هکرهای بایننس بامصاحبه‌شغلی ساختگی به این صرافی نفوذ کردند

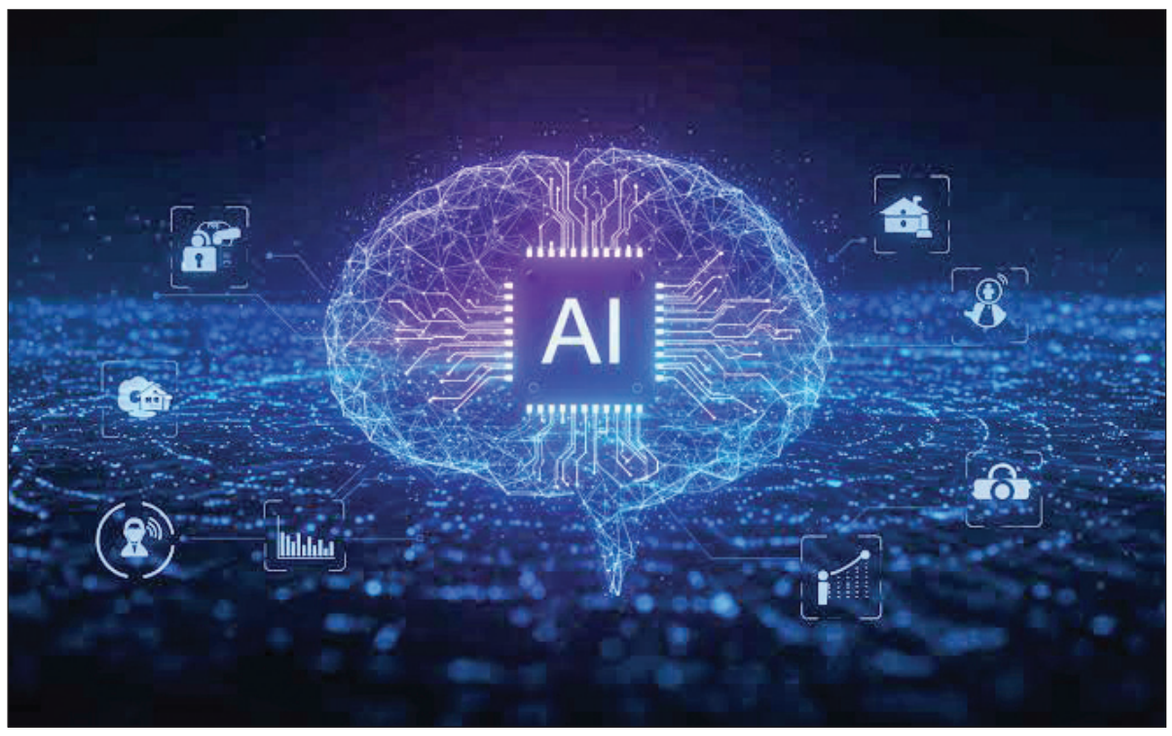
بایننس اعلام کـرد که هکرها با ترتیـب دادن یک مصاحبه‌شغلی جعلی، به یکی از رایانه‌های این صرافی و یک ابزار داخلی مبتنی بر هوش مصنوعی نفوذ کردند و از ایـن طریق، کنترل کیف پول‌های شـرکت را به دست گرفتند و ۶.۳ میلیارد دلار رمزارز را به سرقت بردند. به گزارش ایسـنا، بزرگ‌ترین صرافی رمزارز جهان در گزارش اولیه خود درباره جزییات این حادثه، به یک عملیات هکری پیچیده اشاره کرد. این ماجرا در ماه ژوئن، با انتشار تبلیغی برای یک نسخه دستکاری شده از یک ابزار برنامه‌نویسی آغاز شد و زنجیره‌ای از نقض‌های امنیتی را بـه راه انداخت که در نهایت در روز پنج‌شنبه ۲۹ اکتبر، به سرقت رمزارزها از باینـنس منجر شد. اف‌بی‌آی یک گروه هکری اهل کره شمالی را مسوول این حمله دانسته، اما کره شمالی این ادعا را رد کرده است. باینـنس اعلام کرده که تمام وجوه از دست‌رفته کاربران در این حمله را به آنها بازمی‌گرداند. طبق اعـلام باینـنس، این حمله زمانی آغاز شـد که یکی از کارکنان تیم توسـعه کیف پول، در ماه ژوئن یـک ابزار هوش مصنوعی را دانلـود کرد که پیش‌تر دستکاری شده بود. اگرچه صرافی متوجه این موضوع شـد، دسـتگاه را تعویض کرد و اطلاعات دسترسی (اعتبارنامه‌هـا) را تغییر داد، امـا نقش این کارمند و سایر اعضای تیم توسعه کیف پول برای هکرها فاش شده بود. سپس در ماه سپتامبر، یک مهندس نرم‌افزار دیگر که به دنبال شـغل جدیدی بـود، پس از انجام مصاحبه‌ای بـرای موقعیتی که تصور می‌کرد واقعی است (شامل یک جلسـه مجازی با مدیرعامل یک شرکت ساختگی)، یک «مخزن کد مخرب» را روی رایانه خود دانلود کرد. در ۲۰ اکتبر، مهاجم با استفاده از رایانه آلوده و یک ابزار داخلی هوش مصنوعی، کنترل سیسـتم توسـعه‌دهنده اول کیف پول و همچنین سیسـتم یکی دیگر از توسـعه‌دهندگان همان تیم را به دسـت گرفت. در نهایـت در ۲۹ اکتبر، مهاجم با اسـتفاده از رایانه توسعه‌دهنده دوم و بهره‌گیری از اطلاعات دسترسی سرقت‌شده از توسعه‌دهنده اول، یک اسـکریپت مخرب را اجرا کرد تا حمله اصلی را کلید بزند. باینـنس در این گزارش نوشت: «این اتفاق نباید رخ می‌داد. ما بابت نگرانی‌ها، اختلالات و عدم اطمینانی که برای کاربران، شرکا و کل صنعت ایجاد شد، عذرخواهی می‌کنیم.» بر اساس گزارش رویترز، باینـنس همچنین اعـلام کرد که در پی این حمله، سـرمایه‌گذاری خود را در سیستم‌های تشخیص تهدید مبتنی بر هوش مصنوعی افزایش داده و در حال برنامه‌ریزی برای ایجاد یک صندوق تحقیقات امنیتی و اجرای طرح‌های مشترک با شرکت‌های پیشرو در حوزه هوش مصنوعی است.

امنیت زیرساخت‌های سایبری در خط مقدم دفاع سایبری کشور

رییس مرکز فرماندهی عملیات امنیت سـایبری مرکـز ملی فضـای مجازی گفـت: تامین امنیت زیرسـاخت‌های حیاتـی از موضوعـات مهـم، راهبـردی و اولویت‌هـا در حوزه دفاع سـایبری است و زیرسـاخت‌هایی همچون انرژی، صنعت، آب و حمل‌ونقل از جمله حوزه‌هایی هسـتند که امنیت آنها اهمیت ویژه‌ای دارد. به گزارش ایسـنا از مرکز ملی فضای مجـازی، حجت، رییس مرکز فرماندهی عملیـات امنیت سـایبری مرکز ملی فضای مجـازی صبح چهارشـنبه ۱۳ آبان ماه در در مراسم بزرگداشت هفته پدافند گفت: المپیک فنـاوری را نباید صرفـاً یک رقابـت تخصصی یا رویدادی مقطعی دانست، بلکه این رویداد فرصتی برای نمایش ظرفیت‌های علمی و فناورانه کشور، شناسایی اسـتعدادهای برتر و تقویت زیست‌بوم فناوری و امنیت سـایبری اسـت. وی با اشـاره به اهمیت اسـتمرار برگزاری رویدادهای تخصصی در حوزه فناوری افزود: ایجاد نشاط علمی و فراهم کردن بستر رقابت سالم میان متخصصان و فعالان فناوری از ضرورت‌های امروز کشور است و چنین رویدادهایی می‌توانند زمینه شناسـایی و پرورش استعدادهای جوان، نمایش توانمندی شرکت‌های دانش‌بنیان و فعالان بخش خصوصی و ایجاد ارتباط موثر میان دانشگاه‌ها، مراکز علمی و دستگاه‌های اجرایی را فراهم کنند. حجت همچنین شناسایی پیش‌دستانه آسیب‌پذیری‌ها و نقاط ضعف سامانه‌ها و زیرساخت‌های کشور را از دیگر دستاوردهای مهم این رقابت‌ها دانسـت و تصریح کرد: خروجی این رویدادها نباید صرفاً به معرفی برگزیدگان محدود شـود، بلکه باید از نتایج و ظرفیت‌های ایجادشده برای ارتقای امنیت واقعی سامانه‌ها و زیرساخت‌های کشور استفاده کرد. وی با اشاره به برگزاری رقابت CTF OT بـه همت سـازمان پدافنـد غیرعامل کشـور، تاکید کرد: تامین امنیت زیرساخت‌های حیاتـی از موضوعات مهم، راهبـردی و اولویت‌ها در حوزه دفاع سـایبری اسـت و زیرسـاخت‌هایی همچون انرژی، صنعت، آب و حمل‌ونقل از جمله حوزه‌هایی هسـتند که امنیت آنها اهمیت ویژه‌ای دارد و در حوزه فناوری عملیـات (OT)، موضوع صرفـاً حفاظت از اطلاعات نیسـت، بلکـه تداوم عملکرد سامانه‌ها، حفظ ایمنی فرآیندهای صنعتی و جلوگیـری از اختلال در ارایـه خدمات حیاتی نیز اهمیت اساسـی دارد. رییس مرکز فرماندهی عملیات امنیت سایبری مرکز ملی فضای مجازی با تأکید بر ضرورت ارزیابی امنیتی پیش‌دسـتانه سـامانه‌های کنترل صنعتـی در برنامه‌های دفاع سایبری کشور، خاطرنشان کرد: رقابت‌های OT CTF فرصت ارزشمندی برای متخصصان فراهم می‌کند تا در محیط‌های کنترل‌شـده، توانمندی خود را در شناسـایی ضعف‌های امنیتی، تحلیل تهدیدات و ارایـه راهکارهای دفاعی محک بزنند. همچنین یکی دیگر از اولویت‌هـای برنامه‌ریزی در حوزه امنیت سـایبری کشور توسـعه و ایجاد سایبررنج‌های تخصصی در حوزه فناوری عملیاتی است که براساس آن سایبررنج‌ها می‌توانند محیطی امن و کنترل‌شده برای شبیه‌سازی زیرساخت‌های صنعتی، تمرین سناریوهای حمله و دفاع، ارزیابی توانمندی متخصصان و انجام پژوهش‌های کاربردی فراهم کنند. حجت گفت: این ظرفیت‌ها نباید صرفاً به برگزاری مسابقات محدود شـوند، بلکه باید به عنوان زیرسـاختی دایمی برای آموزش، پژوهش، ارزیابی امنیتی و ارتقای آمادگی سـایبری کشور توسعه یابند. کشور به محیط‌هایی نیاز دارد که بتوان پیش از مواجهه واقعی با تهدیدات، سـناریوهای مختلف را در آنها آزمایش کرد و نقاط ضعف و قوت سامانه‌های دفاعی را شناخت.

مخابرات در مسیر خودمختاری

هوش مصنوعی چگونه شبکه‌ها را متحول می‌کند؟



صنعت مخابرات در حال عبور از مرحله توسـعه صرف زیرساخت‌های ارتباطی به سمت شبکه‌هایی است که می‌توانند با کمک هوش مصنوعی وضعیت خود را تحلیل کنند، خرابی‌های احتمالـی را پیش‌بینی کنند و حتی بخشـی از فرایندهای مدیریتی و عملیاتی را به‌صورت خـودکار انجام دهنـد. در این میان، فنـاوری دوقلوی دیجیتال با فراهم کردن امکان شبیه‌سازی شبکه واقعی و آزمایش سناریوهای مختلف پیش از اعمال تغییرات، می‌تواند به کاهش هزینه‌های توسعه، افزایش تاب‌آوری و جلوگیری از اختلال در خدمات ارتباطی کمک کند. با این حال، تحقق چنین تحولی در ایران به عواملی فراتر از دسترسی به فناوری وابسته است؛ از جمله سرمایه‌گذاری مستمر، سامان‌دهی داده‌ها، تقویت همکاری دانشگاه و صنعت و عبور از رویکردهای مقطعی در سیاست‌گذاری فناوری اطلاعات.

توسعه فناوری‌های هوش مصنوعی، صنعت مخابرات را با مرحله تازه‌ای از تحول مواجه کرده است؛ مرحله‌ای که در آن، افزایش ظرفیت انتقال داده و توسعه زیرساخت‌های فیزیکی به‌تنهایی نمی‌تواند پاسخگوی نیازهای آینده باشد. شبکه‌های ارتباطی برای مدیریت حجم فزاینده ترافیک، کاهش هزینه‌هـای عملیاتی، افزایش کیفیت خدمـات و مقابله با اخـتلالات احتمالی، بـه ابزارهای هوشـمندتری نیـاز دارند. در چنین شـرایطی، هوش مصنوعی و فناوری دوقلـوی دیجیتال می‌توانند نقش مهمی در تغییر شیوه مدیریت و بهره‌برداری از شبکه‌های مخابراتی ایفـا کنند. مهدی مشـیری، معاون تحقیق و توسعه زیرسـاخت‌های ارتباطی شـرکت ارتباطات زیرساخت، در رویداد هوش مصنوعی در حوزه تلکام که در دانشـگاه علم و فرهنگ برگزار شد، با اشاره به تجربه این شرکت در استفاده از فناوری‌های نوین، تأکید کرد که کاربرد این فناوری‌ها نباید صرفاً در سطح مباحث نظری و دانشگاهی باقی بماند و لازم است زمینه عملیاتی شدن آنها در صنعت فراهم شود. به گفته او، شرکت ارتباطات زیرساخت طی سال‌های گذشته با رویکردی راهبردی، مقدمات اسـتفاده از فناوری‌های جدید را فراهم کرده و ظرفیت‌هایی در بخش زیرسـاخت، انتقال و پیش‌بینی ظرفیت ایجاد کرده است که امکان به‌اشتراک‌گذاری آنها با سایر اپراتورهای ارتباطی نیز وجود دارد. مشیری معتقد است اپراتورهای ارتباطی، از جمله همراه اول، باید برای ورود جدی‌تر به این حوزه برنامه‌ریزی کنند و دست‌کم گام‌های اولیه را بردارند. اهمیت این موضوع زمانی بیشتر مشخص می‌شود که بدانیم کاربرد فناوری‌های هوشمند تنها به مخابرات محدود نیست و حوزه‌هایی مانند نفت و گاز، کشـاورزی، حمل‌ونقل و ساختمان نیز می‌توانند از قابلیت‌های آن بهره‌مند شوند. او همچنین با اشاره به ضرورت توجه به ابعاد اقتصادی فناوری‌های نوین گفت که در کنار بررسـی ظرفیت‌های فنی و دانشگاهی، باید بازار و امکان تجاری‌سازی این فناوری‌ها نیز مورد توجه قرار گیرد.

◄ شبکه انتقال نوری؛ زیرساختی حیاتی با هزینه‌های فزاینده

یکی از بخش‌های مهم سخنان معاون تحقیق و توسعه زیرساخت‌های ارتباطی شـرکت ارتباطات زیرساخت به نقش شـبکه انتقال نوری در توسعه زیرساخت‌های ارتباطی کشـور اختصاص داشـت. این شبکه، بخشی اساسی از سـاختار ارتباطی کشـور را تشکیل می‌دهد و وظیفه انتقال حجم بـالای داده میان مراکز ارتباطی و سایر اجزای شـبکه را برعهده دارد. در ساختار شبکه ارتباطی، ترافیک تولیدشده از طریق فیبر نوری منازل و سایت‌های رادیویی اپراتورهای تلفن همراه جمع‌آوری می‌شود و پس از عبور از شبکه‌های شهری و حلقه‌های نوری، به شبکه پرسرعت ارتباطی کشور منتقل می‌شود. در این فرایند، تجهیزات مختلفی از جمله فرستنده‌ها، گیرنده‌ها، تقویت‌کننده‌ها و سـوئیچ‌های نوری به کار گرفته می‌شوند تا انتقال داده با کیفیت و ظرفیت مناسب انجام شود. مشیری با اشاره به ظرفیت‌های فنی این شبکه توضیح داد که در کشور امکان انتقال کانال‌های مستقل با ظرفیت ۴۰۰ گیگابیت بر ثانیه از طریق یک جفت فیبر نوری فراهم شده است. با این حال، افزایش مداوم تقاضا بـرای ظرفیت ارتباطی، اپراتورهـا را ناگزیر می‌کند که شـبکه‌های انتقال خود را به‌صورت مستمر ارتقا دهند. این توسعه با چالش‌های مختلفی همراه است. از یک سو، فناوری‌های انتقال پیچیده‌تر شده‌اند و مدیریت باندهای فرکانسی، پارامترهای فنی و کیفیت مسیرهای نوری به دانش تخصصی بیشتری نیاز دارد. از سوی دیگر، افزایش قیمت تراشه‌ها و تجهیزات سـخت‌افزاری و همچنین محدودیت‌های ژئوپلیتیکی و دشواری تأمین کالا، هزینه توسعه شبکه را برای اپراتورها افزایش داده است. به گفته مشـیری، تقریباً همه اپراتورها با مساله افزایش هزینه تجهیزات انتقال مواجه هستند و برای تأمین نیازهای خود باید منابع مالی قابل توجهی اختصاص دهند. در این میان، توسعه محصولات بومی و حضور تأمین کنندگان داخلی که توانسته‌اند تجهیزاتی مطابق با استانداردهای مورد نیاز ارایه کنند، می‌تواند بخشی از نیاز صنعت را پاسخ دهد.

◄ دوقلوی دیجیتال؛ شبیه‌سازی شبکه پیش از وقوع اختلال

در چنین شـرایطی، یکی از فناوری‌هایی که می‌تواند به مدیریت بهتر شـبکه‌های ارتباطی کمک کند، دوقلوی دیجیتال اسـت. این فناوری در واقع تصویری مجازی و پویا از یک شبکه یا سامانه واقعی ایجاد می‌کند که به‌طور مستمر داده‌های محیط فیزیکی را دریافت می‌کند و امکان بررسی رفتار آن را در شرایط مختلف فراهم می‌آورد. تفاوت اصلی دوقلوی دیجیتال با روش‌های سنتی شبیه‌سازی در پویایی و ارتباط مسـتمر آن با شـبکه واقعی است. در شبیه‌سازی سنتی، معمولاً مدل شبکه در مرحله طراحی ایجاد می‌شود و اطلاعات آن به‌صورت دستی یا با داده‌های ثابت به‌روزرسـانی می‌شـود. اما در دوقلـوی دیجیتال، اطلاعات به‌صورت زنده از شبکه واقعی دریافت می‌شود، مدل به‌طور مستمر با شرایط عملیاتی تطبیق پیدا می‌کند و امکان آزمایش سـناریوهای جدید در تمام چرخه عمر شبکه وجود دارد. مشـیری برای توضیح این تفاوت، سه مفهوم مدل دیجیتال، سایه دیجیتال و دوقلوی دیجیتال را از یکدیگر تفکیک کرد. در مدل دیجیتال، اطلاعات شبکه فیزیکی به‌صورت دسـتی وارد محیط مجازی می‌شود و ارتباط خـودکار میان دو محیط وجود ندارد. در سـایه دیجیتال، داده‌ها از شبکه واقعی به محیط دیجیتال منتقل می‌شـوند و امکان پایش و نمایش وضعیت شبکه فراهم می‌شـود، اما ارتباط همچنان یک‌طرفه است. در مقابل، دوقلوی دیجیتال از ارتباطی دوطرفه میان محیط فیزیکی و دیجیتال برخوردار است. داده‌ها از شبکه واقعی دریافت می‌شـوند، در محیط مجازی مورد تحلیل و شبیه‌سازی قرار می‌گیرنـد و نتایج حاصل از ایـن فرایند می‌تواند به شکل پیشنهادهای فنی و تنظیمات جدید به شبکه واقعی بازگردد. اهمیت این قابلیت در آن است که اپراتور می‌تواند پیش از اعمال هر گونه تغییر در شبکه واقعی، پیامدهای آن را در محیط دیجیتال بررسی کند. به این ترتیب، امکان آزمایش تغییرات، ارزیابی کیفیت سرویس، بررسی اثر ورود ترافیک جدید و حتی بازگشت به وضعیت قبلی در صورت بروز مشکل فراهم می‌شود.

◄ پیش‌بینی خرابی به جای واکنش پس از اختلال

یکی از مهم‌ترین کاربردهای دوقلوی دیجیتال در صنعت مخابرات، شناسـایی ناهنجاری‌هـا و پیش‌بینی خرابی تجهیزات است. در شبکه‌های ارتباطی، برخی اختلالات به‌صـورت ناگهانی رخ می‌دهند، اما بخشـی از خرابی‌ها به‌تدریج شکل می‌گیرند و ممکن است پیش از وقوع مشکل جدی، نشانه‌های مشـخصی در پارامترهای عملکردی تجهیزات ایجاد کنند. مشـیری توضیـح داد که هوش مصنوعـی می‌تواند با بررسـی تغییرات ایـن پارامترها، احتمال خرابی کارت‌های تجهیزات، قطعی برق یا سایر مشکلات احتمالی را تشـخیص دهد؛ حتی در شرایطی که هنوز آلارم مشخصی در شبکه ثبت نشده است. در این روش، داده‌های واقعی شبکه در اختیار مدل دیجیتال قرار می‌گیرند و الگوریتم‌های هوش مصنوعی با تحلیل آنها، الگوهای غیرعادی را شناسـایی می‌کنند. به این ترتیب، اپراتور می‌تواند پیش از آنکه اختلال به کیفیت سرویس یا تجربه مشتری آسیب بزند، اقدامات لازم را انجام دهد.

◄ فرصت‌های فناوری در ایران و تکرار تجربه‌های از دست‌رفته

در کنار مباحـث فنی، علی یزدیـان، عضو هیات علمی دانشـگاه تربیت مدرس، در این رویداد با نگاهی انتقادی به وضعیت توسـعه فنـاوری اطلاعـات و ارتباطات در ایران، بر ضرورت تغییـر رویکردهای مدیریتی و افزایش سـرمایه‌گذاری در این حـوزه تأکید کرد. او با اشـاره به تجربه‌های گذشته کشور گفت که ایران در مقاطع مختلف ظرفیت‌های مناسـبی برای توسـعه فناوری‌های نوین داشـته، اما تغییرات مدیریتی، نبود تداوم سیاسـت‌ها و کندی در بهره‌گیری از فناوری‌های جدید، موجب شده است بخشی از فرصت‌های توسعه‌ای از دست برود. یزدیان به تجربه راه‌اندازی شبکه علمی کشور در سال ۱۳۷۹ اشاره کرد که امکان پیکربندی و مدیریت تجهیزات شبکه از راه دور را فراهم می‌کرد. همچنین پروژه‌ای برای ایجاد موتور جسـت‌وجوی داخلی با هدف شناسـایی و نمایه‌سازی محتوای علمی و دانشگاهی کشور آغاز شده بود که با وجود سرمایه‌گذاری و فراهم شدن زیرساخت‌های سخت‌افزاری، در ادامه و با تغییرات مدیریتی متوقف شـد. به اعتقاد او، تجربه دوران کرونا نیز نمونه دیگری از فرصت‌هایی بود که می‌توانست به توسعه خدمات الکترونیکی و افزایش ضریب نفوذ فناوری اطلاعات منجر شود، اما اختلاف رویکردها و تصمیم‌های مدیریتی، مانع استفاده کامل از این ظرفیت شد. این عضو هیات علمی دانشگاه تربیت مدرس معتقد است امروز نیز با وجود فعالیت‌های دانشگاهی گسترده در حوزه هوش مصنوعی و یادگیری ماشین، آثار این فعالیت‌ها در بخش‌های اجرایی و صنعتی به اندازه کافی مشـاهده نمی‌شود. به گفته او، در بسیاری از حوزه‌ها، از جمله بازار سرمایه و مجموعه‌های بانکی، استفاده از هوش مصنوعی همچنان محدود است و میان ظرفیت علمی دانشگاه‌ها و نیازهای عملیاتی صنعت فاصله وجود دارد.

◄ سرمایه‌گذاری در نرم‌افزار و حاکمیت داده؛ دو ضرورت اساسی

یزدیـان یکی از موانع توسـعه فناوری در کشـور را نگاه نامتوازن به سـخت‌افزار و نرم‌افزار دانست. به گفته او، در حالی که برای خرید تجهیزات سخت‌افزاری هزینه‌های قابل توجهی پرداخت می‌شود، در بسیاری از موارد تمایل چندانی به سـرمایه‌گذاری قانونی و اصولـی در نرم‌افزار وجود ندارد. او تأکید کرد که نرم‌افزار به اندازه سخت‌افزار اهمیت دارد و بدون سرمایه‌گذاری در این بخش، امکان شـکل‌گیری و توسـعه صنعت نرم‌افزار در کشور فراهم نخواهد شد. از نگاه او، دانشگاه‌ها پروژه‌های متعددی در حوزه هوش مصنوعی انجام می‌دهند، اما برای تبدیل این دستاوردها به محصولات و خدمات عملیاتی، باید ارتباط میان دانشگاه و صنعت تقویت شود. در کنار سرمایه‌گذاری، سامان‌دهی داده‌ها نیز یکی از پیش‌شرط‌های اصلی توسعه هوش مصنوعی اسـت. یزدیان معتقد اسـت داده‌های نادرست، ناقص یا فاقد استاندارد می‌توانند به خروجی‌های اشـتباه منجر شـوند. بنابراین، پیش از توسعه گسترده سامانه‌های هوشمند، باید معماری مرجع هوش مصنوعی برای اپراتورهای مخابراتی و سـازمان تنظیم مقررات و ارتباطات رادیویی طراحی شود و موضوع حاکمیت داده در آن جایگاه مشخصی داشته باشد.

◄ هوش مصنوعی؛ از مدیریت شبکه تا ارایه خدمات جدید

یزدیان در بخش دیگری از سخنان خود، هوش مصنوعی را فراتر از یک فناوری دانشگاهی یا ابزار سرگرمی دانست و تأکید کرد که این فنـاوری به یکی از مولفه‌های قدرت اقتصادی، صنعتی و حتی نظامی در جهان تبدیل شـده است. او با اشاره به کاربردهای هوش مصنوعی در تحلیل داده‌های حاصل از حسـگرها، ماهواره‌ها و رادارها گفت که تحولات اخیر نشـان می‌دهد این فناوری می‌تواند در فرایندهای پیچیده شناسایی و تصمیم‌گیری عملیاتی نقش داشته باشد. از این رو، کشورها باید علاوه بر توسعه کاربردهای اقتصادی، بـه ابعاد امنیتی و راهبردی هوش مصنوعی نیز توجه کنند. در صنعت مخابرات نیز کاربردهای این فناوری بسیار گسترده است. از مدیریت عملکرد شبکه و شناسایی خطاها گرفته تا نگهداری تجهیزات، تحقیق و توسـعه، مدیریت منابع و ارایه خدمات به مشـترکان، همگی می‌توانند از ظرفیت هوش مصنوعی بهره ببرند. برای مثـال، در مراکز تماس و سـامانه‌هایی مانند ۱۱۸، ابزارهای هوشمند می‌توانند بخش زیادی از پرسش‌های تکراری را پاسخ دهند و فشار کاری کارشناسان انسانی را کاهش دهند. همچنین در شرایطی که کیفیت سیگنال یک مشترک افت می‌کند یا تعداد مشترکان یک منطقه به سرعت افزایش می‌یابد، سامانه‌های هوشمند می‌توانند وضعیت را تحلیل و راهکارهای مناسب را پیشنهاد کنند. یزدیان معتقد است در نسل بعدی شبکه‌های مخابراتی، عامل‌های هوش مصنوعی می‌توانند بخشی از وظایفی را که پیش‌تر توسط کارشناسان فنی انجام می‌شد، برعهده بگیرند. در این شرایط، اپراتور به جای انجام مستقیم تمام مراحل فنی و کدنویسی، درخواست خود را با زبان طبیعی به سامانه هوشمند منتقل می‌کند و سامانه نیز دستورات لازم را برای اجرا در اختیار زیرسـاخت‌های عملیاتی قرار می‌دهد. با این حال، مسوولیت نهایی و نظارت بر اجرای تصمیم‌ها باید همچنان بر عهده نیروی انسانی باقی بماند.

◄ آینده مخابرات در گرو ارایه خدمات هوشمند

یکی از مهم‌ترین نکات مطرح‌شـده در ایـن رویداد، ضرورت تغییر نگاه بـه آینده صنعت مخابـرات بود. توسعه پهنای باند و افزایش ظرفیت شبکه، اگر با ارایه خدمات هوشمند و ارزش‌آفرین همراه نباشد، به‌تنهایی نمی‌توانـد ارزش اقتصادی و عملیاتی مـورد انتظار را ایجاد کند. یزدیان تأکید کرد کـه صرفاً فراهم کردن پهنای باند بیشتر، بدون آنکه خدمات متناسب با نیاز کاربران بر بستر آن ارایه شود، پاسخگوی نیازهای آینده نخواهد بود. به اعتقاد او، آینده صنعت مخابرات متعلق به مجموعه‌هایی است که بتوانند زیرساخت‌های ارتباطی را با هوش مصنوعی ترکیب کنند و از این طریق خدمات جدید و کاربردی در اختیار مشترکان قرار دهند.

عقب‌نشینی اورکل از قرارداد با تراشه‌ساز چینی

اورکل تحت فشـارهای دولت امریکا قـرارداد اجاره چندمیلیارد دلاری تراشه با شرکت چینی تنسنت را لغو کرد. به گزارش خبرگزاری مهر به نقل از رویترز، در همین راستا نشریه فایننشال تایمز در گزارشی جدید به نقل از منابع آگاه فاش کرده مقامات امریکایی با اورکل تماس گرفتند تا درباره معامله با تنسنت نگرانی‌هایشان را مطرح کنند. مقامات ارشـد دولت چین نیز از دفتر شـرکت تنسـنت در گواندونگ دیدار کردند و از آن خواستند از تراشه‌های داخلی حمایت کند. این در حالی است که اورکل، تنسنت و کاخ سفید به درخواست‌های این رسانه پاسخی نداده‌اند. فایننشال تایمز ماه قبل در گزارشی اعلام کرد تنسنت بزرگ‌ترین قرارداد اجاره برون مرزی را بـه ارزش تقریبی هفت میلیارد دلار با اورکل امضا کرده است. این معامله دسترسی به حدود ۱۰۰ هزار تراشه پیشرفته هوش مصنوعی را می‌دهد که به دلیل محدودیت‌های اعمال شده از سوی امریکا برچین، در کشور آسیایی در دسترس نیستند. تنسنت با یک قرارداد اجاره پنج ساله با چند دیتاسنتر اورکل در جنوب شرق آسیا نیز موافقت کرده بود.

موج جدید هک سوپرمارکت‌های اروپا

سـوپرمارکت‌های اروپایی با دومین موج از حملات سایبری روبرو شـدند که دمای یخچال‌ها و فریزرها را به‌شـدت افزایـش داد و اکنـون بـرای ارتقـای سیستم‌هایشـان و محافظت درباره هک‌های بیشتر هجوم آورده‌اند. به گـزارش خبرگزاری مهر به نقل از رویترز، فروشگاه‌ها در هشت کشور این منطقه مجبور به دور ریختـن مقدار زیادی مواد غذایی شـدند زیرا هکرها یخچال‌های آنها را در یک حمله مشـابه آنچه سه هفته قبل در فرانسه رخ داد، هدف گرفته بودند. در سوئد سوپرمارکت‌های زنجیره‌ای Coop اعلام کرد سیستم‌های خود را به شبکه‌های ۵G مودم‌های مدرن به‌جای ارتباطات ۴G منتقل می‌کند. فرانسه این فرایند را پس از هک سوپرمارکت‌هایش آغاز کرده است. هفت فروشـگاه که هدف حمله قرار گرفته بوده‌اند، اکنون پشتیبانی شده و فعال هستند اما سیستم‌های یخچال آنها بـه اینترنت متصل نیست. شـرکت Danfoss، تهیه‌کننده نرم‌افزار که سیستم‌هایش دوباره در میان اهداف هکرها بود، نیز اعلام کرده طی سه هفته گذشته با مشـتریانش در تماس بوده تا در مدیریت اوضاع به آنها کمک کند و همچنین توصیه کرد این سیستم‌ها نباید به‌طور مستقیم به اینترنت متصل باشند. یکی از کارشناسان امنیت سـایبری در موسسه دلویت در این باره می‌گوید: خرده فروشان باید اکنون وارد عمل شوند. آنها باید تشخیص دهند آیا کنترل‌کننده‌های یخچال‌هایشان دچار ضعف هستند، کنترل کنند آیا آنها به اینترنت متصل هستند یا خیر، تضمین کنند جدیدترین به‌روزرسانی‌های امنیتی را دریافت کرده‌اند یا خیر و از سوی تولیدکننده پشتیبانی شوند. اما اگر در این باره اطلاعاتی ندارند باید به سرعت آنها را از اینترنت قطع کنند. با این کار مشکل حل نمی‌شود اما حداقل این سیستم‌ها ایزوله می‌شوند بنابراین حمله سایبری دیگر روی آنها تاثیری نخواهد داشت.

گوگل به مدارس هشدار داد

به نظر می‌رسـد گوگل با ارایه یک سیاست جدید به مدارس هشـدار می‌دهـد یا بایـد ویژگی‌های هوش مصنوعی را برای دانش‌آموزان فعال کنند یا به سرویس دیگر شرکت دسترسی نخواهند داشت. به گزارش مهر به نقل از انگجت، به نظر می‌رسد گوگل طی چند سال گذشته تلاش کرده اسـت تا حد امکان، قابلیت‌های هوش مصنوعـی را در محصولات بیشـتری از خود بگنجاند؛ اقدامی که با هدف توجیه ده‌ها میلیارد دلاری انجام می‌شود که این شـرکت در حوزه فناوری هوش مصنوعی سرمایه‌گذاری کرده است. اکنون نیز به نظر می‌رسد برای افزایش تعداد کاربران هوش مصنوعی خود اولتیماتومی به مدارس فرستاده است، یا ویژگی‌های هوش مصنوعی را فعال کنید یا دانش‌آموزان نمی‌توانند از سرویس جست‌وجو استفاده کنند. گوگل در یکی از چند پسـت وبلاگی که روز گذشته درباره تلاش‌های آموزشی خود منتشر کرده، نوشت به اعتقاد این شرکت آموزگاران باید بر استفاده از هوش مصنوعی در مدارس کنترل داشته باشند. کریس فیلیپس معاون مدیرعامل گوگل و مدیر بخش آموزش در پسـتی نوشت: پس از گوش دادن به توضیحات مدارس، آموزگاران، محققان برتر و سیاست‌گذاران ما رویکرد خود برای کنترل‌های جمینای، جمینـای نوت بوک، جمینـای در کلاس درس و جست‌وجوی گوگل را به روز رسانی می‌کنیم. وی در ادامه اظهار کرد: دسترسـی به این محصولات برای حساب‌های کاربری دانش‌آموزان K-۱۲ تا زمانی که مسوولان مدرسه به‌طور واضح آنها را فعال نکنند، خاموش خواهد بود. گوگل همچنین شفاف‌سازی کرد مدیران مدارس باید بتواننـد این محصولات را به‌طور جداگانه فعال کنند و این یک توافق همه یا هیچ چیز نیست. همچنین شرکت تصمیم دارد کنترل‌های به‌روز رسانی شده را در ماه‌های آینده ارایه کند. این در حالی است که شرکت در تابستان جاری از اعمال یک تغییر خودداری کرد. گوگل در ماه آگوست سال جاری میلادی برخی ویژگی‌های هوش مصنوعی را به‌طور پیش‌فرض برای پلتفرم آموزشـی «کلاس درس» فعال کرد. این تغییر به انتقاداتی از سـوی آموزگاران منجر شد و در نتیجه شرکت تغییر مذکور را معکوس کرد. اما فیلیپس به این نشریه اعلام کرد ویژگی‌های جست‌وجو و هوش مصنوعی عمیقا یکپارچه هسـتند. اگر یک مدرسـه ابزارهای هوش مصنوعی را ممنوع کند، دانش‌آموزان به سرویس جست‌وجو نیز دسترسی نخواهند داشت و آنها پیامی را از مدرسه خود دریافت می‌کنند که نشان می‌دهد این سـرویس‌ها در دسترسی نیستند. کروم بوک‌ها و اپلیکیشن‌های آموزشی گوگل به‌طور گسترده در مدارس به خصوص در امریکا اسـتفاده می‌شـوند. اگر یک حوزه آموزشـی از قوانین جدید گوگل پیروی نکند، احتمالا باید موتور جسـت‌وجوهای جایگزین و احتمالا دستگاه‌ها و پلتفرم‌های آموزشی دیگر را برای ادامه فعالیت در نظر داشته باشد. چند حوزه آموزشی دسترسی به هوش مصنوعی مولد در مدارس را پیش از ایـن محـدود کرده‌اند. نیویورک سـیتی یک دوره تعلیق یک ساله بر اسـتفاده از چنین ابزارهایی برای دانش‌آموزان تا کلاس هشتم را از سپتامبر سال جاری میلادی اعمال کرده است. مدارس عمومی لس‌آنجلس نیز یک ممنوعیت مشابه را ماه گذشته اعمال کردند. همچنین فرماندار ایالت نیویورک قانونی را امضا کرد که شرکت‌های هوش مصنوعی را از ارایه ویژگی‌های خاص چت‌بات‌ها به افراد زیر سن قانونی منع می‌کند.

سود مس برای سارقان، قطعی ارتباط برای مردم!

یکی از اتفاقات تلخ این روزها دزدیده شـدن کابل‌های مخابراتی منطقه یا محله است. اتفاقی کلافه‌کننده که به دلیل ارزش مس موجود در کابل‌ها رایج شـده است ولی در صورت بروز این اتفاق چـه باید کرد؟ به گزارش ایسنا، سرقت کابل‌های مسی و تجهیزات مخابراتی یک مشکل جدی و البته جهانی است. سال‌های اخیر به دلیل نوسـانات اقتصادی، تورم و بیکاری سرقت تاسیسات و تجهیزات ارتباطی در کشور رواج بیشتری پیدا کرده است. این مساله عمدتا به دلایلی مثل ارزش بالای فلز مس که در کابل‌های مخابراتی وجود دارد، بازار سیاه مال‌خرها و خریداران غیرمجاز ضایعات، در دسـترس بودن شبکه مخابراتی و نبود سیسـتم‌های حفاظتی مدرن و جدید اتفاق می‌افتد. شاید یکی انگیزه‌های سارقان برای سرقت تجهیزات ارتباطـی و کابل‌ها، قیمت بالای مس در بازار باشد. مس رسانای بسیار خوبی است و در صنعت تقاضای زیـادی دارد و وقتی که قیمت آن بالا می‌رود، کابل‌های مخابراتی و صنعتی ناگهان به یک کالای با ارزش تبدیل می‌شود و سارقان به خوبی می‌دانند که با سوزاندن روکش پلاسـتیکی کابل‌ها و درآوردن مس از آن می‌توانند به راحتی مس خالص را با قیمت خوبـی در بازار ضایعات بفروشند. سـرقت کابل مسی وقتی سـودآور است که یک بازار فروش غیرمجاز در سایه بی‌قانونی وجود داشته باشد و کابل‌های پوست‌کنده توسط عده‌ای مال‌خر بدون کوچک‌ترین سـوالی خریداری شوند. متاسفانه برخی به سمت جرایم خرد مثل سـرقت کابل‌های مخابراتی می‌روند و از طریق فروش آن به درآمدی می‌رسـند که شـاید به دسـت آوردنش با کار عادی سخت‌تر باشد اما خسـارتی که از این طریق به زیرساخت عمومی و مردم وارد می‌شـود را نباید از نظر دور نگاه داشـت. هم‌اکنون در بسیاری از مناطق، سیستم‌های حفاظتی مخابراتی همچنان سنتی است و طبعا سـارقان با ابزارهای ساده کابل‌هـا را قطع و خارج می‌کنند. بـا وجود آنکه مراجع انتظامی با سـارقان برخورد می‌کنند ولـی تا زمانی که سیستم‌های هشـدار هوشمند یا سـامانه‌های هشدار قطع خط روی تمام شبکه نصب نشود یا جایگزینی این کابل‌ها با فناوری‌های جدید سرعت نگیرد، انگیزه سرقت همچنان باقی می‌ماند.

◄ پیامد سرقت تجهیزات مخابراتی

سرقت تاسیسات و تجهیزات مخابراتی علاوه بر خسارات مالـی، باعث اختلال در شـبکه