پژوهشگاه
فضای مجازی

گزارش کوتاه سیاستی - ۱۶

حاکمیت دیجیتال اسرائیل

پژوهشگاه فضای مجازی
خرداد ۱۴۰۵

طرح مسئله

قدرت فناورانه اسرائیل بر پایه‌ای بنا شده بود که با الزامات امنیت ملی آن اصطکاک داشت: یک اکوسیستم فناوری توسعه‌یافته که نبض پردازش و نگهداری حیاتی‌ترین داده‌هایش در دست پلتفرم‌های خارجی می‌تپید. این وابستگی زیرساختی، معماری دیجیتال رژیم را از یک مزیت رقابتی و موتور توسعه به یک آسیب‌پذیری استراتژیک تبدیل کرده بود. مؤسسه مطالعات امنیت ملی (INSS) در گزارشی روند تکامل حاکمیت دیجیتال اسرائیل را در سه فاز صورت‌بندی می‌کند و چشم‌اندازی برای ارزیابی حال و آیندهٔ امنیت دیجتال اسرائیل به دست می‌دهد:

- در ابتدا دولت «کاربر» (وابسته به مصرف خدمات وارداتی) بود،
- اکنون در موارد زیادی «مالک» (مسلط بر لایهٔ فیزیکی و معماری زیرساخت) است
- و در نهایت باید «تولیدکننده» (مستقل در کل زنجیره تأمین، از تراشه تا الگوریتم) باشد.

ارزیابی روندهای اخیر نشان می‌دهد اسرائیل اکنون در مسیر یک گذار پرهزینه برای خروج از مرحله نخست و تثبیت موقعیت در جایگاه مالکیت است.

الگوی پیشین دکترین فناوری اسرائیل سال‌ها بر پایه ترجیح منافع اقتصادی و سرعت نوآوری (چابکی توسعه) استوار بود؛ رویکردی که تل‌آویو را با رضایت نسبی در فاز دولتِ کاربر نگه می‌داشت. اما تغییر برآوردهای امنیتی و تصمیم برای گذار به فاز دولتِ مالک، پرده از یک چالش ساختاری میان لایهٔ سیاست‌گذاری و فاز عملیاتی برداشت. مصداق بارز این شکاف اجرایی، سرنوشت برنامه ملی پنج‌ساله هوش مصنوعی است. این طرح که در سال ۲۰۲۱ با بودجه‌ای معادل ۵٫۲۶ میلیارد شکل (حدود ۱٫۴۸ میلیارد دلار) به تصویب رسید، در مرحلهٔ اجرا با کندی و موانع بروکراتیک شدیدی روبرو شد؛ به‌نحوی که تا آوریل ۲۰۲۵ تنها یک‌پنجم از این بودجه تخصیص یافت. پیامد مستقیم این انسداد اداری آن بود که با وجود راه‌اندازی یک آزمایشگاه محاسبات سریع (HPC) در سال ۲۰۲۴ برای تست سیستم‌های خنک‌کننده، هیچ GPU Cluster در سطح ملی عملیاتی نشد و اهداف بنیادین طرح بدون تأمین مالی رها شدند. این کارنامه به‌روشنی نشان می‌دهد که اسرائیل، گرچه در تدوین اسناد بالادستی و استراتژی‌پردازی چابک عمل می‌کند، اما در پیاده‌سازی پروژه‌های کلانی مثل بومی‌سازی و استقرار فیزیکی زیرساخت‌های حاکمیتی، دچار انقطاع است.

تلاش برای حاکمیت حقوقی بر بسترهای خارجی

نخستین واکنش اسرائیل به خطر وابستگی مطلق، تلاش برای اعمال حاکمیت حقوقی بر بسترهای خارجی بود؛ رویکردی که برای نمونه در کلان‌پروژه نیمبوس تبلور یافت. این ابر حاکمیتی که در آوریل ۲۰۲۱ با ارزشی بالغ بر ۱٫۲ میلیارد دلار به شرکت‌های گوگل‌کلود و آمازون واگذار شد، بر پارادایم بومی‌سازی داده‌ها استوار است. شروط حقوقی مندرج در این قرارداد، پیمانکاران بین‌المللی خدمات ابری را ملزم به احداث زیرساخت‌های فیزیکی و استقرار مراکز داده در محدودهٔ سرزمینی، ذخیره‌سازی اطلاعات در داخل مرزها و سلب حق قطع یا محدودسازی خدمات تحت فشارهای ژئوپلیتیک و تحریم‌های خارجی می‌کند. با این حال، لایهٔ عملیاتی این پروژه ابعاد پیچیده‌تری از رصد اطلاعاتی را در خود جای داده است؛ بر اساس مکانیزم‌های تنظیمی، این شرکت‌ها متعهد شده‌اند از طریق سیگنال‌های پنهان در فرآیندهای مالی و پرداختی، یک سیستم هشدار زودهنگام ایجاد کنند تا در صورت مواجه با احکام دادگاه‌های خارجی یا درخواست‌های دسترسی بین‌المللی، دولت اسرائیل را فوراً مطلع کنند.

اسـرائیل بـرای مهـار آسیب‌پذیری‌هـای حقوقـی ایـن مـدل، به‌ویـژه ریسـک تبعیـت شـرکت‌های آمریکایـی از فرامیـن قضایـی فـرامرزی (ماننـد Cloud Act) یـا توقـف خدمـات تحـت فشـار تحریـم، دو لایـه حفاظتـی تعبیـه کـرد:

- ۱. لایـه حقوقی-قـراردادی: ممنوعیـت مطلـق توقـف خدمـات بـه دلایـل سیاسـی یـا تحریمـی در متـن قـرارداد.
- ۲. لایه رصـد اطلاعاتـی و جبرانـی: طراحـی یـک پروتـکل هشـدار مخفـی ناظـر بـر تراکنش‌هـا. بـر اسـاس اسـناد مستنـدِ ایـن سـازوکار، شـرکت‌های چندملیتـی موظفنـد در صـورت مواجهـه بـا احـکام دادگاه‌هـای خارجـی بـرای افشـای داده‌هـای اسـرائیلی، از طریـق سـیگنال‌های پنهـان تعبیه‌شـده در فرآیندهـای پرداخـت مالـی، دولـت را مطلـع سـازند تـا فرصـت پدافنـد حقوقـی یـا سـایبری بـرای تل‌آویـو فراهـم شـود.

ایـن الگـو نشـان‌دهندهٔ تلاشـی بـرای تثبیـت حاکمیـت حقوقـی بـدون در اختیـار داشـتن مالکیـت زیرسـاخت فیزیکـی اسـت؛ رویکـردی کـه اگرچـه مخاطـرات آنـی را کاهـش می‌دهـد، امـا آسیب‌پـذیری بنیادیـنِ ناشـی از اتـکا بـه معمـاری کلان خارجـی را به‌طـور کامـل مرتفـع نمی‌کنـد.

مالکیت بر بسترها

درک محدودیت‌های حاکمیت حقوقی، تل‌آویو را به سمت سرمایه‌گذاری مستقیم در توسعه زیرساخت‌های پردازشی بومی سوق داد؛ گامی که با هدف تثبیت قطعی در فاز دوم حاکمیت یعنی دولتِ مالک برداشته شد. پیشبرد پروژه‌هایی نظیر توسعه ابررایانه نبیوس (ارائه‌دهنده زیرساخت ابری هوش مصنوعی که در سال ۲۰۲۵ مجری استقرار ابررایانه ملی اسرائیل شد؛ توان محاسباتیِ این زیرساخت با وجود بومی بودن لایهٔ مدیریت، وابستگی مطلقی به خوشه‌های پردازشیِ وارداتی نظیر تراشه‌های پیشرفته شرکت آمریکایی انویدیا دارد) و احداث سایت‌های پردازشی مستقل مانند آلفا کمپوس (پروژه‌ای ۱.۳ میلیارد شِکِلی، جهت احداث یک دیتاسنترِ زیرزمینی، فوق‌امنیتی و ۴۲ مگاواتی در شهر نتانیا که هم‌اکنون در مرحله ساخت است و بهره‌برداری عملیاتی از آن برای سال ۲۰۲۷ هدف‌گذاری شده است)، بازتابی از تلاش برای در اختیار گرفتن بستر فیزیکی داده‌هاست.

توسعه این بسترها دو الزام امنیتی و زیرساختی دارد: ۱. تأمین معماری زیرزمینی و فوق‌امنیتی؛ مثلاً پروژه‌هایی نظیر آلفا کمپوس مستقیماً با هدف پدافند غیرعامل در برابر تهدیدات سایبری-کینتیک و حملات موشکی به زیرساخت‌های حیاتی طراحی شده است.

۲. استقرار خوشه‌های متراکم پردازشی، تل‌آویو را با یک چالش پنهان زیرساختی مواجه کرده است: تأمین مگاوات‌ها انرژی پایدار در شبکه برق ایزوله اسرائیل (به تعبیر INSS جزیره برقی) دشوار است زیرا شبکهٔ برق اسرائیل فاقد هرگونه اتصال به کشورهای همسایه است.

تولیدکنندگی دور از دسترس

مسیر برای ورود به فاز سوم (دولتِ تولیدکننده) دشوار است. علی‌رغم توانمندی رژیم صهیونیستی در لایه‌های نرم‌افزاری و طراحی الگوریتم، ایجاد ساختارهای تولیدکننده فناوری‌های جدید به قطعات وارداتی و به‌طور خاص پردازنده‌های شرکت انویدیا احتیاج دارد؛ به‌نحوی‌که علی‌رغم فعالیت بیش از ۱۵۰ مرکز تحقیق و توسعه تراشه و نقش کلیدی در طراحی معماری شبکه‌های پردازشی، توانایی تولید فیزیکی سیلیکون‌های پیشرفته (گره‌های زیر ۵ نانومتر) در داخل مرزهای اسرائیل وجود ندارد. تعلیق پروژه ۲۵ میلیارددلاری احداث کارخانه تراشه‌سازی شرکت اینتل در کریات‌گات نیز دستیابی به این هدف را دشوارتر کرده است و هنوز معماری پردازشی رژیم به حلقه‌های خارجی (به‌ویژه شرکت TSMC تایوان) و واردات قطعات نهایی وابسته است.

توصیه‌های INSS برای تقویت حاکمیت ملی

اول، باید یک استراتژی برای حاکمیت دیجیتال ملی تدوین شود که به‌طور رسمی زیرساخت‌های ابری، مراکز داده، زیرساخت‌های هوش مصنوعی و داده‌ها را به‌عنوان دارایی‌های ملی استراتژیک مشابه زیرساخت‌های انرژی، آب و ارتباطات تعریف کند.

دوم، برای پروژه‌های زیرساخت دیجیتال باید ساختارهای سرمایه‌ای اختصاصی در نظر گرفته شود تا ریسک شکست را کاهش داده و کارآفرینی بخش خصوصی را در مقیاس ملی امکان‌پذیر کند.

سوم، باید یک سیاست زیرساختی یکپارچه در بخش انرژی اجرا شود که مراکز داده و زیرساخت‌های هوش مصنوعی را به‌عنوان مصرف‌کنندگان استراتژیک برق به رسمیت بشناسد و در برنامه‌ریزی تولید، شبکه و ذخیره‌سازی، اولویت را به آنها بدهد.

چهارم، باید یک چارچوب حاکمیتی برای ابر هیبریدی و مدیریت داده‌ها تدوین شود که قوانین روشنی را برای ذخیره‌سازی و پردازش داده‌های حساس تعریف کند و امکان ادغام بین ابر دولتی، ابر خصوصی و خدمات ابر جهانی را تحت نظارت فراهم کند. این چارچوب باید امنیت، حریم خصوصی، رقابت و نوآوری را متعادل کند.

منابع:

1. https://www.inss.org.il/publication/digital-sovereignty/
2. https://www.inss.org.il/wp-content/uploads/2026/02/e230226-1.pdf
3. https://www.israeltechinsider.com/p/national-ai-program-stalls-stealthy
4. https://www.jpost.com/defense-and-tech/article-869063
5. https://www.inss.org.il/publication/electricity-system/?utm_source=chatgpt.com
6. https://www.calcalistech.com/ctechnews/article/sjxr52eh0

دیگر گزارش‌ها



پژوهشگاه فضای مجازی
تیر ۱۴۰۵



پژوهشگاه فضای مجازی
خرداد ۱۴۰۵

دیگر گزارش‌ها



پژوهشگاه فضای مجازی
اردیبهشت ۱۴۰۵



پژوهشگاه فضای مجازی
خرداد ۱۴۰۵

WWW
THECSRI
.IR

«گزارش کوتاه سیاستی» نام دسته‌ای از پژوهش‌های فشرده و مسئله‌محور «پژوهشگاه فضای مجازی» است که با هدف به‌روزرسانی سریع دانش سیاستی مخاطبان طراحی شده است. این گزارش‌ها با خلاصه‌سازی پژوهش‌های تفصیلی، دسترسی سیاست‌گذاران، تصمیم‌گیران و مدیران را به توصیه‌های سیاستی تسهیل می‌کنند.

پژوهشگاه
فضای مجازی