اوقات شرعی به افق تهران

اذان ظهر	اذان مغرب	اذان صبح فردا
۱۲:۱۱	۱۹:۲۸	۳:۳۷
غروب خورشید	**نیمه شب شرعی**	**طلوع فردا**
۱۹:۰۸	۲۳:۲۳	۵:۱۴

اوقات شرعی به افق مشهد

اذان ظهر	اذان مغرب	اذان صبح فردا
۱۱:۳۸	۱۸:۵۶	۳:۰۲
غروب خورشید	**نیمه شب شرعی**	**طلوع فردا**
۱۸:۳۶	۲۲:۴۹	۴:۴۰

صاحب امتیاز: مؤسسه فرهنگی قدس
وابسته به آستان قدس رضوی
مدیرعامل و مدیر مسئول: علی یعقوبی
سردبیر: سید محسن اسدی

آدرس دفتر مرکزی مشهد: بولوار سجاد، نبش سجاد ۱
تلفن: ۱۴- ۳۷۶۸۵۰۱۱ (۰۵۱)

صندوق پستی: ۵۷۷ - ۹۱۷۳۵
دفترتهران: بولوارکشاورز، بین کارگر و جمالزاده، شماره ۳۳۶
تلفن: ۶۶۹۳۷۵۷۵ (۰۲۱)
نمابر: (داخلی ۲۲۶) ۶۶۴۳۰۱۲۲ (۰۲۱)
پیامک: ۳۰۰۰۴۵۶۷
ارتباطات مردمی: ۳۷۶۱۰۰۸۶ (۰۵۱)
امور مشترکین: ۵-۳۷۶۱۸۰۴۴ (۰۵۱)

روابط عمومی: ۳۷۶۶۲۵۸۷ (۰۵۱)
نمابر سردبیر: ۳۷۶۱۰۰۸۷ - ۳۷۶۸۴۰۰۴ (۰۵۱)
سازمان آگهی‌ها: ۳۷۶۲۸۲۰۵ - ۳۷۰۸۸ (۰۵۱)
فاکس: ۳۷۶۱۰۰۸۵ (۰۵۱)
سفارشات چاپی: ۳۷۶۷۶۵۹۶ (۰۵۱)
چاپ مشهد: مجتمع چاپ و نشر قدس
چاپ همزمان تهران: چاپخانه جام‌جم

یافته‌ها

کشف آبا و اجداد جدید انسان

دانشمندان می‌گویند شجره‌نامه انسان شاخه‌های تازه‌ای پیدا کرده است. این یعنی آن‌ها در ژن‌های انسان امروزی نشانه‌هایی از دو نیاکان را پیدا کرده‌اند که تا امروز ناشناخته بودند. گونه‌های منقرض‌شده، بدون فسیل یا دی‌ان‌ای رمزگشایی‌شده؛ اما با ردپایی که در ژنوم ما جا مانده و حالا کشف شده است!

به گزارش یورونیوز، گروهی از پژوهشگران دانشگاه کالیفرنیا بخش‌هایی از دی‌ان‌ای در ژنوم انسان‌های امروزی را شناسایی کرده‌اند که از نیاکان ناشناخته‌ای به جا مانده است. این دانشمندان از این نیاکان با عنوان «نیاکان شبح» یاد می‌کنند، چون تاکنون هیچ چیز درباره این جمعیت‌های منقرض‌شده انسانی شناخته نشده است.

مطالعات قبلی نشان داده بود انسان‌های مدرن با نئاندرتال‌ها و انسان‌های موسوم به دنیسوون آمیزش داشتند و از آن‌ها صاحب فرزند شدند. بسیاری از انسان‌ها هنوز هم ردهای ژنتیکی این برخوردها را در ژنوم خود دارند. اکنون مطالعه‌ای تازه نشان می‌دهد دست‌کم دو گروه انسانی ناشناخته دیگر نیز وجود داشته‌اند که آن‌ها هم دی‌ان‌ای خود را به نیاکان ما منتقل کرده‌اند.

یکی از این نیاکان ناشناخته بیش از ۵۰ هزار سال پیش در آفریقا با نیاکان انسان مدرن آمیزش داشته است. این رویداد پیش از آخرین موج بزرگ کوچ انسان خردمند به اروپا و آسیا رخ داد. ژن‌هایی که در آن زمان منتقل شدند، امروز حدود یک درصد ژنوم همه انسان‌ها را تشکیل می‌دهند؛ تقریباً به همان اندازه که دی‌ان‌ای نئاندرتال‌ها در ژنوم ما حضور دارد.

پژوهشگران معتقدند این تبار مرموز انسانی حدود ۸۰۰ هزار سال پیش از شاخه فرگشتی منتهی به انسان مدرن جدا شده بود.

مطالعات قبلی فقط حدس زده بودند که نوعی «تبار شبح» وجود دارد؛ اما تاکنون تصور می‌شد که این تبار ناشناخته فقط در آفریقایی‌ها دیده می‌شود و معلوم نبود این آمیزش چه زمانی رخ داده است. حالا دانشمندان توانسته‌اند بخش‌های مربوط به دی‌ان‌ای را در ژنوم انسان‌های امروزی شناسایی و نقشه‌برداری کنند و نشان دهند که این تبار شبح در همه انسان‌های امروز وجود دارد، نه فقط در آفریقایی‌ها.

نیاکان دوم که پژوهشگران آن را «نیاکان فوق‌باستانی» می‌نامند حتی رازآمیزتر است. این تبار انسانی حدود ۱٫۸ میلیون سال پیش از دیگر انسان‌تبارها جدا شده بود. به احتمال زیاد بیش از ۲۰۰هزار سال پیش در اوراسیا با دنیسوون‌ها آمیزش داشته و از این مسیر غیرمستقیم، قطعاتی از آن دی‌ان‌ای بسیار کهن سرانجام وارد ژنوم انسان مدرن شده است.

دوردست‌ها

جاسوسی با کنتور هوشمند!

حوالی امروز | فکر نکنید بدبینی به علم و برخی دستاوردهای فناورانه و شایعه‌سازی در مورد آن‌ها (مثل شایعات و دروغ‌های شاخ‌داری که درباره اثرات واکسن کرونا وجود داشت) فقط مخصوص ما ایرانی‌هاست.

اخیراً در آلمان غوغایی به راه افتاده که مدعی است دولت این کشور با نصب کنتورهای برق هوشمند به دنبال جاسوسی از شهروندان است.

این در حالی است که به نوشته «یورونیوز» بسیاری از کشورهای اروپایی سال‌هاست برنامه نصب کنتورهای هوشمند را آغاز کرده و پیش برده‌اند. یعنی در حالی که در فرانسه، ایتالیا، هلند و اسپانیا بیش از ۹۰ درصد کنتورهای برق هوشمند شده و در کل اتحادیه اروپا این رقم به ۶۳ درصد رسیده، آمارها می‌گویند خانوارهای آلمانی تا چند ماه پیش فقط ۵/۵ درصدشان راضی به نصب کنتور هوشمند شده‌اند! هرچند بررسی‌ها وجود چند عامل را سبب این استقبال و همکاری سرد آلمانی‌ها با دولتشان می‌دانند؛ مثلاً در سال ۲۰۱۲ چون هزینه نصب کنتور هوشمند بسیار بالا بوده، مردم از آن استقبال نکرده‌اند؛ اما طی سال‌های اخیر و با ارزان‌تر شدن کنتورها عامل اصلی، بدبینی بوده است!

یعنی سوءاستفاده تاریخی از داده‌های شخصی در آلمان باعث شده شهروندان این کشور نسبت به اشتراک‌گذاری داده‌ها حساسیت ویژه‌ای داشته باشند و این حساسیت به نگاه آن‌ها نسبت به کنتورهای هوشمند هم سرایت کرده است. «یان روزنو» استاد سیاست انرژی و اقلیم در دانشگاه آکسفورد می‌گوید: «تشویق مردم به انعطاف‌پذیری در مصرفشان اگر کنتور هوشمند نداشته باشند کار دشواری است. بی‌گمان بدبینی زیادی درباره کنتورهای هوشمند وجود دارد، درست یا نادرست؛ به‌ویژه در زمینه اشتراک‌گذاری داده‌ها و حریم خصوصی. رسانه‌ها هم سروصدای زیادی راه انداختند که این کنتورها قرار است برای جاسوسی از شما به کار بروند!»

این در حالی است که کارشناسان می‌گویند کنتورهای هوشمند برق از نظر تئوری می‌توانند داده‌های بسیار دقیقی از الگوی مصرف برق یک خانوار ارائه کنند؛ اما به این معنی نیست که آن‌ها هر ثانیه اطلاعات مربوط به خانوارها را ثبت و ضبط می‌کنند چون کنتور هوشمند هر ۱۵ دقیقه یک بار اطلاعات مصرف برق را ثبت می‌کند. ضمن اینکه اطلاعات ثبت شده حتی آن‌قدر دقیق نیستند که بتوانند بگویند در فلان ساعت ماشین لباس‌شویی روشن بوده یا اتوی برقی؟ چه برسد به اینکه بتوانند مثلاً حضور یا عدم حضور صاحبخانه در منزل را مشخص کنند.

آیا در نبرد سایبری، توانایی نفوذ به معنای توانایی بقاست؟

ضعف‌های دفاعی، توانایی‌های تهاجمی

فائزه مجردیان | از یک سو گزارش‌های مایکروسافت و رسانه‌های غربی از اوج‌گیری توان تهاجمی ایران و استفاده هوشمندانه از هوش مصنوعی برای نفوذ سخن می‌گویند؛ اما از سوی دیگر، لرزش زیرساخت‌های بانکی، حملات سایبری مداوم و بحران تمدید گواهی‌های SSL، یک پرسش را پیش می‌کشد: اگر واقعاً توان تهاجمی ما تا این حد ارتقا یافته، پس وضعیت سپر دفاعی ما در برابر ضربات، در کدام نقطه از این معادله قرار دارد؟

■توان تهاجمی بالا

فقط کافی است چند ساعت نتوانید پول جابه‌جا کنید، کارت بانکی‌تان از کار بیفتد یا سامانه یک اداره از دسترس خارج شود تا متوجه شوید وسط جنگ سایبری به سر می‌برید. این جنگ‌های به قول ما امروزی، حالا از پشت صفحه‌های نمایش، راه خودشان را باز کرده‌اند و گاهی با عملیات‌های کوچکی مثل یک اختلال چندساعته در یک سامانه بانکی، همان بلایی را سر یک کشور می‌آورند که سال‌ها پیش، فقط با یک عملیات نظامی ممکن بود.

جالب است بدانید گزارش‌های امنیتی بین‌المللی، ایران را در کنار رقبای قدیمی مثل روسیه، چین و کره شمالی، یکی از فعالان پر سر و صدای فضای سایبری معرفی می‌کنند.

حرف از توسعه قابلیت‌های نفوذ است، از ابزارهای پیشرفته و از اینکه چطور این بازیگران، حالا چشمشان به هوش مصنوعی باز شده تا در عملیات‌های خود، از آن هم استفاده کنند.

حتی مایکروسافت هم در گزارش‌هایش مدعی شده که ایران، مثل بقیه قدرت‌های سایبری دنیا، یاد گرفته از هوش مصنوعی برای شاخ و شانه کشیدن فعالیت‌های دیجیتالش استفاده کند؛ از تولید محتواهای جعلی گرفته تا کمک به نفوذ و جمع‌آوری اطلاعات.

تحلیلگران غربی هم معتقدند هوش مصنوعی، حالا در خدمت عملیات‌های سایبری درآمده و اتفاقاً خیلی هم موفق است.

ایران هم با تکیه بر مغزهای متخصص و البته با هزینه‌ای که خیلی کمتر از غول‌های بزرگ دنیاست، توانسته جای پای خودش را در این عرصه محکم کند.

اما این روایتی که گفتیم، یک جای کارش می‌لنگد. اکثر این تحلیل‌ها فقط از زاویه توان تهاجمی به موضوع نگاه می‌کنند؛ یعنی کشوری که می‌تواند در فضای دیجیتال، به زیرساخت‌های رقیبش فشار بیاورد و آن‌ها را به لرزه درآورد؛ اما نیمه دیگر، ماجرای دفاع و مقاومت است؛ اینکه وقتی ضربه خوردیم، چقدر سریع می‌توانیم خودمان را جمع‌وجور کنیم و خدمات را به حالت اول برگردانیم؛ موضوعی که در ادبیات امنیت سایبری با مفهوم تاب‌آوری دیجیتال شناخته می‌شود.

> کشوری که بتواند خدمات حیاتی خود را حفظ کند، اعتماد کاربران را نگه دارد و در برابر فشارهای فناورانه مقاومت کند، بخش مهمی از قدرت واقعی خود را بدست آورده است

■آسیب‌پذیری در لایه‌های پنهان

در واقع منظورمان این است که قدرت یک کشور را نباید فقط با میزان نفوذ به سامانه‌های دیگران سنجید. بانک‌ها، سیستم‌های ارتباطی و زیرساخت‌های اینترنتی، همان نقاط ضعف حساسی هستند که کوچک‌ترین لرزش در آن‌ها، می‌تواند زندگی میلیون‌ها نفر را آشفته کند.

همین چند وقت پیش، وقتی چهار بانک بزرگ کشور ناگهان دچار اختلال شدند، تازه متوجه شدیم داستان چقدر جدی است.

خدمات الکترونیکی بانک‌های ملی، تجارت، صادرات و توسعه صادرات، برای مدتی از کار افتادند و این اختلال ناگهانی ترس زیادی درست کرد.

اگرچه شورای هماهنگی بانک‌های دولتی اعلام کرد که نگران نباشید، فقط یک حمله سایبریِ محدود بوده و دست کسی به اطلاعات مشتریان نرسیده و خسارت مالی بزرگی گزارش نشده؛ اما این حادثه نشان داد یک اختلال کوتاه در زیرساخت‌های دیجیتال می‌تواند خیلی سریع از یک مشکل فنی به یک بحران عمومی تبدیل شود.

از طرفی داستان امنیت، فقط به حمله مستقیم هکرها و فرو ریختن سرورها ختم نمی‌شود و ممکن است آسیب‌پذیری‌ها در لایه‌های پنهان اینترنت مثل زیرساخت کلید عمومی یا همان PKI و گواهی‌های SSL خودش را نشان دهد.

ساده‌تر بگویم SSL مثل یک مهر اعتماد است که به وب‌سایت‌ها زده می‌شود تا به کاربر بفهماند نگران نباشد، این مسیر امن است و اطلاعاتش در راه گم یا دستکاری نمی‌شود؛ اما این مهر اعتماد، همین‌طوری و الکی صادر نمی‌شود؛ بلکه باید از طرف مراکز معتبر جهانی یا همان CAها تأیید شود تا مرورگرها اجازه دهند شما با خیال راحت در یک سایت بچرخید.

«خبرآنلاین» از قول یکی از کارشناسان می‌نویسد: تحریم‌ها و محدودیت‌هایی که برخی از این مراکز بین‌المللی برای ایران اعمال کرده‌اند، تمدید این گواهی‌های امنیتی را برای بسیاری از وب‌سایت‌ها به یک کابوس تبدیل کرده است. بنابراین جنگ سایبری گاهی خودش را با قطع کردن زنجیره اعتماد و محدود کردن دسترسی به استانداردهای جهانی فناوری نشان می‌دهد.

■دوام آوردن

حالا شاید این سؤال پیش بیاید که خب، چرا خودمان یک مرکز صدور گواهی داخلی راه نمی‌اندازیم و کار را تمام کنیم؟ کارشناسان می‌گویند راه‌اندازی یک مرجع داخلی به این سادگی‌ها نیست. گواهی‌هایی که خودمان صادر می‌کنیم، به‌طور پیش‌فرض در مرورگرهای جهانی (مثل کروم یا سافاری) معتبر شناخته نمی‌شوند.

یعنی اگر بخواهید از آن‌ها استفاده کنید، مرورگر با یک هشدار قرمز و ترسناک، جلو کاربران را می‌گیرد. برای اینکه این گواهی‌های داخلی، اعتبار جهانی پیدا کنند، باید از هفت‌خان رستم فنی و امنیتی بگذرد تا روزی مرورگرها هم آن‌ها را به عنوان یک مهر قابل‌اعتماد بپذیرند.

از سوی دیگر، میدان جنگ سایبری امروز بسیار گسترده‌تر از گذشته شده و دارد علاوه بر سرورها و رایانه‌ها، داده‌های کاربران، شبکه‌های اجتماعی و رفتارهای آنلاین را هم در برمی‌گیرد. در سال‌های اخیر، گزارش‌های متعددی درباره استفاده از شبکه‌های اجتماعی برای عملیات روانی، جمع‌آوری اطلاعات و مهندسی اجتماعی منتشر شده و هوش مصنوعی هم اوضاع را سخت‌تر و پیچیده‌تر کرده است.

چون هم می‌تواند محتوای جعلی تولید و هم شناسایی الگوهای رفتاری و اجرای برخی عملیات‌های سایبری را سریع‌تر و دقیق‌تر کند.

پس امروز داستان قدرت سایبری داستان دوام آوردن است. کشوری که توانایی نفوذ دارد؛ اما زیرساخت‌هایش در برابر اختلال‌ها آسیب‌پذیر است، هنوز با چالش بزرگی روبه‌رو است.

در مقابل، کشوری که بتواند خدمات حیاتی خود را حفظ کند، اعتماد کاربران را نگه دارد و در برابر فشارهای فناورانه مقاومت کند، بخش مهمی از قدرت واقعی خود را بدست آورده است.

بنابراین در این میدان تازه، پیروزی فقط نصیب کسانی نمی‌شود که ابزار حمله بیشتری دارند؛ بلکه به کسانی می‌رسد که علاوه بر آن بتوانند در برابر حمله‌ها دوام بیاورند.

جهان امروز

رقابت چین و آمریکا به جاهای باریک کشید

جنگ بر سر ربات‌های دوپا و چهارپا!

مجید تربت‌زاده | سه‌شنبه هفته گذشته بود که آمریکا اعلام کرد: «واردات ربات‌های انسان‌نما یا چهارپای جدید از تولیدکنندگان خارجی ممنوع است!» آمریکایی‌ها اعلام کردند این ربات‌ها «خطرات غیرقابل قبولی» برای امنیت ملی این کشور ایجاد می‌کنند.

ناگفته معلوم است که ماجرا رقابت تنگاتنگ چین و آمریکا در زمینه توسعه هوش مصنوعی است. این نکته هم واضح است که این ممنوعیت به جز رقابت علمی، در اصل انگیزه‌های اقتصادی دارد؛ یعنی در حالی که پیش از این اعلام شده بود چینی‌ها در زمینه هوش مصنوعی از آمریکا عقب افتاده‌اند؛ اما بازار ربات‌های انسان‌نما در اختیار چین بود و بخش عمده ربات‌های مورد نیاز در جهان توسط چینی‌ها تأمین می‌شد.

■بهانه امنیت ملی

«سی‌ان‌ان» در این باره نوشته است: «تحلیلگران می‌گویند چین به لطف مقیاس تولید و توانایی تجاری‌سازی سریع محصولات، در زمینه برنامه‌های کاربردی و سخت‌افزارهای مبتنی بر هوش مصنوعی مانند ربات‌ها پیشتاز شده است». بنابراین مشخص است که دل‌نگرانی اول آمریکایی‌ها امنیت اقتصادی ماجرا بوده و بعد هم امنیت در زمینه‌های دیگر. بدیهی هم بود که این ممنوعیت آمریکایی، تا حد زیادی صادرات ربات‌های چینی را دچار مشکل کرده و آن‌ها را نگران کند.

به خصوص اینکه بیشتر طرف‌های تجاری چینی‌ها شرکت‌های آمریکایی بودند. برای همین هم وزیر خارجه چین اعلام کرد: آمریکا همیشه مفهوم امنیت ملی را بهانه کرده و از آن برای سرکوب شرکت‌های چینی، سوءاستفاده می‌کند. این رفتار، قدرت رقابت آمریکا را بالا نمی‌برد؛ بلکه بیشتر به منافع کسب و کارها و مصرف‌کنندگان آمریکایی لطمه می‌زند.

دو روز بعد هم وزارت بازرگانی چین وارد ماجرا شد و ایالات متحده را به «قلدری یک‌جانبه» و «دستکاری بازار» متهم کرد و از واشنگتن خواست فوراً این ممنوعیت را لغو کند وگرنه با اقدامات متقابل روبه‌رو خواهد شد.

■سرانجام کار

در دعوای تازه چین و آمریکا این واقعیت را هم باید در نظر گرفت که سال گذشته، شرکت‌های چینی ۹۰ درصد از صادرات جهانی این محصولات را به خود اختصاص دادند، در حالی که رقبای آمریکایی مانند تسلا و Figure AI حتی برای شروع تولید انبوه با مشکل مواجه بودند.

اضافه بر این، یک ماه پیش غول فناوری آمریکایی «انویدیا» اعلام کرده بود با یکی از برترین سازندگان ربات‌های انسان‌نمای چینی وارد همکاری خواهد شد؛ اما بلافاصله دولت آمریکا به بهانه خطرات امنیتی دستور لغو همکاری را صادر کرده بود.

تحلیلگران حوزه هوش مصنوعی و ربات‌های انسان‌نما درباره سرانجام این رقابت، بهانه‌های آمریکایی و تهدیدهای چینی‌ها به تلافی کردن، به «سی‌ان‌ان» گفته‌اند اقدامات آمریکا ممکن است در کوتاه‌مدت برای شرکت‌های چینی، کمی دردسرساز باشد؛ اما در مجموع تأثیر کلی اقدامات آمریکا «حداقلی» است به خصوص اینکه بسیاری از فروشندگان چینی به اروپا به عنوان مقصد اصلی خود نگاه می‌کنند. همچنین با توجه به کمبود تولید و محدودیت‌های فعلی شرکت‌های آمریکایی، بعید است ممنوعیت‌های آمریکایی بتواند مسیر رشد شرکت‌های چینی را متوقف کند.