فرانگرش

وقتی ماشین‌ها حمله می‌کنند

تهدیدهای سایبری هوش مصنوعی پیشرو و پاسخ‌های سیاستی در بخش مالی

When machines attack: frontier AI cyber threats and policy responses in the financial sector

BIS

این سند[1]، Occasional Paper شماره ۲۸ مؤسسه ثبات مالی (FSI) وابسته به بانک تسویه بین‌المللی (BIS) است که در سپتامبر ۲۰۲۶ توسط Juan Carlos Crisanto، Adrien Currat و Jeffery Yong منتشر شده است. موضوع آن بررسی قابلیت‌های سایبری مدل‌های هوش مصنوعی پیشرو (Frontier AI) و پیامدهای احتیاطی آن برای ناظران بخش مالی است؛ با این هدف که نشان دهد این مدل‌ها چگونه چرخه تهدید سایبری را تغییر می‌دهند و مقامات مالی چگونه بدون ایجاد رژیم مقرراتی کاملاً جدید، چارچوب‌های موجود تاب‌آوری عملیاتی و مدیریت ریسک سایبری را تقویت می‌کنند. دامنه سند، بخش مالی و نهادهای ناظر و تنظیم‌گر بین‌المللی و ملی است.

چکیده

مدل‌های پیشرفته هوش مصنوعی[2]، چشم‌انداز تهدیدات سایبری را به‌طور اساسی متحول کرده‌اند. این مدل‌ها برخلاف نسل‌های پیشین هوش مصنوعی، قادرند به‌صورت مستقل آسیب‌پذیری‌های حیاتی را شناسایی کنند، اکسپلویت‌های[3] مؤثر توسعه دهند و عملیات سایبری چندمرحله‌ای و پیچیده‌تری را اجرا کنند. در نتیجه، میزان تخصص، زمان و منابع موردنیاز برای انجام حملات پیچیده کاهش می‌یابد. در عین حال، این قابلیت‌ها فرصت‌های دفاعی قابل‌توجهی نیز فراهم می‌کنند که از جمله آن‌ها می‌توان به شناسایی سریع‌تر آسیب‌پذیری‌ها، کشف تهدیدات و واکنش به حوادث سایبری اشاره کرد.

ریسک این تحولات برای مؤسسات مالی ناشی از کوتاه‌تر شدن مهلت رفع آسیب‌پذیری‌های سایبری، افزایش احتمال نفوذ و تشدید وابستگی به اشخاص ثالث است. مدل‌های پیشرفته هوش مصنوعی با کاهش فاصله زمانی میان شناسایی آسیب‌پذیری و بهره‌برداری از آن و خودکارسازی زنجیره‌سازی اکسپلویت‌ها[4]، احتمال وقوع رخنه‌های امنیتی[5] را به‌طور قابل‌توجهی افزایش می‌دهند؛ به‌گونه‌ای که نرم‌افزارهای به‌روزرسانی‌نشده در بسیاری از حوادث، به اصلی‌ترین مسیر اولیه نفوذ تبدیل می‌شوند. اتکای مؤسسات مالی به ارائه‌دهندگان مشترک خدمات ابری، نرم‌افزار و مدل‌های پیشرفته هوش مصنوعی نیز ریسک ناشی از تمرکز و دسترسی حاکمیتی را به همراه دارد؛ به‌طوری‌که اختلال در فعالیت یک ارائه‌دهنده یا تصمیم سیاستی آن می‌تواند پیامدهایی زنجیره‌ای در مؤسسات و حوزه‌های قضایی مختلف ایجاد کند.

مقامات مالی در حال همگرایی بر سر اتخاذ رویکردی عمل‌گرایانه برای مواجهه با این تحولات هستند. به‌جای ایجاد چارچوب‌های جدید و اختصاصی امنیت سایبری برای هوش مصنوعی، آن‌ها درصدد تقویت چارچوب‌های موجود مدیریت ریسک سایبری و تاب‌آوری عملیاتی هستند و هم‌زمان، انتظارات نظارتی را با محیط جدید تهدیدات سایبری تطبیق می‌دهند. در سیاست‌های اتخاذشده، بیش از پیش بر حاکمیتی تأکید می‌شود که بتواند از تصمیم‌گیری به‌موقع، تسریع فرایند نصب وصله‌های امنیتی و ارتقای قابلیت‌های واکنش و بازیابی پشتیبانی کند. بنابراین، هوش مصنوعی پیشرفته، مبانی تاب‌آوری سایبری را به‌طور بنیادین تغییر نمی‌دهد، بلکه سرعت و شدت اجرای رویه‌های تثبیت‌شده در این حوزه را به میزان قابل‌توجهی افزایش می‌دهد.

1. Juan Carlos Crisanto, Adrien Currat and Jeffery Yong (2026), «When machines attack: frontier AI cyber threats and policy responses in the financial sector», BIS, FSI, N28, September.
2. Frontier artificial intelligence (AI)
3. Exploits
4. Exploit chaining
5. Llikelihood of breach

دیدگاه فرانگر

کشور ما ایران و به خصوص صنعت بانکی آن، تحت شدیدترین حملات سایبری قرار داشته و دارد. همان طور که در این مقاله آمده، ظهور هوش مصنوعی پیش‌رفته، شدت و میزان تأثیرگذاری و گستردگی این تهدیدات را به مراتب افزایش داده است. از طرف دیگر، تحریم‌های شدید اقتصادی و تکنولوژیکی، دست‌رسی سیستم بانکی ما به ابزارهای مقابله با تهدیدات را به شدت محدود کرده است. دشواری استفاده‌ی ما از جدیدترین ابزارهای فناورانه، وصله‌ها، و عدم دریافت هر گونه پشتیبانی از تولیدکنندگان ابزارهای رایانشی، کار را برای مدافعان سایبری کشور دشوار کرده است. لذا دیدگاه فرانگر آن است که علاوه بر توجه جدی به توصیه‌های مقاله در ارتباط با استفاده‌ی گسترده از هوش مصنوعی پیش‌رفته برای امور دفاع سایبری، نظام بانکی باید تمرکز زیادی بر تاب‌آوری سایبری داشته باشد. تاب‌آوری سایبری کلید تداوم ارائه‌ی خدمات بانکی در صورت بروز هرگونه بحرانی می‌باشد.

مشاوره مدیریت و فناوری فرانگر

FARANEGAR MANAGEMENT
& TECHNOLOGY CONSULTING

برمدار هوشمندی؛ به سوی خردمندی

faranegar.net



برای دریافت آرشیو مطالب
فرانگرش اسکن کنید