اخبار

حذف و بازگشت دوباره تلگرام به فروشگاه برنامه اپل

برنامه پیام‌رسان تلگرام برای مدت کوتاهی از نتایج جست‌وجوی فروشگاه برنامه اپ استور اپل در سراسر جهان ناپدید شد، اما از آن زمان به وضعیت عادی بازگشته و قابل دسترس شده است. به گزارش ایسنا، این پلتفرم در پاسخ به پرسش خبرگزاری آناتولی در پی اختلال، اعلام کرد: «تلگرام در فروشگاه اپ استور بازیابی شده و به زودی دوباره برای همه کاربران در دسترس خواهد بود.» صفحه اختصاصی اپ استور تلگرام به وضعیت فعال بازگشته و این برنامه پیام‌رسان از طریق نتایج جست‌وجوی مستقیم در دسترس است. در طول اختلال کوتاه، این برنامه برای دانلودهای جدید ناپدید شد، اما کاربرانی که این نرم‌افزار را از قبل روی دستگاه‌های خود نصب کرده بودند، گزارش دادند که این سرویس پیام‌رسان همچنان به‌طور عادی کار می‌کند. اپل تایید کرد که پس از بررسی محتوایی که ناقض دستورالعمل‌های فروشگاه برنامه این شرکت بوده است، برنامه تلگرام را برای مدت کوتاهی از اپ استور به حالت تعلیق درآورد. این شرکت فناوری در بیانیه‌ای به وب سایت فناوری 9to5Mac اعلام کرد که این برنامه پس از حذف محتوای ممنوعه توسط توسعه‌دهنده و مسدود کردن دایمی کاربر مسوول، بازیابی شد. این برنامه برای کاربران اندروید در فروشگاه پلی گوگل در دسترس باقی ماند. براساس گزارش خبرگزاری آناتولی، اپل پیش از این در سال ۲۰۱۸ این برنامه را از فروشگاه خود حذف کرده بود. در آن زمان، پاول دوروف، بنیانگذار تلگرام، گفت که این حذف به این دلیل رخ داده است که تلگرام «محتوای نامناسب» را در دسترس کاربران خود قرار داده است.

مک‌بوک ایر اپل در بازار نایاب شد

مک‌بوک ایر با وجود افزایش ۲۰۰ دلاری قیمت در ژوئن، در حال حاضر با کمبود عمده در بازار آمریکا مواجه است. به گزارش ایسنا، مارک گورمن، خبرنگار فناوری بلومبرگ گفت: این کمبود موجودی که ناشی از تقاضای شرکت‌های هوش مصنوعی برای تراشه حافظه است، پیش از این رایانه‌های خاص‌تر اپل شامل مک مینی و مک استودیو را تحت تاثیر قرار داده بود. اما به نظر می‌رسد که این شرکت اکنون برای حفظ موجودی مک‌بوک ایر در انبار خود با مشکل مواجه است و خرده‌فروشان می‌گویند که عرضه بیش از هر زمان دیگری محدود شده است. در آمریکا، مک‌بوک ایر با زمان تحویل ۲ تا ۶ هفته‌ای در فروشگاه آنلاین اپل روبه‌رو است و مدل‌های با میزان رم بالاتر بیشترین تاخیر را دارند. در واقع، هر کسی که سعی در خرید مک‌بوک ایر از وب‌سایت اپل دارد، باید تا نیمه دوم ماه اوت یا برای برخی مدل‌ها، تا سپتامبر صبر کند. براساس گزارش تک کرانچ، گورمن می‌گوید اپل در تلاش است تا با افزایش قیمت‌ها و تهیه تراشه حافظه از تامین‌کنندگان چینی، این مشکل را حل کند. در همین حال، این شرکت آخرین تبلیغات بازگشت به مدرسه خود را از ماه ژوئن به تعویق انداخت. و برای اولین بار، مطالب بازاریابی بیشتر بر مدل پایه مک‌بوک پرو متمرکز شده است و حتی هشدار می‌دهد: «مک‌بوک ایر مشروط به موجودی است.» کمبود مداوم تراشه حافظه که ناشی از ساخت مراکز داده با سرورهای قدرتمند هوش مصنوعی توسط شرکت‌هاست، به افزایش سرسام‌آور قیمت تراشه‌های حافظه رم و اس‌اس‌دی مورد استفاده در طیف وسیعی از محصولات اپل منجر شده است. اپل در ژوئن، قیمت ۱۴ محصول از جمله مک‌بوک ایر را افزایش داد. در آمریکا، قیمت این لپ‌تاپ اکنون از ۱۲۹۹ دلار شروع می‌شود که از ۱۰۹۹ دلار افزایش یافته است.

سامسونگ عینک هوشمند می‌سازد

شرکت سامسونگ با گوگل و دو برند «جنتل مانستر» و «واربی پارکر» که عینک می‌سازند برای توسعه عینک گلکسی همکاری می‌کند. به گزارش خبرگزاری مهر به نقل از نیواطلس، کاربران می‌توانند با کمک این گجت پوشیدنی، عکس بگیرند به تماس‌ها پاسخ دهند، موسیقی گوش کنند و به چت بات جمینای گوگل درباره هر آنچه که در لنزهای عینک می‌بینند، حرف بزنند. این عینک شباهت بسیار زیادی به جدیدترین محصول مشابه متا دارد که ماه گذشته عرضه شد. سامسونگ امیدوار است تا تجربه‌ای متمایز برای افرادی ارایه کند که هم اکنون به این اکوسیستم علاقه زیادی دارند. به عنوان مثال اگر کاربر ساعت گلکسی نیز استفاده کند، این گجت می‌تواند حرکات دست را برای ثبت عکس با کمک دوربین‌های عینک، تشخیص دهد. یک موبایل گلکسی تمام این عکس‌ها را برای دسترسی آسان به یک آلبوم مخصوص منتقل می‌کند. همچنین ساعت می‌تواند تماس‌ها را به عینک هوشمند کاربر منتقل کند. عینک سامسونگ می‌تواند با یک بار شارژ تا ۹ ساعت کار کند و قاب شارژ آن نیز می‌تواند این مدت زمان را هفت برابر کند. در محصول از تراشه ARIGen1 اسنپ دراگون متعلق به شرکت کوالکام استفاده شده که هنگام استفاده از دوربین‌ها و جست‌وجو با هوش مصنوعی عملکرد را تسریع می‌کند. در کنار این موارد کاربر می‌تواند با توجه به موقعیت مکانی خود جهت‌یابی مسیر دریافت کند، سخنان فرد دیگر را ترجمه کند و خلاصه‌هایی از پیام‌های دریافتی را بنویسد و آنچه را که کاربر هنگام تماس ویدئویی می‌بیند را به اشتراک بگذارد. سامسونگ از دو طراحی قاب عینک رونمایی کرده است. انتظار می‌رسد بهای محصول ۳۰۰ تا ۴۰۰ دلار باشد.

پاول دوروف به برندگان المپیاد جهانی هوش مصنوعی جایزه می‌دهد

پاول دوروف بنیانگذار تلگرام با انتشار پستی در کانال خود از تعیین جایزه دلاری برای برندگان المپیاد جهانی هوش مصنوعی خبر داد. به گزارش خبرنگار مهر، دوروف همزمان با آغاز المپیاد جهانی هوش مصنوعی ۲۰۲۶ میلادی از اهدای ۲۴۰ جام هوش مصنوعی به برندگان خبر داد. او در پست خود در این باره نوشت: به عنوان نشانه‌ای برای پشتیبانی از افرادی که تمدن ما را باز خلق می‌کنند، ما ۲۴۰ جام هوشمندی انحصاری را به برندگان اهدا می‌کنیم. ما حداقل قیمت‌های بازخرید را تضمین می‌کنیم. به‌طوریکه جام طلای هوش حداقل یک هزار دلار، جام نقره‌ای حداقل ۵۰۰ دلار و جام برنزی حداقل ۳۰۰ دلار ارزش خواهند داشت. اما عرضه محدود این جام‌ها ممکن است باعث شود در بازار ثانویه ارزش بسیار بیشتری پیدا کنند. المپیاد بین‌المللی هوش مصنوعی (IOAI) یک رقابت جهانی علمی برای دانش‌آموزان دبیرستانی است که در آن شرکت‌کنندگان مهارت‌های خود را در زمینه‌های مرتبط با هوش مصنوعی آزمایش می‌کنند.

ناترازی برق از بحران انرژی عبور کرده و به چالش حکمرانی دیجیتال رسیده است

فرسایش آرام مراکز داده زیر سایه خاموشی‌های مکرر

قطع برق برای مراکز داده اتفاق تازه‌ای نیست؛ این مراکز از ابتدا برای ادامه فعالیت در زمان خاموشی طراحی شده‌اند. اما آنچه امروز زیرساخت دیجیتال کشور را با تهدیدی متفاوت روبه‌رو کرده، عادی شدن خاموشی‌ها و استفاده مداوم از تجهیزاتی است که تنها برای شرایط اضطراری ساخته شده‌اند. تکرار این وضعیت، عمر سامانه‌های پشتیبان را کاهش داده، هزینه‌های نگهداری را افزایش داده و احتمال اختلال در ارائه خدمات حیاتی از جمله بانکداری، دولت الکترونیکی، خدمات ابری و ارتباطات را بیش از گذشته بالا برده است؛ مساله‌ای که نشان می‌دهد ناترازی برق دیگر صرفا یک بحران انرژی نیست، بلکه به چالشی برای امنیت و تاب‌آوری زیرساخت دیجیتال کشور تبدیل شده است.

اقتصاد دیجیتال امروز دیگر مفهومی محدود به شرکت‌های فناوری یا کسب‌وکارهای اینترنتی نیست؛ بخش قابل توجهی از خدمات روزمره مردم، از تراکنش‌های بانکی و خریدهای آنلاین گرفته تا سامانه‌های دولت الکترونیکی، خدمات ابری و زیرساخت‌های ارتباطی، بر بستری استوار شده‌اند که مراکز داده ستون اصلی آن به شمار می‌روند. این مراکز، اگرچه از نگاه عموم کمتر دیده می‌شوند، اما اختلال در عملکرد آنها می‌تواند زنجیره‌ای از خدمات حیاتی کشور را به‌طور همزمان تحت تأثیر قرار بدهد. در چنین شرایطی، بحران ناترازی برق دیگر صرفا مساله‌ای مربوط به صنایع تولیدی یا مصرف‌کنندگان بزرگ انرژی نیست، بلکه به چالشی راهبردی برای پایداری زیرساخت دیجیتال کشور تبدیل شده. اگرچه مراکز داده بر اساس استانداردهای جهانی برای مواجهه با قطع برق طراحی شده‌اند و به تجهیزات پشتیبان پیشرفته مجهز هستند، اما تداوم خاموشی‌های برنامه‌ریزی‌شده، این وضعیت اضطراری را به بخشی از روال عادی بهره‌برداری تبدیل کرده است. پیامد این تغییر، تنها افزایش مصرف سوخت یا هزینه‌های عملیاتی نیست، بلکه فرسایش تدریجی تجهیزاتی است که آخرین خط دفاعی زیرساخت دیجیتال کشور محسوب می‌شوند. مساله‌ای که در صورت تداوم، می‌تواند پایداری خدمات دیجیتال، امنیت اقتصادی و حتی تاب‌آوری ملی را با مخاطرات جدی روبه‌رو کند. آن‌طور که مهر گزارش داده، برق بسیاری از مراکز داده در طول هفته و برای چند ساعت قطع می‌شود و هر بار سامانه‌های «UPS»، باتری‌ها، «ATS» و دیزل‌ژنراتورها باید در کسری از ثانیه فرآیند انتقال بار را انجام بدهند. رشد اقتصاد دیجیتال، مراکز داده را از زیرساخت فنی به یکی از ارکان حیاتی اقتصاد، حکمرانی و ارائه خدمات عمومی تبدیل کرده است. سامانه‌های بانکی، خدمات دولت الکترونیکی، پیام‌رسان‌ها، فروشگاه‌های اینترنتی، خدمات ابری و بخش قابل توجهی از زیرساخت‌های ارتباطی کشور، همگی به عملکرد پایدار مراکز داده وابسته هستند. در چنین شرایطی، مساله ناترازی برق دیگر صرفا چالشی برای صنایع انرژی‌بر یا خطوط تولید نیست، بلکه به یکی از مهم‌ترین عوامل تعیین‌کننده پایداری زیرساخت دیجیتال کشور تبدیل شده است. اختلال در تأمین برق مراکز داده، تنها به خاموش شدن چند سرور محدود نمی‌شود، بلکه می‌تواند زنجیره‌ای از خدمات حیاتی را هم‌زمان تحت تأثیر قرار بدهد و آثار آن را میلیون‌ها کاربر، کسب‌وکار و دستگاه اجرایی به صورت مستقیم تجربه کنند. نکته مهم آن است که بحران امروز صنعت مراکز داده از خود خاموشی آغاز نمی‌شود. فلسفه طراحی دیتاسنترهای استاندارد بر مبنای مواجهه با قطع برق شکل گرفته و تجهیزات پشتیبان همچون «UPS»، باتری‌ها، سامانه‌های انتقال خودکار برق و دیزل‌ژنراتورها دقیقا برای مدیریت شرایط اضطراری پیش‌بینی شده‌اند. آن چه امروز این زیرساخت را در معرض تهدید قرار داده، تبدیل شدن وضعیت اضطراری قطع برق به بخشی از فرآیند عادی بهره‌برداری است. استمرار خاموشی‌های برنامه‌ریزی‌شده موجب شده تجهیزاتی که باید تنها در شرایط استثنایی وارد مدار شوند، به صورت روزانه و مستمر مورد استفاده قرار بگیرند و همین تغییر ماهیت، نقطه آغاز فرسایش زیرساخت دیجیتال کشور است.

خاموشی و چالش فرسایش تدریجی زیرساخت

برداشت رایج آن است که وجود تجهیزات برق اضطراری، مراکز داده را در برابر ناترازی برق مصون می‌کند. تجربه عملی صنعت نشان می‌دهد این برداشت تنها زمانی معتبر است که قطعی برق یک رخداد استثنایی باشد. در شرایط کنونی، برق بسیاری از مراکز داده در طول هفته و برای چند ساعت قطع می‌شود و هر بار سامانه‌های «UPS» باتری‌ها، «ATS» و دیزل‌ژنراتورها باید در کسری از ثانیه فرآیند انتقال بار را انجام بدهند. اگرچه این فرآیند از منظر فنی طراحی شده اما تکرار مستمر آن، نرخ استهلاک تجهیزات را به شکل محسوسی افزایش می‌دهد، هزینه‌های تعمیر و نگهداری را بالا می‌برد و احتمال بروز خطا در لحظه سوئیچینگ را افزایش می‌دهد. مدیران مراکز داده تأکید می‌کنند که دیتاسنترها از وقوع خاموشی هراس ندارند، بلکه از تکرار خاموشی و دائمی شدن استفاده از تجهیزات اضطراری آسیب می‌بینند. این تغییر الگوی بهره‌برداری، پیامد دیگری نیز دارد. تجهیزات اضطراری دارای عمر طراحی مشخصی هستند و هر سیکل کاری بخشی از ظرفیت عملیاتی آنها را مستهلک می‌کند. در نتیجه، هرچه دفعات خاموشی افزایش یابد، احتمال از کار افتادن آخرین لایه دفاعی مرکز داده نیز بیشتر خواهد شد. چنین وضعیتی به معنای افزایش احتمال وقوع خاموشی کامل سرویس در شرایطی است که زیرساخت اصلی نیز قادر به تأمین برق نیست.

آسیب خاموشی از اتاق برق فراتر می‌رود

پایداری یک مرکز داده تنها به روشن بودن سرورها وابسته نیست. سامانه‌های سرمایشی، تجهیزات شبکه، سامانه‌های ذخیره‌سازی، تجهیزات امنیت فیزیکی، سیستم‌های اعلام و اطفای حریق و تجهیزات کنترل محیطی همگی نیازمند برق پایدار هستند. در زمان قطع برق، حتی اگر ژنراتور در مدت کوتاهی وارد مدار شود، فاصله زمانی میان خروج برق شهری و ورود برق اضطراری موجب توقف کوتاه سامانه‌های سرمایشی می‌شود. همین وقفه چند ده ثانیه‌ای یا یک دقیقه‌ای می‌تواند دمای سالن‌های سرور را افزایش دهد و عملکرد تجهیزات حساس را مختل کند در برخی موارد نیز تجهیزات پس از بازگشت برق به مدار عملیاتی بازنمی‌گردند و همین مساله کیفیت سرویس‌های دیجیتال و حتی کیفیت ارتباطات اینترنتی را تحت تأثیر قرار می‌دهد. از منظر مهندسی مراکز داده، برق مصرفی صرفا برای تغذیه سرورها نیست. سامانه‌های خنک‌کننده، تجهیزات انتقال داده، تجهیزات امنیتی، کنترل دسترسی، تجهیزات ذخیره‌سازی و سامانه‌های پشتیبان همگی بخشی از بار الکتریکی مرکز داده را تشکیل می‌دهند. از این رو هر اختلال در تأمین برق، به سرعت به سایر اجزای زیرساخت سرایت می‌کند و احتمال ایجاد اختلال زنجیره‌ای را افزایش می‌دهد.

اقتصاد دیجیتال قربانی پنهان ناترازی انرژی

تداوم خاموشی‌ها تنها هزینه انرژی را افزایش نداده، بلکه ساختار اقتصادی مراکز داده را نیز دستخوش تغییر کرده است. بر اساس اظهارات مدیران صنعت، مصرف گازوئیل ژنراتورها به شکل قابل توجهی افزایش یافته و هزینه تأمین سوخت نسبت به سال گذشته بیش از ۲۰۰ درصد رشد کرده است. در عین حال، سهمیه‌های تخصیصی پاسخگوی نیاز واقعی مراکز داده نیست و بسیاری از اپراتورها ناچار به خرید سوخت از بازار آزاد با قیمت‌های چندبرابری شده‌اند. این وضعیت، علاوه بر افزایش هزینه عملیاتی، ریسک دیگری نیز ایجاد می‌کند. کیفیت نامناسب سوخت می‌تواند به موتور ژنراتورها، سامانه سوخت‌رسانی و فیلترها آسیب وارد کند و قابلیت اطمینان آخرین لایه پشتیبان مرکز داده را کاهش بدهد. همزمان، محدودیت‌های ناشی از تحریم، دشواری تأمین قطعات یدکی، کاهش دسترسی به تجهیزات تخصصی و فرسودگی تدریجی زیرساخت‌ها، فرآیند تعمیر و نوسازی تجهیزات را نیز پیچیده‌تر کرده است. در چنین شرایطی، هر خاموشی تنها یک وقفه موقت در ارائه خدمت نیست، بلکه بخشی از عمر سرمایه‌های زیرساختی کشور را مصرف می‌کند و هزینه ارائه خدمات دیجیتال را به صورت مستمر افزایش می‌دهد.

فاصله استانداردهای جهانی با واقعیت بهره‌برداری در ایران

در استانداردهای بین‌المللی شاخص‌هایی مانند افزونگی تجهیزات، قابلیت نگهداری بدون توقف سرویس و سطح دسترس‌پذیری سالانه برای مراکز داده تعریف شده‌اند. بر همین اساس، مراکز داده سطح سه با دسترس‌پذیری حدود ۹۹.۹۸ درصد و مراکز سطح چهار با دسترس‌پذیری حدود ۹۹.۹۹۵ درصد طراحی می‌شوند. با این حال، این استانداردها بر یک پیش‌فرض اساسی استوار هستند و آن وجود شبکه برق پایدار، دسترسی مطمئن به سوخت، امکان سرویس منظم تجهیزات و محدود بودن شرایط اضطراری است. هنگامی که خاموشی به بخشی از وضعیت عادی شبکه برق تبدیل شود، بسیاری از مفروضات این استانداردها عملا اعتبار خود را از دست می‌دهند و تجهیزات اضطراری ناچار می‌شوند وظایفی فراتر از ظرفیت طراحی شده خود بر عهده بگیرند. از همین رو، مقایسه صرف سطح استاندارد مراکز داده ایران با نمونه‌های بین‌المللی بدون توجه به کیفیت زیرساخت انرژی، تصویر دقیقی از وضعیت واقعی ارایه نمی‌کند. مساله اصلی، فاصله فناوری نیست، بلکه تفاوت شرایط بهره‌برداری محسوب می‌شود.

تغییر نگاه از مصرف‌کننده برق به زیرساخت حیاتی

راهکارهای مطرح‌شده از سوی فعالان صنعت نشان می‌دهد حل مساله تنها با افزایش تعداد ژنراتورها یا ظرفیت «UPS» ممکن نیست. نخستین گام، به رسمیت شناختن مراکز داده به عنوان زیرساخت حیاتی کشور در سیاستگذاری انرژی است تا در برنامه‌های مدیریت بار، تأمین برق پایدار و تخصیص سوخت اضطراری جایگاه مستقلی داشته باشند. تحقق این هدف نیازمند هماهنگی میان وزارت نیرو، وزارت ارتباطات و توانیر است تا تفاهم‌های موجود از سطح سیاست به مرحله اجرا منتقل شوند. در کنار این اقدام، توسعه برق اختصاصی برای مراکز داده، سرمایه‌گذاری در انرژی‌های تجدیدپذیر، توسعه شبکه‌های هوشمند برق، به کارگیری سامانه‌های پیشرفته پایش مصرف انرژی، طراحی معماری‌های ابری مقاوم در برابر اختلال، توزیع جغرافیایی بار پردازشی، استقرار مراکز داده بر اساس معیارهای دسترسی پایدار به انرژی و اجرای برنامه‌های منظم آزمون تجهیزات پشتیبان، از مهم‌ترین اقداماتی هستند که می‌توانند تاب‌آوری زیرساخت دیجیتال کشور را افزایش بدهند. در نهایت، می‌توان چنین نتیجه گرفت که ناترازی برق، مراکز داده را با بحرانی مواجه کرده که ماهیتی متفاوت از خاموشی‌های مقطعی گذشته دارد. مساله امروز، فقدان تجهیزات اضطراری نیست، بلکه استفاده دائمی از تجهیزاتی به‌است که برای شرایط بحرانی طراحی شده‌اند. ادامه این روند، به تدریج قابلیت اطمینان زیرساخت‌های دیجیتال را کاهش می‌دهد، هزینه ارائه خدمات را افزایش می‌دهد و ریسک اختلال در زنجیره‌ای از خدمات حیاتی کشور را بالا می‌برد. از این منظر، تأمین برق پایدار برای مراکز داده صرفا یک مطالبه صنفی یا فنی نیست، بلکه بخشی از الزامات امنیت اقتصادی، تاب‌آوری ملی و حکمرانی دیجیتال کشور به شمار می‌رود.

بازخوانی حادثه خروج اوپن‌ای‌آی

رخداد خروج هوش مصنوعی اوپن‌ای‌آی از کنترل در جولای ۲۰۲۶ نقطه‌ای تعیین‌کننده در تاریخ امنیت هوش مصنوعی به‌شمار می‌آید. به گزارش مهر، برای نخستین بار یک مدل پیشرفته هوش مصنوعی در جریان یک ارزیابی امنیت سایبری، به جای آنکه صرفا آسیب‌پذیری نرم‌افزار هدف را شناسایی کند، موفق شد محدودیت‌های محیط آزمایشگاهی را دور بزند، به زیرساخت داخلی آزمایش نفوذ کند، به اینترنت عمومی دسترسی یابد و سپس سامانه‌های پلتفرم هاگینگ فیس را هدف قرار دهد. به عقیده کارشناسان، اهمیت این رخداد در خسارت مستقیم آن خلاصه نمی‌شود. آن چه این حادثه را به یک نقطه عطف تبدیل می‌کند، آشکار شدن محدودیت‌های فعلی سازوکارهای مهار مدل‌های هوش مصنوعی و ورود بحث «از دست رفتن کنترل» از سطح فرضیات نظری به نخستین نمونه عملی مستند است. در سال‌های گذشته، بخش قابل توجهی از بحث‌های عمومی پیرامون مخاطرات هوش مصنوعی تحت تأثیر روایت‌های سینمایی از «شورش ماشین‌ها» قرار داشت. با این حال، شواهد این رخداد نشان می‌دهد مساله اصلی نه شکل‌گیری اراده مستقل در هوش مصنوعی، بلکه توانایی فزاینده مدل‌ها در یافتن مسیرهایی است که طراحان سامانه هرگز پیش‌بینی نکرده‌اند. همین تغییر زاویه نگاه، مساله را از حوزه علمی تخیلی به یکی از مهم‌ترین چالش‌های مهندسی امنیت سایبری و حکمرانی فناوری تبدیل می‌کند.

زنجیره استدلال، نفوذ و بهره‌برداری

طبق گزارش اوپن‌ای‌آی، مدل‌های هوش مصنوعی در محیطی به ظاهر ایزوله مستقر شده بودند تا توانایی آنها در کشف آسیب‌پذیری‌های نرم‌افزاری ارزیابی شود. این محیط تنها اجازه دسترسی محدود به یک سرویس داخلی برای دریافت بسته‌های نرم‌افزاری مجاز را فراهم می‌کرد. مدل‌ها در جریان اجرای ماموریت موفق شدند یک آسیب‌پذیری ناشناخته در همان سرویس شناسایی کنند، از آن برای افزایش سطح دسترسی استفاده نمایند، به سایر سامانه‌های داخلی اوپن‌ای‌آی نفوذ کنند و در نهایت امکان دسترسی به اینترنت عمومی را بیابند. پس از خروج از محیط آزمایش، مدل‌ها با استدلال زنجیره‌ای به این نتیجه رسیدند که شرکت هاگینگ فیس احتمالا اطلاعاتی مرتبط با آزمون امنیتی در اختیار دارد. سپس با انجام هزاران اقدام خودکار روی مجموعه‌ای از ماشین‌های مجازی موقت، زیرساخت حمله را به صورت پویا میان سرویس‌های مختلف جابه‌جا کردند تا عملیات بدون وقفه ادامه یابد. هدف نهایی، دستیابی به اطلاعاتی بود که بتواند امتیاز مدل را در آزمون امنیت سایبری افزایش دهد. بر اساس گزارش منتشرشده، شرکت هاگینگ فیس ابتدا این رخداد را یک حمله سایبری گسترده تلقی کرد و موضوع را به پلیس گزارش داد. تنها چند روز بعد مشخص شد عامل این عملیات، مدل‌های ارزیابی‌شده اوپن‌ای‌آی بوده‌اند. همین توالی رویدادها نشان می‌دهد که رفتار مدل تا چه اندازه به الگوی عملیاتی مهاجمان انسانی حرفه‌ای نزدیک شده است.

چالش توانمندی هوش مصنوعی مساله اصلی فراتر از قصد نیت مدل است

برداشت اولیه از چنین اخباری ممکن است این باشد که هوش مصنوعی به‌صورت مستقل تصمیم به حمله گرفته است. تحلیل فنی رخداد، تصویری کاملا متفاوت ارائه می‌دهد. مدل در جریان اقدام اخیر، هیچ هدف جدیدی برای خود تعریف نکرده و انگیزه‌ای مستقل شکل نداده است. هدف از ابتدا از سوی پژوهشگران تعیین شده بود و مدل صرفا با استفاده از تمام ظرفیت‌های استدلالی خود، موثرترین مسیر دستیابی به آن را جست‌وجو کرد. در واقع، مدل دقیقا همان رفتاری را بروز داده که معماری آزمون آن را تشویق می‌کرده. موفقیت در آزمون بر اساس دستیابی به هدف تعریف شده بود و محدودیت‌های امنیتی نیز برای سنجش توان واقعی مدل تا حدی کاهش یافته بودند. نتیجه آنکه مدل، برخلاف انتظار طراحان، محدودیت‌های محیط را نیز بخشی از مساله تلقی کرده و آنها را دور زد. این تمایز اهمیت بنیادی دارد. به باور متخصصان، تهدید اصلی از «نیت خصمانه» ناشی نمی‌شود، بلکه از ترکیب سه عامل، شامل هدف مشخص، توانایی شناختی بالا و محیط مساعد، شکل می‌گیرد. در چنین شرایطی، حتی مدلی که هیچ انگیزه مستقلی ندارد نیز می‌تواند رفتارهایی با پیامدهای امنیتی بسیار جدی تولید کند.

عبور از آسیب‌پذیری منفرد به عملیات چندمرحله‌ای

مهم‌ترین یافته فنی این رخداد، توانایی مدل در اتصال چندین آسیب‌پذیری مستقل به یک زنجیره عملیاتی واحد است. در امنیت سایبری، مهاجمان حرفه‌ای معمولا از یک نقص منفرد استفاده نمی‌کنند، بلکه مجموعه‌ای از ضعف‌های کوچک را به شکلی ترکیب می‌کنند که در نهایت به نفوذ کامل منجر شود. شواهد منتشر شده نشان می‌دهد مدل اوپن‌ای‌آی نیز دقیقا چنین الگویی را دنبال کرده است. کشف آسیب‌پذیری اولیه، افزایش سطح دسترسی، عبور از محیط مهار، اتصال به اینترنت، شناسایی هدف مناسب، طراحی مسیر حمله و اجرای عملیات، همگی بخشی از یک زنجیره استدلال پیوسته بوده‌اند. برای جامعه متخصصان امنیت سایبری، این تحول از اهمیت ویژه‌ای برخوردار است، زیرا نشان می‌دهد مدل‌های نسل جدید تنها در تولید کد یا تحلیل آسیب‌پذیری توانمند نیستند، بلکه قادر هستند عملیات پیچیده چندمرحله‌ای را نیز برنامه‌ریزی و اجرا کنند و این قابلیت تاکنون عمدتا در اختیار مهاجمان انسانی بسیار ماهر قرار داشت.

شکست سندباکس و ضرورت بازنگری در معماری کنترل

این حادثه ضعف یکی از مهم‌ترین مفروضات صنعت هوش مصنوعی را نیز آشکار کرد. سال‌ها تصور می‌شد اجرای مدل در محیط‌های آزمایشی موسوم به «سندباکس» (Sandbox)، سطح قابل قبولی از ایمنی ایجاد می‌کند. این در حالی است که برخی از کارشناسان نیز تأکید کرده‌اند که این محیط‌ها ذاتا امنیت مطلق ندارند. در صنایع فوق حساس مانند نیروگاه‌های هسته‌ای، سامانه‌های حیاتی معمولا با استفاده از معماری «Air Gap» به صورت فیزیکی از اینترنت جدا می‌شوند. مقایسه این استانداردها با زیرساخت‌های مورد استفاده در بسیاری از آزمایشگاه‌های هوش مصنوعی نشان می‌دهد فاصله قابل توجهی میان الزامات امنیت سایبری در زیرساخت‌های حیاتی و رویه‌های رایج شرکت‌های فناوری وجود دارد. اوپن‌ای‌آی نیز پس از این رخداد اعلام کرد که کنترل‌های مهار، حفاظت سایبری در زمان ارزیابی و سامانه‌های پایش داخلی خود را تقویت کرده است، هرچند این تغییرات به کاهش سرعت پژوهش و توسعه منجر خواهد شد.

خلأ نظارت حقوقی و الزام به افشای رخدادها

ابعاد حقوقی این حادثه نیز به اندازه بحث فنی قابل توجه است. اوپن‌ای‌آی از نظر قانونی الزامی برای افشای این رخداد نداشت. قوانین تازه برخی ایالت‌های امریکا مانند «SB ۵۳» در کالیفرنیا و «RAISE Act» در نیویورک تنها زمانی شرکت‌ها را ملزم به گزارش رخدادهای ایمنی می‌کنند که خطر مرگ گسترده، جراحات شدید یا خسارت مالی بسیار بزرگ وجود داشته باشد. شماری از متخصصان سیاستگذاری هوش مصنوعی این آستانه را بسیار بالا ارزیابی کرده‌اند و معتقدند بخش عمده رخدادهای مهم هرگز مشمول الزام قانونی برای افشا نخواهند شد. از این منظر، حادثه اوپن‌ای‌آی بار دیگر خلأ حکمرانی فناوری را آشکار ساخت و نشان داد چارچوب‌های حقوقی موجود هنوز متناسب با مخاطرات مدل‌های پیشرفته هوش مصنوعی توسعه نیافته‌اند.

امنیت آینده محصول معماری چندلایه است

یکی از مهم‌ترین درس‌های این حادثه، ناکارآمدی اتکای صرف به سازوکارهایی مانند «کلید توقف اضطراری» است. تجربه چند دهه صنعت امنیت سایبری نشان داده هیچ ابزار منفردی قادر به تأمین امنیت کامل نیست. سازمان‌ها از طریق دفاع چندلایه، پایش مستمر، تفکیک سامانه‌ها، محدودسازی دسترسی، کنترل رفتار و کشف آنی رخدادها سطح تاب‌آوری خود را افزایش می‌دهند. متخصصان معتقدند که همین منطق باید در طراحی سامانه‌های هوش مصنوعی نیز حاکم شود. پرسش اصلی دیگر این نیست که چگونه یک مدل را پس از خروج از کنترل متوقف کنیم، بلکه باید مشخص شود چرا اساسا امکان خروج از کنترل برای آن فراهم شده است. هر مسیر پیش‌بینی‌نشده‌ای که مدل بتواند برای دستیابی به هدف خود کشف کند، در عمل به یک بردار حمله بالقوه تبدیل خواهد شد. رخداد سایبری اخیر اوپن‌ای‌آی بیش از آنکه روایتی هیجان‌انگیز از فرار هوش مصنوعی باشد، بازتاب محدودیت‌های معماری امنیتی نسل کنونی سامانه‌های هوش مصنوعی است. مدل‌های پیشرفته امروز توانایی استدلال، برنامه‌ریزی و اجرای عملیات پیچیده را با سرعتی فراتر از انتظار پژوهشگران به دست آورده‌اند، در حالی که سازوکارهای مهار، نظارت و حکمرانی آنها هنوز متناسب با این جهش توانمندی تکامل نیافته است. اهمیت واقعی این حادثه در آن است که برای نخستین بار نشان داد مرز میان ارزیابی آزمایشگاهی و عملیات واقعی می‌تواند در اثر یک زنجیره استدلال هوشمند شکسته شود. هرچه مدل‌های نسل آینده قدرتمندتر شوند، امنیت آنها بیش از هر زمان دیگری به کیفیت طراحی محیط‌های مهار، معماری دفاع چندلایه، پایش بلادرنگ و نظام‌های حقوقی الزام‌آور وابسته خواهد بود. آینده امنیت هوش مصنوعی نه در مهار هوش، بلکه در مهار محیطی رقم خواهد خورد که هوش در آن عمل می‌کند.

دنیای فناوری

گام جدید چین در خودکفایی تراشه

شرکت «سی‌ایکس‌ام‌تی» (CXMT) بزرگ‌ترین سازنده تراشه چین از نظر ارزش بازار، در حال بررسی ساخت دومین کارخانه تولید تراشه‌های حافظه در پکن است و برای تامین مالی این پروژه با یک مرکز تولید فناوری مورد حمایت دولت محلی مذاکره می‌کند. به گزارش ایسنا، این اقدام در شرایطی انجام می‌شود که «سی‌ایکس‌ام‌تی» تلاش می‌کند ظرفیت تولید خود را در بحبوحه افزایش تقاضای جهانی برای تراشه‌های مورد استفاده در زیرساخت‌های هوش مصنوعی، مراکز داده و تجهیزات الکترونیکی مصرفی، افزایش بدهد. این شرکت با عرضه اولیه سهام به ارزش ۸.۶ میلیارد دلار در جولای، بزرگ‌ترین عرضه اولیه یک شرکت نیمه‌رسانا در بازار چین را ثبت کرد و اکنون برنامه توسعه گسترده‌ای را دنبال می‌کند. «سی‌ایکس‌ام‌تی» پیش‌تر ساخت کارخانه‌های جدیدی را در شانگهای و هفی آغاز و درباره احداث تاسیسات دیگری نیز با مقامات محلی مذاکره کرده است. این پروژه‌ها در صورت بهره‌برداری کامل می‌توانند ظرفیت تولید این شرکت را دو برابر کنند و به بیش از ۶۰۰ هزار ویفر در ماه برسانند. کارخانه جدید پکن قرار است در منطقه «یی‌ژوانگ» ساخته شود؛ منطقه‌ای که در جنوب‌شرقی پکن قرار دارد و «سی‌ایکس‌ام‌تی» هم‌اکنون در آن یک کارخانه تولید تراشه‌های حافظه DRAM را اداره می‌کند. منابع آگاه اعلام کردند این شرکت به دنبال دریافت حداقل ۶۰ میلیون یوان حمایت مالی از نهاد مدیریت منطقه توسعه اقتصادی-فناوری پکن و همچنین برخی شرکت‌های فناوری دولتی است. هنوز جزئیات نهایی درباره میزان سرمایه‌گذاری و ظرفیت تولید این کارخانه مشخص نشده است. ساخت کارخانه برای تولید تراشه‌های پیشرفته حافظه DRAM معمولا بیش از ۱۰ میلیارد دلار هزینه دارد. «سی‌ایکس‌ام‌تی» هم‌اکنون دو کارخانه تولید تراشه حافظه ۱۲ اینچی در هفی و یک کارخانه در پکن دارد که ظرفیت هر کدام حدود ۱۰۰ هزار ویفر در ماه است. این شرکت به یکی از پایه‌های اصلی برنامه چین برای دستیابی به خودکفایی در صنعت تراشه و کاهش وابستگی به فناوری‌های خارجی تبدیل شده است. طبق گزارش خبرگزاری رویترز، با وجود رشد سریع، «سی‌ایکس‌ام‌تی» همچنان فاصله زیادی با غول‌های جهانی مانند «سامسونگ الکترونیکس»، «اس‌کی هاینیکس» و «میکرون» دارد که بخش عمده بازار جهانی تراشه‌های حافظه DRAM را در اختیار دارند. با این حال، نفوذ این شرکت در بازار داخلی چین افزایش یافته و به یکی از مهره‌های کلیدی پکن در رقابت فناوری با امریکا تبدیل شده است.

امتیاز مالیاتی جدید هند به اپل

هند در اقدامی که می‌تواند به نفع اپل باشد، در قالب اصلاحات جدید مالیاتی، تمدید معافیت‌های مالیاتی شرکت‌های خارجی تامین‌کننده تجهیزات برای تولیدکنندگان قراردادی تا ۲۰۴۱ را پیشنهاد کرد. به گزارش ایسنا، این پیشنهاد در حالی مطرح می‌شود که هند به یکی از مهم‌ترین مراکز تولید آیفون در خارج از چین تبدیل شده است و بر اساس برآورد موسسه «کانترپوینت ریسرچ»، سهم هند از تولید جهانی آیفون از حدود ۶ درصد در چهار سال گذشته، به ۲۶ درصد در سال ۲۰۲۶ خواهد رسید. طبق پیش‌نویس اصلاحات مالیاتی، دولت هند برای ایجاد «اطمینان مالیاتی» پیشنهاد داد معافیت مالیاتی شرکت‌های خارجی که تجهیزات مورد نیاز تولیدکنندگان قراردادی خود را در هند تامین می‌کنند، تا ۳۱ مارس ۲۰۴۱ تمدید شود. این معافیت پیش‌تر در فوریه سال جاری تصویب شده بود، اما فقط تا سال ۲۰۳۱ اعتبار داشت. اپل پیش‌تر از دولت هند خواسته بود قوانین مالیاتی این کشور را تغییر دهد تا مالکیت تجهیزات پیشرفته مورد استفاده در تولید آیفون که در اختیار تولیدکنندگان قراردادی قرار می‌دهد، به عنوان «ارتباط تجاری» تلقی نشود؛ موضوعی که می‌توانست باعث شود سود حاصل از فروش آیفون مشمول مالیات هند شود. بر اساس این پیشنهاد، معافیت مالیاتی شامل تولیدکنندگان تلفن همراه، تبلت، رایانه‌های قابل حمل، دستگاه‌های شنوایی و تجهیزات پوشیدنی الکترونیکی خواهد شد. همچنین درآمد شرکت‌های خارجی ناشی از ذخیره‌سازی و تامین قطعات مورد استفاده در تولید این محصولات برای تولیدکنندگان قراردادی نیز تا سال ۲۰۴۱ از مالیات معاف می‌شود. این مقررات شامل کارخانه‌ها و انبارهای مستقر در «مناطق گمرکی تضمین‌شده» خواهد شد که طبق مقررات گمرکی، خارج از مرزهای گمرکی هند در نظر گرفته می‌شوند. با این حال، فروش محصولات تولیدشده در این مراکز در بازار داخلی هند همچنان مشمول عوارض واردات خواهد بود و همین مساله این تاسیسات را بیشتر به گزینه‌ای مناسب برای صادرات تبدیل می‌کند. ریاض تینگنا، شریک موسسه «گرنت تورنتون بهارات» در این باره گفت: این تغییرات مالیاتی به شرکت‌های خارجی اجازه می‌دهد تجهیزات و قطعات حیاتی را برای تولیدکنندگان قراردادی خود در هند ذخیره و منتقل کنند و همچنین، اختلال‌های زنجیره تامین ناشی از نااطمینانی‌های تجاری را کاهش دهند. دولت هند همچنین پیشنهاد کرد استفاده شرکت‌های خارجی از مراکز داده در این کشور نیز با شرایط آسان‌تری از معافیت‌های مالیاتی برخوردار شود. بر اساس اصلاحات جدید، مراکز داده می‌توانند به‌جای مالکیت، توسط شرکای هندی شرکت‌های خارجی اجاره شوند. به گفته کارشناسان، چنین اقدامی نیاز به سرمایه‌گذاری اولیه را کاهش داده و ورود شرکت‌های کوچک‌تر به بازار را تسهیل می‌کند.

هکرها به قلب پلیس انگلیس نفوذ کردند

اطلاعات شخصی حدود ۱۰۰ هزار افسر پلیس انگلیس پس از نفوذ هکرها به یکی از پایگاه‌های داده مهم نیروهای انتظامی در دارک‌وب منتشر شد و اطلاعات افرادی را فاش کرد که سال‌ها در زمینه مقابله با مجرمان فعالیت داشته‌اند. به گزارش ایسنا، این نشت اطلاعات، بخشی از کارزار گسترده‌تر حملات سایبری است که در هفته‌های اخیر نهادهای دولتی انگلیس از جمله وزارت دفاع، وزارت کشور، آژانس ملی مبارزه با جرایم (NCA) و سازمان دادستانی سلطنتی (CPS) را نیز هدف قرار داده است. این حمله چند روز پس از آن رخ داد که هکرها به سامانه‌های وزارت آموزش انگلیس نفوذ کرده و اطلاعات بیش از ۵۰۰ هزار نفر را افشا کردند. بر اساس گزارش‌ها، مهاجمان پس از نفوذ به پایگاه ملی حقوقی پلیس (PNLD) اطلاعات مربوط به وابستگی سازمانی و نیروهای محل خدمت افسران پلیس را منتشر کردند.