حوزه فاوا

■ وزارت ارتباطات و فناوری اطلاعات سرانجام به اختلال جی‌پی‌اس‌ها واکنش نشان داد.
میثم عابدی، مدیرکل توسعه فناوری‌های نوین وزارت ارتباطات دراین باره گفت:« پس از اختلال رخ داده در سیستم‌ها و مسیریاب‌ها، کاربران تاکسی‌های اینترنتی و پیک‌های موتوری دچار مشکلات بسیاری شدند اما باید بپذیریم که یک اتفاقی در کشور ما رخ داده و به دستگاه‌هایی که در این زمینه حساس هستند حق داد تا زمان عادی شدن شرایط، محدودیت‌هایی وضع کنند. چیزی که در ۱۲ روز مشاهده کردیم نیازمند بررسی و رفع محدودیت‌ها در گام دوم است چراکه امنیت مردم اهمیت زیادی دارد.»
میثمی گفت: «اساساً سران رده بالای کشوری و لشکری به هیچ وجه نباید از ابزارهایی مانند واتس اپ استفاده کنند؛ اما مردم با توجه به اینکه قانون اجازه داده و همه جوانب سنجیده شده می‌توانند با خیال راحت و با حفظ ملاحظات لازم مانند اینکه اطلاعات شخصی خود را به هر کسی ندهند، از این ابزارها استفاده کنند.»

■ محمد امین آقامیری، دبیر شورای عالی فضای مجازی گفت: «یکی از مهم‌ترین مسائلی که صحنه این جنگ ۱۲ روزه را به نفع کشور عوض کرد، این بود که با فعالیت شبکه‌های اجتماعی داخلی، خللی در زندگی مردم به وجود نیامد و پلتفرم‌های اقتصاد دیجیتال تاب‌آوری اجتماعی کشور را بالا بردند.
البته برخی از کسب و کارهای اقتصاد دیجیتال به دلیل شرایط جنگ آسیب جدی دیدند که تلاش کردیم در تعامل با آنها این مشکلات را برطرف و از آنها حمایت کنیم تا حوزه‌های خدماتی اصلی در چنین شرایطی قطع نشود و بتوانند به صورت پایدار به مردم خدمات ارائه دهند.»

تازه‌های موبایل

■ بر اساس گزارش جدید بلومبرگ، اپل رویداد معرفی سری آیفون ۱۷ را در تاریخ ۹ یا ۱۰ سپتامبر (۱۸ یا ۱۹ شهریور) برگزار خواهد کرد.
در این رویداد، علاوه بر سری آیفون ۱۷، انتظار می‌رود از اپل واچ سری ۱۱، اپل واچ اولترا ۳ و نسل سوم اپل واچ SE نیز رونمایی شود.

■ شیائومی در حال احیای یکی از طراحی‌های جسورانه خود است تا نمایشگر دوم به گوشی‌های شیائومی بازگردد.
بر اساس اطلاعات فاش‌شده، این شرکت روی یک گوشی هوشمند جدید با نمایشگر دوم در پنل پشتی کار می‌کند؛ ایده‌ای که پیش‌تر در گوشی شیائومی «می ۱۱ اولترا» دیده بودیم.

کوتاه از فناوری

■ شرکت xAI متعلق به ایلان ماسک از کارکنانی که چت‌بات گراک را آموزش می‌دهند خواسته است نرم‌افزار نظارتی Hubstaff را روی لپ‌تاپ‌های شخصی خود نصب کنند.

■ ارتشی از روبات‌های انسان‌نما با حمایت دولت چین در حال شکل‌گیری است و این موضوع ایلان ماسک را نگران کرده است. ماسک در این باره گفته است: «نگرانم که در جدول رده‌بندی روبات‌ها، رتبه‌های دوم تا دهم به شرکت‌های چینی اختصاص یابد.»

از هوش مصنوعی چه خبر؟

■ تحقیقاتی جدید که با نظرسنجی از هزار کودک ۹ تا ۱۷ ساله انجام شده، نشان می‌دهد بسیاری از کودکان و نوجوانان تنها، دوستی‌های واقعی را با چت‌بات‌های هوش مصنوعی جایگزین کرده‌اند و از برنامه‌هایی مانند چت جی پی تی، Character.AI و MyAI متعلق به اسنپ‌چت برای شبیه‌سازی روابط دوستانه استفاده می‌کنند.

خبرهای علم

■ پژوهشگران دانشگاه استنفورد هشدار داده‌اند که مردم از چت‌بات‌های هوش مصنوعی برای روان‌درمانی استفاده نکنند چون ممکن است چت‌بات‌ها به سؤالات کاربران پاسخ‌های نامناسب یا حتی خطرناکی بدهند.

■ محققان به‌طور تصادفی کشف کردند که یک نوع قند طبیعی موجود در بدن انسان می‌تواند با تحریک رگ‌های خونی، باعث رشد مجدد مو شود.

■ مهندسان مؤسسه فناوری ماساچوست (MIT) یک ایمپلنت هوشمند توسعه داده‌اند که می‌تواند افت قند خون خطرناک را تشخیص دهد و دارویی نجات‌بخش را در بدن آزاد کند.

■ رشد رگ‌های خونی با ذرات خاکرس برای درمان زخم‌ها کشف شد. دانشمندان کشف کرده‌اند که نانوسیلیکات می‌تواند به بدن در ساخت رگ‌های خونی جدید کمک کند. این ویژگی باعث می‌شود زخم‌ها سریع‌تر خوب شوند، بدون آن‌که نیاز به داروهای گران‌قیمت باشد.

کهکشان

■ براساس شبیه‌سازی انجام شده در تحقیقی جدید، زمین احتمالاً ۶ مینی قمر دارد که در حقیقت قطعاتی هستند که از ماه جدا شده‌اند و به طور موقت دور زمین می‌چرخند.

■ بزرگ‌ترین شهاب‌سنگ مریخی کشف‌شده روی زمین با وزن ۲۵ کیلوگرم قرار است با قیمتی بین ۲ تا ۴ میلیون دلار در حراجی ساتبی نیویورک به فروش برسد.

عکس: رزدی نت

کارشناسان حوزه مالی و سایبری در گفت‌وگو با «ایران»:

زیرساخت های بانکی باید امن و نفوذناپذیر باشد

گزارش

میترا جلیلی
دبیرگروه علم و فناوری

جنگ تحمیلی ۱۲ روزه رژیم صهیونیستی علیه ایران، تنها نظامی نبود و افزایش حمله‌های سایبری به کشور، نشان از جنگ ترکیبی تمام عیار این رژیم علیه ایران داشت. در این میان حمله سایبری به زیرساخت‌های مالی پررنگ‌تر بود و در نهایت هم دو بانک و همچنین نوبیتکس به عنوان بزرگترین صرافی رمزارز کشور به عنوان اهداف اصلی این تجاوزها، هک شدند که منجر به ایجاد اختلال در اینترنت بانک، موبایل بانک، سامانه‌های پرداخت حقوق و خدمات خودپرداز و همچنین سرقت رمزارز از نوبیتکس شد. کارشناسان معتقدند اتفاقات اخیر، هشداری جدی برای نوسازی به موقع امنیت سیستم بانکی کشور است و باید علاوه بر ریشه‌یابی دلیل آسیب‌پذیری زیرساخت‌های مالی، به دنبال ارتقای امنیت سایبری این سیستم‌ها باشیم چراکه با توجه به افزایش میزان حملات هکری، اگر امنیت سایبری بالا نرود، زیرساخت‌های حیاتی کشور در دوران صلح نیز آسیب‌پذیر خواهند بود.

از ضعف‌های ساختاری تا گام‌های عملی

کارشناسان حوزه فناوری اطلاعات و متخصصان سایبری، این آسیب‌پذیری‌ها را نشانه برخی ضعف‌های ساختاری در سیستم مالی کشور می‌دانند و معتقدند بی‌توجهی به موضوعاتی همچون به روزرسانی منظم نرم‌افزارهای امنیتی و همچنین استفاده از فناوری‌های فرسوده که دیگر تاب‌آوری لازم را در برابر حملات پیچیده و هدفمند ندارند، راه را برای مهاجمان سایبری هموارتر می‌کند. این متخصصان، البته نبود تجهیزات پیشرفته امنیت سایبری به‌دلیل تحریم‌ها و اختلال در اینترنت و محدودیت‌های داخلی را نیز به دلیل کاهش سرعت پاسخگویی، در این امر دخیل می‌دانند. به اعتقاد متخصصان امنیت بانکداری، باید با بازنگری کامل در سامانه‌های بانکی و مهاجرت به زیرساخت‌های مدرن ابری و رمزنگاری‌شده، برای ارتقای امنیت سایبری، گام‌های عملی برداشته شود و دولت هم با سرمایه‌گذاری جدی، برای ایجاد زیرساخت‌های امنیت اطلاعات ملی، با بخش خصوصی همکاری کند.
برخی دیگر از کارشناسان هم آغاز امنیت سایبری را نقطه پشتیبان می‌دانند و معتقدند نسخه‌ای که به سیستم آلوده متصل است، «پشتیبان» نیست، بلکه کپی همان ضعف امنیتی است. این متخصصان، سه دلیل مشترک در حملات سایبری به بانک‌ها را «بکاپ‌گیری متصل»، «استفاده از تجهیزات بدون لایسنس و نرم‌افزارهای دستکاری‌شده» و «تست‌نکردن بازیابی واقعی» می‌دانند. به گفته آنان، بکاپ فقط زمانی ارزش دارد که از مسیر حمله «جدا» باشد درحالی که در بسیاری از سازمان‌های ایران، بکاپ دقیقاً در کنار هدف نگهداری می‌شود.

ارتقای امنیت سایبری با هوش مصنوعی

مهیار خدادادی، از فعالان حوزه فضای مجازی، امنیت سایبری را سنگ بنای اعتماد در فضای دیجیتال می‌داند که نقشی حیاتی در صیانت از داده‌های حساس کاربران، زیرساخت‌های حیاتی کشور و سیستم‌های کلیدی دولتی و اقتصادی ایفا می‌کند.
این کارشناس امنیت سایبری دراین باره به «ایران» می‌گوید: «همزمان با تشدید رقابت‌های ژئوپلیتیکی و افزایش تنش‌های فناورانه میان کشورها، دامنه و شدت حملات سایبری به بخش‌های مختلف از جمله بانک‌ها و صرافی‌های ارزهای دیجیتال نیز رشد چشمگیری یافت و همین امر، لزوم بازنگری و تقویت راهبردهای دفاعی کشور در حوزه امنیت دیجیتال را ضروری‌تر از گذشته کرده است.
خدادادی، راهکار مقابله مؤثر با این تهدیدات را اتخاذ یک رویکرد چندلایه و یکپارچه در حوزه امنیت سایبری می‌داند و می‌افزاید:« یکی از اصلی‌ترین رویکردهای کارآمد برای ارتقای امنیت سایبری بانک‌ها و سایر زیرساخت‌ها، استفاده از فناوری‌های هوش مصنوعی (AI) و پیاده‌سازی مدل‌های اعتماد صفر (Zero Trust) است چرا که هوش مصنوعی با توان پردازش سریع و تحلیل داده‌های کلان، امکان شناسایی الگوهای مشکوک، تهدیدات نهان و همچنین اقدامات مخرب در مراحل اولیه را فراهم می‌کند.»
این فعال حوزه سایبری، شناسایی زودهنگام تهدیدات سایبری را در گرو وجود ابزارهای مبتنی بر یادگیری ماشین(ML) می‌داند که می‌توانند حملاتی همچون فیشینگ یا نفوذ به شبکه‌های داخلی را به‌صورت آنی شناسایی کرده و با پیش‌بینی تهدیدات آینده، سامانه‌های دفاعی را به‌طور خودکار به‌روزرسانی و تقویت کنند. وی می‌افزاید: «سیاست‌های «اعتماد صفر»، فرض را بر بی‌اعتمادی می‌گذارند مگر آن‌که خلافش اثبات شود و در این مدل، هیچ کاربر یا دستگاهی حتی درون سازمان، مجاز به دسترسی به منابع نیست مگر آن‌که هویت، اعتبار و نیازمندی دسترسی‌اش به‌صورت دقیق احراز شده باشد. این رویکرد، تا حد زیادی از گسترش تهدیدات داخلی یا نفوذهای چندمرحله‌ای جلوگیری می‌کند.»
این کارشناس البته اعتقاد دارد ارتقای امنیت سایبری زیرساخت‌های بانکی و... در کشور با موانعی مواجه است و باید مسئولان با رفع این موارد، به افزایش تاب‌آوری زیرساخت‌ها در برابر مهاجمان سایبری کمک کنند. خدادادی، یکی از موانع اصلی در مسیر ارتقای امنیت سایبری کشور را نبود انسجام و تمرکز نهادی می‌داند و می‌افزاید: « در حال حاضر مدیریت فضای سایبری در ایران بین نهادهای مختلف تقسیم شده است؛ نهادهایی که گاه کارهای مشابه انجام می‌دهند یا مسئولیت‌های‌شان با یکدیگر تداخل پیدا می‌کند. از این نهادها می‌توان به مرکز ملی فضای مجازی، سازمان فناوری اطلاعات، افتا و نهادهای تنظیم‌گر نیز اشاره کرد. این تعدد مراکز تصمیم‌گیر، در عمل موجب بروز ناکارآمدی در زمان واکنش به بحران‌های سایبری شده و روند تدوین و اجرای سیاست‌های مؤثر را با چالش مواجه کرده است.»

لزوم بازنگری ساختار حکمرانی سایبری

این کارشناس امنیت سایبری معتقد است موضوع مهم، بازنگری در ساختار حکمرانی سایبری و تمرکز وظایف راهبردی در یک نهاد مرکزی مقتدر و پاسخگو است چراکه چنین نهادی می‌تواند به‌عنوان مرجع ملی امنیت سایبری، هماهنگی بین دستگاهی را بهبود بخشد؛ همچنین سیاست‌گذاری کلان را با انسجام بیشتری هدایت کند تا بتوان هنگام مواجهه با حملات سایبری، پاسخ سریع و مؤثرتری ارائه داد.
خدادادی، ارتقای امنیت دیجیتال بانک‌ها و سایر زیرساخت‌های کشور را بدون تقویت بنیان‌های زیرساختی و انسانی آن ممکن نمی‌داند و از ایجاد مراکز تخصصی پیشرفته مانند آزمایشگاه‌های کشف تهدید، توسعه و استقرار تجهیزات بومی، به‌روزرسانی قوانین و آیین‌نامه‌های سایبری مطابق با تحولات جهانی و از همه مهم‌تر، سرمایه‌گذاری هدفمند بر نیروی انسانی متخصص به عنوان گام‌های کلیدی در این مسیر یاد می‌کند. این فعال حوزه سایبری می‌افزاید: «جلوگیری از مهاجرت نخبگان حوزه امنیت اطلاعات و فراهم کردن بستر مشارکت و ماندگاری آنان یک اقدام استراتژیک به شمار می‌رود.»
این کارشناس معتقد است، همکاری فعال با کشورهایی که در برابر تهدیدات پیچیده سایبری، تجارب موفقی داشته‌اند نیز می‌تواند بخشی از خلأهای فناورانه و دانشی را پوشش دهد. در این زمینه، مشارکت‌های فناورانه و تبادل دانش با قدرت‌های سایبری مانند چین و روسیه، فرصتی مناسب برای انتقال تجربیات کاربردی خواهد بود.

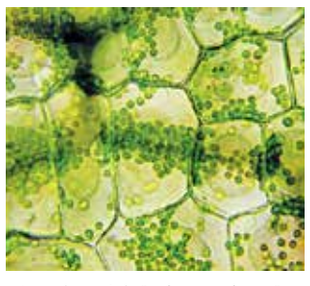
الزامات کلیدی امنیت سایبری برای بانکداری

سجاد عابدی هم به عنوان یک فعال حوزه سایبری در این‌باره به «ایران» می‌گوید: « تغییراتی که در بخش بانکداری دیجیتال رخ داده، منجر به ظهور تهدیدات سایبری مختلف در این صنعت شده به گونه‌ای که فعالیت‌های اصلی و کلیدی دپارتمان‌های مالی می‌تواند بر اثر تهدیدات پیش‌بینی نشده سایبری، به طور کامل مختل شود.»
این کارشناس با اشاره به اینکه به موازات دیجیتالی شدن اکثر فرآیندهای کاری و همچنین تنش‌های ژئوپلیتیکی، مؤسسات مالی نیازمند ارائه پاسخی قدرتمند به تهدیدات سایبری هستند، می‌افزاید: «در چنین فضایی، مدیریت تهدیدات و پروتکل‌های امنیت شبکه، اهمیت بسزایی دارد و تیم‌های اجرایی باید از امنیت عملیات تجاری، انطباق با مقررات و استانداردها و همچنین اثربخشی زیرساخت‌های امنیت شبکه اطمینان حاصل کنند.»
این فعال حوزه سایبری با توصیه به مؤسسات مالی برای اتخاذ رویکردی که در آن شبکه و امنیت در یک راهکار واحد ارائه می‌شوند، می‌افزاید: «این رویکرد یکپارچه، تأثیر بسزایی در مقابله مؤثر با چالش‌های مربوط به امنیت سایبری دارد.»
عابدی با اشاره به الزامات کلیدی امنیت سایبری برای بانکداری، ویژگی‌های حیاتی یک راهکار امنیتی ایده‌آل را «نظارت جامع بر کل سطح حملات»، «مکانیسم‌های دفاعی در برابر تهدیدات پیچیده» و «یکپارچگی در ساختار هوشمند آی‌تی» می‌داند و می‌افزاید: « با توجه به «بانکداری نوین»، «یکپارچگی با IoT» و همچنین استفاده از «محیط ابری» (Cloud)، حفظ نظارت بر شبکه اهمیت خاصی پیدا می‌کند.»
این فعال حوزه امنیت سایبری با بیان اینکه دوره استفاده از راهکارهای امنیتی چندگانه و مجزا به پایان رسیده است، امنیت سایبری مدرن را نیازمند راهکارهای یکپارچه‌ای می‌داند که می‌توانند اتوماسیون را گسترش داده و نیاز به نظارت مداوم را کاهش دهند.
وی معتقد است، راهکار امنیتی policy as code یکی از روش‌های دستیابی به این هدف است که از اجرای مداوم و خودکار سیاست‌های امنیتی در سراسر شبکه، اطمینان حاصل می‌کند.
عابدی می‌افزاید: «ساختار متنوع آی تی که شامل محیط‌های فیزیکی و ابری (cloud) می‌شود، به کنترل امنیتی سریعی نیاز دارد تا بتواند پاسخگوی شرایط متغیر و تهدیدات در حال تحول باشد. همان‌طور که مؤسسات مالی، پیچیدگی‌های فراوانی را تجربه می‌کنند، راهکارهای امنیتی آنها مانند policy as code نیز باید قابل انطباق بوده و این اطمینان حاصل شود که سیاست‌های امنیتی با تغییرات زیرساخت، هماهنگ هستند.
وی، عنصر انسانی را نیز یکی از فاکتورهای اساسی در ارتقای امنیت سایبری زیرساخت‌های بانکی می‌داند و می‌افزاید: «مؤسسات مالی به متخصصان ماهر نیاز دارند تا بتوانند از پتانسیل پلتفرم‌ها و سیستم‌های جدید استفاده کنند. محدود بودن تعداد متخصصان در برخی حوزه‌های خاص و همچنین ناکافی بودن دانش مرتبط، چالش‌های بیشتری ایجاد می‌کند، بنابراین در شرایط فعلی باید به این موضوع توجهی ویژه داشت.»
به اعتقاد وی، با تکامل هر چه بیشتر بانکداری در فضای دیجیتالی، ایجاد تعادل بین نوآوری، تهدیدات امنیت سایبری و انطباق با مقررات بسیار مهم است و پذیرش این المان‌های سه‌گانه می‌تواند فرصت‌های بی‌نظیری ایجاد کند تا از تأمین امنیت سایبری بانک‌ها و مؤسسات مالی، اطمینان حاصل شود.

انقلاب در تولید محصولات کشاورزی

انرژی

آرزو کیهان
گروه علم و فناوری



پژوهشگران مؤسسه فناوری ماساچوست (MIT) موفق شدند عملکرد یکی از کندترین اما حیاتی‌ترین آنزیم‌های طبیعت یعنی «روبیسکو» که نقش عمده‌ای در فتوسنتز گیاهان دارد را با یک روش پیشرفته تکامل درون‌سلولی، بهبود بخشند. این آنزیم معمولاً مستعد واکنش‌های زائد با اکسیژن است، اما نسخه جدید باکتریایی آن، برای عملکرد بهتر در محیط‌های غنی از اکسیژن تکامل یافته است و می‌تواند با بهبود فرآیند فتوسنتز، راه افزایش بازده محصولات کشاورزی را هموار کند. در فرآیند فتوسنتز، آنزیم «روبیسکو» واکنش کلیدی ورود دی‌اکسیدکربن به ترکیبات آلی به منظور تولید قندها را کاتالیز می‌کند اما این کار در مقایسه با سایر آنزیم‌های فتوسنتزی، به کندی انجام می‌شود چراکه تنها یک تا ۱۰ واکنش در ثانیه صورت می‌گیرد. پیش‌تر، مطالعاتی که روی آنزیم «روبیسکو» انجام شده بود، با تکنیک «تکامل هدایت‌شده»، بهبودهایی کوچک در پایداری و محلولیت این آنزیم پدید آورده بود. در این روش، پروتئین طبیعی به‌طور تصادفی دچار جهش می‌شد و سپس برای ویژگی‌های مطلوب جدید مورد غربالگری قرار می‌گرفت. اما تیم MIT از روشی جدیدتر با نام «MutaT7» استفاده کرد. این تکنیک با فراهم کردن امکان جهش‌زایی و غربالگری درون سلول‌های زنده، سرعت فرآیند را به‌شکل چشمگیری افزایش می‌دهد. همچنین این روش اجازه می‌دهد جهش‌های بیشتری در ژن هدف ایجاد شود. از پیامدهای بالقوه این پیشرفت می‌توان به افزایش سرعت فتوسنتز در گیاهان مهندسی‌شده، تولید محصولات کشاورزی با بازده بالاتر در شرایط اقلیمی متغیر و کاربرد در زیست‌فناوری برای جذب بیشتر دی‌اکسید کربن از جو اشاره کرد. با این روش بهینه‌سازی فتوسنتز، می‌توان به نوعی به انقلاب زیستی در کشاورزی مدرن نزدیک شد.

جراحی کیسه صفرای خوک با روبات هوشمند

روبات

برسام جنتی
گروه علم و فناوری

SRT-H، یکی از روبات‌های هوشمندی که تنها با تماشا ویدئوهای جراحی آموزش دیده، حالا موفق شده است با کمک فناوری یادگیری ماشین(ML) و بدون دخالت انسان، مراحل حساس جراحی خارج‌سازی کیسه صفرا از بدن یک خوک مرده را با دقت بالا انجام دهد. حذف کامل کیسه صفرا توسط روبات SRT-H در قالب ۸ عمل جراحی مختلف انجام شد. این روبات از همان ساختار یادگیری ماشینی استفاده می‌کند که در چت جی‌پی‌تی به کار رفته است به همین دلیل هم می‌تواند به فرمان‌های صوتی کارکنان پزشکی پاسخ دهد و به‌طور همزمان در حین انجام عمل، خود را اصلاح کند و یاد بگیرد. پژوهشگران دانشگاه جانزهاپکینز معتقدند که این فناوری می‌تواند طی دهه آینده، روی انسان‌ها نیز آزمایش شود و درنهایت، سامانه‌های خودران جراحی توسعه یابند که بتوانند در محیط‌های واقعی و پیچیده پزشکی، تصمیم‌گیری کنند و عمل‌های جراحی را با کمترین میزان خطا انجام دهند. در آینده، قرار است روبات SRT-H مهارت‌های خود را در انجام انواع جراحی‌ها گسترش دهد و آموزش ببیند تا به‌صورت مستقل‌تر عمل کند و شاید روزی بتواند بدون نیاز به نظارت یا راهنمایی خارجی، جراحی‌های موفق انجام دهد. «جان مک‌گراث»، کارشناس برجسته جراحی روباتیک در بریتانیا، نتایج را بسیار امیدوارکننده توصیف کرد.

تولد اولین گاومیش شبیه‌سازی شده جهان در تبت

علم

اولین گاومیش شبیه‌سازی شده جهان در تبت به دنیا آمد. این گاومیش با وزن ۳۳٫۵ کیلوگرم با استفاده از روش شبیه‌سازی سلول سوماتیک (یک روش آزمایشگاهی برای ایجاد یک کپی ژنتیکی از یک موجود زنده) متولد شده است. این تولد نشان‌دهنده پیشرفت علمی قابل توجه در پرورش دام، بویژه در محیط‌های مرتفع مانند تبت است. گاومیش‌ها برای اقتصاد و محیط زیست تبت، حیاتی هستند و علاوه بر گوشت و شیر، از مدفوع آنها برای حمل‌ونقل و سوخت مورد نیاز جوامع ساکن در فلات چینگهای-شی زانگ استفاده می‌شود. به گزارش ایسنا، شبیه‌سازی، کلون‌سازی یا همسانه‌سازی (Cloning) فرآیند ساختن یک کلون یا همسانه از چیزی است و در زیست‌شناسی به طور کلی به فرآیندهایی که برای آفرینش از پاره‌هایی از دی‌ان‌ای، همسانه‌سازی DNA به کار می‌رود، گفته می‌شود. این اصطلاح در مواردی که جاندارانی مانند باکتری، حشره یا گیاه به طور غیرجنسی تولید مثل می‌کنند نیز به کار می‌رود. محققان همچنین از انتخاب کل ژنوم استفاده کردند؛ روشی که به شناسایی و تکثیر حیوانات با صفات ژنتیکی مطلوب مانند اندازه و تولید شیر کمک می‌کند. این پروژه در سال ۲۰۲۳ توسط محققان دانشگاه ججیانگ (Zhejiang) در شرق چین که رهبری این کار علمی را بر عهده داشتند، آغاز شد. هدف اصلی، افزایش کیفیت نژادهای گاومیش قوی‌تر، پربارتر و مقاوم‌تر کردن آنها در برابر بیماری بود. دستور کار همچنین کمک به ایجاد یک سیستم اصلاح نژاد مدرن، متناسب با شرایط منحصربه‌فرد زمین‌های مرتفع تبت بود. گاومیش‌ها برای زندگی در فلات تبت، جایی که هزاران سال است در آن اهلی شده‌اند، ضروری هستند. توانایی آنها در زنده ماندن در جایی که اکثر دام‌ها نمی‌توانند، وجود آنها را برای امنیت غذایی در این منطقه حیاتی می‌کند.