

شرط بندی بد «سیلیکون ولی» بر روی خلیج (فارس)

چرا پروژه برون سپاری هوش مصنوعی از آغاز محکوم به فنا بود.

آرون بی آرتنیک

۱۱ ژوئن ۲۰۲۶

این مقاله در مجله «سیاست خارجی» آمریکا به آدرس ذیل منتشر شده است:

<https://www.foreignaffairs.com/persian-gulf/silicon-valleys-bad-bet-gulf>



بعد از حمله به شارجه، امارات متحده عربی، مارچ ۲۰۲۶

اشاره:

این جستار که در مجله معتبر Foreign Affairs منتشر شده، توسط یکی از برادران دانشمند و دیپلمات محترم به اینجانب معرفی شد که بدینوسیله قدردانی میکنم. جان کلام مقاله این است که حملات سنگین موشکی ایران در جنگ اخیر نشان داد که سیاست شرکتهای آمریکائی برای ایجاد مراکز داده در کشورهای حاشیه خلیج فارس از آغاز اشتباه بوده است و باید هرچه سریعتر این مراکز به نقاط امن تری مانند ایالات متحده منتقل شوند. به نظر اینجانب مطرح شدن این ایده، خصوصا در شرائطی که ناسیونالیسم اقتصادی در آمریکا به سرعت رو به گسترش است، بایستی زنگ خطری برای اعراب خلیج فارس باشد که میخواهند با پول، همه چیز اعم از امنیت و فناوری و پرستیژ و سایر موارد را بخرند و یقینا آثار جراحت درافتادن با ایران تا سالها بر پیکر ضعیف و البته پر زرق و برق اعراب باقی خواهد ماند. امیداست که درس گرفته باشند و درس گرفته باشیم. خداوند روح رهبر شهید و طهرانی مقدم و حاجی زاده را شاد کند.

دکتر حمیدرضا حقیقت – خرداد ۱۴۰۵

وقتی دونالد ترامپ، رئیس جمهور آمریکا، در ماه مه ۲۰۲۵ از سفر به خلیج فارس بازگشت، از قراردادهای دوجانبه ۲٫۲ تریلیون دلاری که ایالات متحده با قطر، عربستان سعودی و امارات متحده عربی امضا کرده بود، خبر داد. علاوه بر مشارکتهای دفاعی و اقتصادی، بخش قابل توجهی از این قراردادها به هوش مصنوعی و به طور خاص، ساخت زیرساختهای هوش مصنوعی آمریکا در خلیج فارس اختصاص داشت. پیشنهاد شرکت های فناوری آمریکایی قانع کننده بود: انرژی ارزان فراوان، دسترسی به سرمایه از صندوق های ثروت ملی، موانع نظارتی کمتر برای ساخت مراکز داده و تأیید دولت ایالات متحده برای فروش تراشه های قبلاً محدود شده. برای واشنگتن، این قراردادها فرصتی برای سرعت بخشیدن به پیشرفت ها در قابلیت های هوش مصنوعی آمریکا و تشویق کشورهای خلیج فارس به همکاری کمتر با چین در زمینه هوش مصنوعی ارائه می داد. اما رویدادهای اخیر یک خطر بزرگ را آشکار کرده است: زیرساخت هایی که چنین فناوری حیاتی به آن متکی است، مورد حمله قرار گرفته و در آتش جنگی گرفتار شده است که برای آن آماده نبود. در اول مارس، ایران دو مرکز داده خدمات وب آمازون در امارات متحده عربی را با رگباری از پهپادهای شاهد هدف قرار داد. یک مرکز خدمات وب آمازون در بحرین نیز آسیب دید، احتمالاً با بقایای یک حمله در نزدیکی آن. سپاه پاسداران انقلاب اسلامی ادعا کرد که این تأسیسات از عملیات هوش مصنوعی ارتش ایالات متحده پشتیبانی می کنند، که می تواند آنها را طبق قوانین درگیری مسلحانه به اهداف مشروع تبدیل کند. اگرچه ارتش ایالات متحده از AWS (سرویس وب آمازون) استفاده می کند، اما هیچ مدرک عمومی در دسترس نیست که نشان دهد چگونه که سپاه پاسداران ایران ادعا کرد این تأسیسات خاص از عملیات نظامی ایالات متحده پشتیبانی کرده اند. بستن مؤثر تنگه هرمز و اختلال در دریای سرخ، کابل های زیردریایی را که بخش عمده ای از ترافیک داده ها بین آسیا، اروپا و خلیج فارس را حمل می کنند، نیز در معرض خطر قرار داده است. این کمپین ها هزینه های کوتاه مدت جدی را بر کاربران این شبکه ها، چه غیرنظامی و چه نظامی، تحمیل می کنند. اما مشکل بزرگتر این است که سرمایه گذاری در خلیج فارس محدود به همکاری های جدید دوجانبه فناوری بین ایالات متحده و تعداد انگشت شماری از پادشاهی های خلیج فارس نیست و شبکه ای از وابستگی های دیجیتال ایجاد کرده است که اکنون به ده ها کشوری که هیچ نقشی در این ترتیبات نداشتند و از خطری که متحمل می شدند، آگاه نبودند، گسترش یافته است. شرط بندی ایالات متحده روی خلیج فارس برای زیرساخت هوش مصنوعی یک اشتباه بود. واشنگتن با تشویق شرکت های آمریکایی به ساخت زیرساخت های حیاتی آسیب پذیر و غیرفعال در خلیج فارس، روی یک محیط امنیتی ناپایدار قمار کرده که اغلب، حداقل تا حدی، نتیجه مداخله ایالات متحده، از جمله آخرین جنگ با ایران است. هنگامی که سرمایه گذاری های زیرساخت دیجیتال انجام می شود، وابستگی هایی که ایجاد می شوند، به سختی قابل جبران هستند: پروژه های زیرساخت فیزیکی چند میلیارد دلاری را نمی توان به سادگی متوقف کرد و سرمایه آنها را نیز نمی توان به راحتی توزیع کرد، به ویژه هنگامی که به عنوان پایه و اساس یکی از ارزشمندترین فناوری های جهان عمل می کنند. هزینه هایی که شرکت ها، مصرف کنندگان و منافع امنیت ملی ایالات متحده اکنون با آن مواجه هستند، احتمالاً ادامه خواهد یافت یا حتی بیشتر افزایش خواهد یافت. برخی از پروژه ها در حال حاضر به این نقطه بازگشت ناپذیر رسیده اند و شرکت ها احتمالاً مجبور خواهند شد این هزینه ها را متحمل شوند. با این حال، برای سرمایه گذاری هایی که در مراحل اولیه ساخت و برنامه ریزی هستند، شرکت های فناوری باید در مورد چرخش خود به خلیج فارس تجدید نظر کنند و با واشنگتن همکاری کنند تا پروژه ها را به جایی که امن ترین است و با افزایش هزینه های انرژی و سایر هزینه ها، به طور فزاینده ای رقابتی می شود، یعنی ایالات متحده برگردانند. واکنش زنجیره تأمین خلیج فارس تقریباً ۱٫۵ درصد از ظرفیت محاسباتی جهان را در خود جای داده است، تقریباً دو برابر سهم آن از جمعیت جهان. این ممکن است کم به نظر برسد، اما ظرفیت آن سالانه حدود نه درصد در حال افزایش است. معاملات بلندپروازانه ای که از سفر خلیج فارس ترامپ در سال ۲۰۲۵ حاصل شد، بخش قابل توجهی از این رشد سریع است. شرکت آمریکایی AMD، یک شرکت تراشه سازی، از همکاری ۱۰ میلیارد دلاری با Humain، شرکت هوش مصنوعی صندوق سرمایه گذاری مستقل عربستان سعودی، خبر داد. شرکت آمریکایی Nvidia، سازنده تراشه، متعهد به ارسال ۱۸۰۰۰ تراشه پیشرفته برای تقویت زیرساخت هوش مصنوعی عربستان سعودی شد. یک کنسرسیوم از شرکت های آمریکایی، برنامه ریزی برای ایجاد یک پردیس هوش مصنوعی با شرکت هوش مصنوعی اماراتی G42 را تحت پوشش مشارکت شتاب دهی هوش مصنوعی ایالات متحده و امارات متحده عربی که در این سفر امضا شد، آغاز کرد. کابل های زیردریایی در دریای سرخ، حدود ۹۰ درصد از ترافیک داده بین اروپا و آسیا و حدود ۱۷ درصد از کل ترافیک اینترنت جهانی را حمل می کنند. هنگامی که مراکز داده آمازون در امارات متحده عربی از دسترس خارج شدند، آسیب در سراسر اقتصاد دیجیتال خلیج فارس گسترش یافت و بانک های بزرگ، برنامه های پرداخت، خدمات درخواست خودرو و تحویل، ارائه دهندگان نرم افزارهای سازمانی و برخی از عملیات حداقل یک شرکت بزرگ داده آمریکایی، Snowflake، را از کار انداخت. اما اثرات این حمله محدود به خاورمیانه نبود.

بسیاری از شرکت‌های آسیب‌دیده اصلاً در منطقه فعالیت نمی‌کردند، بلکه از ارائه‌دهندگان ابری استفاده می‌کردند که حجم کار خود را از طریق سرورهای مستقر در خلیج فارس هدایت می‌کردند. و برخی ممکن است حتی از عبور داده‌هایشان از خلیج فارس تا زمان از کار افتادن آن سرورها آگاه نبودند. چارچوب ساخت هوش مصنوعی خلیج فارس برای چنین خطراتی طراحی نشده بود. بخش عمده‌ای از آن توسط ابتکار Pax Silica، تلاشی به رهبری ایالات متحده برای ایمن‌سازی زنجیره‌های تأمین هوش مصنوعی، هدایت شده بود. از زمان ایجاد این ابتکار در ماه دسامبر، قطر، امارات متحده عربی و ۱۲ کشور دیگر در اروپا و آسیا این توافق‌نامه را امضا کرده‌اند. اما سازوکارهای پیشنهادی آن - از جمله سرمایه‌گذاری‌های مشترک، سرمایه‌گذاری مشترک و قدرت خرید مشترک برای تضمین معاملات مطلوب‌تر - برای مدیریت رقابت فناوری در زمان صلح با چین طراحی شده بود، نه برای دفاع از زنجیره تأمین فیزیکی در برابر موشک‌ها و پهپادها. آنها به نگرانی‌های مهم مربوط به رقابت، از جمله اقداماتی برای جلوگیری از انتقال تراشه‌های پیشرفته به دشمنان ایالات متحده توسط کشورها؛ بررسی ساختارهای مالکیت خارجی، مانند روابط سابق G42 با هواوی؛ و ایجاد الزامات گزارش‌دهی و نظارت برای سخت‌افزارهای آمریکایی مستقر در خارج از کشور پرداختند. اما فراتر از یک کلیشه مبهم که از تلاش‌ها برای «تقویت بیشتر همکاری‌های اقتصادی و امنیت ملی» حمایت می‌کرد، چیز زیادی در مورد آنچه که وقتی خود زیرساخت به یک هدف نظامی تبدیل می‌شود، اتفاق می‌افتد، نگفتند. چالش تبدیل شدن یک مرکز داده تجاری به یک هدف نظامی قابل پیش‌بینی بود. محققان حقوقی سال‌ها در مورد این احتمال بحث کرده‌اند. کابل‌های زیردریایی همچنین در دریای بالتیک، اطراف تایوان و حتی در دریای سرخ، جایی که جنگ در اطراف یمن در سال ۲۰۲۴ به سه کابل آسیب رساند، هدف قرار گرفته‌اند. آنچه در حمله ماه مارس به AWS جدید بود، تنها روش بود: حملات موشکی و پهپادی به مراکز داده به جای کشیدن لنگرها در کف اقیانوس. ایالات متحده دهه‌ها صرف ایجاد چارچوب‌هایی برای محافظت از زیرساخت‌های حیاتی داخلی در برابر دقیقاً همین نوع تهدید کرده است، از جمله با تعیین بخش‌های زیرساختی خاص به عنوان حیاتی و الزام استانداردهای امنیتی فیزیکی برای شبکه برق. اما به دلایلی، شاید به دلیل احساس کاذب امنیت منطقه‌ای یا به دلیل تمایل به عدم رنجاندن شرکای مذاکره‌کننده خود همین تفکر را در مورد زیرساختی که شرکت‌های آمریکایی را به ساخت آن در خارج از کشور تشویق می‌کرد، به کار نبرد. بخشی از معامله که برای بسیاری از شرکت‌ها، محاسبات ریاضی که خلیج فارس را در ماه مه ۲۰۲۵ جذاب می‌کرد، دیگر معتبر نیست. هیچ راه واقع‌بینانه‌ای برای محافظت از یک مرکز داده تجاری در برابر موشک‌های کروز یا انبوهی از پهپادها وجود ندارد. مقاومت‌سازی یک مرکز داده به گونه‌ای که گویی یک تأسیسات نظامی است، هم بسیار گران و هم در نهایت ناکافی خواهد بود. همانطور که سال‌ها جنگ بین روسیه و اوکراین ثابت کرده است، هیچ پدافند هوایی نمی‌تواند ۱۰۰ درصد حملات ورودی را رهگیری کند. مهمترین مسئله برای شرکت‌ها، مسئولیت قانونی است. ابزاری که بسیاری از شرکت‌ها توقف عملیات خود را توجیه کرده و در نتیجه مسئولیت خود را محدود کرده‌اند، اعلان‌های فورس ماژور است که عملاً یک شرکت را از انجام عملیات مورد انتظار خود به دلیل رویدادی خارج از کنترلش معاف می‌کند. اما دادگاه‌ها و مفسران حقوقی اعلام کرده‌اند که چنین دفاعیاتی ممکن است در خاورمیانه، که سابقه مستندی از بی‌ثباتی سیاسی و دهه‌ها درگیری دارد، معتبر نباشد. شرکت‌هایی که در طول یا پس از یک دوره تنش آشکار قرارداد منعقد کرده‌اند، ممکن است دریابند که بیمه‌گران یا دادگاه‌ها اختلال نظامی را به عنوان یک خطر قابل پیش‌بینی در نظر می‌گیرند. زنجیره مسئولیت پایین‌دستی طولانی است: هر مشتری سازمانی که عملیاتش به دلیل قطعی AWS متوقف شده است، اکنون در حال ارزیابی موقعیت قراردادی خود است. ارائه‌دهندگان ابر ممکن است خود را ملزم به پذیرش ضرر و زیان و جبران خسارت مشتریان برای اختلالات در خدمات بدانند. بنابراین، آن دسته از شرکت‌های هوش مصنوعی که پروژه‌هایی در دست ساخت دارند، در حال ارزیابی مجدد این موضوع هستند که آیا چنین پروژه‌هایی هنوز قابل اجرا هستند یا خیر. هزینه‌های مراکز داده جدید در خلیج فارس به طور قابل توجهی در حال افزایش است زیرا آنها نیاز به اضافه کردن سیستم‌های پشتیبان بیشتر، افزایش اقدامات امنیتی فیزیکی و پرداخت حق بیمه بالاتر دارند. وقتی ۱۲ عضو گروه بین‌المللی باشگاه‌های P&I گروهی از انجمن‌های بیمه متقابل که پوشش مسئولیت دریایی را برای ۸۷ درصد از تناژ اقیانوس‌پیماهای جهان ارائه می‌دهند، لغو پوشش ریسک جنگ دریایی خود را برای خلیج فارس اعلام کردند، بازار بیمه بیشتر متوجه شد که مشخصات ریسک منطقه اساساً تغییر کرده است. برای برخی از پروژه‌های خلیج فارس، هزینه کلی اصلاح‌شده اکنون از هزینه ساخت ظرفیت معادل در مکان‌هایی که انرژی معمولاً گران‌تر است، از جمله شمال اروپا، هند یا جنوب یا غرب ایالات متحده، فراتر می‌رود. آن محاسبات ریاضی که خلیج فارس را در ماه مه ۲۰۲۵ جذاب می‌کرد، دیگر صادق نیست. کسانی که هنوز در مرحله برنامه‌ریزی هستند، ممکن است همچنان به ساخت زیرساخت‌های هوش مصنوعی در خلیج فارس ادامه دهند. بسته‌های تشویقی دولت‌های خلیج فارس برای ساخت و ساز، روی کاغذ جذاب باقی مانده است. اما بسیاری احتمالاً تصمیم می‌گیرند ضررهای

خود را کاهش دهند و به جای دیگری بروند. هرگونه ارزیابی صادقانه اکنون مستلزم قیمت‌گذاری در بیمه ریسک جنگ است، که نرخ‌های آن از زمان شروع جنگ تقریباً پنج برابر شده است، و همچنین هزینه‌های امنیتی، قرار گرفتن در معرض مسئولیت‌های فورس مازور، عواقب اعتباری فعالیت در یک منطقه جنگی فعال و احتمال از سرگیری خصومت‌ها در هر لحظه. شرکت‌هایی که در حال حاضر در خلیج فارس فعالیت می‌کنند، چاره‌ای جز تقسیم ریسک خود ندارند. آمازون، مایکروسافت، گوگل و اوراکل، یعنی چهار شرکتی که بر بازار تسلط دارند، هر کدام حداقل دو خوشه مرکز داده در منطقه را اداره می‌کنند و میزبان عملیات گسترده‌ای مانند سیستم‌های بانکی منطقه‌ای و برنامه‌های تلفن همراه برای مصرف‌کنندگان هستند. همه آنها باید بارهای کاری حساس را به تأسیسات مناطق دیگر منتقل کنند و پوشش بیمه‌ای را برای کارهایی که باقی مانده است، افزایش دهند. آنها همچنین باید شفافیت در مورد عملیات خلیج فارس خود را افزایش دهند. بسیاری از مشتریان آنها نمی‌دانند که بارهای کاری آنها از طریق مراکز داده خلیج فارس انجام می‌شود، که در صورت قطع برق در آینده، خطر خشم یا حتی طرح دعوی را به همراه دارد. اگر شرکت‌ها داده‌ها و پروژه‌های نظامی و تجاری را تا حد امکان به طور عمومی از هم جدا کنند و عملیات واقعاً حساس را در خارج از خاورمیانه مستقر کنند، بیشترین محافظت را خواهند داشت. این احتمال وجود دارد که هیچ یک از زیرساخت‌های دیجیتال مستقر در خلیج فارس به طور خاص برای عملیات نظامی استفاده نشود. اما تا زمانی که ارتش ایالات متحده به فعالیت خود در خاورمیانه ادامه دهد، زیرساخت‌های ایالات متحده هدف قرار خواهند گرفت. به خصوص که شرکت‌های هوش مصنوعی تجاری وظایف مرتبط با دفاع بیشتری را بر عهده می‌گیرند. این نه تنها برای ایالات متحده، بلکه برای شرکای آن نیز یک مشکل است. چشم‌انداز تبدیل شدن به یک قطب جهانی هوش مصنوعی، نوید مشاغل جدید، بازده بالا برای صندوق‌های ثروت ملی خلیج فارس و اعتبار فناوری را می‌داد. همچنین کشورهای خلیج فارس را به اهداف با ارزش تری برای هر دشمن ایالات متحده تبدیل کرد. تا زمانی که ارائه دهندگان خدمات ابری هوش مصنوعی آمریکایی، تأسیساتی را در قلمرو خود اداره می‌کنند که ممکن است به وظایف دولت ایالات متحده خدمت کند، تمایز بین زیرساخت‌های غیرنظامی و نظامی در نظر دشمنان مبهم خواهد بود. هرگونه قرارداد آینده در منطقه به مفادی نیاز دارد که صراحتاً مسئولیت را در صورت اقدام نظامی تحت حمایت دولت تعیین کند. عناصری که توافق‌نامه‌های الگوی قبل از جنگ به اندازه کافی به آنها نمی‌پردازند. شرکت‌ها در حال حاضر تمرکز جغرافیایی خود را متنوع می‌کنند و پروژه‌ها را به شمال اروپا، جنوب شرقی آسیا و هند منتقل می‌کنند. فراتر از پکس سیلیکا، تشویق فعال دولت ایالات متحده برای توسعه هوش مصنوعی خلیج فارس از طریق معاملات سرمایه‌گذاری دوجانبه، مجوزهای صادرات تراشه و چارچوب پکس سیلیکا، یک اشتباه محاسباتی بزرگ بود، به خصوص با توجه به اقدامات بعدی آن در ایران. مجموعه وابستگی‌های متقابل ناشی از اقدامات آن، پتانسیل آسیب رساندن به منافع اقتصادی و امنیت ملی ایالات متحده را دارد. حتی اگر واشنگتن در مورد کاهش حضور نظامی خود در خاورمیانه جدی باشد، که هنوز نشان نداده است، بی‌ثباتی مداوم منطقه، آن را برای میزبانی از فناوری که برای رشد اقتصادی و رقابت قدرت‌های بزرگ بسیار حیاتی است، نامناسب می‌کند. چارچوب‌های مشارکت فناوری نه تنها باید یکپارچگی زنجیره تأمین و رونق اقتصادی، بلکه امنیت فیزیکی آن زیرساخت‌های حیاتی و هزینه‌های بالقوه فاجعه‌بار آسیب به آن را نیز در نظر بگیرند. راه حل، نه عقب‌نشینی از توافق پکس سیلیکا است و نه اجازه دادن به پژمرده شدن آرام آن. قرار بود معاملات تراشه و چارچوب پکس سیلیکا کشورهای خلیج فارس را به مدار فناوری آمریکا و دور از چین بکشاند. عقب‌نشینی می‌تواند با آسیب رساندن به روابط مهم با کشورهای خلیج فارس و جسورتر کردن پکن، اثر معکوس داشته باشد. مداخله ایالات متحده در ایران، فرصتی را برای چین فراهم کرده است: شرکت‌هایی مانند هواوی در حال حاضر مشتریان خلیج فارس را در معرض خطرات «وابستگی به یک منطقه» قرار می‌دهند. در عوض، ایالات متحده باید بر تقویت و ایجاد همکاری هوش مصنوعی در حوزه‌های سودمندتر، مانند حوزه‌هایی که به سمت تجمیع قدرت خرید ایالات متحده و کشورهای حوزه خلیج فارس برای نهادهای معدنی حیاتی و برای بازسازی ظرفیت تولید در خاک متحدان معطوف هستند، تمرکز کند، در عین حال تعهدات مربوط به زیرساخت‌های حیاتی آسیب‌پذیر را کاهش دهد. می‌توان حجم کار را منتقل کرد، سرمایه‌گذاری‌های آینده را می‌توان تغییر مسیر داد و پروژه‌هایی را که هنوز در مرحله برنامه‌ریزی هستند، می‌توان به طور کامل مورد بازنگری قرار داد. فرصت تصمیم‌گیری در این زمینه‌ها رو به اتمام است. شرط‌بندی بر اینکه جنگ فعلی یک انحراف و استثنا است یا پیش‌نمایشی از آینده منطقه، روز به روز کمتر عاقلانه به نظر می‌رسد. بسته‌های تشویقی برای سرمایه‌گذاری در خلیج فارس که برای زمان صلح طراحی شده بودند، بی‌معنی می‌شوند. هر چه ایالات متحده و متحدانش بیشتر برای محافظت از زیرساخت‌های حیاتی خود با انتقال آن به جای دیگر و تعریف مجدد مشارکت‌های هوش مصنوعی خود صبر کنند، انجام این کار، گران‌تر، پیچیده‌تر و در نهایت خطرناک‌تر خواهد شد.

