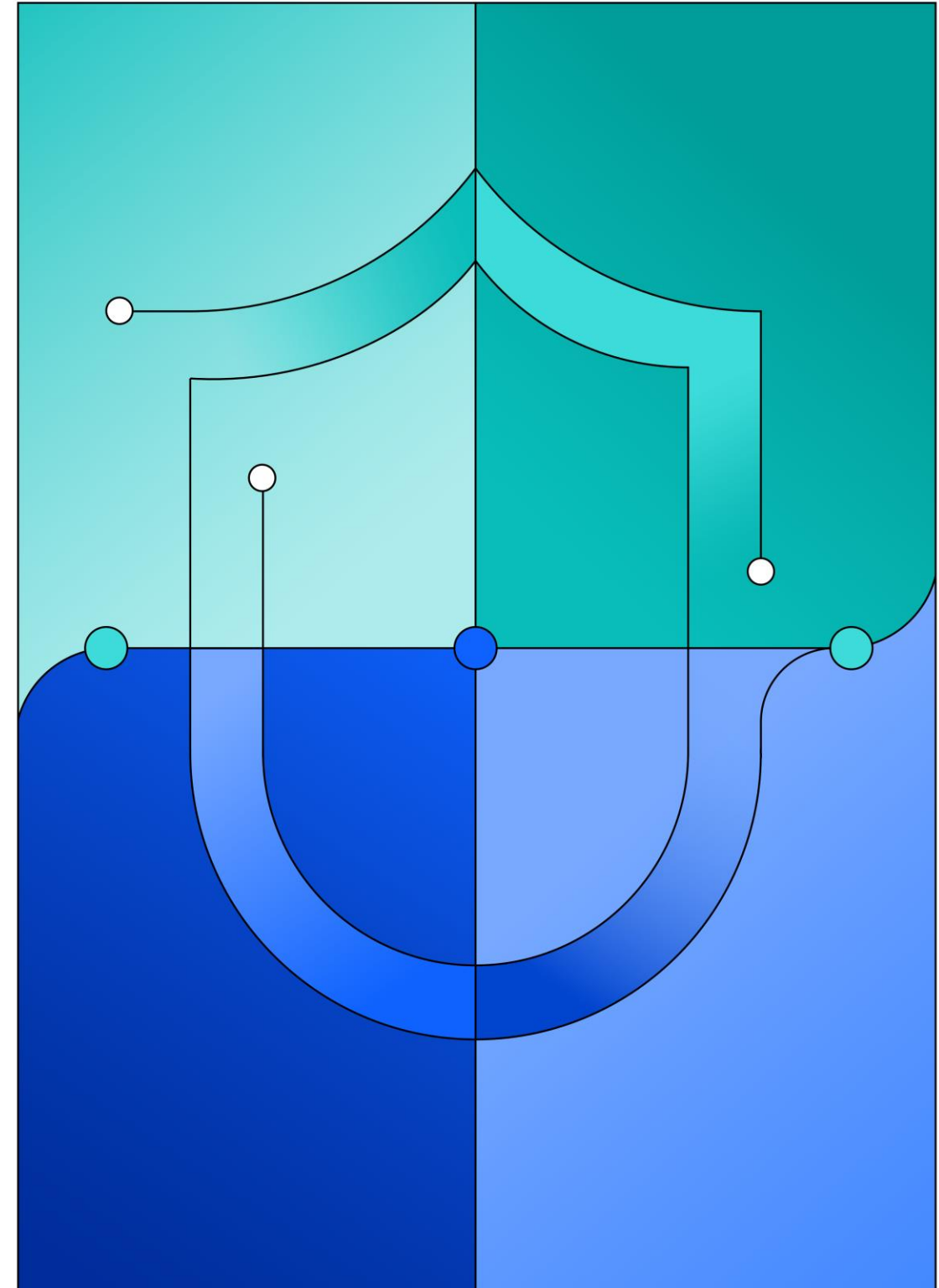


صنایع دفاعی و اطلاعاتی در دوران هوش مصنوعی

دیدگاه‌های رهبران ناتو و ائتلاف Five Eyes



فهرست

پیش‌گفتار..... ۳

مقدمه

رهبری و تصمیم‌گیری در تداوم رقابت..... ۵

بخش ۱

اولویت‌های هوش مصنوعی دفاعی روشن است، اما پیشرفت یکنواخت نیست.... ۷

بخش ۲

شرایطی که موفقیت هوش مصنوعی در حوزه دفاعی را شکل می‌دهند..... ۱۵

بخش ۳

بنیان‌های هوش مصنوعی به زیرساخت‌های استراتژیک ملی تبدیل شده‌اند..... ۱۸

راهنمای عملیاتی

تبدیل جاه‌طلبی‌های هوش مصنوعی به واقعیت عملیاتی..... ۲۱



کریستینا کابایه فوگت
Cristina Caballé Fuguet

نایب رئیس
بخش عمومی بین‌المللی
IBM

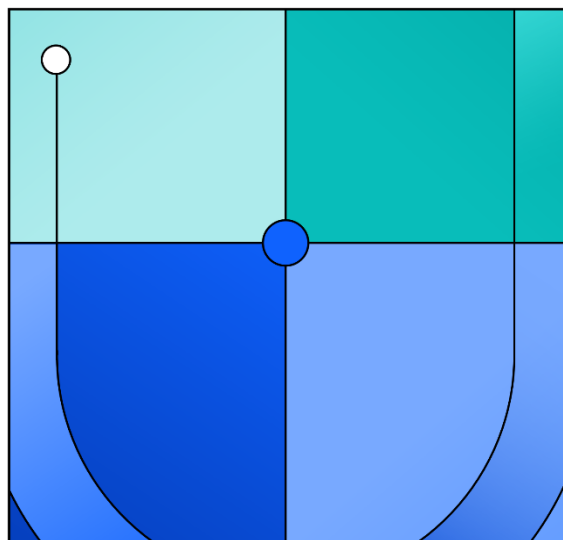
در طول تاریخ، فرماندهان نظامی بارها با مقاطعی روبه‌رو شده‌اند که ماهیت منازعه و حتی مفهوم رهبری، دستخوش تحولات بنیادین قرار گرفته است. از مکانیزه‌شدن جنگ‌ها گرفته تا ظهور قدرت هوایی و سپس فضای سایبری، هر یک از این دگرگونی‌ها نه تنها مستلزم توسعه قابلیت‌های جدید بودند؛ بلکه شیوه‌های تازه‌ای از اندیشیدن، تصمیم‌گیری و فرماندهی را نیز طلب می‌کردند. امروز، هوش مصنوعی نیز چنین نقطه عطفی را رقم زده است.

این نگاه نه بر مبنای نظریه‌های انتزاعی، بلکه بر پایه تجربه زیسته فرماندهان نظامی شکل گرفته است؛ فرماندهان که در حال حاضر مستقیماً با این تحولات مواجه هستند. این گزارش بر اساس مصاحبه‌هایی تدوین شده که در اوایل سال ۲۰۲۶ و با همکاری مؤسسه Oxford Economics با ۶۰۰ نفر از مدیران ارشد سازمان‌های دفاعی کشورهای عضو ناتو و ائتلاف Five Eyes انجام شده است. این افراد از وزارتخانه‌های دفاع، نیروهای مسلح، فرماندهی‌های مشترک و سازمان‌های دفاعی انتخاب شده‌اند و نماینده سازمان‌هایی با اندازه‌ها و نقش‌های عملیاتی گوناگون هستند. در مجموع، دیدگاه‌های آنان طیف کامل مأموریت‌های دفاعی چنددامنه‌ای شامل سازمان‌های نظامی، پشتیبانی نظامی و پشتیبانی خدمات نظامی را پوشش می‌دهد و تصویری واقع‌بینانه از سطح آمادگی کنونی، اولویت‌های نوسازی و موانعی که مانع دستیابی به اثرگذاری عملیاتی می‌شوند را ارائه می‌کند.

در سازمان‌های دفاعی سراسر جهان، هوش مصنوعی دیگر نه یک هدف آرمانی دور از دسترس است و نه صرفاً یک آزمایش فنی محدود. این فناوری به تدریج به بخشی جدایی‌ناپذیر از نحوه برنامه‌ریزی، تصمیم‌گیری و اقدام فرماندهان تبدیل شده است؛ آن هم اغلب در شرایطی که با عدم قطعیت، محدودیت زمانی شدید و پیامدهای سنگین همراه است. نزدیک به دوسوم فرماندهان نظامی، هم‌اکنون هوش مصنوعی را برای راهبرد سازمان خود «بسیار مهم» یا «فوق‌العاده مهم» ارزیابی می‌کنند و انتظار می‌رود این نسبت تا سال ۲۰۲۸ به بیش از هشت نفر از هر ده فرمانده برسد. این تغییر نشان‌دهنده درک این موضوع است که هوش مصنوعی در سال‌های آینده نقشی تعیین‌کننده در آمادگی دفاعی، بازدارندگی و اثربخشی عملیاتی ایفا خواهد کرد.

درعین‌حال، محیطی که نیروهای مسلح در آن فعالیت می‌کنند، با بی‌ثباتی مداوم همراه است؛ از تنش‌های ژئوپلیتیکی و جنگ‌های هیبریدی گرفته تا تهدیدهای سایبری و فضای اطلاعاتی مورد مناقشه. هوش مصنوعی قرار نیست مسئولیت فرماندهی را از دوش انسان بردارد و اساساً نیز نباید چنین کند. قضاوت، پاسخگویی و مسئولیت‌پذیری همچنان ذاتاً ویژگی‌هایی انسانی هستند. اما اگر هوش مصنوعی با رویکردی سنجیده پیاده‌سازی و با سازوکارهای مسئولانه حکمرانی شود، می‌تواند توان تصمیم‌گیری انسان را تقویت کند و به فرماندهان کمک کند تا در محیط‌های پیچیده، با شفافیت، سرعت و انسجام بیشتری عمل کنند.

نکات کلیدی



هوش مصنوعی قرار نیست
بار مسئولیت فرماندهی را از
دوش انسان بردارد و اساساً
نیز نباید چنین کند.

■ سرمایه‌گذاری در حال افزایش است، اما بخش عمده کاربردهای مأموریت‌محور هوش مصنوعی همچنان در مرحله اجرای آزمایشی باقی مانده‌اند.

با وجود آنکه پیش‌بینی می‌شود هزینه‌کرد در حوزه هوش مصنوعی تا سال ۲۰۲۸ بیش از دو برابر شود، به‌کارگیری این فناوری در حوزه‌های کلیدی مأموریتی از فرماندهی و کنترل گرفته تا لجستیک، اطلاعات، مراقبت و شناسایی (ISR) و عملیات سایبری، همچنان عمدتاً به ارزیابی‌ها و پروژه‌های پایلوت محدود است و امروزه تنها نمونه‌های اندکی از استقرار گسترده و عملیاتی هوش مصنوعی در این حوزه‌ها وجود دارد.

■ آمادگی سامانه‌ها، مهم‌ترین گلوگاه در عملیات دفاعی مبتنی بر هوش مصنوعی است.

با وجود سرمایه‌گذاری‌های قابل‌توجه در حوزه داده و ابزارهای هوش مصنوعی، در حال حاضر تنها حدود یک‌سوم سامانه‌های اصلی مأموریتی و کسب‌وکاری برای بهره‌گیری از هوش مصنوعی آمادگی لازم را دارند. اگرچه سامانه‌های هوش مصنوعی بینش‌ها و تحلیل‌های ارزشمندی تولید می‌کنند، اما این خروجی‌ها هنوز نمی‌توانند وارد جریان‌های کاری قابل‌اعتماد شوند؛ یعنی همان فرایندهایی که تصمیم‌های عملیاتی در آن‌ها اتخاذ می‌شود. تا زمانی که این سامانه‌ها برای دریافت، پردازش و اقدام بر مبنای خروجی‌های هوش مصنوعی نوسازی نشوند، سرمایه‌گذاری بیشتر در توسعه مدل‌ها یا گردآوری داده‌ها، روند بازدهی روبه‌رشدی به همراه نخواهد داشت و اثربخشی آن به تدریج کاهش می‌یابد.

■ تاب‌آوری و حاکمیت هوش مصنوعی اکنون به موضوعی مرتبط با زیرساخت‌های ملی و ائتلافی تبدیل شده‌اند.

بیش از دوسوم فرماندهان نظامی، حاکمیت داده و امنیت سایبری را از مهم‌ترین اولویت‌های ملی برای تضمین تاب‌آوری هوش مصنوعی می‌دانند. درعین‌حال، نزدیک به ۶۰ درصد آنان معتقدند که خطر راهبردی بزرگ‌تر، عقب‌مانده از رقبا و دشمنان در پذیرش و به‌کارگیری هوش مصنوعی است. این دیدگاه نشان می‌دهد که کشورها و ائتلاف‌ها باید میان سرعت استقرار، حفظ حاکمیت و کنترل و همچنین قابلیت همکاری متقابل میان متحدان، تعادل برقرار کنند.

مقدمه

رهبری و تصمیم‌گیری در تداوم رقابت

فرماندهان نظامی وارد دوره‌ای شده‌اند که در آن سرعت و پیچیدگی فعالیت‌های نظامی با شتابی بیش از توان ساختارهای کنونی تصمیم‌گیری در حال افزایش است.

پاسخ‌گویی به این چالش صرفاً با به‌کارگیری فناوری‌های جدید امکان‌پذیر نیست؛ بلکه مستلزم تغییر در شیوه مدیریت اطلاعات، فرایندهای تصمیم‌گیری و نحوه سازمان‌دهی نهادهای دفاعی است. هوش مصنوعی به‌تدریج به بخشی از این تحول تبدیل می‌شود. اگر این فناوری به‌درستی به کار گرفته شود، می‌تواند به تصمیم‌گیران در مدیریت پیچیدگی‌ها کمک کند؛ اما اگر به‌صورت نادرست یا شتاب‌زده استفاده شود، خود می‌تواند بر این پیچیدگی‌ها بیفزاید.

فرماندهان نظامی امروز در محیطی فعالیت می‌کنند که دیگر نه با بحران‌های مقطعی، بلکه با رقابتی مستمر و پایان‌ناپذیر تعریف می‌شود. رقابت راهبردی به وضعیتی دائمی تبدیل شده و مرز میان صلح، بحران و درگیری بیش از هر زمان دیگری کم‌رنگ شده است. امروزه فعالیت‌های نظامی، عملیات سایبری و کارزارهای اطلاعاتی به‌طور هم‌زمان در حوزه‌های مختلف جریان دارند و اغلب نیز پایین‌تر از آستانه‌های سنتی تشدید تنش انجام می‌شوند؛ وضعیتی که به‌جای رویدادهای مجزا، فشاری مداوم و مستمر بر سازمان‌های دفاعی و نظامی وارد می‌کند.^۱

ابعاد بی‌ثباتی جهانی نیز این واقعیت را تأیید می‌کند. شمار درگیری‌های مسلحانه در سراسر جهان به بالاترین سطح خود طی چند دهه اخیر رسیده است و ارزیابی‌های مختلف نشان می‌دهند که شدت این وضعیت از پایان جنگ سرد تاکنون بی‌سابقه بوده و حتی بر اساس برخی شاخص‌ها، باید تا دوران جنگ جهانی دوم به عقب بازگشت تا شرایطی مشابه یافت.^۲ در نتیجه، نهادهایی که برای فعالیت در محیطی نسبتاً قابل‌پیش‌بینی طراحی شده بودند، اکنون ناچارند در شرایطی مملو از عدم قطعیت، سرعت بالا و تغییرات مداوم عمل کنند؛ آن هم درحالی‌که حاشیه خطا بسیار محدود است.

این تحول، ریتیم و شتاب، عملیات دفاعی را به‌طور اساسی دگرگون کرده است. نیروهای مسلح دیگر برای مجموعه‌ای از جنگ‌های مقطعی که میان آن‌ها دوره‌هایی از ثبات نسبی وجود دارد آماده نمی‌شوند؛ بلکه باید به‌صورت مستمر آمادگی نظامی، بازدارندگی و حضور عملیاتی خود را حفظ کنند، آن هم اغلب به‌طور هم‌زمان در چندین صحنه عملیاتی و مأموریت مختلف. الگوی هزینه‌کرد دفاعی نیز این تغییر را منعکس می‌کند. از میانه دهه ۲۰۱۰، کشورهای عضو ناتو به‌تدریج از الگوی نوسازی مقطعی فاصله گرفته و به سمت سرمایه‌گذاری مستمر حرکت کرده‌اند؛ سرمایه‌گذاری‌هایی که علاوه بر سامانه‌ها و تجهیزات سنتی، بر تاب‌آوری، دفاع سایبری، داده و قابلیت‌های مبتنی بر نرم‌افزار نیز تمرکز دارد.^{۳،۴}

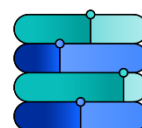
هم‌زمان با افزایش سرعت عملیات، فرصت تصمیم‌گیری کوتاه‌تر و حجم اطلاعات به‌مراتب بیشتر شده است. اکنون داده‌ها از منابع بسیار متنوع‌تری وارد می‌شوند؛ منابعی که بسیاری از آن‌ها ممکن است مورد مناقشه، دچار اختلال یا حتی به طور عمدی دست‌کاری شده باشند. فرماندهان نظامی باید تقریباً به‌صورت بلادرنگ، اطلاعات و داده‌های عملیاتی، لجستیکی، اطلاعاتی، سایبری و ملاحظات سیاسی را با یکدیگر تلفیق کنند؛ آن‌هم در شرایطی که اطلاعات موجود اغلب ناقص یا مبهم است. پژوهش‌های مربوط به تصمیم‌گیری نظامی مبتنی بر هوش مصنوعی نشان می‌دهد که این فشردگی زمانی و افزایش پیچیدگی، هم‌اکنون نیز شیوه فرماندهی و کنترل در سطح عملیاتی را دگرگون کرده و هم ارزش بالقوه سامانه‌های دستیار تصمیم‌گیری مبتنی بر هوش مصنوعی و هم مخاطرات آن‌ها را افزایش داده است.^۵

در چنین شرایطی، چالش اصلی رهبران دیگر صرفاً نوسازی تجهیزات و سامانه‌ها نیست. مسئله اساسی آن است که چگونه می‌توان در محیطی که پیچیدگی اجتناب‌ناپذیر است و خطاها می‌توانند سریع‌تر از توان سازوکارهای سنتی سازمانی گسترش یابند، شفافیت فرماندهی، سلامت و یکپارچگی اطلاعات و انسجام در اقدام را حفظ کرد. حفظ برتری راهبردی بیش از هر زمان دیگری به توانایی نهادها در «درک محیط، تصمیم‌گیری و اقدام» تحت فشار مستمر وابسته شده است.^{۶،۷}

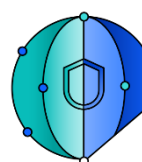
در چنین فضایی، هوش مصنوعی به‌عنوان یکی از عوامل کمک‌کننده کلیدی در حال ظهور است؛ نه به این دلیل که عدم قطعیت را از میان می‌برد، بلکه چون می‌تواند به رهبران در مدیریت آن کمک کند. اگر این فناوری به‌صورت مسئولانه به کار گرفته شود، قادر است حجم عظیمی از جریان‌های داده را تلفیق کند، الگوهایی را آشکار سازد که برای تیم‌های انسانی قابل‌مشاهده نیستند و اجرای سریع‌تر و منسجم‌تر مأموریت‌ها را در سازمان‌های نظامی پیچیده ممکن سازد. بااین‌حال، ارزیابی‌های نهادهای فعال در حوزه امنیت و حکمرانی به طور مستمر هشدار می‌دهند که همین سامانه‌ها، اگر سریع‌تر از ظرفیت سازمان‌ها برای جذب و مدیریت آن‌ها مستقر شوند، مخاطرات تازه‌ای در زمینه اعتماد، حکمرانی، تاب‌آوری و حاکمیت ایجاد خواهند کرد.^{۸،۹}

این گزارش در چهار بخش تنظیم شده است:

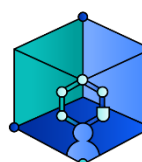
بخش نخست به بررسی نگاه فرماندهان نظامی به هوش مصنوعی می‌پردازد؛ از اهمیت راهبردی این فناوری و روند روبه‌رشد سرمایه‌گذاری‌ها گرفته تا پیشرفت نامتوازی که موجب شده بخش عمده قابلیت‌های هوش مصنوعی در مرحله پایلوت باقی بمانند.



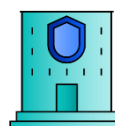
بخش دوم فراتر از این روندها رفته و شرایط لازم برای انتقال هوش مصنوعی از مرحله آزمایش به بهره‌برداری عملیاتی را بررسی می‌کند. این بخش بر آمادگی داده‌ها، آمادگی سامانه‌ها، سرعت فرایندهای تأمین و تدارکات و توسعه توانمندی‌های داخلی تمرکز دارد.



بخش سوم دامنه تحلیل را به سطح ملی و ائتلافی گسترش می‌دهد؛ جایی که مؤلفه‌های بنیادین هوش مصنوعی شامل داده، توان پردازشی، زیرساخت، حکمرانی و سرمایه انسانی، بیش‌ازپیش به‌عنوان اجزای زیرساخت راهبردی کشورها تلقی می‌شوند.



راهنمای عملیاتی نیز یافته‌های گزارش را به مجموعه‌ای از گام‌های عملی تبدیل می‌کند که سازمان‌های نظامی و دولت‌ها می‌توانند برای تقویت زیرساخت‌های هوش مصنوعی، کاهش ریسک‌های ساختاریافته و تبدیل جاه‌طلبی‌های فناورانه به مزیت عملیاتی پایدار و قابل‌اعتماد از آن‌ها بهره بگیرند.



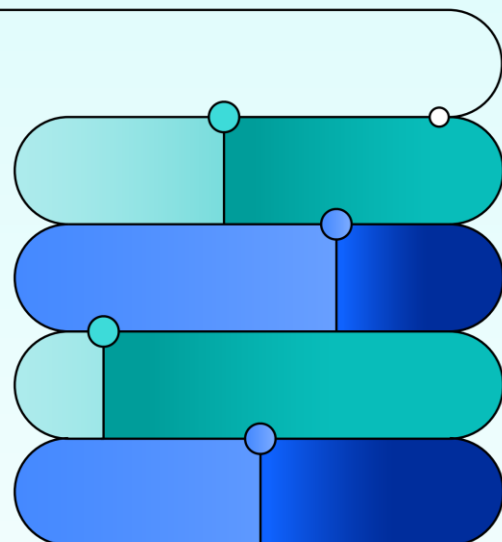
بخش ۱

اولویت‌های هوش مصنوعی دفاعی روشن است، اما پیشرفت یکنواخت نیست

نتایج این پژوهش الگوی روشنی را نشان می‌دهد. سازمان‌های دفاعی، هوش مصنوعی را یک ضرورت راهبردی می‌دانند و سرمایه‌گذاری قابل‌توجهی نیز برای آن انجام می‌دهند؛ اما تنها بخش کوچکی از آن‌ها توانسته‌اند این فناوری را به تأثیرگذاری عملیاتی چشمگیری تبدیل کنند.

شکاف موجود نه ناشی از کمبود اراده یا منابع مالی، بلکه حاصل دشواری انتقال هوش مصنوعی به سامانه‌هایی است که تصمیم‌های واقعی و حیاتی در آن‌ها اتخاذ می‌شود.

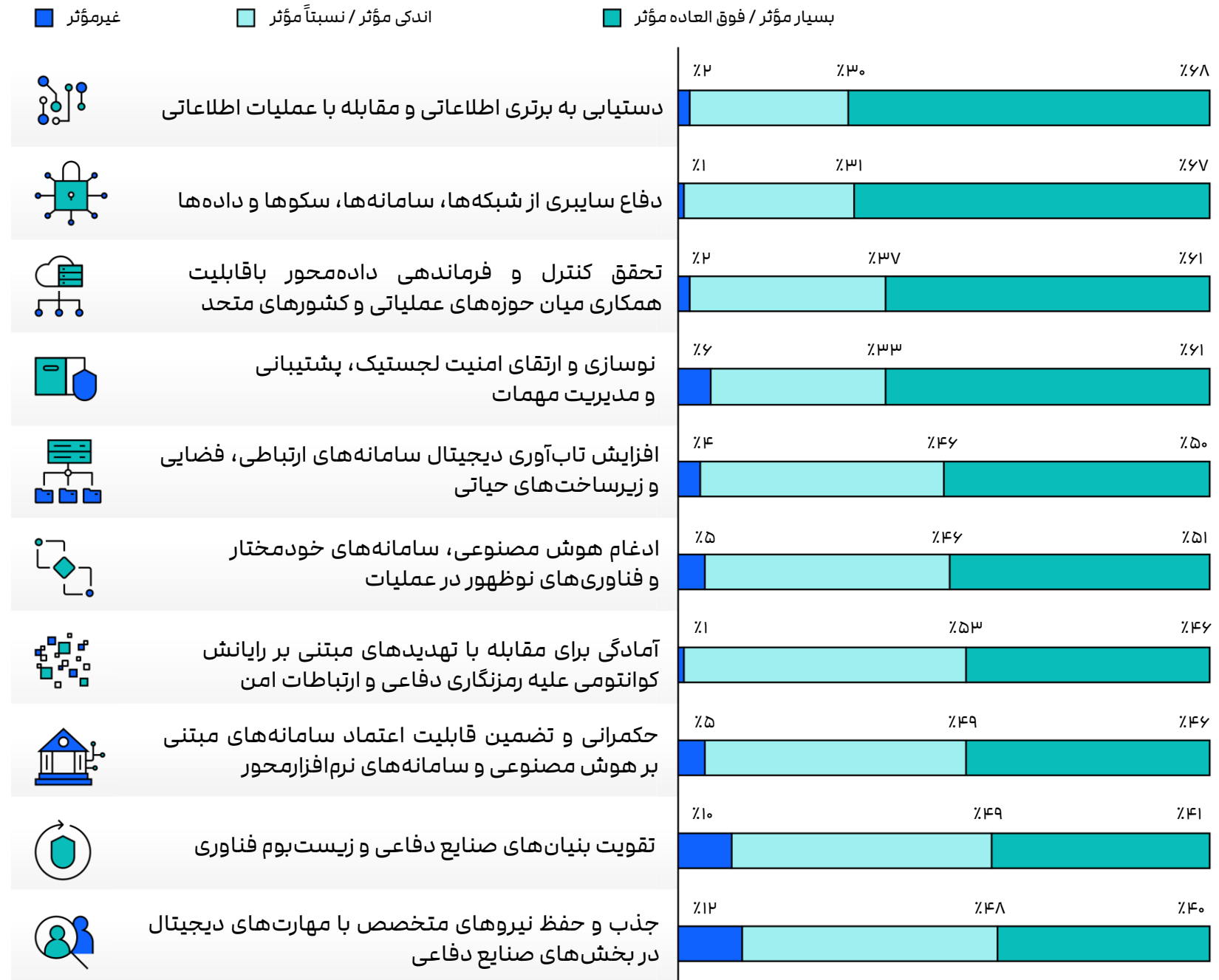
در میان سازمان‌های مورد بررسی، فرماندهان نظامی هم‌اکنون نیز هوش مصنوعی را یکی از ارکان اصلی اثربخشی نظامی آینده می‌دانند. نزدیک به ۶۳ درصد آنان، هوش مصنوعی را در راهبرد سازمان خود «بسیار مهم» یا «فوق‌العاده مهم» ارزیابی می‌کنند و پیش‌بینی می‌شود این رقم تا سال ۲۰۲۸ به ۸۶ درصد برسد؛ زیرا شمار بیشتری از فرماندهان، هوش مصنوعی را در بالاترین سطح اهمیت راهبردی، یعنی «فوق‌العاده مهم»، طبقه‌بندی خواهند کرد.



فرماندهان نظامی بیش از گذشته به این واقعیت پی برده‌اند که بدون داده‌های قابل‌اعتماد، زیرساخت‌های امن و سامانه‌های یکپارچه، حتی پیشرفته‌ترین قابلیت‌های هوش مصنوعی نیز نمی‌توانند ارزش عملیاتی قابل‌توجهی ایجاد کنند.

شکل ۱

دیدگاه فرماندهان نظامی درباره ظرفیت هوش مصنوعی در کاهش ریسک های عملیاتی



این دیدگاه بازتابی از مخاطراتی است که فرماندهان نظامی در فعالیت های روزمره خود با آن مواجه اند. نزدیک به ۷۰ درصد آنان معتقدند که هوش مصنوعی طی سه سال آینده می تواند در کاهش ریسک های کلیدی عملیاتی «بسیار مؤثر» یا «فوق العاده مؤثر» باشد؛ ریسک هایی که از دفاع سایبری و فرماندهی و کنترل داده محور و قابل همکاری میان نیروها گرفته تا تأمین امنیت زنجیره لجستیک و مقابله با عملیات اطلاعاتی را در بر می گیرد. (شکل ۱)

پرسش: به نظر شما، هوش مصنوعی تا چه اندازه می تواند طی سه سال آینده (تا سال ۲۰۲۸) در کمک به سازمان شما برای کاهش ریسک های زیر مؤثر باشد؟

افزایش سرمایه‌گذاری

پیش‌بینی می‌شود سهم هوش مصنوعی از بودجه فناوری اطلاعات سازمان‌های نظامی طی سه سال آینده به طور قابل‌توجهی افزایش یابد. در مجموع، سازمان‌های مورد بررسی انتظار دارند سرمایه‌گذاری‌شان در حوزه هوش مصنوعی تا سال ۲۰۲۸ بیش از دوبرابر شود؛ تغییری که نشان‌دهنده گذار از اجرای آزمایش‌های محدود و انتخابی به تعهدی گسترده در سطح کل سازمان است.

تمرکز سرمایه‌گذاری‌های سازمان‌های نظامی نیز تصویر روشن‌تری از اولویت‌های آن‌ها ارائه می‌دهد. در سال ۲۰۲۶، بخش عمده فعالیت‌های مرتبط با هوش مصنوعی بر تقویت مدیریت داده، ارتقای کیفیت داده و حکمرانی داده متمرکز است و پس از آن، هوش مصنوعی سنتی و تحلیل‌های پیشرفته در جایگاه دوم قرار دارند. با نگاه به سال ۲۰۲۸، زیرساخت‌های داده همچنان مهم‌ترین حوزه سرمایه‌گذاری باقی خواهند ماند؛ اما انتظار می‌رود بیشترین نرخ رشد به هوش مصنوعی مولد و هوش مصنوعی عامل‌محور اختصاص یابد. این روند نشان‌دهنده حرکت تدریجی سازمان‌های دفاعی به سمت قابلیت‌هایی سازگارتر، هوشمندتر و خودمختارتر است. (شکل ۲)

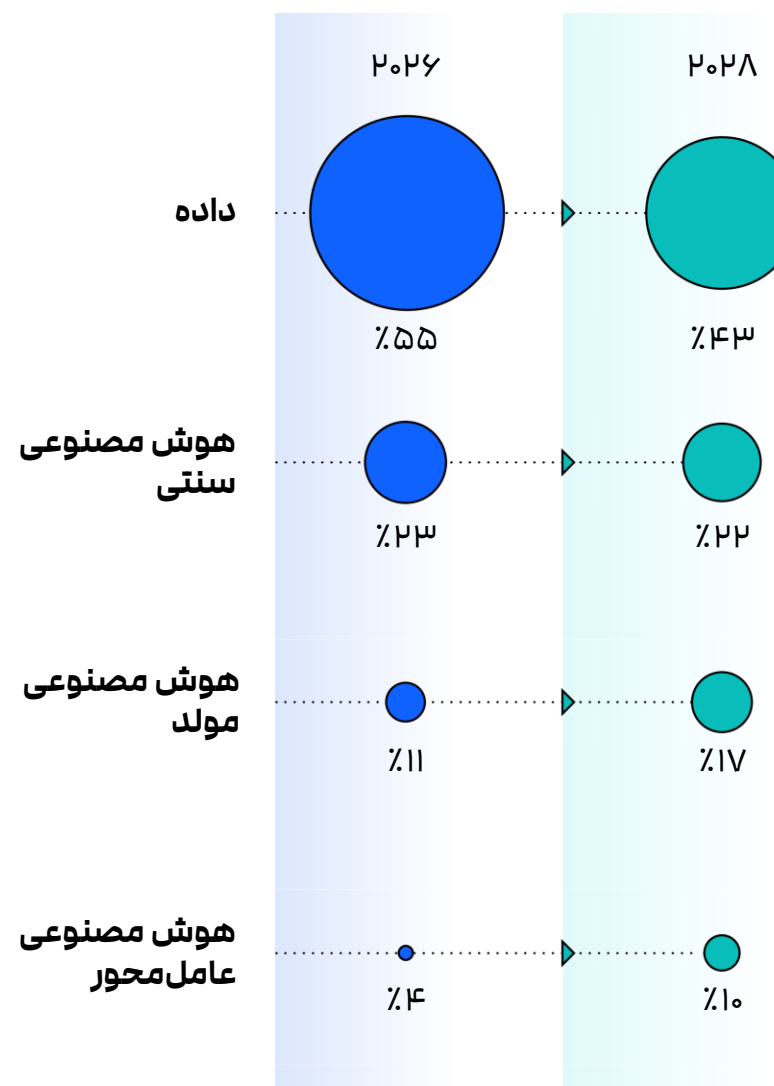
مجموع این الگوهای سرمایه‌گذاری نشان می‌دهد که فرماندهان نظامی با رویکردی سنجیده در حال ایجاد زیرساخت‌های لازم برای استقرار قابل‌اعتماد و مقیاس‌پذیر هوش مصنوعی در سطح عملیاتی هستند. این الگوی سرمایه‌گذاری حاصل تجربه‌های ارزشمندی است که طی سال‌های اخیر به دست آمده است. فرماندهان نظامی بیش از گذشته دریافته‌اند که بدون داده‌های قابل‌اعتماد، زیرساخت‌های امن و سامانه‌های یکپارچه، حتی پیشرفته‌ترین قابلیت‌های هوش مصنوعی نیز قادر به ارزش‌آفرینی واقعی در میدان عمل نخواهند بود.

پرسش: بودجه هوش مصنوعی سازمان خود را در چهار دسته زیر، برای وضعیت فعلی (سال ۲۰۲۶) و پیش‌بینی سه سال آینده (سال ۲۰۲۸)، توزیع کنید:
داده و فعالیت‌های مرتبط با داده (مدیریت، کیفیت و حکمرانی داده)
هوش مصنوعی سنتی و تحلیل‌های پیشرفته
هوش مصنوعی مولد
هوش مصنوعی عامل‌محور

شکل ۲

به طور میانگین، پیش‌بینی می‌شود تا سال ۲۰۲۸ سهم بودجه هوش مصنوعی سازمان‌ها از حوزه‌های مرتبط با داده و هوش مصنوعی سنتی کاسته شده و به سمت هوش مصنوعی مولد و هوش مصنوعی عامل‌محور منتقل شود.

درصدها نشان‌دهنده توزیع هزینه‌کرد هوش مصنوعی سازمان‌ها است.



نقطه نظر

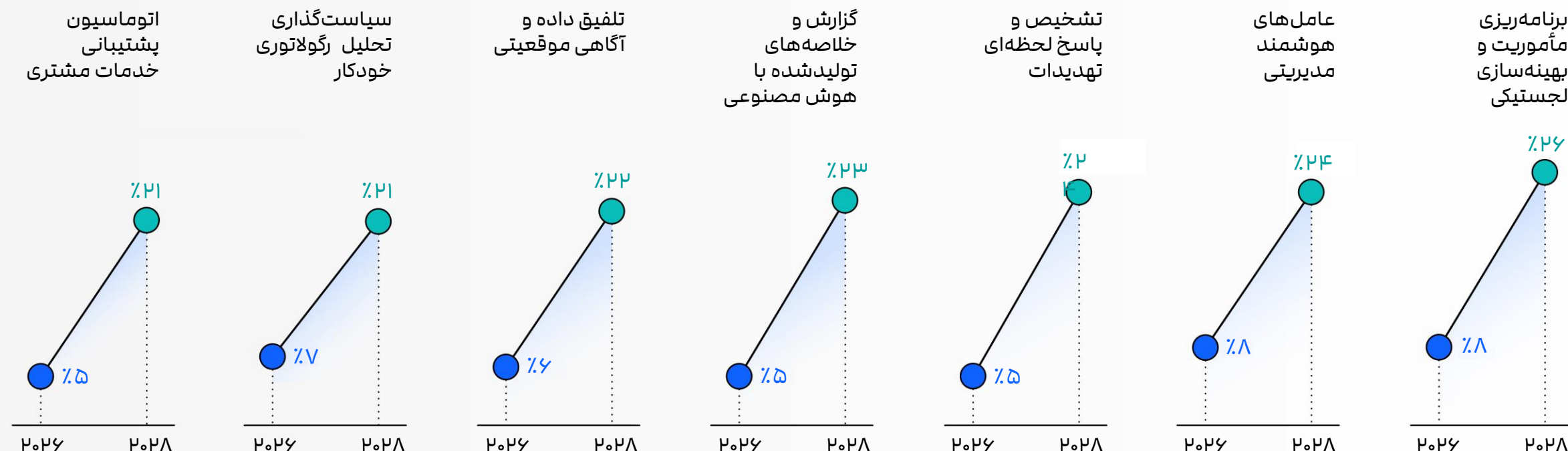
هوش مصنوعی عامل محور: شتاب اولیه، آمادگی نامتوازن

هوش مصنوعی عامل محور به سامانه‌هایی اشاره دارد که قادرند با میزان محدودی از دستوردهی انسانی، اقداماتی را آغاز کنند، وظایف را هماهنگ کنند یا جریان‌های کاری را با شرایط جدید تطبیق دهند. امروزه این فناوری در مقایسه با زیرساخت‌های داده و هوش مصنوعی سنتی، سهم نسبتاً کوچکی از هزینه‌کردهای هوش مصنوعی را به خود اختصاص داده است. با این حال، هوش مصنوعی عامل محور در میان سازمان‌های دفاعی با استقبال مواجه شده است؛ حتی در شرایطی که آمادگی سازمانی برای استفاده گسترده از آن همچنان محدود است. (شکل ۳)

شکل ۳

بلوغ هوش مصنوعی عامل محور در مأموریت‌های دفاعی: وضعیت پایه در سال ۲۰۲۶ در مقایسه با چشم‌انداز ۲۰۲۸

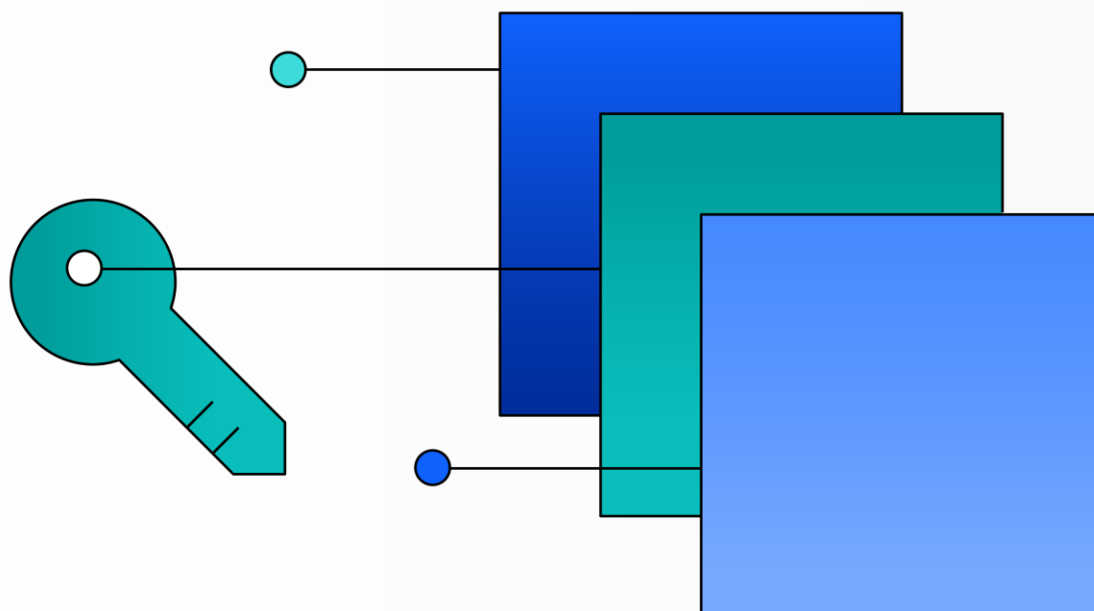
درصد مربوط به سال ۲۰۲۶ نشان‌دهنده سازمان‌هایی است که تاکنون هوش مصنوعی عامل محور را برای این مورد کاربردی مشخص پیاده‌سازی کرده‌اند. درصدهای سال ۲۰۲۸ نشان‌دهنده سهم سازمان‌هایی است که انتظار دارند تا سال ۲۰۲۸ هوش مصنوعی عامل محور را برای این مورد کاربردی پیاده‌سازی کنند.



فناوری هوش مصنوعی عامل‌محور با سرعتی بیشتر از توسعه چارچوب‌های حکمرانی موردنیاز برای مدیریت آن در حال پیشرفت است. بااین‌حال، مدیران و فرماندهان انتظار دارند تا سال ۲۰۲۸، سرمایه‌گذاری در هوش مصنوعی عامل‌محور در کنار هوش مصنوعی مولد، سریع‌تر از هر دسته دیگر از فناوری‌های هوش مصنوعی رشد کند. (شکل ۲)

نخستین تجربه‌ها و آزمایش‌های این فناوری عمدتاً در حوزه‌های برنامه‌ریزی و پشتیبانی تصمیم‌گیری، عملیات سایبری، هماهنگی لجستیکی و جریان‌های کاری سازمانی متمرکز شده‌اند. فرماندهان نظامی مزایای بالقوه این فناوری را در کاهش بار شناختی، تسریع هماهنگی میان واحدها و افزایش انسجام و ثبات عملکرد می‌دانند. بااین‌حال، همین فرماندهان تأکید می‌کنند که حکمرانی، قابلیت توضیح‌پذیری و نظارت انسانی، پیش‌شرط‌های ضروری برای استقرار گسترده‌تر این فناوری هستند؛ حوزه‌هایی که بسیاری از آنان ادعان دارند هنوز به بلوغ کافی نرسیده‌اند.

در شرایط کنونی، هوش مصنوعی عامل‌محور به آزمونی عملی برای سنجش آمادگی نهادهای سازمان‌ها تبدیل شده است؛ آزمونی که مشخص می‌کند آیا سازمان‌های دفاعی ساختارها و سازوکارهای نظارتی لازم برای مدیریت سامانه‌هایی را دارند که نه تنها تحلیل می‌کنند، بلکه قادر به اقدام مستقل نیز هستند یا خیر.



شکل ۴

وضعیت پذیرش فعلی هوش مصنوعی در حوزه های عملیاتی نظامی



اطلاعات، مراقبت و شناسایی

عملیات فضای مجازی

فرماندهی و کنترل

لجستیک نظامی

ادغام هوش مصنوعی در
وسایل نقلیه نیمه خودران

عملیات اطلاعات و دیپ فیک

ادغام هوش مصنوعی در
وسایل نقلیه خودران

پزشکی و خدمات درمانی

وضعیت کنونی هوش مصنوعی در حوزه دفاعی: تحت سلطه پروژه های پایلوت، با موفقیت محدود و نتایج نامتوازن

با وجود افزایش سرمایه گذاری ها و تأکید راهبردی بر اهمیت هوش مصنوعی، میزان تأثیرگذاری عملیاتی این فناوری همچنان نامتوازن است. تنها ۱۰ درصد از فرماندهان نظامی، سازمان خود را در پذیرش و به کارگیری هوش مصنوعی در شرایط کنونی «فوق العاده موفق» توصیف می کنند؛ در حالی که بیش از ۸۰ درصد، سطح موفقیت سازمان خود را تنها «متوسط» یا «محدود» ارزیابی می کنند. این فاصله، یک چالش پایدار را آشکار می کند؛ هوش مصنوعی هنوز به صورت یکنواخت و فراگیر در جریان های کاری حیاتی مأموریتی ادغام نشده است. الگوهای پذیرش نیز دلیل این وضعیت را نشان می دهند. در حوزه های مأموریتی مانند اطلاعات، مراقبت و شناسایی، عملیات سایبری، لجستیک و فرماندهی و کنترل، بیشتر سازمان ها همچنان در مرحله ارزیابی یا اجرای پروژه های پایلوت قرار دارند و تعداد سازمان هایی که در حال حاضر هوش مصنوعی را در مقیاس عملیاتی به کار گرفته اند، اندک است. (شکل ۴)

در حوزه های کارکردی مانند فناوری اطلاعات، امنیت اطلاعات، نگهداری و زنجیره تأمین، میزان پیشرفت تا حدودی بیشتر است، اما حتی در این حوزه ها نیز پروژه های آزمایشی همچنان غالب هستند. (شکل ۵)

پرسش: سازمان شما در حال حاضر (سال ۲۰۲۶) در چه مرحله ای از پذیرش هوش مصنوعی در حوزه های کاربردی دفاعی زیر قرار دارد و انتظار دارید طی سه سال آینده (سال ۲۰۲۸) به چه سطحی برسد؟

شکل ۵

وضعیت پذیرش فعلی هوش مصنوعی
در حوزه‌های کارکردی نظامی

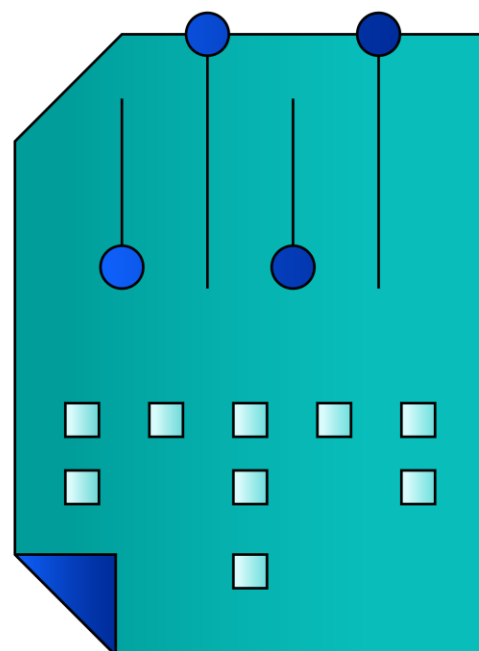


پرسش: سازمان شما در حال حاضر (سال ۲۰۲۶) در چه مرحله‌ای از پذیرش هوش مصنوعی در حوزه‌های کارکردی زیر قرار دارد و انتظار دارید طی سه سال آینده (سال ۲۰۲۸) به چه سطحی برسد؟

مجموع این یافته‌ها، چالش اصلی را آشکار می‌کند. هوش مصنوعی به عنوان یک فناوری ضروری شناخته شده، منابع مالی متناسب با اهمیت آن اختصاص یافته و آزمایش‌های گسترده‌ای نیز روی آن انجام شده است؛ اما موفقیت واقعی به این بستگی دارد که سازمان‌ها تا چه اندازه بتوانند این فناوری را در سامانه‌های عملیاتی و نهادی که تصمیم‌های حیاتی مأموریتی را شکل می‌دهند، ادغام کنند. هرچا این یکپارچه‌سازی به کمک پشتیبانی سامانه‌های مدرن، داده‌های تحت حکمرانی مناسب و مسئولیت‌پذیری مشخص انجام شده است؛ فرماندهان ارزش‌آفرینی بیشتری از هوش مصنوعی را گزارش کرده‌اند. اما هرچا چنین ادغامی اتفاق نیفتاده، روند پیشرفت متوقف شده است.

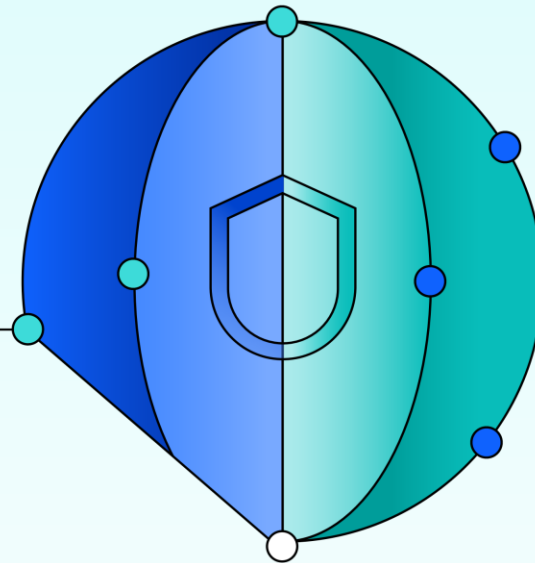
این شکاف پایدار میان جاه‌طلبی و اجرا اکنون ویژگی اصلی چشم‌انداز هوش مصنوعی در حوزه دفاعی است. بخش بعدی گزارش به بررسی محدودیت‌های پشت این شکاف می‌پردازد و توضیح می‌دهد که چرا ریشه این چالش‌ها کمتر در خود فناوری و بیشتر در آمادگی سامانه‌ها و نهادهایی است که باید پذیرای آن باشند.

هوش مصنوعی به عنوان فناوری ضروری شناخته شده، منابع مالی متناسب با آن اختصاص یافته و به طور گسترده آزمایش شده است؛ اما موفقیت به این بستگی دارد که سازمان‌ها بتوانند آن را در سامانه‌های عملیاتی و نهادی مؤثر بر تصمیم‌های حیاتی مأموریتی ادغام کنند.



بخش ۲

شرایطی که موفقیت هوش مصنوعی در حوزه دفاعی را شکل می‌دهند



کلید درک روند پیشرفت نامتوازن هوش مصنوعی، در سامانه‌هایی نهفته است که این فناوری قرار است در آن‌ها فعالیت کند.

داده‌های نظرسنجی نشان می‌دهد که پذیرش هوش مصنوعی کمتر به پیشرفت مدل‌های هوش مصنوعی وابسته است و بیشتر به شرایطی بستگی دارد که امکان عملکرد قابل‌اعتماد این مدل‌ها را درون سامانه‌های پیچیده عملیاتی و نهادی فراهم می‌کنند.

چهار عامل به طور مستمر بیشترین اهمیت را نشان می‌دهند: آمادگی داده‌ها، آمادگی سامانه‌ها، سرعت فرایندهای تأمین و تدارکات و در نهایت توازن میان قابلیت‌های داخلی و وابستگی به منابع خارجی. هر یک از این عوامل نقش مشخصی ایفا می‌کنند؛ اما در کنار یکدیگر تعیین می‌کنند که آیا هوش مصنوعی می‌تواند از مرحله پروژه‌های پایلوت عبور کند و در مقیاس گسترده، اثرگذاری مأموریتی ایجاد کند یا خیر.

رویکردهای نوظهوری مانند «مدل‌های زبانی جغرافیایی» (Geospatial Language Models) که توسط سازمان‌هایی مانند NASA و ESA در حال بررسی هستند؛ نشان می‌دهند که چگونه داده‌های بزرگ‌مقیاس رصد زمین می‌توانند به بینش‌های عملیاتی تبدیل شوند؛ از تحلیل عوارض زمین گرفته تا برنامه‌ریزی مأموریت‌ها. این مدل‌ها اهمیت روزافزون سامانه‌های هوش مصنوعی چندوجهی را برجسته می‌کنند؛ سامانه‌هایی که تصاویر، داده‌های مکانی و زبان را با یکدیگر ترکیب می‌کنند تا تصمیم‌گیری‌های دفاعی سریع‌تر و آگاهانه‌تر شوند.

آمادگی داده‌ها: یک زیربنای ضروری، اما نه یک عامل تمایزکننده

فرماندهان نظامی تخمین می‌زنند که تقریباً نیمی از داده‌های سازمانی‌شان برای استفاده در هوش مصنوعی مفید است؛ اما تنها حدود یک‌سوم این داده‌ها قابل‌استفاده هستند؛ یعنی پاک‌سازی، ساختاربندی یا استانداردسازی شده‌اند تا سامانه‌های هوش مصنوعی بتوانند با آن‌ها کار کنند. همچنین تنها حدود یک‌دهم این داده‌ها در حال حاضر در این سامانه‌ها استفاده می‌شوند. این شکاف، میزان توانایی هوش مصنوعی برای فعالیت در حوزه‌های مختلف یا در مقیاس گسترده را محدود می‌کند. بنابراین، آمادگی داده‌ها یک پیش‌نیاز اساسی محسوب می‌شود، اما عاملی نیست که سازمان‌های پیشرو را از سایر سازمان‌ها متمایز کند. بسیاری از سازمان‌ها کیفیت و دسترسی‌پذیری داده‌های خود را بهبود داده‌اند، اما همچنان برای ایجاد اثرگذاری عملیاتی با مشکل مواجه‌اند؛ زیرا سامانه‌های پایین‌دستی که باید خروجی‌های هوش مصنوعی را دریافت کنند، توانایی دریافت یا اقدام بر اساس این خروجی‌ها را ندارند. هنگامی که آمادگی سامانه‌ها و بلوغ فناوری نیز در نظر گرفته می‌شود، آمادگی داده به‌تنهایی نمی‌تواند سبب موفقیت در پذیرش هوش مصنوعی کند.

آمادگی سامانه‌ها؛ گلوگاه راهبردی

محدودیت تعیین‌کننده‌تر، آمادگی سامانه‌ها است؛ یعنی توانایی سامانه‌های اصلی عملیاتی و سازمانی برای یکپارچه‌سازی هوش مصنوعی و تبدیل بینش‌های تولیدشده به اقدام. به طور میانگین، کمتر از یک سوم سامانه‌ها در حال حاضر برای استفاده از هوش مصنوعی آماده گزارش شده‌اند.

برای فرماندهان عملیاتی، اثر این مسئله کاملاً محسوس است. در محیط‌هایی که سامانه‌ها پراکنده، شکننده یا توسط معماری‌های قدیمی محدود شده‌اند، ممکن است هوش مصنوعی بینش‌های ارزشمندی تولید کند، اما این خروجی‌ها با تأخیر ارائه می‌شوند، در قالب نامناسب منتقل می‌شوند یا خارج از جریان‌های کاری مورداعتماد سازمان قرار می‌گیرند. در چنین محیط‌هایی، هوش مصنوعی بیشتر به تهیه گزارش‌ها و ارائه‌های توجیهی کمک می‌کند تا به تصمیم‌گیری‌های واقعی. آمادگی سامانه‌ها اکنون به قوی‌ترین شاخص پیش‌بینی‌کننده پذیرش هوش مصنوعی و مهم‌ترین گلوگاه راهبردی برای استقرار این فناوری در مقیاس گسترده تبدیل شده است.

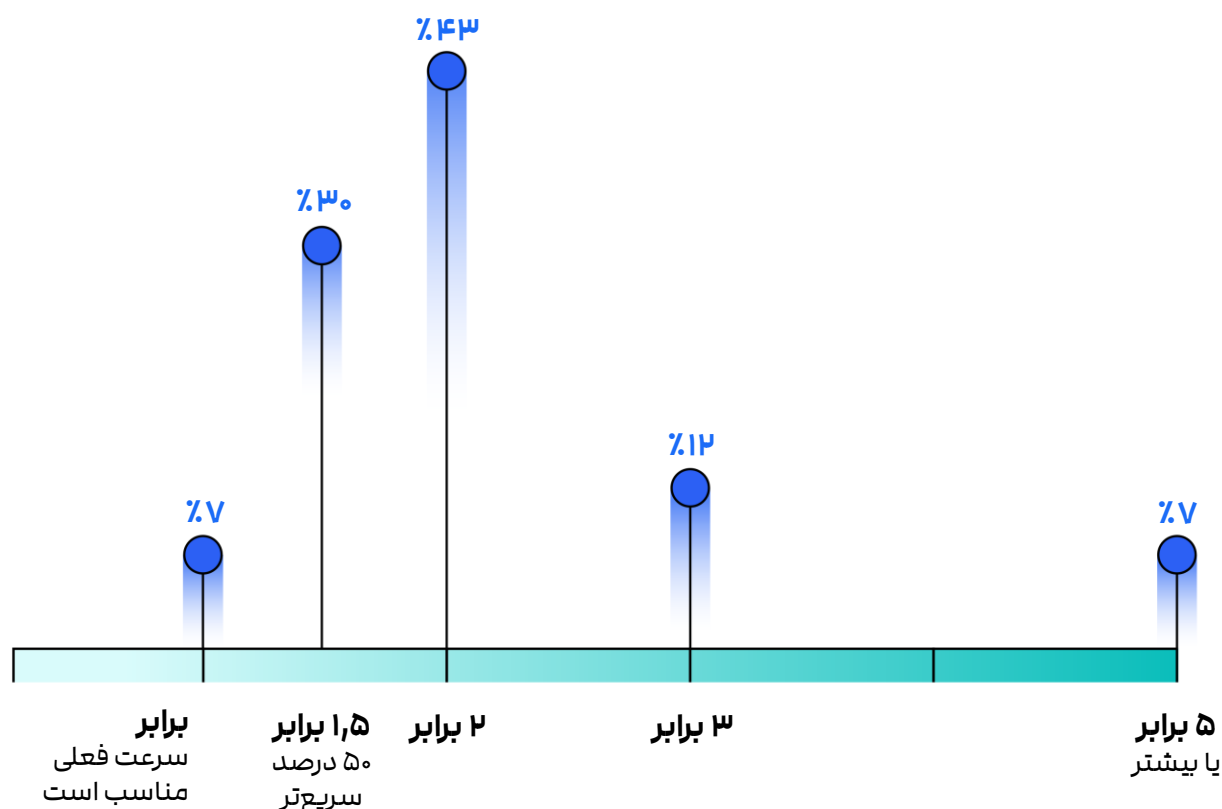
سرعت فرایندهای تأمین: فشار مشترک، ریسک مشترک

فرماندهان نظامی همچنین به فرایندهای تأمین، خرید و مجوزدهی به عنوان محدودیت‌های پایدار اشاره می‌کنند. بیش از ۶۰ درصد آنان معتقدند چرخه‌های تأمین باید حداقل دوبرابر یا بیشتر سریع‌تر شوند تا بتوانند طی سه سال آینده با پیشرفت‌های هوش مصنوعی همگام باقی بمانند. (شکل ۶)

نکته مهم این است که از نظر آماری، سرعت فرایندهای تأمین سازمان‌های پیشرو را از سایر سازمان‌ها متمایز نمی‌کند. این مسئله یک چالش ساختاری مشترک میان متحدان است. ریسک اصلی در اثر تجمعی این وضعیت نهفته است؛ زمانی که همه سازمان‌ها با سرعت پایین حرکت می‌کنند، دشمنانی که با محدودیت‌های مشابه مواجه نیستند، مزیت نسبی به دست می‌آورند. بنابراین، سرعت تأمین بیش از آنکه یک مشکل مربوط به بهره‌وری داخلی باشد، یک ریسک مرتبط با مزیت رقابتی در برابر رقبا و دشمنان محسوب می‌شود.

شکل ۶

فرماندهان معتقدند چرخه‌های تأمین باید به شکل قابل توجهی سریع‌تر شوند



پرسش: سازمان شما باید چرخه فعلی تأمین خود را تا چه ضریبی تسریع کند تا بتواند طی سه سال آینده (تا سال ۲۰۲۸) با پیشرفت‌های هوش مصنوعی همگام شود؟

پذیرش کارکردی مهم‌تر از پروژه‌های پایلوت است

تحلیل‌ها الگوی دیگری را نیز آشکار می‌کنند. ادغام هوش مصنوعی در سامانه‌های کارکردی و سازمانی مانند لجستیک، نگهداری و تعمیرات، تأمین، دفاع سایبری و امنیت اطلاعات نسبت به پروژه‌های پایلوت صرفاً مأموریتی، بهتر می‌توانند بلوغ کلی هوش مصنوعی در سازمان‌ها پیش‌بینی کنند. نتیجه این موضوع روشن است: سامانه هوش مصنوعی که شیوه اداره و عملکرد داخلی سازمان را بهبود می‌دهد، اغلب سریع‌ترین مسیر برای دستیابی به هوش مصنوعی‌ای است که نحوه اجرای مأموریت‌ها را نیز ارتقا می‌دهد.

وابستگی و تاب‌آوری

مشارکت با بخش خصوصی همچنان ضروری است. با این حال، سازمان‌هایی که وابستگی بالایی به ارائه‌دهندگان خارجی گزارش می‌کنند، سطح پایین‌تری از آمادگی داخلی و سرعت کندتری در حرکت به سمت هوش مصنوعی عملیاتی دارند. این الگو با یافته‌های گزارش پیشین IBM با عنوان AI Decision Advantage for Defense نیز همخوانی دارد؛ گزارشی که نشان می‌داد وابستگی به منابع خارجی در مراحل اولیه پذیرش هوش مصنوعی بیشترین میزان را دارد و با حرکت سازمان‌ها به سمت پیاده‌سازی و بهره‌برداری عملیاتی کاهش می‌یابد.^{۱۰}

مسئله اصلی، خود همکاری نیست، بلکه عدم توازن است؛ یعنی وضعیتی که در آن دانش، کنترل یا تداوم عملکرد نمی‌تواند در شرایط فشار، در داخل سازمان حفظ شود. با عمیق‌تر شدن ادغام هوش مصنوعی در عملیات، فرماندهان بیش از گذشته قابلیت داخلی را نه صرفاً یک ملاحظه هزینه‌ای، بلکه یک الزام برای تاب‌آوری سازمانی می‌دانند.

با این حال، این محدودیت‌های اجرایی تنها به مرزهای سازمان‌های دفاعی منفرده محدود نمی‌شوند. هرچه هوش مصنوعی عمیق‌تر در عملیات ادغام می‌شود، عوامل بنیادینی که موفقیت را در سطح سازمانی تعیین می‌کنند، بیش‌ازپیش بر تاب‌آوری ملی، حاکمیت فناورانه و اثربخشی ائتلاف‌ها تأثیر می‌گذارند. بخش بعدی گزارش، تمرکز را از اجرای هوش مصنوعی در داخل سازمان‌های دفاعی به واقعیت دیگری منتقل می‌کند؛ اینکه خود زیرساخت‌های بنیادین هوش مصنوعی به بخشی از زیرساخت راهبردی ملی تبدیل شده‌اند.

مجموع این یافته‌ها به یک نتیجه روشن منتهی می‌شود؛ مانع اصلی دستیابی به مزیت هوش مصنوعی دیگر کمبود جاه‌طلبی، منابع مالی یا آزمایش و تجربه نیست؛ بلکه مسئله اصلی، توانایی اجرا در حوزه‌های داده، سامانه‌ها، فرایندهای تأمین و قابلیت‌های سازمانی است.

بخش ۳

بنیان‌های هوش مصنوعی به زیرساخت‌های استراتژیک ملی تبدیل شده‌اند

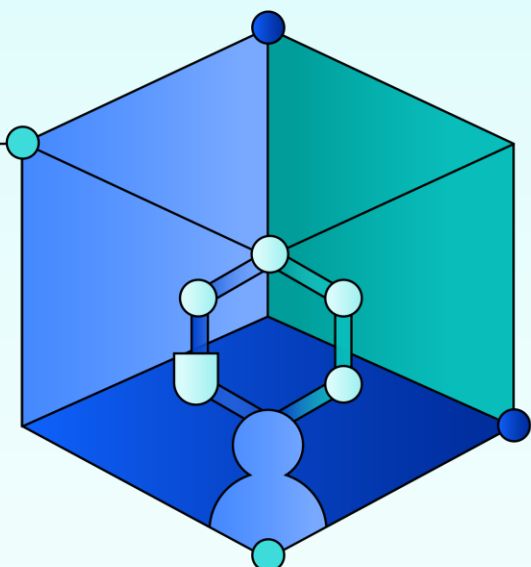
فراتر از اجرای سازمانی، فرماندهان نظامی بیش از گذشته
به هوش مصنوعی از منظر ملی و ائتلافی نگاه می‌کنند.

اکثریت فرماندهان نظامی معتقدند که هوش مصنوعی طی سه سال آینده به
شکل قابل توجهی توانمندی‌های عملیاتی و سطح آمادگی دفاعی را ارتقا خواهد
داد؛ درعین حال، همین فرماندهان اذعان دارند که این فناوری‌ها در صورت
استفاده نادرست یا حکمرانی غلط، می‌توانند خطرهای نظام‌مند و گسترده‌ای
ایجاد کنند. این دوگانگی؛ یعنی هوش مصنوعی به عنوان یک شتاب‌دهنده
توانمندی‌ها و هم‌زمان تقویت‌کننده مخاطرات باعث شده است تمرکز بحث از
برنامه‌ها و پروژه‌های منفرد به سمت زیرساخت‌های اساسی تغییر کند که در
عمل، سبب تقویت قابلیت‌های دفاعی و اثربخشی ائتلاف‌ها می‌شود.

«بالاترین اولویت ما، ایجاد زیرساخت‌های داده و
هوش مصنوعی مستقل، امن و دارای حاکمیت ملی
است؛ زیرساخت‌هایی که بتوانند به صورت مستقل
فعالیت کنند و درعین حال، قابلیت همکاری کامل با
متحدان ما را حفظ کنند.»

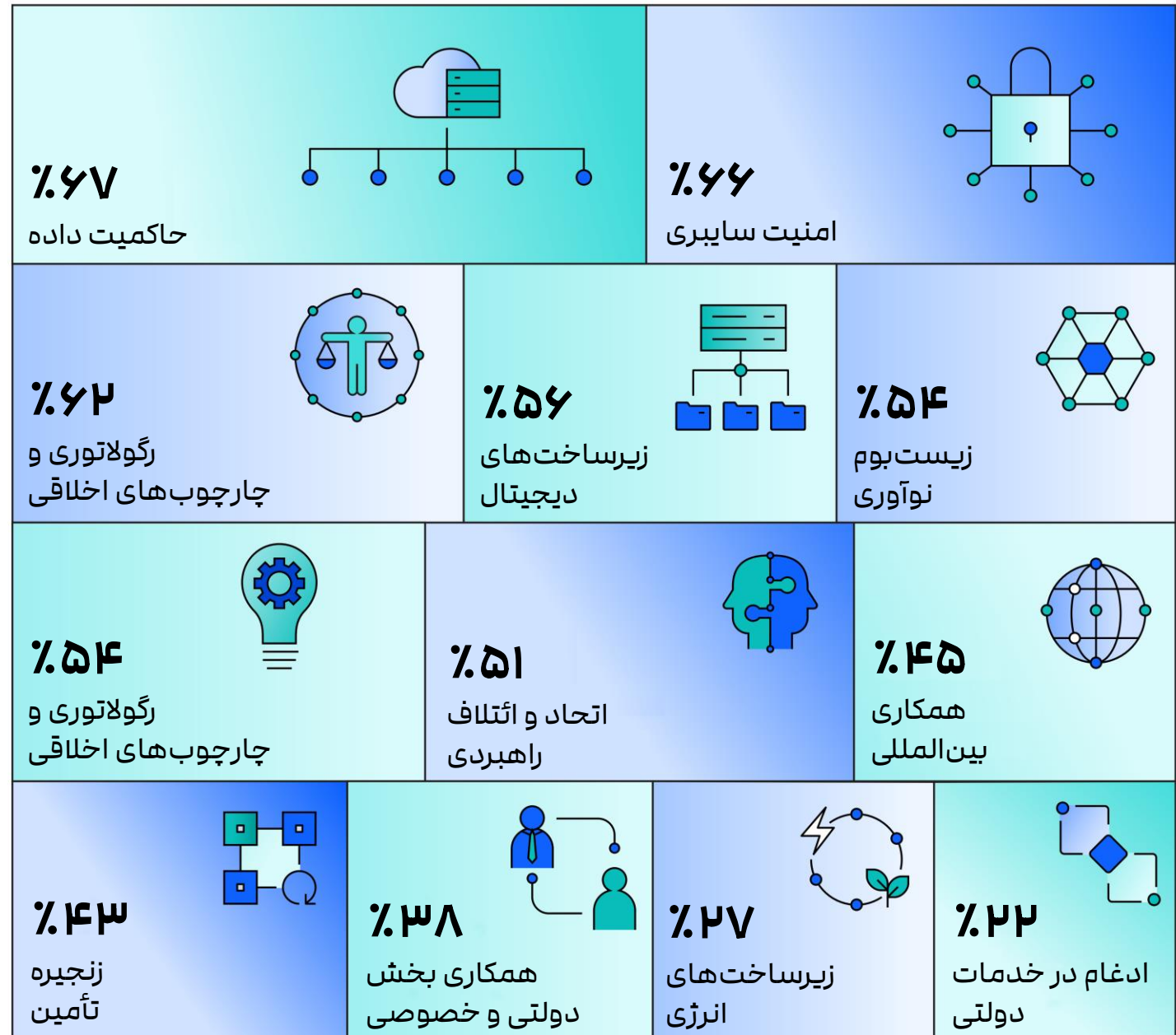
مدیر ارشد فناوری

سازمان پشتیبانی نظامی، لهستان



شکل ۴

اولویت‌های تاب‌آوری / حاکمیتی هوش مصنوعی



پرسش: کدام یک از موارد زیر برای ایجاد تاب‌آوری / حاکمیت ملی هوش مصنوعی در کشور شما از همه مهم‌تر است؟

هنگامی که از فرماندهان نظامی خواسته شد مهم‌ترین اولویت‌ها برای ایجاد تاب‌آوری ملی در حوزه هوش مصنوعی و تضمین حاکمیت واقعی بر این فناوری را مشخص کنند، آنان به قابلیت‌هایی در سطح زیرساخت اشاره کردند. (شکل ۷) مهم‌ترین اولویت‌ها عبارت‌اند از حاکمیت داده، امنیت سایبری، زیرساخت‌های دیجیتال و توان پردازشی، چارچوب‌های قانونی و اخلاقی، توسعه نیروی انسانی متخصص. تقریباً دوسوم رهبران، حاکمیت داده و امنیت سایبری را در میان مهم‌ترین اولویت‌های خود قرار می‌دهند. این موضوع نشان‌دهنده دیدگاهی روشن است: کنترل، امنیت و اعتماد، پایه‌های هر مزیت معتبر در حوزه هوش مصنوعی هستند.

«اگر مجبور باشم تنها یک اولویت اصلی را نام ببرم، آن تضمین حفظ کنترل حاکمیتی بر داده‌ها، توان پردازشی و سامانه‌های حیاتی هوش مصنوعی خواهد بود؛ به‌ویژه در حوزه دفاع و امنیت ملی.»

مدیر ارشد فناوری
سازمان پشتیبانی نظامی، کانادا

دیدگاه‌های متفاوت درباره مخاطرات اما با اهمیت‌های مشابه

اظهارنظرهای فرماندهان نشان می‌دهد که این اولویت‌ها در کشورهای مختلف چگونه نمود پیدا می‌کنند. در کشورهایی که زیرساخت‌های دیجیتال و بلوغ رایانش ابری در سطح بالاتری قرار دارد، فرماندهان بیشتر بر حکمرانی، تضمین قابلیت اعتماد و چارچوب‌های اعتمادسازی تمرکز می‌کنند. در کشورهایی که پذیرش هوش مصنوعی را در سال‌های اخیر با سرعت بیشتری آغاز کرده‌اند، تمرکز بیشتر بر کنترل داده، امنیت سایبری و توسعه قابلیت‌های داخلی قرار دارد.

این تفاوت‌ها نشان‌دهنده مسیرهای آغازین متفاوت هستند، نه اهداف متفاوت. مقصد نهایی در همه موارد یکسان است؛ یعنی زیرساخت‌های هوش مصنوعی قابل‌اعتماد، دارای حاکمیت و امن.

فرماندهان همچنین در نحوه ایجاد تعادل میان ضرورت اقدام سریع و احتیاط، دیدگاه‌های متفاوتی دارند. نزدیک به ۶۰ درصد از فرماندهانی که با آن‌ها مصاحبه شد معتقدند خطر بزرگ‌تر، عقب ماندن از رقبا و دشمنان در پذیرش هوش مصنوعی است؛ درحالی‌که گروه دیگر، بر خطر حرکت بیش از حد سریع بدون وجود سازوکارهای کنترلی و حفاظتی کافی تأکید دارند. این تفاوت دیدگاه‌ها بر تصمیم‌های مربوط به سرمایه‌گذاری و حکمرانی ملی تأثیر می‌گذارد، اما واقعیت گسترده‌تر را تغییر نمی‌دهد؛ پذیرش نامتوازن هوش مصنوعی میان متحدان، یک ریسک جمعی ایجاد می‌کند. زمانی که سطح بلوغ هوش مصنوعی میان اعضای یک ائتلاف تفاوت زیادی داشته باشد، اثربخشی عملیات ائتلافی می‌تواند به ضعیف‌ترین حلقه زنجیره وابسته شود.

مجموع این یافته‌ها به‌روشنی نشان می‌دهد که آمادگی برای هوش مصنوعی دیگر صرفاً موضوع بهینه‌سازی عملکرد سازمانی نیست؛ بلکه به مسئله‌ای مرتبط با زیرساخت ملی تبدیل شده است. ایجاد تاب‌آوری، حاکمیت و قابلیت همکاری متقابل، اکنون نیازمند تصمیم‌های آگاهانه و راهبردی است؛ تصمیم‌هایی درباره اینکه چه چیزهایی باید تحت کنترل ملی باقی بمانند، چه قابلیت‌هایی باید به اشتراک گذاشته شوند و چه استانداردهایی باید میان سازمان‌های دفاعی و ائتلاف‌ها یکسان‌سازی شوند.

در ادامه گزارش، راهنمای عملیاتی این اولویت‌های سطح ملی را به مجموعه‌ای از گام‌های عملی تبدیل می‌کند که فرماندهان می‌توانند همین امروز برای تقویت زیرساخت‌های هوش مصنوعی، کاهش ریسک‌های ساختاریافته و تبدیل آمادگی فناورانه به یک مزیت پایدار انجام دهند.

«بالاترین اولویت باید تضمین کنترل بر سخت‌افزار، نرم‌افزار و فرایند استقرار هوش مصنوعی باشد؛ زیرا این موارد برای تاب‌آوری دفاعی و اطلاعاتی حیاتی هستند.»

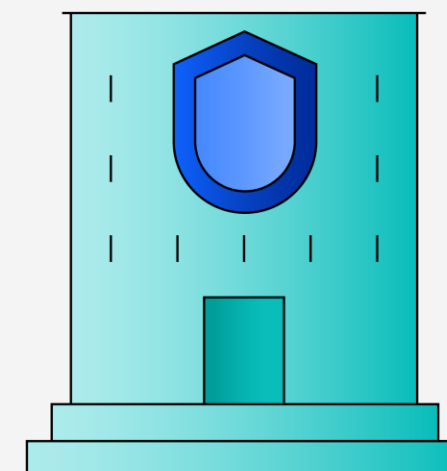
مدیر ارشد اطلاعات
سازمان پشتیبانی نظامی، استرالیا

راهنمای عملیاتی:

تبدیل جاه‌طلبی‌های هوش مصنوعی به واقعیت عملیاتی

اقدامات زیر بازتاب‌دهنده مواردی هستند که فرماندهان نظامی آن‌ها را برای سه سال آینده غیرقابل چشم‌پوشی می‌دانند؛ اقداماتی که اگر به‌درستی اجرا شوند، هوش مصنوعی را به عاملی برای تقویت آمادگی، تاب‌آوری و اعتماد تبدیل می‌کنند، نه اینکه آن را به یک وابستگی شکننده بدل سازند.

اقدامات سازمانی: سازمان‌های دفاعی



۱ نوسازی سامانه‌های اصلی برای اینکه هوش مصنوعی در جریان‌های کاری واقعی فعالیت کند.

هوش مصنوعی زمانی که بینش‌های تولیدشده توسط آن خارج از سامانه‌های عملیاتی و سازمانی باقی بمانند، نمی‌تواند ارزش‌آفرینی کند. سکوها قدیمی، معماری‌های پراکنده و یکپارچه‌سازی‌های شکننده باید نوسازی شوند تا خروجی‌های هوش مصنوعی بتوانند مستقیماً به تصمیم‌ها و اقدامات عملیاتی تبدیل شوند.

«نوسازی سامانه‌های قدیمی ضروری است؛ زیرا بسیاری از سکوها فعلی، توانایی ما برای استفاده مؤثر و مقیاس‌پذیر از هوش مصنوعی را محدود می‌کنند.»

مدیر ارشد اطلاعات
واحد نیروهای رزمی، فرانسه

۲ آمادگی داده را به‌عنوان یک انضباط عملیاتی مستمر در نظر بگیرید.

داده‌های تمیز، تحت حکمرانی مناسب و دارای قابلیت همکاری متقابل، باید به‌صورت مستمر و به‌عنوان بخشی از عملیات روزمره نگهداری شوند. ابتکارهای مقطعی و یک‌باره در حوزه داده نمی‌توانند عملکرد یا اعتمادپذیری هوش مصنوعی را در مقیاس گسترده حفظ کنند.

«اصلاحات زیربنایی در گام نخست از طریق فراهم‌کردن داده‌های تمیز و مطمئن، تنها مسیر دستیابی به خروجی‌های هوش مصنوعی است که مردم واقعاً به آن‌ها اعتماد کنند.»

مدیر ارشد اطلاعات
سازمان پشتیبانی خدمات نظامی، آلمان

۳

توانمندی پایدار داخلی در حوزه هوش مصنوعی را برای تقویت تاب‌آوری عملیاتی توسعه دهید.

پذیرش پایدار هوش مصنوعی به توسعه مهارت‌های درون‌سازمانی، انباشت دانش نهادی و ایجاد مالکیت کامل بر چرخه عمر داده‌ها، مدل‌ها و سامانه‌ها در داخل سازمان وابسته است. توانمندی داخلی مواردی مانند تداوم عملکرد، انطباق‌پذیری و حفظ کنترل را در شرایطی تضمین می‌کند که محیط عملیاتی تغییر می‌کند یا دسترسی به پشتیبانی خارجی محدود می‌شود.

«ما باید متخصصان هوش مصنوعی خودمان را در داخل سازمان تربیت کنیم؛ افرادی که بتوانند به همه کارکنان کمک کنند تا از هوش مصنوعی به شکل مؤثرتری استفاده کنند.»

مدیر ارشد اطلاعات

سازمان پشتیبانی نظامی، ایالات متحده

۴

گذار از پروژه‌های پایلوت به استقرار مأموریت‌محور را تسریع کنید.

طرح‌های ابتکاری مرتبط با هوش مصنوعی باید به طور قطع از مرحله آزمایش و اجرای پایلوت عبور کنند و در جریان‌های کاری اولویت‌دار سازمان ادغام شوند؛ به گونه‌ای که برای آن‌ها مسئولیت مشخص، شاخص‌های قابل‌اندازه‌گیری و پاسخگویی عملیاتی تعریف شده باشد.

«باید از اجرای آزمایش‌های پراکنده هوش مصنوعی عبور کنیم و این فناوری را به مجموعه‌ای از قابلیت‌های حیاتی مأموریتی تبدیل کنیم که فعالانه مورد استفاده قرار می‌گیرند و ارتباط آن‌ها با نتایج عملیاتی کاملاً مشخص است.»

مدیر ارشد اطلاعات

سازمان پشتیبانی رزمی، فرانسه

۵

اعتماد، نظارت و مسئولیت‌پذیری انسانی را از همان ابتدا در طراحی سامانه‌ها نهادینه کنید.

قابلیت توضیح‌پذیری، امکان ممیزی و مسئولیت‌پذیری شفاف انسانی باید از نخستین مراحل طراحی در سامانه‌های هوش مصنوعی لحاظ شوند. هرچه سطح خودمختاری سامانه‌ها و میزان تأثیر آن‌ها بر تصمیم‌گیری‌ها افزایش می‌یابد، این موارد نیز می‌بایست پررنگ‌تر شوند.

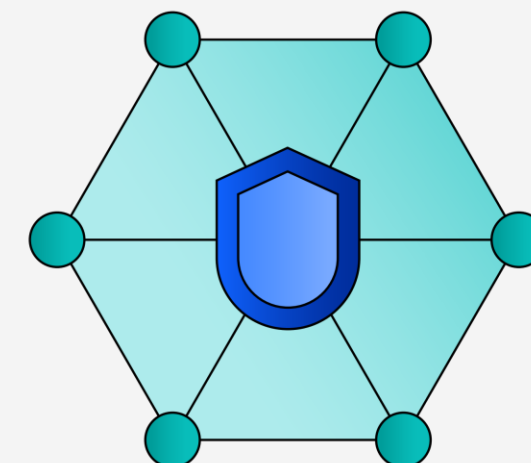
«اصلاحات زیربنایی در گام نخست از طریق فراهم‌کردن داده‌های تمیز و مطمئن، تنها مسیر دستیابی به خروجی‌های هوش مصنوعی است که مردم واقعاً به آن‌ها اعتماد کنند.»

مدیر ارشد اطلاعات

سازمان پشتیبانی خدمات نظامی، بریتانیا

اقدامات ملی:

دولت‌ها و زیست‌بوم‌های دفاعی



۱ کنترل حاکمیتی بر داده‌ها، توان پردازشی و سامانه‌های حیاتی هوش مصنوعی را تضمین کنید.

امنیت ملی به کنترل تضمین‌شده بر زیرساخت‌های هوش مصنوعی وابسته است؛ موضوعی که صرفاً به مالکیت محدود نمی‌شود، بلکه شامل دسترسی تضمین‌شده، حکمرانی و قابلیت بهره‌برداری در شرایط اختلال نیز می‌شود.

«اگر مجبور باشم تنها یک اولویت اصلی را نام ببرم، آن تضمین حفظ کنترل حاکمیتی بر داده‌ها، توان پردازشی و سامانه‌های حیاتی هوش مصنوعی خواهد بود.»

مدیر ارشد اطلاعات

سازمان پشتیبانی نظامی، کانادا

۲

در زیرساخت ملی هوش مصنوعی تاب‌آور و ایمن سرمایه‌گذاری کنید.

زیرساخت‌های هوش مصنوعی شامل رایانش ابری، توان پردازشی، انرژی و شبکه‌ها باید به‌عنوان زیرساخت راهبردی در نظر گرفته شوند؛ زیرساخت‌هایی که توانایی فعالیت در برابر حملات سایبری، اختلال در زنجیره تأمین و فشارهای ژئوپلیتیکی را داشته باشند.

«ایجاد یک زیرساخت هوش مصنوعی دارای حاکمیت ملی، پیش‌شرط تاب‌آوری کشور است؛ زیرا مانع از آن می‌شود که دشمنان خارجی به دسترسی‌های موردنیاز برای ازکارانداختن شبکه‌های دفاعی حیاتی ما دست یابند.»

مدیر ارشد اطلاعات

واحد نیروهای رزمی، دانمارک

۳

چارچوب‌ها و استانداردهای ملی الزام‌آور برای حکمرانی هوش مصنوعی ایجاد کنید.

برای نهادینه کردن امنیت، اصول اخلاقی و پاسخگویی، در عین فراهم کردن سرعت، قابلیت همکاری و اعتماد میان سازمان‌های دفاعی، به چارچوب‌های روشن ملی نیاز است.

«یک نظام واحد و منسجم حکمرانی ملی هوش مصنوعی پیاده‌سازی کنید که امکان پیشرفت را فراهم کند و همزمان امنیت و پاسخگویی را تضمین کند.»

مدیر ارشد اطلاعات

سازمان پشتیبانی خدمات رزمی، هلند

۴

مسیرهای پرورش نیروی متخصص هوش مصنوعی داخلی را در مقیاس گسترده ایجاد کنید.

تاب‌آوری بلندمدت در حوزه هوش مصنوعی به آموزش، حفظ نیروهای متخصص و ایجاد مسیرهای شغلی همسو با مأموریت‌ها وابسته است؛ عواملی که قابلیت داخلی کشورها را حفظ کرده و وابستگی خارجی را کاهش می‌دهند.

«باید از اجرای آزمایش‌های پراکنده هوش مصنوعی عبور کنیم و این فناوری را به مجموعه‌ای از قابلیت‌های حیاتی مأموریتی تبدیل کنیم که فعالانه مورد استفاده قرار می‌گیرند و ارتباط آن‌ها با نتایج عملیاتی کاملاً مشخص است.»

مدیر ارشد اطلاعات

سازمان پشتیبانی رزمی، فرانسه

۵

حاکمیت فناورانه را به گونه‌ای طراحی کنید که ائتلاف‌ها را مستحکم کند، نه اینکه موجب انزوا شود.

حاکمیت ملی باید با قابلیت همکاری مطمئن میان متحدان سازگار باشد. استانداردهای مشترک و همکاری مبتنی بر اعتماد، برای اثربخشی دفاع جمعی ضروری هستند.

«سامانه‌های هوش مصنوعی دارای حاکمیت ملی باید ضمن حفظ کنترل کشورها، قابلیت همکاری متقابل با متحدان را نیز حفظ کنند.»

مدیر ارشد اطلاعات

واحد نیروهای رزمی، هلند

کریستینا کابایه فوگت

Cristina Caballé Fuguet

نایب رئیس، بخش عمومی بین‌المللی IBM

www.linkedin.com/in/cristina-caballe-77516938/

نبیل ابوتانوس

Nabil Aboutanos

شریک ارشد، مدیر بخش دولتی مرکز مشاوره IBM

www.linkedin.com/in/nabil-aboutanos-0020a950/

رودری اروس‌میت

Rhodri Arrowsmith

مدیر بخش دولتی بریتانیا و ایرلند، شریک مدیریتی مشتریان مرکز مشاوره IBM

www.linkedin.com/in/rhodriarrowsmith-9b49a3/

کاترین گارنر

Catherine Garner

شریک مرکز مشاوره IBM

www.linkedin.com/in/catherinegarner-9560a4b2/

کریستینا رهبری بخش عمومی بین‌المللی IBM را بر عهده دارد؛ بخشی که در بیش از ۱۷۰ کشور، نوآوری، راهکارهای متمایز صنعتی و خدمات مشاوره‌ای را برای دولت‌ها ارائه می‌کند. او به دلیل رهبری فکری و ثبت اختراعات خود شناخته شده است. کریستینا بیش از ۲۵ سال تجربه در بخش دولتی دارد و عضو چندین هیئت صنعتی، از جمله AFCEA International است.

نبیل به عنوان نایب رئیس و شریک ارشد در مرکز مشاوره IBM کانادا فعالیت می‌کند و مدیریت بخش دولتی این مجموعه را بر عهده دارد. او مشتریان دولتی در سطوح فدرال، استانی و شهری را در مسیر تحول دیجیتال گسترده، همسوسازی سیاست‌ها و نوسازی ارائه خدمات هدایت می‌کند.

رودری رهبری ابتکارهای تحول و مشاوره در بخش سلامت عمومی و دولتی IBM در بریتانیا را بر عهده دارد. او تجربه مشاوره راهبردی را با اجرای عملیاتی در حوزه‌هایی مانند ERP/HCM، پلتفرم‌های دیجیتال و اکوسیستم‌های مشارکتی ترکیب می‌کند تا نتایج بهتری برای شهروندان ایجاد شود.

کاترین ۲۵ سال تجربه همکاری با سازمان‌های دولتی و نهادهای سلامت در استرالیا و نیوزیلند در تمامی سطوح را دارد و در طراحی، توسعه و پیاده‌سازی طیف گسترده‌ای از راهکارهای کسب‌وکاری مشارکت داشته است. او علاوه بر تجربه کاری در استرالیا، با تعدادی از مشتریان دولتی در بریتانیا نیز همکاری کرده است.

سوزان وج

Susan Wedge

شریک مدیریتی، بازار دولت فدرال ایالات متحده مرکز مشاوره IBM

www.linkedin.com/in/susanewedge/

نوریکو یاماشیتا

Noriko Yamashita

شریک بخش دولتی IBM ژاپن

www.linkedin.com/in/norikoyamashita-a1897593/

کی‌وون سونگ

Kee Won Song

مدیر پژوهش‌های جهانی دولتی مؤسسه ارزش‌آفرینی کسب‌وکار IBM

www.linkedin.com/in/keewonsong/

دیو زاهارچوک

Dave Zaharchuk

مدیر پژوهش مؤسسه ارزش‌آفرینی کسب‌وکار IBM

www.linkedin.com/in/david-zaharchuk/

سوزان یک مدیر کسب‌وکار، توسعه‌دهنده استعداد و مشاور باتجربه است که بر ارائه راهکارهای نوآورانه فناوری برای مشتریان بخش خدمات عمومی تمرکز دارد. او سابقه موفقیت در دستیابی به نتایج تجاری و دستاوردهای مشتریان در مقیاس گسترده دارد.

یاماشیتا مسئول حوزه بخش دولتی در ژاپن، شامل سازمان‌های دولتی و مؤسسات آموزشی است. او با دهه‌ها تجربه، به نهادهای دولتی کمک می‌کند تا از طریق فناوری و خدمات مشاوره‌ای، خدمات شهروندی را ارتقا دهند و اهداف مأموریتی خود را محقق کنند.

کی‌وون به مشتریان دولتی درباره چالش‌های پیچیده امنیتی، فناوری و نوآوری مشاوره می‌دهد و از تجربه گسترده خود در حوزه‌های راهبرد، عملیات و تحلیل داده‌محور بهره می‌گیرد. تخصص او ایجاد پیوند میان فناوری‌های نوظهور و تصمیم‌گیری‌های حیاتی مأموریتی برای ارتقای اثربخشی بخش دولتی است.

دیو مدیر پژوهش در مؤسسه ارزش‌آفرینی کسب‌وکار IBM است و پژوهش‌های مرتبط با موضوعات حیاتی بخش دولتی را هدایت می‌کند. او در سطح جهانی به دلیل دیدگاه‌های راهبردی خود شناخته شده است و به رهبران ارشد دولتی در حوزه‌های راهبرد، نوآوری و تحول مشاوره می‌دهد.

این مطالعه توسط مؤسسه ارزش‌آفرینی کسب‌وکار IBM با همکاری Oxford Economics در ژانویه ۲۰۲۶ انجام شده است. این پژوهش بر اساس یک نظرسنجی از ۶۰۰ مدیر ارشد اطلاعات و مدیر ارشد فناوری در سازمان‌های نظامی و کشورهای عضو ناتو و ائتلاف فایو آیز انجام شده است.

پاسخ‌دهندگان پیش از ورود به مطالعه غربالگری شدند تا اطمینان حاصل شود که مسئولیت مستقیم در زمینه راهبرد یا پیاده‌سازی هوش مصنوعی دارند. این نظرسنجی ترکیبی از پرسش‌های مبتنی بر مقیاس لیکرت، پرسش‌های عددی و پرسش‌های باز بود و موضوعاتی مانند سرمایه‌گذاری، آمادگی، بلوغ فناوری، موانع و ملاحظات مرتبط با تاب‌آوری ملی را پوشش می‌داد.

این روش‌شناسی بر پژوهش‌های پیشین IBM در حوزه دفاع، از جمله گزارش AI Decision Advantage for Defense، بنا شده است و امکان مقایسه طولی یافته‌ها را فراهم می‌کند؛ درعین‌حال، پرسش‌های جدیدی درباره هوش مصنوعی مولد، هوش مصنوعی عامل‌محور، سرعت فرایندهای تأمین و حاکمیت فناوریانه نیز به آن افزوده شده است.



رویکرد تحلیلی پژوهش با آماده‌سازی و اعتبارسنجی داده‌های پایه آغاز شد؛ این مرحله شامل بررسی کامل بودن پاسخ‌ها، ارزیابی سازگاری پاسخ‌ها و نرمال‌سازی متغیرهای مبتنی بر مقیاس بود. برای ایجاد الگوهای پایه در حوزه‌های سرمایه‌گذاری، مراحل پذیرش و ابعاد آمادگی از آمار توصیفی استفاده شد.

سپس، تحلیل با استفاده از مقایسه‌های دوگانه و بررسی روابط میان ویژگی‌های سازمانی، بلوغ هوش مصنوعی، آمادگی سامانه‌ها، پذیرش کارکردی و اولویت‌های ملی ادامه یافت. تمرکز ویژه‌ای بر تمایز میان آزمایش‌های سطح پیلوت و استقرار عملیاتی وجود داشت؛ همچنین استفاده‌های خاص مأموریتی از هوش مصنوعی با پذیرش آن در سامانه‌های سازمانی و کارکردی مقایسه شد.

در موارد مناسب، معناداری آماری با استفاده از آستانه $p < 0.05$ ارزیابی شد. نتایج تنها بر معناداری آماری تکیه نداشتند، بلکه قدرت جهت‌گیری، سازگاری میان گروه‌های مختلف و ارتباط عملی یافته‌ها نیز موردتوجه قرار گرفت. پاسخ‌های کیفی نیز با روش تحلیل موضوعی بررسی شدند تا زمینه لازم برای تفسیر یافته‌های کمی فراهم شود و دیدگاه رهبران درباره اعتماد، حکمرانی و تاب‌آوری آشکار شود.

مؤسسه ارزش‌آفرینی کسب‌وکار IBM یک پرسش‌نامه جامع و چندبخشی طراحی کرد که بر پایه پژوهش‌های پیشین IBV در حوزه دفاعی، از جمله AI Decision Advantage for Defense، شکل گرفته بود. این پرسش‌نامه ضمن امکان مقایسه روندهای زمانی، حوزه‌های جدید پژوهشی را نیز پوشش می‌داد.

ابزار نهایی پژوهش، ترکیبی از پرسش‌های مقیاس لیکرت، عددی، طبقه‌بندی‌شده و باز بود تا هم معیارهای کمی و هم زمینه‌های کیفی را ثبت کند.

این نظرسنجی موضوعات زیر را بررسی کرد:

- **اهمیت راهبردی** هوش مصنوعی و سطح سرمایه‌گذاری پیش‌بینی‌شده
- **آمادگی داده‌ها**، آمادگی سامانه‌ها و میزان ادغام هوش مصنوعی در جریان‌های کاری عملیاتی
- **پذیرش و سطح بلوغ** هوش مصنوعی سنتی، هوش مصنوعی مولد و هوش مصنوعی عامل‌محور
- **موانع مقیاس‌پذیری** هوش مصنوعی از جمله سرعت فرایندهای تأمین و قابلیت‌های سازمانی
- **ملاحظات سطح ملی**، مانند حاکمیت هوش مصنوعی، امنیت سایبری، زیرساخت‌ها و قابلیت همکاری میان متحدان

Oxford Economics فرایند جمع‌آوری داده‌ها را مدیریت کرد و با استفاده از اجرای مستقل نظرسنجی، کنترل‌های کیفی و پروتکل‌های ناشناس‌سازی، بی‌طرفی، محرمانگی و سازگاری داده‌ها میان کشورهای مختلف را تضمین کرد.

Contributors

Andrew Boyd

US Defense Industry Leader, IBM Consulting

Lorenzo Cattano

Australia Defence Leader, IBM Consulting

Jörg Kunz

Germany Defense Leader, IBM Consulting

Dan McBride

UK Defence Leader, IBM Consulting

Greg Porpora

Global Defense CTO and Distinguished Engineer, IBM Consulting

Steve Rawsthorn

Executive Chairman, SiXworks

Meeyoung Yoon

Global Defense Industry Solutions Leader, IBM Consulting

Douna Daou

Design Lead, IBM Institute for Business Value

Kristine Rodriguez

Editor-in-Chief, IBM Institute for Business Value

Carol Bertocci

Business Analytics Consultant, IBM Institute for Business Value

Related reports

Government in the AI era

ibm.biz/gov-ai-era

Elusive threats, elastic defense: Securing AI at scale

ibm.biz/ai-cybersecurity

Defense Manufacturing in the AI Era

ibm.biz/defense-in-ai-era

About Research Insights

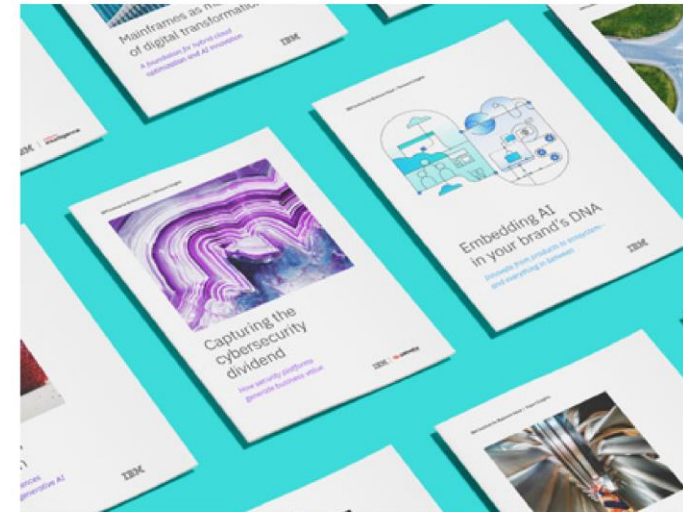
Research Insights are fact-based strategic insights for business executives on critical public- and private-sector issues. They are based on findings from analysis of our own primary research studies. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights.

To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also find us on LinkedIn at ibm.co/ibv-linkedin.



Subscribe to our IdeaWatch newsletter

Just the insights. At your fingertips. Delivered monthly.

Brought to you by the IBM Institute for Business Value, ranked #1 in thought leadership quality by Source Global Research for the third consecutive year.

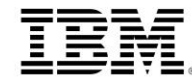
Research-based thought leadership insights, data, and analysis to help you make smarter business decisions and more informed technology investments.

Subscribe now: ibm.biz/ideawatch



Notes and sources

- 1 “The Secretary General’s Annual Report, 2024.” NATO. Accessed April 24, 2026. <https://www.nato.int/en/about-us/official-texts-and-resources/secretary-generals-annual-report/the-secretary-general-s-annual-report-2024>
- 2 “Global Peace Index 2024.” Institute for Economics and Peace. Accessed April 24, 2026. <https://www.economicsandpeace.org/wp-content/uploads/2024/06/GPI-2024-web.pdf>
- 3 NATO press release. “Defence Expenditure of NATO Countries (2014-2024).” Accessed April 24, 2026. https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2024/6/pdf/240617-def-exp-2024-en.pdf
- 4 Dian, Dr. Nan, Lorenzo Scarazatto, and Jade Guiberteau Ricard. “NATO’s new spending target: challenges and risks associated with a political signal.” Stockholm International Peace Research Institute. June 27, 2025. <https://www.sipri.org/commentary/essay/2025/natos-new-spending-target-challenges-and-risks-associated-political-signal>
- 5 Probasco, Emelia, Helen Toner, Matthew Burtell, and Tim G. J. Rudner. “AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks.” Center for Security and Emerging Technology. April 2025. <https://cset.georgetown.edu/wp-content/uploads/CSET-AI-for-Military-Decision-Making.pdf>
- 6 “The Secretary General’s Annual Report, 2024.” NATO. Accessed April 24, 2026. <https://www.nato.int/en/about-us/official-texts-and-resources/secretary-generals-annual-report/the-secretary-general-s-annual-report-2024>
- 7 Probasco, Emelia, Helen Toner, Matthew Burtell, and Tim G. J. Rudner. “AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks.” Center for Security and Emerging Technology. April 2025. <https://cset.georgetown.edu/wp-content/uploads/CSET-AI-for-Military-Decision-Making.pdf>
- 8 Probasco, Emelia, Helen Toner, Matthew Burtell, and Tim G. J. Rudner. “AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks.” Center for Security and Emerging Technology. April 2025. <https://cset.georgetown.edu/wp-content/uploads/CSET-AI-for-Military-Decision-Making.pdf>
- 9 “Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions.” Organisation for Economic Co-operation and Development. September 18, 2025. https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html
- 10 *AI decision advantage for defense: Closing the gap between development and deployment.* IBM Institute for Business Value. May 2024. ibm.co/ai-decision-advantage-for-defense



© Copyright IBM Corporation 2026

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | May 2026

IBM, the IBM logo, ibm.com and Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at: ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.