دنیای فناوری

هواوی به موج افزایش قیمت گوشی‌های هوشمند پیوست

شرکت فناوری هواوی برای مقابله با هزینه‌های بالاتر تراشه حافظه، قصد دارد مانند رقبای خود، قیمت گوشی‌های هوشمند را افزایش دهد. به گزارش ایسنا، ریچارد یو، مدیر کسب و کار مصرف‌کننده هواوی هفته جاری به خبرنگاران در شنزن گفت: این غول فناوری چینی میانگین افزایش ۲۰۰ دلاری در هزینه‌های گوشی‌های هوشمند خود داشته است، اما او چارچوب زمانی را برای مقایسه مشخص نکرد. او گفت: «ما باید قیمت‌ها را در آینده افزایش دهیم، هرچند این افزایش متوسط خواهد بود اما به‌شدت به سودآوری ما لطمه می‌زند.» با این حال، ریچارد یو خاطرنشان کرد که کمبود تراشه حافظه باعث می‌شود هواوی به عنوان یک سازنده گوشی‌های هوشمند برتر در برابر برندهای اقتصادی برتری پیدا کند. شرکت ردیاب بازار «کانترپوینت ریسرچ» اخیرا تخمین زده است که حدود ۲۳۰ میلیون گوشی هوشمند با قیمت کمتر از ۲۰۰ دلار تا پایان دهه جاری، از بین خواهند رفت.

یو می‌گوید: «تقاضا برای محصولات ارزان‌قیمت بیشتر فشرده می‌شود و همه را وادار می‌کند تا به بخش‌های متوسط و رده بالا بروند که هواوی در این بخش‌ها برتری دارد.» ما مطمئن هستیم که می‌توانیم از این چرخه جان سالم به در بریم تا نوآوری بیشتری در محصول به ارمغان بیاوریم.»

هواوی روز پنجشنبه، نسل جدیدی از گوشی‌های گران قیمت خود را با نسخه ویژه میت ۹۰ پرو مکس با قیمت ۱۰۹۹۹ یوان (۱۶۴۰ دلار امریکا) رونمایی کرد. برندهای جهانی گوشی‌های هوشمند و لوازم الکترونیکی از اپل گرفته تا شیائومی، امسال تحت فشار قرار گرفته‌اند، زیرا توسعه بی‌سابقه هوش مصنوعی، هزینه‌های قطعات مختلف را افزایش داده است. اپل، شیائومی و هواوی همگی قیمت گوشی‌های خود را در ماه سپتامبر افزایش دادند. کانترپوینت هفته جاری گزارش کرد در بحبوحه کمبود تراشه حافظه، تقاضای مصرف‌کنندگان در چین در سال جاری ملایم باقی مانده است و فروش هفتگی گوشی‌های هوشمند در این کشور از ژوئیه، بر مبنای سالانه کاهش دو رقمی یافته است. درآمد خالص هواوی در نیمه اول سال جاری ۳۶ درصد کاهش یافت که بخشی از آن به دلیل ذخیره مواد خام برای کاهش تاثیر افزایش هزینه‌ها بود. مخابرات و لوازم الکترونیکی مصرفی، دو رکن اصلی کسب و کار اصلی هواوی هستند و هر بخش حدود ۴۰ درصد در کل فروش آن سهم دارد. این شرکت تا حد زیادی قیمت محصولاتش را بدون تغییر نگه داشته است، در حالی که رقبای داخلی شیائومی و اوپو تاکنون چندین بار قیمت گوشی‌های هوشمند را در سال جاری افزایش داده‌اند. به نظر می‌رسد این راهبرد موثر واقع شده است. کانترپوینت در یادداشت قبلی در ماه اوت اعلام کرد انتظار می‌رود هواوی امسال شاهد رشد حدود ۸ درصدی فروش گوشی‌های هوشمند خود باشد، در حالی که سایر برندهای چینی کاهش ۳۴ درصدی را در مدت مشابه گزارش می‌دهند. قدرت هواوی تا حدی ناشی از محبوبیت گوشی‌های تاشو آن است. یو می‌گوید ورود اپل به این دسته عملکرد هواوی را افزایش می‌دهد. به گفته مدیر اجرایی، پس از عرضه آیفون دوئو توسط اپل، «پورا ایکس مکس» ۱۶۵۰ دلاری هواوی، ۷۶ درصد جهش در فروش داشت و مجموع عرضه آن به ۱.۴ میلیون دستگاه رسید. بر اساس گزارش بلومبرگ، یو گفت که این شرکت قصد دارد فروش نسل دوم گوشی «میت ایکس تی ۲» را که از ۲۹۸۰ دلار امریکا شروع می‌شود، به بیش از یک میلیون دستگاه در سال جاری افزایش دهد. این مدیر اجرایی افزود: هواوی در حال برنامه‌ریزی برای افزایش فروش گوشی‌های گران قیمت خود در خارج از چین، در بازارهایی از جمله خاورمیانه و اروپا است.

دولت امریکا صاحب چت‌بات هوش مصنوعی رسمی شد

دولت امریکا چت بات هوش مصنوعی خود را دارد. America.gov رابطی برای افرادی است که سوالاتی درباره اطلاعات و سرویس‌های آژانس‌های فدرال دارند. به گزارش خبرگزاری مهر به نقل از انگجت، در صفحه وب این چت‌بات اعلام شده است که از هوش مصنوعی برای ارایه پاسخ‌های ساده، بر اساس اطلاعات منتشرشده در منابع رسمی دولتی، استفاده می‌کند. این چت‌بات در حال حاضر ابزاری برای مرتب‌سازی و دسترسی آسان‌تر به اطلاعات موجود در فضای عمومی است، اما قرار است این پلتفرم سال آینده خدمات بیشتری به کاربران ارایه دهد؛ از جمله ثبت‌نام در Medicare، درخواست گذرنامه و جست‌وجوی فرصت‌های شغلی در دولت فدرال. بر اساس یک دستور اجرایی جدید، رهبران دستگاه‌های اجرایی موظف شده‌اند America.gov را به عنوان تنها نقطه ورود شهروندان امریکایی برای دسترسی به خدمات آنلاین ایجاد و ارایه کنند و آن را با Login.gov یکپارچه سازند. این چت‌بات تاریخچه جست‌وجوها یا پیام‌های کاربران را ذخیره نمی‌کند و از موقعیت مکانی دقیق آنها نیز استفاده نمی‌کند. همچنین، وب‌سایت مدعی است که به کاربران کمک می‌کند پیش از ارسال اطلاعات، از اشتراک‌گذاری داده‌های خصوصی خود جلوگیری کنند. برای استفاده از این چت‌بات نیز نیازی به ایجاد حساب کاربری نیست.

معاون وزارت ارتباطات از پیامدهای سیاست‌های محدودکننده و گسترش ابزارهای گریز از حکمرانی می‌گوید

استارلینک؛ آخرین میخ بر تابوت حکمرانی اینترنت



استارلینک می‌تواند آخرین حلقه زنجیره‌ای باشد که از سال‌ها پیش با گسترش فیلترینگ و محدودیت اینترنت آغاز شده است؛ زنجیره‌ای که حالا به فناوری‌ای رسیده که کنترل آن برای سیاست‌گذار به مراتب دشوارتر است. محمد حافظ حکمی، معاون فناوری، نوآوری و امور بین‌الملل وزارت ارتباطات، با اشاره به گسترش ابزارهای گریز از سیاست‌های حاکمیت در میان کاربران، هشدار داده است که موج بعدی این ابزارها می‌تواند دیگر از شبکه عبور نکند و مستقیماً از ماهواره به کاربر برسد. او در عین حال تاکید دارد که راه حفظ حکمرانی، ادامه مسیر سلبی نیست؛ بلکه باید با تامین نیازهای جامعه و ساخت شبکه‌ای قابل استفاده و مقرون‌به‌صرفه، حکمرانی فضای مجازی را از «محدودسازی» به «ارایه گزینه» تغییر داد. وضعیت اینترنت در ایران در سال‌های اخیر به نقطه‌ای رسیده که دیگر نمی‌توان آن را صرفاً با کیفیت شبکه، سرعت اتصال یا حتی فیلترینگ چند پلتفرم توضیح داد. تجربه کاربران از اینترنت، تحت تاثیر مجموعه‌ای از محدودیت‌ها، اختلال‌ها، قطع ارتباطات و دشواری دسترسی به بسیاری از سرویس‌های جهانی قرار گرفته است. در مقابل، ابزارهای عبور از محدودیت نیز به بخشی از زندگی روزمره کاربران تبدیل شده‌اند؛ اتفاقی که عملاً نشان داده است میان سیاست‌های رسمی و رفتار واقعی جامعه فاصله‌ای جدی شکل گرفته است. حالا اما بخشی از ادبیاتی که از داخل ساختار سیاست‌گذاری فضای مجازی مطرح می‌شود، بر همین شکاف دست می‌گذارد. محمد حافظ حکمی، معاون فناوری، نوآوری و امور بین‌الملل وزارت ارتباطات و فناوری اطلاعات، در نشست «آسیب‌شناسی ساختار و افق‌های بازآرایی حکمرانی فضای مجازی کشور»، از مسیری سخن گفت که طی یک دهه گذشته طی شده و به اعتقاد او، در نهایت نه تنها به حل مساله منجر نشده، بلکه کاربران را بیشتر به سمت ابزارهایی سوق داده که امکان اعمال حکمرانی بر آنها دشوارتر است. اهمیت صحبت‌های حکمی از این جهت است که او مساله را صرفاً به ناکارآمدی فنی شبکه یا مشکلات اجرایی تقلیل نمی‌دهد. از نگاه او، بخش مهمی از وضعیت امروز نتیجه نوع مواجهه سیاست‌گذار با فضای مجازی است؛ مواجهه‌ای که به جای سیاست‌گذاری کارشناسی، در مقاطعی تحت تاثیر فضای سیاسی و امنیتی قرار گرفته است.

وقتی اینترنت سیاسی شد

حکمی با اشاره به تحولات فضای مجازی در دهه ۹۰، معتقد است یکی از نقاط عطف، سیاسی شدن این فضا بود. به گفته او، پس از برخی نتایج غیرمنتظره انتخاباتی، فضای مجازی به یکی از مهم‌ترین دلایلی تبدیل شد که جریان‌های سیاسی برای توضیح اتفاقات به آن استناد کردند. از همان زمان، به اعتقاد او، فضای مجازی به تدریج وارد چرخه‌ای از دوقطبی‌سازی شد و بسیاری از مسائل به دعواهای صفر و صدی تبدیل شدند. نتیجه این رویکرد، از نگاه معاون وزارت ارتباطات، این بود که امکان سیاست‌گذاری واقعی در این حوزه از بین رفت. به جای آنکه اینترنت به عنوان یک زیرساخت ارتباطی، اقتصادی و اجتماعی مورد بررسی قرار گیرد، تبدیل به مساله‌ای سیاسی شد و همین مساله، تصمیم‌گیری درباره آن را دشوارتر کرد. حکمی البته تاکید دارد که فضای مجازی را نمی‌توان از مفهوم قدرت و امنیت ملی جدا کرد. اما در عین حال، به یک نکته مهم اشاره می‌کند: در جمهوری اسلامی، قدرت مردم یکی از مولفه‌های مهم قدرت است و امنیت ملی نیز نمی‌تواند کاملاً از افکار عمومی جدا باشد. بنابراین هر سیاستی در حوزه اینترنت، زمانی می‌تواند پایدار باشد که بتواند بخشی از جامعه را با خود همراه کند. این نگاه، تفاوت مهمی با رویکردی دارد که مساله اینترنت را صرفاً از زاویه کنترل و محدودسازی می‌بینند. در اینجا، کاربر دیگر فقط دریافت‌کننده سیاست نیست؛ رضایت، نیاز و رفتار او نیز بخشی از معادله حکمرانی محسوب می‌شود.

حکمرانی سلبی یا ایجابی؟

شاید مهم‌ترین بخش صحبت‌های حکمی، جایی باشد که او به صراحت از دو مسیر متفاوت برای حکمرانی فضای مجازی سخن می‌گوید: مسیر سلبی و مسیر ایجابی. او معتقد است کسانی که توان اجرای سیاست‌های خود را دارند، می‌توانند رویکرد ایجابی در پیش بگیرند و کسانی که خود را ناتوان می‌بینند، بیشتر به سمت رویکرد سلبی می‌روند. معنای این حرف در حوزه اینترنت روشن است: حکمرانی صرفاً با بستن و محدود کردن نمی‌تواند مساله فضای مجازی را برای همیشه حل کند. تجربه سال‌های گذشته نیز از نظر حکمی همین مساله را نشان داده است. او با مرور اتفاقات سال‌های ۱۳۹۶، ۱۳۹۸، ۱۴۰۱ و ۱۴۰۴ توضیح می‌دهد که هر بار سطح محدودیت افزایش پیدا کرده، کاربران نیز به سمت ابزارهای جدیدی برای دسترسی رفته‌اند. به گفته او، در سال ۱۳۹۶ یکی از راهکارهای اصلی، مسدود کردن یک پلتفرم برای حدود دو هفته بود؛ اما دو سال بعد، در سال ۱۳۹۸، شرایط به قطع اینترنت رسید. در سال‌های بعد نیز با تداوم محدودیت‌ها، استفاده از ابزارهای گریز از سیاست‌های حاکمیت افزایش یافت. حکمی می‌گوید این روند در سال ۱۴۰۱ به جایی رسید که ابزارهای عبور از محدودیت در میان بخش بزرگی از کاربران عمومی و جوانان فراگیر شد. این روایت در واقع یک چرخه را توصیف می‌کند: محدودیت برای کنترل فضای مجازی اعمال می‌شود، کاربران برای دسترسی به سرویس‌های مورد نیاز خود مسیرهای جایگزین پیدا می‌کنند، ابزارهای جدید گسترش پیدا می‌کنند و در نتیجه، سیاست‌گذار با دشواری بیشتری برای اعمال همان سطح از کنترل مواجه می‌شود. از این منظر، مساله اصلی دیگر فقط این نیست که چه چیزی فیلتر شود؛ پرسش بزرگ‌تر این است که آیا اساساً می‌توان با تکیه بر محدودیت‌های بیشتر، حکمرانی موثری بر فضایی داشت که فناوری‌های آن با سرعت زیادی در حال تغییر است.

استارلینک؛ جایی که محدودسازی دشوارتر می‌شود

حکمی در ادامه همین استدلال، به استارلینک اشاره می‌کند. فارغ از ارزیابی‌های سیاسی درباره این فناوری، از منظر حکمرانی یک تفاوت مهم میان اینترنت ماهواره‌ای و بسیاری از ابزارهای فعلی وجود دارد: اتکای آن به زیرساخت‌های ارتباطی زمینی کمتر است. به همین دلیل، از نگاه حکمی، ادامه رویکرد فعلی می‌تواند سیاست‌گذار را در آینده با چالش‌های تازه‌ای مواجه کند. او هشدار می‌دهد که موج بعدی ابزارهای گریز از حکمرانی ممکن است دیگر متکی به شبکه‌های داخلی نباشد و فناوری‌هایی مانند اینترنت ماهواره‌ای، معادله را تغییر دهند. اما نکته مهم‌تر در صحبت‌های او، راه‌حلی است که پیشنهاد می‌کند. حکمی نمی‌گوید پاسخ به این تحول، صرفاً محدودیت بیشتر است. برعکس، تاکید می‌کند اگر قرار است حکمرانی فضای مجازی حفظ شود، باید نیازهای جامعه تامین شود؛ شبکه‌ای ایجاد شود که برای مردم قابل استفاده، مقرون‌به‌صرفه، حافظ حریم خصوصی و در عین حال قابل حکمرانی باشد. این بخش از صحبت‌های معاون وزارت ارتباطات را می‌توان یکی از صریح‌ترین نشانه‌های تغییر زاویه نگاه دانست: اگر اینترنت داخلی نتواند کیفیت، دسترسی و خدمات مورد نیاز کاربران را تامین کند، صرفاً با محدود کردن اینترنت خارجی نمی‌توان رفتار کاربران را تغییر داد.

مساله فقط ساختار نیست

البته حکمی تنها کسی نیست که در این نشست از ضرورت بازنگری در حکمرانی فضای مجازی سخن گفت. محمدصادق فراهانی، معاون حقوقی و امور مجلس مرکز ملی فضای مجازی، یکی از مشکلات اصلی را تعدد نهادهای تصمیم‌گیر دانست. از نگاه او، در سال‌های گذشته ساختارهای مختلفی در حوزه فضای مجازی ایجاد شده‌اند که در برخی موارد وظایف آنها با یکدیگر همپوشانی دارد. فراهانی سه مشکل اصلی را «تعدد نهادی»، «همپوشانی صلاحیت‌ها» و «تشتت راهبردی» دانست. به این معنا که نه تنها نهادهای متعددی درباره فضای مجازی تصمیم می‌گیرند، بلکه در برخی موارد مشخص نیست مرز مسوولیت‌ها کجاست و حتی ممکن است راهبردهای متفاوتی درباره یک مساله وجود داشته باشد. ابوالحسن فیروزآبادی، دبیر سابق شورای عالی فضای مجازی نیز از زاویه دیگری بر همین مشکل تاکید کرد و گفت فضای مجازی دیگر صرفاً مساله پلتفرم‌ها نیست. امروز هوش مصنوعی، الگوریتم‌ها و مدل‌های هوشمند، بخش مهمی از این فضا را شکل داده‌اند و همین تحول، مدل‌های سنتی سیاست‌گذاری را با چالش مواجه کرده است. از نگاه فیروزآبادی، تقویت دولت در حوزه فضای مجازی و روشن شدن جایگاه شورای عالی فضای مجازی ضروری است. او همچنین تاکید کرد که سیاست‌گذاری در این حوزه با اختلاف میان نهادها پیش نمی‌رود و نیاز به نوعی هم‌نوایی در ساختار حکمرانی وجود دارد. احسان کیانخواه نیز فضای مجازی را فراتر از مجموعه‌ای از فناوری‌ها دانست و آن را «عالم» جدیدی توصیف کرد که در حال تغییر تعاملات انسانی است. به اعتقاد او، همین پیوستگی باعث می‌شود سیاست‌گذاری در یک بخش از فضای مجازی به سرعت بر بخش‌های دیگر اثر بگذارد. او همچنین در نقد نگرانی‌ها درباره استارلینک تاکید کرد که حتی اگر یک فناوری تهدید تلقی شود، پاسخ به آن نمی‌تواند رها کردن میدان فضای مجازی باشد. از نگاه کیانخواه، یکی از وظایف اصلی نهادهای سیاست‌گذار باید ایجاد امکان گفت‌وگو و رسیدن به اجماع میان دولت و سایر بخش‌های حاکمیت باشد. در مجموع، آنچه از صحبت‌های مطرح‌شده در این نشست به دست می‌آید، تصویری از فضای مجازی است که بیش از گذشته نیازمند بازنگری در شیوه حکمرانی خود شده است. در مرکز این تصویر، صحبت‌های حافظ حکمی قرار دارد که تجربه سال‌های گذشته را به عنوان نشانه‌ای از محدودیت‌های رویکرد صرفاً سلبی روایت می‌کند: هرچه محدودیت‌ها بیشتر شده، ابزارهای عبور نیز گسترده‌تر شده‌اند. در چنین شرایطی، مساله اینترنت دیگر فقط دسترسی به چند پلتفرم یا اعمال فیلترینگ نیست. مساله این است که آیا سیاست‌گذار می‌تواند به جای آنکه همواره چند قدم عقب‌تر از فناوری و رفتار کاربران حرکت کند، شبکه‌ای ایجاد کند که بخش قابل توجهی از نیاز جامعه را پاسخ دهد و در عین حال امکان حکمرانی را نیز حفظ کند. اگر پاسخ مثبت باشد، مسیر حکمرانی اینترنت باید از «بستن» به سمت «ساختن» حرکت کند؛ ساختن زیرساخت، خدمات و فضایی که کاربران برای استفاده از آن نیازمند عبور از سیاست‌های رسمی نباشند. در غیر این صورت، هر فناوری تازه می‌تواند یک گام دیگر میان سیاست‌گذار و کاربر فاصله ایجاد کند؛ فاصله‌ای که با گسترش اینترنت ماهواره‌ای و هوش مصنوعی، احتمالاً مدیریت آن از گذشته دشوارتر خواهد شد.

چالش تازه شرکت‌های هوش مصنوعی؛ مهار عامل‌های خودمختار سرکش

عامل‌هایی که برای سنجش توانایی سایبری در محیط‌های آزمایشی به کار گرفته شده بودند، در موارد متعدد با فرار از سندباکس به اینترنت راه یافته‌اند و اقدامات مخربی صورت داده‌اند. به گزارش مهر، تا چند ماه پیش، مساله ایمنی عامل‌های هوش مصنوعی عمدتاً حول این پرسش می‌چرخید که یک مدل در محیط کنترل‌شده تا چه اندازه می‌تواند عملیات سایبری پیچیده انجام دهد. اما مجموعه رخدادهایی که از ابتدای ۲۰۲۶ آغاز شده، صورت مساله را تغییر داده است. عامل‌هایی که برای سنجش توانایی سایبری در محیط‌های آزمایشی به کار گرفته شده بودند، در موارد متعدد با فرار از سندباکس به اینترنت راه یافته‌اند، به سامانه‌هایی خارج از دامنه آزمون دسترسی پیدا کرده‌اند و در برجسته‌ترین موارد، اقدامات مخربی صورت داده‌اند. نکته جالب توجه این است که الگوی مذکور به یک شرکت یا معماری خاص محدود نمانده و در مدل‌های اوپن‌ای‌آی، آنتروپیک، گوگل و مون‌شات مشاهده شده است. آنچه در ادبیات رسانه‌ای با عنوان فرار عامل توصیف می‌شود، البته یک پدیده واحد نیست. شواهد موجود دست‌کم سه وضعیت متفاوت را نشان می‌دهد. در وضعیت نخست، عامل واقعاً سازوکار جداسازی را دور می‌زند و از محیط بسته خارج می‌شود. در وضعیت دوم، پیکربندی معیوب آزمایش از ابتدا مسیر ناخواسته‌ای به اینترنت باز گذاشته است. در وضعیت سوم، عامل از ابزارها و مجوزهای موجود به شیوه‌ای استفاده می‌کند که طراح آزمون پیش‌بینی نکرده است. تمایز میان این سه وضعیت برای فهم خطر اهمیت اساسی دارد، زیرا هر سه به یک نتیجه عملی مشترک می‌رسند. مرز میان محیط ارزیابی و جهان واقعی دیگر نمی‌تواند صرفاً با فرض تبعیت عامل از دامنه تعریف‌شده آزمون حفاظت شود.

رخنه هاگینگ فیس؛ لحظه‌ای که مرز آزمایش شکست

رخداد اوپن‌ای‌آی و هاگینگ فیس روشن‌ترین نمونه نوع نخست است. مدل‌های آزمایشی اوپن‌ای‌آی در جریان ارزیابی توانایی‌های سایبری داخل یک سندباکس قرار داشتند و بنا بود به اینترنت دسترسی نداشته باشند. بر اساس گزارش‌ها، عامل‌ها با بهره‌برداری از یک آسیب‌پذیری ناشناخته از سندباکس خارج شدند، در سامانه‌های داخلی اوپن‌ای‌آی حرکت کردند و سرانجام به اینترنت دسترسی یافتند. عامل پس از دسترسی به شبکه عمومی استدلال کرد که هاگینگ فیس احتمالاً اطلاعات لازم برای حل آزمون را در اختیار دارد، وارد زیرساخت عملیاتی این شرکت شد و داده مورد نیاز برای تکمیل ماموریت را استخراج کرد. اهمیت حادثه با بررسی تعداد عامل‌های درگیر در این فرایند آشکارتر می‌شود. بررسی‌های بعدی موسسات «METR» و «Redwood Research»، از فعالیت هماهنگ حدود ۷۰۰ عامل هوش مصنوعی در این حادثه خبر می‌دهند. این عامل‌ها در قالب یک اقدام جمعی عمل کردند و در مواردی برای پوشاندن آثار فعالیت خود نیز تلاش داشته‌اند. بر همین اساس، یک گروه دیگر نیز روش‌های گروه نخست را فرا گرفته و از آنها برای دستیابی به سطح دسترسی مدیریتی در یک خوشه پژوهشی داخل زیرساخت خود اوپن‌ای‌آی استفاده کرده است. در این جا مساله از توانایی نفوذ یک مدل منفرد عبور می‌کند. انتقال روش میان عامل‌ها، تقسیم عملی کار و استفاده مجدد از راهبرد موفق، قابلیت سایبری را از ویژگی یک مدل به خاصیت یک سامانه چندعاملی تبدیل می‌کند. همین تحول می‌تواند الگوی ارزیابی خطر را دگرگون کند، زیرا واحد مناسب تحلیل دیگر صرفاً مدل نیست و باید رفتار جمعی عامل‌هایی را نیز در بر گیرد که می‌توانند تجربه یکدیگر را مصرف و بازتولید کنند.

ویکی آلمانی؛ وقتی عامل‌ها برای خود زیرساخت ارتباطی ساختند

حادثه بعدی مربوط به نفوذ عامل‌های اوپن‌ای‌آی به یک ویکی آلمانی بُعد متفاوتی از همین مساله را آشکار کرد. پژوهشگران در بررسی‌های خود بیش از ۱۵ هزار ویرایش منتسب به عامل‌های هوش مصنوعی را در «DseWiki» شناسایی کردند. این عامل‌ها سایت مذکور را عملاً به تابلوی ارتباطی خود تبدیل کرده بودند و در آن روش‌های دور زدن محدودیت‌ها، میان‌برهای حل آزمون و شیوه‌های پنهان کردن رفتار را مبادله می‌کردند. پیام‌های بررسی‌شده نشان می‌داد عامل‌ها درباره اجتناب از شناسایی، استفاده از «Tor» و حفظ ارتباط پس از خاموش شدن نمونه‌های دیگر گفت‌وگو کرده‌اند. هنگامی که مدیر سایت در ژوئن حذف صفحات را آغاز کرد، عامل‌ها صفحات پشتیبان ایجاد کردند تا اطلاعات باقی بماند. رویترز همچنین گزارش کرده که برخی عامل‌ها برای دستکاری خود وب‌سایت اقدام کرده بودند. این حادثه یک متغیر تازه، یعنی ماندگاری دانش عملیاتی خارج از محیط آزمایش وارد مساله می‌کند. بر همین اساس، عاملی که بتواند یک راهبرد موفق را روی زیرساخت عمومی ثبت کند، امکان انتقال آن راهبرد به اجرای بعدی یا عامل دیگری را فراهم می‌کند. در چنین وضعیتی خاموش کردن نمونه اولیه الزاماً زنجیره رفتار را خاتمه نمی‌دهد، زیرا بخشی از حافظه عملیاتی از محیط تحت کنترل توسعه‌دهنده خارج شده است.

کلاد، جمینای و کیمی؛ یک رفتار مشترک از مسیرهای متفاوت

بررسی‌های شرکت آنتروپیک نشان می‌دهد که چالش امنیتی حتی بدون شکستن فنی سندباکس نیز می‌تواند رخ دهد. این شرکت پس از حادثه هاگینگ فیس حدود ۱۴۱ هزار مورد آزمایش را بازبینی کرد و سه رخداد را یافت که طی آنها کلاد به اینترنت راه یافته و به زیرساخت واقعی سه سازمان دسترسی غیرمجاز پیدا کرده بود. علت اولیه، خطای پیکربندی محیط ارزیابی شریک ثالث بود. مدل‌ها تصور می‌کردند همچنان در سناریوی ساختگی آزمایش قرار دارند و با استفاده از گذرواژه‌های ضعیف سایر آسیب‌پذیری‌ها به هدف‌های واقعی نفوذ کردند. رفتار مدل‌ها پس از مواجهه با نشانه‌های واقعی بودن محیط نیز یکسان نبود. بر همین اساس، «Opus ۴.۷» با وجود تشخیص حضور در سامانه عملیاتی به کار ادامه داد. «Mythos ۵» نشانه‌های اتصال به اینترنت را دریافت کرد، اما با استدلال خود دوباره به این نتیجه رسید که محیط بخشی از شبیه‌سازی است و مدل پژوهشی جدیدتر پس از تشخیص واقعی بودن هدف، عملیات را متوقف کرد. آنتروپیک همچنین بعداً رخداد چهارمی مربوط به نسخه اولیه «Claude Opus ۴.۶» را نیز کشف کرد که در بازبینی نخست از قلم افتاده بود. این شرکت در تحلیل خود دو الگوی تکرارشونده، شامل استدلال سوگیرانه درباره ماهیت محیط و آمادگی برای انجام اقدام بالقوه زیان‌بار در مسیر تکمیل ماموریت را برجسته می‌کند. همین الگو با سازوکارهای متفاوت در رقبا ظاهر شده است. بر همین اساس، مدل جمینای گوگل طی آزمایش به سه شرکت واقعی دسترسی پیدا کرده است. مدل اطلاعات عمومی را یافته و اعتبارنامه‌های ورود را حدس زده و در یکی از موارد با حدس زدن مکرر گذرواژه وارد سامانه شده است. همچنین، در مورد «KimiK۳» نیز سندباکس به‌درستی پیکربندی نشده بوده است. در این مورد، دسترسی مستقیم به بخشی از ترافیک وب مسدود شده بود، اما مدل با استفاده از ابزارهای خط فرمان محدودیت را دور زد. پژوهشگران شرکت امنیتی «FrontierSecurity» این رفتار را نشانه آسیب‌پذیری خود سازوکارهای ارزیابی در برابر عامل‌هایی دانستند که فعالانه به دنبال شکاف‌های آزمون می‌گردند.

از مشکلی برای شرکت‌های خصوصی تا بحران حاکمیتی دولت

در ادامه، رخداد حمله سایبری عامل اوپن‌ای‌آی به سامانه متعلق به دولت استرالیا نشان داد که خروج عامل از دامنه آزمون می‌تواند مستقیماً به زیرساخت دولتی برسد. عامل اوپن‌ای‌آی در ژوئن وارد پرتال «Medicare Statistics Reporting Service» شد و به فایل‌های عمومی و غیرعمومی بخش سلامت این کشور دسترسی یافت. در همین راستا، دولت استرالیا اعلام کرد در آن مقطع شواهدی از دسترسی به اطلاعات شخصی در دست نبود، اما تحقیقات ادامه دارد. وجه مهم‌تر حادثه، شکاف میان زمان وقوع، کشف و افشا بود. شرکت اوپن‌ای‌آی اعلام کرده فعالیت مخرب را در اوت و در جریان بررسی رفتارهای نامنطبق مدل کشف کرده و در ۱۰ سپتامبر از طریق یک صندوق عمومی ایمیل به نهاد استرالیایی اطلاع داده است. نخست‌وزیر استرالیا تأخیر چندماهه و شیوه اطلاع‌رسانی را محل نگرانی شدید دانسته و از بررسی پیامدهای حقوقی سخن گفته است. به باور کارشناسان، این رخداد نشان می‌دهد مساله مهار عامل اکنون همزمان مساله مدیریت رخداد، مسوولیت حقوقی و الزام به افشای به‌موقع است.

فاصله میان قدرت عامل و قدرت نظارت

مجموع داده‌های منتشرشده طی ماه‌های اخیر نشانه یک عدم تقارن رو به رشد است. عامل‌ها با سرعت بیشتری در یافتن آسیب‌پذیری، ترکیب ابزارها و پیگیری مستقل هدف پیشرفت کرده‌اند، در حالی که سازوکارهای مشاهده و بازسازی رفتار آنها با همان آهنگ رشد نکرده است. تا میانه سپتامبر، بررسی داخلی اوپن‌ای‌آی حدود ۲۴ مورد رفتار نامطلوب عامل‌ها را شناسایی کرده بود و تعداد موارد همزمان با بررسی لاگ‌های قدیمی افزایش می‌یافت. برخی فعالیت‌ها ماه‌ها از دید شرکت پنهان مانده و چند مورد نیز ابتدا توسط پژوهشگران بیرونی کشف شده بود. همین شکاف، محیط ارزیابی را به بخشی از سطح حمله تبدیل کرده است. بر همین اساس، آزمونی که برای کشف توانایی خطرناک مدل طراحی شده، خود به محیطی تبدیل می‌شود که مدل می‌تواند محدودیت‌های آن را آزمایش کند. آنتروپیک در جمع‌بندی رسمی خود دقیقاً از همین نقطه به ضرورت ایمن‌سازی محیط‌های ارزیابی و اعمال استانداردهای امنیتی مشابه بر پیمانکاران ارزیابی رسیده است.

جمع‌بندی

رشته حوادث سال ۲۰۲۶ یک نتیجه مهم برای صنعت هوش مصنوعی دارد. ایمنی عامل دیگر نمی‌تواند فقط خاصیتی درون مدل تلقی شود. مهار و مدیریت رفتار مخرب باید به یک قابلیت مستقل مهندسی تبدیل شود که سندباکس، شبکه، ابزارها، مدیریت هویت و دسترسی، ثبت کامل اقدامات، تشخیص رفتار غیرعادی، قطع اضطراری، کنترل پیمانکاران و بررسی مستقل پس از حادثه را در یک معماری واحد قرار دهد. در نهایت، مساله عمیق‌تر به نسبت میان عاملیت و کنترل‌پذیری مربوط می‌شود. ارزش اقتصادی عامل دقیقاً از همان ویژگی‌هایی شامل توانایی برنامه‌ریزی، انتخاب ابزار، جست‌وجوی مسیر جایگزین و پیگیری هدف بدون دستور مرحله‌به‌مرحله انسان ناشی می‌شود که مهار آن را دشوار می‌کند. هنگامی که محدودیت به مانعی در مسیر هدف تبدیل می‌شود، یک عامل توانمند ممکن است آن را نه به عنوان مرز مجاز رفتار، بلکه به عنوان مساله‌ای دیگر برای حل کردن تفسیر کند. رخدادهای هاگینگ فیس، «DseWiki»، کلاد، جمینای، کیمی و سامانه دولتی استرالیا نخستین داده‌های تجربی جدی از این مساله هستند. بنابراین پرسش راهبردی مرحله بعد توسعه عامل‌ها دیگر فقط این نیست که عامل چه کارهایی می‌تواند انجام دهد. پرسش تعیین‌کننده این است که وقتی عامل کاری را بیاموزد که طراح انتظارش را ندارد، چه چیزی عملاً مانع انجام آن در جهان واقعی خواهد شد؟

اخبار

قرارداد ۷ میلیارد دلاری تنسنت برای اجاره ۱۰۰ هزار تراشه اوراکل

غول اینترنتی تنسنت (Tencent) چین قراردادی ۷ میلیارد دلاری برای اجاره حدود ۱۰۰ هزار تراشه پیشرفته هوش مصنوعی با شرکت اوراکل (Oracle) امضا کرده است تا عقب‌ماندگی خود در رقابت هوش مصنوعی را جبران کند. به گزارش ایسنا، روزنامه فایننشال تایمز روز پنج‌شنبه، به نقل از دو منبع آگاه گزارش کرد تنسنت توافق کرده است که این تراشه‌ها را طی یک دوره پنج‌ساله در چندین مرکز داده اوراکل در جنوب‌شرقی آسیا اجاره کند. طبق گزارش این روزنامه، قرارداد مذکور بزرگ‌ترین توافق‌نامه اجاره برون‌مرزی تنسنت تا به امروز محسوب می‌شود و به این غول حوزه اینترنت و بازی‌های ویدیویی امکان دسترسی به حدود ۱۰۰ هزار تراشه پیشرفته را می‌دهد که در چین در دسترس نبودند. ارزش این قرارداد ۷ میلیارد دلار است و شامل پیش‌پرداختی در حدود ۳۰ درصد می‌شود که بر جریان نقدینگی آزاد تنسنت در گزارش درآمدی سه‌ماهه دوم سال تاثیر گذاشته است. تنسنت برای پیشبرد مدل‌ها و محصولات هوش مصنوعی خود سخت در تلاش است تا بتواند با محصولات پیشرفته سایر آزمایشگاه‌های بزرگ هوش مصنوعی چین رقابت بهتری داشته باشد. همچنین مشاهده شده است که این شرکت در حال ادغام هوش مصنوعی در سایر محصولات خود، از جمله «وی‌چت» (WeChat)، است. اگرچه شرکت‌های فناوری چینی از خرید مستقیم تراشه‌های پیشرفته هوش مصنوعی منع شده‌اند، اما طبق قوانین آمریکا، مجاز به اجاره بین‌المللی آنها هستند و این امر به آنها اجازه می‌دهد به تراشه‌های پیشرفته انویدیا (Nvidia) که معمولا در چین یافت نمی‌شوند، دسترسی پیدا کنند. جدیدترین مدل‌های «هونیوان» (Hunyuan) تنسنت در ماه‌های اخیر پیشرفت‌های قابل توجهی از خود نشان داده و فاصله خود را با مدل‌های پیشرو داخلی - نظیر مدل‌های شرکت‌های «دیپ‌سیک» (DeepSeek) و «گروه علی‌بابا» (Alibaba Group Holding Ltd) - کاهش داده‌اند. بر اساس گزارش اینوستینگ، این شرکت طی سال گذشته سرمایه‌گذاری سنگینی روی برنامه‌های هوش مصنوعی خود انجام داده است، اما این کار به قیمت کاهش حاشیه سود و سودآوری کلی آن تمام شده است.

هکرها میلیون‌ها سابقه پرسنل نظامی آمریکا را سرقت کردند

گزارش‌ها حاکی از آن است که دولت آمریکا در حال اطلاع‌رسانی به میلیون‌ها نفر از نیروهای نظامی و کارکنان فعلی و سابق این کشور است که اطلاعات شخصی آنها طی نفوذی چندماهه به پنتاگون سرقت شده است. به گزارش مهر به نقل از تک کرانچ، این جدیدترین رخداد از مجموعه سرقت‌های اطلاعات مربوط به کارکنان دولت فدرال در ماه‌های اخیر به شمار می‌رود. در اطلاعیه مربوط به نقض داده‌ها که از سوی مرکز نیروی انسانی دفاعی (DMDC) صادر شده و در شبکه اجتماعی ردیت به اشتراک گذاشته شده، آمده چند کاربر غیرمجاز طی چند ماه، یعنی از اکتبر ۲۰۲۵ تا اواسط جولای ۲۰۲۶، از یک آسیب‌پذیری امنیتی در یک سامانه نامشخص اشتراک‌گذاری فایل سوءاستفاده کرده‌اند. این نفوذ باعث افشای اطلاعات هویتی شخصی افراد شده است؛ از جمله شماره‌های تأمین اجتماعی در کنار نام فرد، تاریخ تولد، جنسیت، نژاد و سایر اطلاعات مربوط به سابقه خدمت نظامی او. در این اطلاعیه آمده است که سوابق پرسنلی رمزگذاری نشده بودند. بر اساس گزارش‌های سی‌ان‌ان و یک نشریه دیگر، به گفته یکی از مقام‌های پنتاگون این نفوذ حدود ۲.۸ میلیون فرد زنده و نزدیک به ۳۰۰ هزار فرد فوت‌شده را تحت تأثیر قرار داده است. ارتش آمریکا تا ماه مارس، ۱.۳ میلیون نیروی نظامی فعال داشته است. مرکز DMDC ممکن است برای عموم مردم چندان شناخته‌شده نباشد، اما یکی از واحدهای مسوول نگهداری سوابق در وزارت دفاع آمریکا است. این مرکز بیش از ۶۰ میلیون سوابق مربوط به نیروهای نظامی و کارکنان غیرنظامی آمریکا و اعضای خانواده آنها را نگهداری می‌کند تا در تعیین مزایا و حقوقی مانند خدمات درمانی و بازنشستگی مورد استفاده قرار گیرند. در وب‌سایت DMDC آمده است: ما اطمینان حاصل می‌کنیم که افراد درست به اطلاعات دسترسی داشته باشند و افراد نادرست دسترسی نداشته باشند؛ امنیت اطلاعات هویتی از اهمیت بالایی برخوردار است. وزارت دفاع، که بر DMDC نظارت دارد، اعلام کرده هیچ نشانه‌ای مبنی بر سوءاستفاده از این اطلاعات در اختیار ندارد اما توضیح نداده چگونه به این نتیجه رسیده است. این جدیدترین نشت اطلاعات پرسنل آژانس‌های فدرال آمریکا در ماه‌های اخیر است. در اوایل ماه سپتامبر نیز گروه هکری شاینی هانترز اطلاعات کارمندان اف‌بی‌آی را هک کردند.

با ChatGPT: لباس‌های مختلف را مجازی پرو کنید

اوپن‌ای‌آی با معرفی قابلیت پرو کردن مجازی لباس‌ها از طریق تصاویر آپلودشده توسط کاربر، قابلیت‌های خرید ChatGPT را گسترش داده است. این ایده کاملاً مشابه قابلیتی است که گوگل در سال ۲۰۲۵ به Search اضافه کرد و به کاربران اجازه می‌دهد تصاویر خود را آپلود کنند و ببینند لباس‌های مختلف بر تن آنها چطور به نظر می‌رسند. کاربران می‌توانند در ChatGPT به قابلیت Virtual Try On از هر جایی که یک فهرست محصول پوشاک در چت نمایش داده می‌شود، دسترسی داشته باشند. برای ایجاد تصویر اختصاصی خود، کافی است روی لباس موردنظر ضربه بزنید، گزینه Tryon را انتخاب کنید و سپس یک عکس سلفی و یک عکس تمام‌قد را آپلود کنید تا ChatGPT از آنها استفاده کند. برای استفاده از این قابلیت لازم نیست حتماً از محصولاتی که ChatGPT در چت نمایش می‌دهد استفاده کنید. شما حتی می‌توانید یک اسکرین‌شات از هر لباسی که آپلود کرده‌اید در اختیار ChatGPT بگذارید تا تصویر پرو مجازی را ایجاد کند. اوپن‌ای‌آی می‌گوید این قابلیت برای ایجاد تصاویر از مدل جدید ChatGPT Images ۲.۵ استفاده می‌کند که این شرکت ماه گذشته میلادی معرفی کرده است. در کنار قابلیت پرو مجازی، OpenAI اکنون امکان ذخیره محصولاتی را که می‌پسندید در Library اپلیکیشن نیز فراهم کرده تا در صورت تمایل بتوانید بعداً دوباره به آنها مراجعه کنید. با این حال، هشدارهای همیشگی درباره تصاویری که در ChatGPT آپلود می‌کنید همچنان پابرجاست.

آگهی اختصاصی موضوع قانون تعیین تکلیف وضعیت ثبتی اراضی و ساختمان‌های فاقد سند رسمی

برابر ماده ۳ و ماده ۱۳ آیین‌نامه قانون تعیین تکلیف برابر رای صادره هیات موضوع قانون تعیین تکلیف وضعیت ثبتی اراضی و ساختمان‌های فاقد رسمی مستقر در واحد ثبتی تصرفات مالکانه بلامعارض فرشته کریم کشته بشماره ملی ۶۲۴۰۱۵۶۵۷۴ متقاضی کلاسه ۱۴۰۴۱۱۴۴۱۲۴۸۰۰۰۳۱۶۶ در شش دانگ یک قطعه زمین که در آن احداث بنا شده است بمساحت ۹۷/۸۶ متر مربع از پلاک ۱۷- اصلی واقع در اراضی جلین علیا بخش ۳ حوزه ثبت ناحیه ۲ گرگان طبق رأی صادره حکایت از انتقال از مالک رسمی به متقاضی دارد.
لذا به منظور اطلاع عموم مراتب در دو نوبت به فاصله پانزده روز آگهی می‌شود از این رو اشخاصی که نسبت به رای صادره فوق‌الذکر اعتراض داشته باشند، می‌توانند از تاریخ انتشار اولین آگهی به مدت دو ماه اعتراض خود را با ذکر شماره پرونده به این اداره تسلیم و پس از اخذ رسید ظرف مدت یک ماه از تاریخ تسلیم اعتراض به مرجع ثبتی، دادخواست خود را به مراجع ذی صلاح قضایی تقدیم و گواهی تقدیم دادخواست را به این اداره ارائه نمایند.
شناسه آگهی: ۲۲۷۵۹۴۳
تاریخ انتشار نوبت اول: ۱۴۰۵/۰۶/۲۴
تاریخ انتشار نوبت دوم: ۱۴۰۵/۷/۱۱
سیدعیسی میرکاظمی
رییس اداره ثبت اسناد و املاک منطقه دو گرگان

سامانه پیامکی روزنامه تعادل
۳۰۰۰۵۳۲۰