها یک دارایی اقتصادی، بلکه یکی از مهم‌ترین مؤلفه‌های امنیت عمومی و حکمرانی مطلوب به شمار می‌رود. هر روز میلیون‌ها نفر از خدمات بانکی، مخابراتی، حمل‌ونقل، سلامت و سایر زیرساخت‌های دیجیتال استفاده می‌کنند و امنیت این خدمات به‌طور مستقیم با حقوق شهروندان گره خورده است. در چنین شرایطی، پرسش مهم این است که آیا اطلاعات مربوط به حملات سایبری باید منتشر شود یا خیر؟ این موضوع در نگاه نخست، تقابلی میان «امنیت» و «شفافیت» به نظر می‌رسد؛ اما بررسی دقیق‌تر نشان می‌دهد که مسئله اصلی، یافتن تعادلی میان حق مردم برای دانستن و ضرورت حفاظت از اطلاعات حساس است. از منظر آزادی دسترسی به اطلاعات، انتشار گزارش‌های مربوط به حملات سایبری مزایای قابل توجهی دارد. نخست آنکه آگاهی عمومی و یادگیری جمعی را افزایش می‌دهد. هنگامی که جزئیات کلی یک حمله، شیوه نفوذ مهاجمان و نقاط ضعف مورد سوءاستفاده به‌صورت مدیریت‌شده منتشر می‌شود، سایر سازمان‌ها و نهادها می‌توانند از تجربه دیگران درس بگیرند و از تکرار همان خطاها جلوگیری کنند. دومین و شاید مهم‌ترین فایده انتشار اطلاعات، تقویت شفافیت و مسئولیت‌پذیری است. تجربه جهانی نشان داده است که در بسیاری از موارد، حملات سایبری تنها نتیجه توانمندی مهاجمان نیست، بلکه حاصل بی‌توجهی، ضعف مدیریتی، سرمایه‌گذاری ناکافی در امنیت اطلاعات یا تأخیر در به‌روزرسانی سامانه‌ها نیز هست. در غیاب شفافیت، برخی شرکت‌ها و ارائه‌دهندگان خدمات می‌توانند این کاستی‌ها را پشت عنوان کلی «حمله سایبری» پنهان کنند و از پاسخ‌گویی بگریزند. حق دسترسی شهروندان به اطلاعات اقتضا می‌کند کاربران، مشتریان و ذی‌نفعان بدانند آیا اطلاعات آنان در معرض خطر قرار گرفته است یا خیر. همچنین سرمایه‌گذاران و نهادهای ناظر باید بتوانند عملکرد واقعی سازمان‌ها را ارزیابی کنند. به همین دلیل است که در بسیاری از کشورها، قوانین گزارش‌دهی اجباری نقض داده‌ها و رخدادهای سایبری به بخشی از نظام حکمرانی دیجیتال تبدیل شده است. انتشار داده‌های مرتبط با حملات سایبری همچنین به ارتقای امنیت ملی کمک می‌کند. نهادهای مسئول امنیت سایبری با تجمیع و تحلیل این اطلاعات می‌توانند الگوهای حملات را شناسایی کرده، هشدارهای زودهنگام صادر کنند و از وقوع حملات مشابه علیه سایر سازمان‌ها جلوگیری کنند. پژوهشگران و شرکت‌های امنیتی نیز از این داده‌ها برای توسعه ابزارهای دفاعی و تقویت تاب‌آوری سایبری استفاده می‌کنند. با این حال، مخالفان انتشار اطلاعات نیز دغدغه‌های قابل توجهی دارند. افشای جزئیات فنی یک حمله ممکن است به مهاجمان دیگر کمک کند تا همان روش را علیه اهداف جدید به کار بگیرند. علاوه بر این، انتشار بی‌ضابطه اطلاعات می‌تواند به حریم خصوصی افراد آسیب بزند، روند تحقیقات قضائی را مختل کند یا خسارات اقتصادی و اعتباری سنگینی برای سازمان‌های قربانی به همراه داشته باشد. این نگرانی‌ها واقعی هستند، اما راه‌حل آنها پنهان‌کاری نیست؛ بلکه طراحی سازوکارهای هوشمندانه برای انتشار اطلاعات است. تجربه کشورهای پیشرو نشان می‌دهد که می‌توان میان امنیت و شفافیت تعادل برقرار کرد. گزارش‌دهی اجباری به نهادهای مسئول، انتشار عمومی اطلاعات به‌صورت مرحله‌ای، حذف جزئیات حساس و رعایت الزامات حریم خصوصی ازجمله ابزارهایی هستند که این تعادل را ممکن می‌کنند. در ایران نیز با توجه به افزایش حملات سایبری علیه بخش‌های دولتی و خصوصی، زمان آن رسیده است که چارچوب‌های حقوقی روشنی برای گزارش‌دهی و انتشار اطلاعات مرتبط با رخدادهای سایبری تدوین شود. چنین چارچوبی باید از یک سو حق مردم را برای آگاهی از تهدیدها و مخاطراتی که متوجه اطلاعات و خدمات آنان است، تضمین کند و از سوی دیگر مانع افشای اطلاعاتی شود که امنیت ملی یا روند مقابله با مهاجمان را به خطر می‌اندازد.

در نهایت، امنیت پایدار در سایه پنهان‌کاری حاصل نمی‌شود. جامعه‌ای امن‌تر است که در آن مسئولان، شرکت‌ها و نهادهای ارائه‌دهنده خدمات در برابر افکار عمومی پاسخ‌گو باشند و شهروندان نیز به اطلاعاتی که بر حقوق و منافع آنان تأثیر می‌گذارد، دسترسی داشته باشند. شفافیت مسئولانه نه‌تنها اعتماد عمومی را افزایش می‌دهد، بلکه مهم‌ترین ابزار برای جلوگیری از تکرار خطاها، ارتقای امنیت سایبری و تقویت حکمرانی دیجیتال در کشور است.

صلح تاکتیکی، فشار راهبردی

ادامه از صفحه اول

واشینگتن می‌داند مدیریت هم‌زمان بحران ایران و روسیه نیازمند توزیع دقیق منابع، توجه سیاسی و توان عملیاتی است. اگر جنگ اوکراین از سطح قابل مدیریت خارج شود، آمریکا ناچار است ظرفیت خود را به اروپا منتقل کند و فشار بر ایران کاهش می‌یابد. بنابراین، حفظ اوکراین در وضعیت کنترل‌شده، پیش‌شرط حفظ فشار بر ایران است. این رابطه نه سیاسی، بلکه ساختاری است؛ محدودیت ظرفیت آمریکا دو بحران را به یکدیگر گره می‌زند. در میدان اوکراین، آمریکا و ناتو درگیر یک جنگ نیابتی هستند که هدف آن جلوگیری از گسترش نفوذ روسیه و حفظ اعتبار بازدارندگی غرب است. این جنگ نباید به نقطه فروپاشی اوکراین برسد، اما نباید به سطح تنش غیرقابل پیش‌بینی با روسیه هم کشیده شود. به همین دلیل واشینگتن سطح تنش را در یک محدوده قابل کنترل نگه می‌دارد؛ محدوده‌ای که به دوره‌های آرامش تاکتیکی نیاز دارد، اما نه به دلیل صلح و دوستی، بلکه به دلیل این محاسبه که هرگونه خروج از این محدوده، مستلزم تخصیص مجدد منابع از سایر نقاط جهان است. در میدان ایران نیز منطق مشابه برقرار است. آمریکا می‌خواهد ایران را مهار کند، اما نه تا حدی که منطقه وارد یک جنگ گسترده شود. هرگونه جنگ تمام‌عیار با ایران، نه‌تنها فراتر از ظرفیت کنونی واشینگتن، بلکه مستلزم عقب‌نشینی راهبردی از اروپا یا شرق آسیا خواهد بود که خود قیمتی فراتر از منافع فوری دارد. در نتیجه، در این میدان هم هدف تنظیم تنش است، نه تشدید دائمی آن. این تنظیم گاهی به شکل آتش‌بس محدود، گاهی به شکل کاهش فشار نظامی و گاه به شکل پیام غیرمستقیم ظاهر می‌شود. در این میان، رفتار ترامپ یک لایه رفتاری به این معماری ساختاری اضافه می‌کند، اما نه به‌عنوان خالق آن، بلکه به‌عنوان کارگزار هوشمندی که این محدودیت را بهینه‌سازی می‌کند. ترامپ سیاست خارجی را از زاویه معامله می‌بیند. برای او، هر بحران یک اهرم است. آرام‌سازی یک بحران، یعنی آزادکردن ظرفیت برای فشار بر بحران دیگر. تشدید یک بحران یعنی بالابردن قیمت معامله در میدان دیگر و به همین دلیل، جابه‌جایی ریتم تنش میان ایران و اوکراین را می‌توان در چارچوب منطق چانه‌زنی ترامپ خواند، اما با این تفاوت که او سرعت و دامنه این جابه‌جایی را افزایش می‌دهد، بدون آنکه خود بنیان‌گذار آن الگو باشد. بااین‌حال، این الگو به معنای کنترل کامل نیست و هزینه‌هایی نیز برای خود واشینگتن دارد، ازجمله فرسایش اعتماد متحدان اروپایی که آرام‌سازی مقطعی ایران را با بی‌توجهی به نگرانی‌های اسرائیل قاطی می‌کنند و بازیگرانی مانند چین نیز به سرعت این نوسانات را می‌خوانند و برای خنثی‌سازی آن برنامه‌ریزی می‌کنند. افزون بر این آمریکا نه ایران را کاملا در اختیار دارد، نه روسیه را. آنچه انجام می‌دهد، تنظیم سطح تنش است، نه تعیین مسیر بحران. ایران و روسیه هر دو بازیگرانی مستقل و هزینه‌پذیر هستند. بنابراین واشینگتن می‌تواند سقف و کف تنش را تا حدی تنظیم کند، اما نمی‌تواند نتیجه نهایی را تعیین کند. در نهایت، صلح تاکتیکی در این تصویر نه نشانه ضعف است و نه نشانه تمایل واقعی به پایان بحران. این صلح بخشی از یک معماری فشار است که هدف آن جلوگیری از هم‌زمانی دو بحران غیرقابل مدیریت است. آمریکا می‌داند اگر هر دو میدان به نقطه اوج برسند، توان پاسخ‌گویی ندارد. به همین دلیل، آرام‌سازی یک جبهه به صورت آگاهانه به ابزار فشار در جبهه دیگر تبدیل می‌شود. تا زمانی که آمریکا نتواند یکی از دو بحران را به صورت پایدار ببندد، این الگو ادامه پیدا می‌کند. صلح تاکتیکی در یک میدان، ابزار فشار راهبردی در میدان دیگر باقی خواهد ماند. برای ایران و روسیه فهم این معماری، بخشی از فهم واقعی محدودیت و ظرفیت آمریکا و نیز آسیب‌پذیری‌های خود این الگو است، نه اغراق در قدرت آن و نه دست‌کم‌گرفتن آن.

۲۸ روز بعد از دستور رئیس‌جمهوری برای اتصال اینترنت

بازگشت اینترنت هنوز کامل نشده

اختلالات چه تأثیری در بخش‌های مختلف می‌گذارند(جدول شماره ۱)		
شاخص عملکردی	اپراتورهای سیار (موبایل)	اپراتورهای ثابت (مخابرات و FCPها)
سرعت و پایداری لایه شبکه	نوسان شدید، قطعی متناوب در ساعات اوج مصرف	سرعت پایین‌تر اما پایداری نسبی در صورت اتصال
مسدودسازی پروتکل‌های تونل‌زنی	واکنش سریع و تهاجمی سیستم‌هایDPI به ترافیک مشکوک	اعمال محدودیت بیشتر روی سرعت آپلود و اختلال در UDP
انسجام در اعمال محدودیت‌ها	تفاوت فاحش براساس منطقه جغرافیایی و دکل مخابراتی	پیروی از مسیریابی‌های استاتیک و اعمال فیلترینگ یکپارچه‌تر

شرق: شبکه ارتباطی و زیرساخت اینترنت در ایران، پس از نزدیک به سه ماه قطعی و اعمال محدودیت، اکنون در وضعیتی قرار دارد که کارشناسان فنی آن را یک «بازگشایی ناقص» توصیف می‌کنند. بررسی‌های تخصصی، داده‌های ترافیکی و مشاهدات میدانی «شرق» نشان می‌دهد که با وجود اعلام رسمی مبنی بر رفع محدودیت‌ها و بازگشت اینترنت به شرایط پیش از بحران به دستور رئیس‌جمهوری، ساختار شبکه همچنان درگیر اختلالات سیستماتیک و رفتارهای متناقض نظارتی است. این تغییرات زیرساختی، مفهوم اینترنت را از یک شبکه یکپارچه جهانی به مجمع‌الجزایری از ارتباطات ناپایدار، مبهم و فیلترشده تقلیل داده است. گزارش پیش‌رو، با رویکردی تحلیلی و مبتنی بر داده‌های شبکه‌ای، به بررسی شش محور بنیادین از وضعیت فعلی اینترنت ایران می‌پردازد. این تحلیل نشان می‌دهد که چگونه تداخل سیاست‌های نظارتی با مکانیسم‌های پایه اینترنت، نه‌تنها پیکره اقتصاد دیجیتال و کسب‌وکارهای خرد را در معرض آسیب قرار داده، بلکه امنیت اطلاعاتی سازمان‌ها و شهروندان را نیز با تهدید مواجه کرده است.

۱. بحران انزوای دیتاسنترها: قطع شریان‌های حیاتی زیرساخت داخلی

یکی از حیاتی‌ترین چالش‌هایی که پس از صدور دستور بازگشایی اینترنت همچنان پابرجاست، تداوم قطع ارتباط بخشی از دیتاسنترهای داخلی با شبکه بین‌الملل است. در روزهای نخست بازگشایی (مانند سه‌شنبه پنجم خرداد و پنجشنبه هفتم خرداد)، درصد قابل توجهی از دیتاسنترها برای دقایق یا ساعاتی به اینترنت جهانی متصل شدند، اما این اتصال به‌سرعت و به‌طور کامل از دست رفت. تحلیلگران شبکه این پدیده را فراتر از یک اختلال فنی ساده ارزیابی می‌کنند. شواهد حاکی از آن است که این قطعی‌ها ریشه در تصمیمات نظارتی با هدف جلوگیری از میزبانی زیرساخت‌های فیلترشکن روی سرورهای داخلی دارد. در حال حاضر، تبعیض آشکاری در اتصال دیتاسنترها به اینترنت به چشم می‌خورد؛ به‌طوری که اتصال برخی مراکز میزبانی مشروط به احراز هویت دقیق مشتریان و پایش مستمر ترافیک شده است، اما از سوی دیگر سایر مراکز در انزوای کامل قرار دارند. این وضعیت ضربه مهلکی به ارائه‌دهندگان خدمات ابری (Cloud Providers) و اکوسیستم استارتاپی وارد کرده است. زمانی که دیتاسنترهای داخلی از اینترنت جهانی منفک می‌شوند، سرورهای میزبان کسب‌وکارهای ایرانی توانایی برقراری ارتباط با وب‌سرویس‌های بین‌المللی، دریافت به‌روزرسانی‌های نرم‌افزاری و تمدید گواهینامه‌های امنیتی نظیر SSL را از دست می‌دهند. همچنین، کنترل‌پنل‌های رایج مدیریت سرور نظیر cPanel به دلیل عدم دسترسی به سرورهای لایسنس بین‌المللی از کار می‌افتند که این امر مدیریت وب‌سایت‌ها را عملا غیرممکن می‌کند.

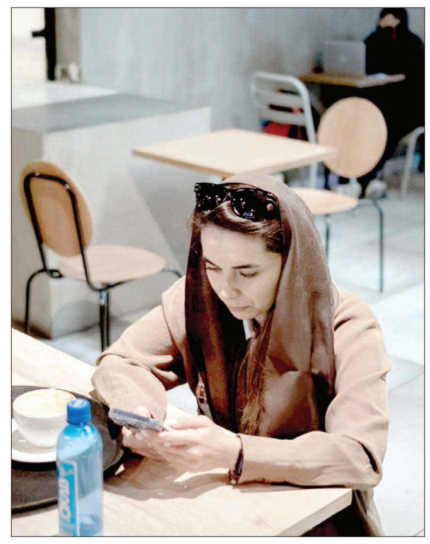
۲. توهم اتصال در لبه‌های شبکه: دستکاری پروتکل‌ها و مسئله پورت‌های ناامن

بررسی وضعیت لبه‌های شبکه (Network Edges) و دروازه‌های ارتباطی بین‌المللی شرکت ارتباطات زیرساخت، پرده از یک مداخله در لایه انتقال برمی‌دارد. در ظاهر، گره‌های خارج از شبکه ایران قابل رؤیت هستند و دستورات پایه نظیر Ping به‌درستی پاسخ می‌دهند، اما زمانی که کاربران و سرویس‌ها قصد برقراری ارتباط و تبادل داده را دارند، با اختلالات شدیدی نظیر ازدست‌رفتن بسته‌ها (Packet Loss)، اتمام زمان درخواست (Timeout) و بازنشانی ارتباط (Connection Reset) مواجه می‌شوند. این اختلالات ریشه در عملکرد سیستم‌های بازرسی عمیق بسته‌ها (DPI) دارد. در بسیاری از سیستم‌های ارتباطات، به تجهیزات فیلترینگ اجازه می‌دهند تا فرایند دست‌دهی اولیه (TCP Handshake) میان کاربر و سرور با موفقیت انجام شود؛ اما به محض آغاز تبادل ترافیک اصلی و ارسال بسته‌های حاوی داده (نظیر TLS Client Hello)، ارتباط مسدود و ترافیک رها (Drop) می‌شود. این مکانیسم مخرب باعث می‌شود کلاینت‌ها و سرورها در یک چرخه بی‌پایان از تلاش برای اتصال مجدد گرفتار شوند؛ که نتیجه آن اشغال شدید منابع سخت‌افزاری، افزایش نجومی تأخیر (Latency) و افت شدید کیفیت تجربه کاربری است. بدترین پیامد این نوع فیلترینگ، بازماندن ترافیک صرفا روی پروتکل HTTP (پورت ۸۰) و مسدودسازی ارتباطات رمزنگاری‌شده (پورت ۴۴۳) در برخی مسیرهای بین‌المللی است. این رویکرد دو پیامد ویرانگر دارد: نخست آنکه پروتکل HTTP هیچ‌گونه رمزنگاری روی داده‌ها انجام نمی‌دهد. هدایت اجباری ترافیک به سمت این پروتکل به این معناست که تمامی اطلاعات هویتی، رمزهای عبور و داده‌های حساس کاربران به‌صورت متن‌باز (Plain Text) در شبکه منتقل شده و به‌سادگی قابل شنود است. دوم آنکه معماری وب مدرن این رویه را نمی‌پذیرد. امروزه مرورگرها، سیستم‌عامل‌های موبایل و استانداردهای جهانی وب (مانند HSTS) توسعه‌دهندگان را ملزم به استفاده از بستر امن HTTPS می‌کنند؛ بنابراین بازبودن شبکه صرفا روی HTTP، باعث از کار افتادن مطلق اپلیکیشن‌های بانکی، فروشگاه‌های آنلاین و وب‌سرویس‌ها می‌شود، زیرا نرم‌افزارهای مدرن از ارسال داده بر بستر ناامن خودداری می‌کنند.

۳. مجمع‌الجزایر اپراتورها: فقدان یکپارچگی و رفتار سلیقه‌ای در شبکه

یکی از پیچیده‌ترین معضلات فنی در وضعیت فعلی، رفتار کاملا متناقض و جزیره‌ای ارائه‌دهندگان خدمات اینترنت (اپراتورهای همراه و ثابت) است. شواهد نشان می‌دهد محدودیت‌ها دیگر از یک قانون و الگوی واحد در سطح شرکت زیرساخت پیروی نمی‌کنند، بلکه اختلالات به‌شدت منطقه‌ای و وابسته به نوع اپراتور اعمال می‌شوند. این رفتار سلیقه‌ای، شبکه را به یک ساختار غیرقابل پیش‌بینی تبدیل کرده است. ممکن است یک پروتکل ارتباطی یا یک پورت خاص روی شبکه یکی از اپراتورهای سیار باز باشد، اما همان پروتکل روی اپراتور سیار دیگر یا ارائه‌دهندگان اینترنت ثابت (ADSL/VDSL) کاملا مسدود باشد. حتی در یک شهر، کیفیت دسترسی از یک دکل مخابراتی تا دکل دیگر متفاوت است.

این تنوع در رفتار شبکه، فرایند عیب‌یابی (Troubleshooting) را برای تیم‌های زیرساخت و توسعه‌دهندگان نرم‌افزار به امری طاقت‌فرسا مبدل کرده است. کسب‌وکارها نمی‌توانند تشخیص دهند که قطعی سرویس آنها ناشی از باگ نرم‌افزاری است یا اعمال محدودیت‌های پنهان و سلیقه‌ای توسط یک تأمین‌کننده خاص.



وضعیت پروتکل‌های مختلف در شرایط بازگشایی اینترنت		
پروتکل‌های قدیمی: عملا مُرده		
پروتکل	وضعیت در ایران	دلیل
OpenVPN (استاندارد)	✕ مسدود	اثر انگشت‌شناخته‌شده
WireGuard	✕ مسدود	الگوی ترافیک متمایز
L2TP/IPSec	✕ مسدود	پورت‌های شناخته‌شده
PPTP	✕ مسدود	پروتکل قدیمی و آسیب‌پذیر
پروتکل‌های مقاوم‌تر: بازی ادامه دارد		
پروتکل	وضعیت	توضیح
VLESS + Reality	فعال (فعلا)	ترافیک شبیه HTTPS عادی
Trojan	ناپایدار	شناسایی‌تدریجی
Hysteria2	ناپایدار	مبتنی بر QUIC، گاهی کار می‌کند
TUIC	ناپایدار	مشابه Hysteria2
(Shadowsocks (AEAD	ناپایدار	بسته به سرور و پیکربندی

۴. تناقض فیلترینگ: مرگ شبکه‌های سازمانی و جولان ابزارهای گمنام

در میان استراتژی‌های مسدودسازی ترافیک، تناقضی حیرت‌انگیز نهفته است؛ پروتکل‌های معتبر، استاندارد و سازمانی ایجاد شبکه خصوصی مجازی (VPN) از کار افتاده‌اند، درحالی‌که فیلترشکن‌های گمنام و بی‌هویت به‌راحتی در شبکه فعالیت می‌کنند. پروتکل‌هایی نظیر L2TP/IPSec، OpenVPN و WireGuard ابزارهای استانداردی هستند که در سراسر جهان برای برقراری ارتباطات امن میان شعب شرکت‌ها، فراهم‌سازی بستر دورکاری و محافظت از داده‌های حیاتی سازمانی مورد استفاده قرار می‌گیرند. این پروتکل‌ها (به‌ویژه OpenVPN) دارای امضای دیجیتال (Signature) مشخصی در بسته‌های داده خود هستند و به همین دلیل در همان ابتدای فرایند دست‌دهی توسط سیستم‌های فیلترینگ ایران شناسایی و در سطح شبکه تأمین‌کنندگان اینترنت مسدود می‌شوند. مسدودسازی این پروتکل‌ها، شبکه‌های داخلی شرکت‌ها (Intranet) و زیرساخت‌های بانکی و سازمانی را فلج کرده است. در نقطه مقابل، ابزارهای تونل‌زنی مبتنی بر لایه هفت (مانند کانفیگ‌های پراکسی) یا فیلترشکن‌های گمنامی که ترافیک خود را با استفاده از روش‌های مبهم‌سازی (Obfuscation) شبیه به ترافیک وب معمولی (HTTPS) جلوه می‌دهند، از سد فیلترینگ عبور می‌کنند. این سیاست دوگانه، شرکت‌ها و کاربران را ناچار می‌کند برای حفظ ارتباطات خود به ابزارهای غیررسمی و کانفیگ‌های ناشناس پناه ببرند. استفاده از این ابزارها که غالبا توسط افراد ناشناس توسعه یافته‌اند، خطر نشت اطلاعات، حملات روز صفر (Zero-day) و آلودگی به بدافزارها را به‌شدت افزایش می‌دهد و هم‌زمان، بازار سیاه و اقتصاد پنهان عظیمی را برای فروشندگان این ابزارها رقم زده است.

۵. سراب آی‌پی سفید و تخریب ساختارهای ارتباطی کسب‌وکارها

در دوران اوج قطعی‌ها، معماری اینترنت کشور به مدل «لیست سفید» (Whitelist) یا «Default-Deny Network» تغییر یافت؛ مدلی که در آن تمامی ارتباطات بین‌المللی مسدود است، مگر آنکه آدرس آی‌پی مقصد از پیش تأیید شده باشد. با اعلام بازگشایی شبکه، انتظار می‌رفت این محدودیت‌ها برچیده شوند، اما مشاهدات نشان داد که بازگشایی ناقص، همان ارتباطات قبلی مبتنی بر آی‌پی سفید را نیز مختل کرده است. کسب‌وکارها که در دوران قطعی، معماری شبکه و مسیریابی‌های خود را با هزاران زحمت براساس مدل آی‌پی سفید تنظیم کرده بودند، با بازگشایی شبکه مجبور شدند بار دیگر ساختار ارتباطی خود را دستکاری کنند. مشکل مضاعف این است که چندین مدل مختلف از آی‌پی سفید در سطح شبکه پیاده‌سازی شده است؛ برخی براساس پورت، برخی براساس پروتکل و برخی براساس حجم ترافیک عمل می‌کنند و هیچ‌کدام رویه یکپارچه‌ای ندارند.

۶. دی‌ایندکس شدن و فاجعه سئو

خسارت‌بارترین نتیجه اجرای سیاست لیست سفید، نابودی جایگاه وب‌سایت‌های ایرانی در موتورهای جست‌وجو (SEO) است. ربات‌ها و خزنده‌های گوگل (Googlebot) که از دیتاسنترهای بین‌المللی برای بررسی صفحات وب به سمت سرورهای ایرانی درخواست می‌فرستند، در برخورد با محدودیت‌های دسترسی، با خطاهایی نظیر Timeout و Unreachable Origin مواجه می‌شوند. موتور جست‌وجوی گوگل، وب‌سایت‌هایی را که سرور آنها در دسترس نباشد، به‌سرعت از نتایج جست‌وجو حذف (De-index) می‌کند. این پدیده، کانال اصلی ترافیک و درآمد کسب‌وکارهای کوچک و متوسط را کاملا نابود کرده است. درحالی‌که شرکت‌های بزرگ و خصولتی توانسته‌اند با استفاده از رانت فنی، آدرس‌های خود را در لیست سفید قرار دهند، کسب‌وکارهای خرد بدون هیچ پشتوانه‌ای قربانی این ساختار شده‌اند. بازسازی جایگاه سئو پس از چنین آسیبی، نیازمند ماه‌ها زمان و هزینه‌های گزاف است.

۷. خلأ پاسخ‌گویی در مسئله مدیریت زیرساخت

در میان این حجم از اختلالات بنیادین، یکی از بزرگ‌ترین معضلات اکوسیستم فناوری ایران، فقدان یک مرجع مشخص و پاسخ‌گو برای حل مشکلات است. متولیان اینترنت در کشور به‌جای ارائه راهکارهای فنی و شفاف‌سازی، در یک چرخه مستمر از فرافکنی گرفتار شده‌اند. وزارت ارتباطات و فناوری اطلاعات، به‌عنوان بالاترین نهاد سیاست‌گذار، ریشه اختلالات و قطعی‌های پراکنده را به فرسودگی باتری دکل‌های مخابراتی و قطعی مکرر برق مربوط می‌داند و در برابر اختلالات ایجادشده در لایه پروتکل‌ها و فیلترینگ سلیقه‌ای سکوت می‌کند. از سوی دیگر، شرکت ارتباطات زیرساخت که مدیریت درگاه‌های بین‌المللی را بر عهده دارد، اعلام می‌کند که مدیریت محتوا و مسدودسازی پورت‌ها در حیطه اختیارات این شرکت نیست. این در حالی است که اختلالات شبکه برای خود شرکت زیرساخت نیز بالغ بر هزار میلیارد تومان عدم‌النفع مالی در پی داشته و توان تأمین هزینه‌های جاری این شرکت‌ها را با بحران مواجه کرده است. همچنین به گفته مدیرعامل این شرکت در نشست خبری خرداد وزیر ارتباطات به «شرق»، وضعیت شبکه به حالت اول دی برگشته و ترافیک روی ۷۸ درصد است. در این میان، سازمان تنظیم مقررات و ارتباطات رادیویی (رگولاتوری) که ذاتا موظف به نظارت بر کیفیت خدمات اپراتورها و حمایت از حقوق کاربران است، در قبال اعمال محدودیت‌های غیرشفاف، انسداد پروتکل‌ها و خطاهای سیستم‌های DPI (موسوم به False Positives) کاملا منفعلانه عمل کرده است. این ساختار نظارتی متشتت باعث شده است صدها کسب‌وکاری که ترافیک عادی آنها به اشتباه مسدود شده، ندانند شکایت خود را باید به کدام نهاد قانونی ارجاع دهند.

از فاصله تا حقیقت

بررسی همه‌جانبه زیرساخت‌های ارتباطی ایران گویای حقیقتی تلخ است: اقتصاد دیجیتال کشور در حال دست‌وپنجه نرم‌کردن با محدودیت‌هایی بی‌سابقه، متناقض و مخرب است. اصرار بر اجرای رویکرد «لیست سفید» و قطع ارتباط دیتاسنترها، توان رقابتی استارتاپ‌های ایرانی را از بین برده و مسدودسازی پروتکل‌های رمزنگاری معتبر نظیر OpenVPN، شرکت‌ها را به سمت استفاده از ابزارهای ناامن و گمنام سوق داده است. تا زمانی که سیاست‌گذاران در نهادهای متولی، مسئولیت این اختلالات مهندسی‌شده را نپذیرفته و مکانیسم‌های بازرسی عمیق بسته‌ها (DPI) را که عامل اصلی قطعی‌های هندشیک و ناپایداری TCP هستند متوقف نکنند، شبکه ملی در یک فرسایش مداوم باقی خواهد ماند. بازگشت واقعی به شرایط عادی نیازمند پایان‌دادن به رفتارهای جزیره‌ای اپراتورها، احیای بی‌طرفی شبکه و به رسمیت شناختن حقوق بنیادین کسب‌وکارها در دسترسی آزاد و امن به شریان‌های بین‌المللی اطلاعات است؛ در غیر این صورت، مرگ تدریجی اقتصاد دیجیتال و انزوای تکنولوژیک کشور، امری اجتناب‌ناپذیر خواهد بود.

رادارهای جهانی چه می‌گویند؟ توهم اتصال در لایه‌های پنهان شبکه

داده‌ها دروغ نمی‌گویند. در حالی که مراجع رسمی داخلی ممکن است وضعیت شبکه را عادی جلوه دهند و قطعی‌ها را به مشکلات موضعی یا فرسودگی تجهیزات ربط دهند، مانیتورهای جهانی رصد اینترنت روایت کاملا متفاوتی از کالبدشکافی اینترنت ایران ارائه می‌دهند. بررسی داده‌های دو مرجع معتبر یعنی رادار کلادفلر (Cloudflare Radar) و پروژه IODA نشان می‌دهد که ما با یک قطعی ساده روبه‌رو نیستیم، بلکه با یک «اختلال مهندسی‌شده» مواجه هستیم.

۱. معمای IODA؛ جاده باز است اما ماشین‌ها متوقف می‌شوند. پروژه IODA (مستقر در دانشگاه کالیفرنیا) اینترنت کشورها را از سه لایه مختلف بررسی می‌کند. نگاهی به نمودارهای ایران در این پلتفرم، پرده از یک واقعیت تلخ برمی‌دارد: در لایه مسیریابی جهانی یا BGP (که شبیه به تابلوهای راهنمای جاده است)، وضعیت ایران کاملا سبز و متصل است؛ یعنی سرورهای جهانی آدرس‌های ایران را می‌بینند. اما در نمودار Active Probing (که نشان‌دهنده رسیدن واقعی بسته‌های داده یا همان حرکت ماشین‌ها در جاده است)، شاهد افت‌های شدید و نوسانات عجیب هستیم. این یعنی درخواست کاربر ایرانی به لبه شبکه می‌رسد (همان دست‌دهی اولیه)، اما در تله سیستم‌های بازرسی عمیق (DPI) گرفتار شده و هرگز به مقصد برنمی‌گردد. این دقیقا همان پدیده‌ای است که کارشناسان به آن «توهم اتصال» می‌گویند.

۲. روایت کلادفلر؛ مجمع‌الجزایر اپراتورها و تنزل امنیت کلادفلر که بخش عظیمی از ترافیک وب جهان را مدیریت می‌کند، در بخش رادار خود رفتار شبکه ایران را به تفکیک اپراتورها (ASN) ثبت کرده است. تحلیل این داده‌ها دو بحران بزرگ را در این روزها نشان می‌دهد: رفتار سلیقه‌ای و جزیره‌ای: مقایسه ترافیک اپراتورهای ثابت و سیار (مثل همراه اول، ایرانسل و مخابرات) در کلادفلر نشان می‌دهد که هیچ الگوی واحدی وجود ندارد. در یک ساعت مشخص، ممکن است ترافیک یک اپراتور به‌شدت محدود شود، درحالی‌که دیگری وضعیت پایدارتری دارد. این امر نشان‌دهنده اعمال محدودیت‌های نامتمرکز و بعضا منطقه‌ای است. سقوط ترافیک رمزنگاری‌شده: یکی از نگران‌کننده‌ترین داده‌های رادار کلادفلر، افت نسبت ترافیک امن (HTTPS) به ترافیک ناامن (HTTP) در برخی مسیرهاست. بازگذاشتن پورت‌های ناامن و اختلال در پروتکل‌های امنیتی، عملا داده‌های کاربران و کسب‌وکارها را در معرض خطر جدی شنود و دستکاری قرار می‌دهد.

تلاقی داده‌های IODA و کلادفلر ثابت می‌کند که اقتصاد دیجیتال ایران قربانی قطع‌شدن کابل‌ها نشده، بلکه قربانی فیلترینگ چندلایه، پردازش و دخالت در بسته‌های ترافیکی شده است که رمق شبکه را گرفته و کیفیت را فدای کنترل کرده است.