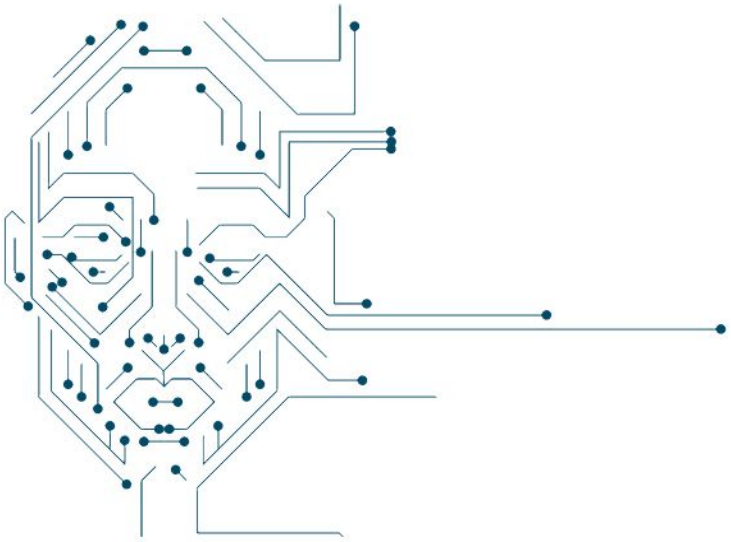
پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)
ITRC

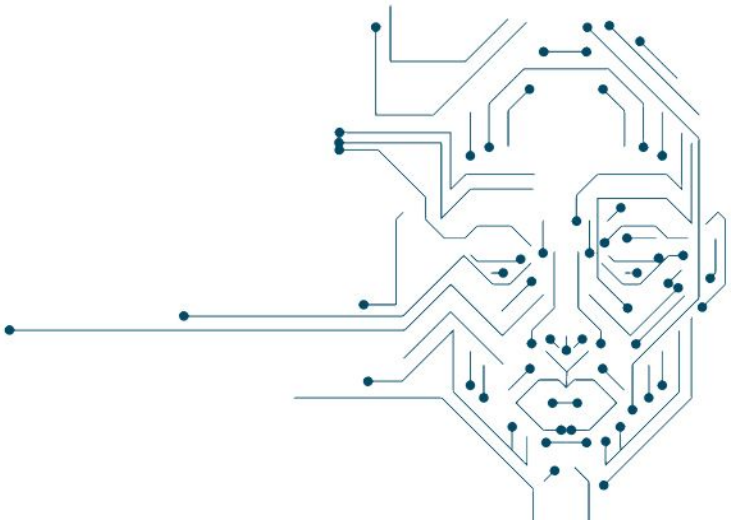
سیاست نامه هوش مصنوعی - شماره سوم- مرداد ۱۴۰۴

هوش مصنوعی در جنگ ترکیبی؛
استفاده نظامی رژیم صهیونیستی علیه ایران و الزامات سیاستی



ITRC
پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

فهرست



نبردها به میدان رقابت الگوریتم‌ها بدل شدند!

خلاصه مدیریتی

تحولات اخیر در حوزه هوش مصنوعی نظامی و استفاده گسترده رژیم صهیونیستی از فناوری‌های مبتنی بر هوش مصنوعی در حملات علیه ایران در جنگ ۱۲ روزه اخیر، نشانه ای آشکار از آغاز عصر جدیدی از جنگ‌های ترکیبی در منطقه است. این گزارش سیاستی، با بررسی ابعاد مختلف بکارگیری هوش مصنوعی در جنگ اخیر، نشان می‌دهد پهپادهای خودران هدف‌زن، سامانه‌های خودمختار کشنده، حملات سایبری مبتنی بر هوش مصنوعی و عملیات‌های جنگ روایت‌ها، قدرت تهاجمی دشمن را به‌طور بی‌سابقه‌ای افزایش داده است. کشور ما در سال های اخیر با تکیه بر توان دانشمندان و متخصصان خود، به پیشرفت های خیره کننده و غرورآفرینی در حوزه موشکی و پهپاد دست یافته و جایگاه بازدارندگی دفاعی کشور را به سطحی کم نظیر در جهان ارتقا داده است. با این حال، تجربه این جنگ نشان داد که شکاف فناورانه ایران با دشمنان منطقه‌ای در حوزه سیستم‌های تسلیحاتی هوشمند و زیرساخت‌های مقاوم دیجیتال، تهدیدی جدی علیه امنیت ملی و اقتدار دفاعی محسوب می شود. علاوه بر تهدیدات نظامی، اتکای شدید خدمات حیاتی و دولت الکترونیک کشور به اتصال دائم اینترنت و فقدان معماری آفلاین‌محور، آسیب‌پذیری‌های جدی برای امنیت ملی در سناریوهای جنگ ترکیبی هوش مصنوعی محور ایجاد کرده است. با این حال، هوش مصنوعی تنها تهدید نیست؛ بلکه فرصتی راهبردی برای ارتقاء قدرت دفاعی، تاب‌آوری زیرساخت‌ها، امنیت سایبری و توان مقابله با جنگ روایت‌ها به شمار می‌آید. همانگونه که متخصصان ایرانی با عزم و اراده ملی در حوزه موشکی و پهپادی به دستاوردهای غرورآفرین رسیدند، امروز نیز ضروری است در عرصه هوش مصنوعی نظامی با شتاب و جسارت به فوریت عمل شود تا امنیت ملی و اقتدار منطقه ای کشور بیش از پیش، تثبت گردد. اقدامات راهبردی پیشنهادی:

کوتاه‌مدت (در حدود یک تا سه ماه):

- تشکیل کارگروه ملی هوش مصنوعی نظامی و دفاعی.
- ارزیابی فوری آسیب‌پذیری زیرساخت‌های حیاتی در برابر حملات هوش مصنوعی محور.
- تدوین الزامات فنی طراحی دولت الکترونیک مقاوم و آفلاین‌محور.

میان‌مدت (در حدود شش ماه تا یک سال):

- توسعه نمونه‌های اولیه سامانه‌های خودمختار بومی دفاعی.
- راه‌اندازی مرکز ملی پایش محتوای جعلی مبتنی بر هوش مصنوعی.
- تدوین چارچوب ملی اخلاقی و حقوقی هوش مصنوعی نظامی.

بلندمدت (در حدود سه تا پنج سال):

- تدوین سند ملی حکمرانی هوش مصنوعی نظامی و دکترین جنگ‌های هوش مصنوعی محور.
- توسعه مدل‌های زبانی بزرگ تخصصی امنیت سایبری و دفاعی.
- پیگیری دیپلماسی منطقه‌ای برای محدودسازی توسعه سلاح‌های خودمختار کشنده.

هوش مصنوعی در جنگ ترکیبی
تهدیدات و الزامات سیاستی ایران

آغاز عصر جنگ ها با محوریت هوش مصنوعی در منطقه و ضرورت اقدام فوری

خلاء چارچوب های حقوقی و اخلاقی

فقدان حکمرانی هوش مصنوعی تظامی

اطلاعات جعلی و جنگ روایت ها

قدرت افزایی عملیات های شناختی مبتنی بر هوش مصنوعی

آسیب پذیری زیرساخت ها

ضرورت Edge AI و دولت الکترونیک آفلاین

نبرد هوایی هوشمند

توسعه پهپادهای انتحاری هدف زن علیه افراد و زیرساخت‌ها

سلاح های خودمختار

افزایش سرعت و دقت عملیات تظامی دشمن

فرصت ها	تهدیدها
ارتقا بازدارندگی دفاعی	افزایش شکاف فناورانه با دشمنان منطقه ای
▪ افزایش تاب آوری زیرساخت ها ▪ توسعه امنیت سایبری مبتنی بر هوش مصنوعی ▪ تدوین چارچوب های اخلاقی و حقوقی پیشرو در منطقه	▪ آسیب پذیری زیرساخت ها ▪ توسعه اطلاعات جعلی شخصی سازی شده ▪ فقدان مسئولیت پذیری حقوقی در کاربرد بر علیه غیرنظامیان

توصیه های سیاستی

بلندمدت	میان مدت	کوتاه مدت
تدوین دکترین ملی جنگ های مبتنی بر هوش مصنوعی توسعه LLM های امنیتی بومی دیپلماسی منطقه ای محدودسازی کاربرد سلاح های خودمختار	توسعه سامانه های خودمختار بومی پایش هوشمند محتوای جعلی تدوین چارچوب اخلاقی و حقوقی کاربرد هوش مصنوعی در سیستم های نظامی	تشکیل کارگروه ملی هوش مصنوعی نظامی و دفاعی ارزیابی آسیب پذیری زیرساخت ها تدوین الزامات دولت الکترونیک مقاوم

پیشگفتار

تحولات پرشتاب فناوری‌های پیشرفته، به‌ویژه هوش مصنوعی، ماهیت قدرت ملی و مفهوم امنیت را در نظام بین‌الملل دگرگون ساخته است. جنگ اخیر رژیم صهیونیستی علیه جمهوری اسلامی ایران، نقطه عطفی در تاریخ منطقه بود که طی آن، برای نخستین‌بار فناوری‌های هوش مصنوعی محور در مقیاسی عملیاتی و ترکیبی علیه کشور به‌کار گرفته شد. این رویداد، نه‌تنها بیانگر شکاف فناورانه ایران با دشمنان منطقه‌ای است، بلکه هشداری جدی درباره ابعاد نوظهور تهدیدات نظامی، سایبری و شناختی مبتنی بر هوش مصنوعی محسوب می‌شود. «رصدنامه سیاستی هوش مصنوعی – ویژه نامه شماره سوم» با هدف بررسی ابعاد استفاده نظامی از هوش مصنوعی در جنگ ترکیبی علیه ایران و ارائه الزامات سیاستی کشور تدوین گردیده است. در این گزارش، تلاش شده ضمن مروری بر کاربردهای نظامی، امنیتی، سایبری و جنگ روایت‌های هوش مصنوعی، پیامدهای راهبردی و شکاف‌های فناورانه کشور شناسایی و راهکارهای سیاستی کوتاه‌مدت، میان‌مدت و بلندمدت برای ارتقاء تاب‌آوری و قدرت دفاعی جمهوری اسلامی ایران ارائه گردد. امید است این گزارش بتواند با ارائه تصویری واقعی و آینده‌نگر از تحولات هوش مصنوعی در حوزه امنیت ملی، مبنایی برای تصمیم‌گیری‌های هوشمندانه و راهبردی مدیران ارشد کشور فراهم آورد.

تهیه‌کنندگان (به ترتیب حروف الفبا): کاظم احمدی، متین سادات برقعی، ناهید بزرگ‌خو
زهرا داودآبادی، اعظم صادق‌زاده،فریده شهیدی، فاطمه کسائی نجفی، نیلوفر مرادحاصل
اعظم سادات مرتضوی، فاطمه ناصر اسلامی، افسانه واحدیان، آنیتا هادی‌زاده
ویراستاری: زهرا داودآبادی
بازبینی و تدوین نهایی: اعظم صادق‌زاده

پژوهشگاه ارتباطات و فناوری اطلاعات/ مرداد ۱۴۰۴

سلاح‌های خودمختار و بازدارندگی آینده:
ظرفیت‌ها، تهدیدها و موقعیت ایران در رقابت جهانی

ادغام هوش مصنوعی در سیستم‌های نظامی، نقطه عطفی در تاریخ جنگ‌های مدرن ایجاد کرده است. «سلاح‌های خودمختار » به عنوان فناوری‌های نسل جدید، با امکان انتخاب و درگیری با اهداف بدون مداخله انسانی، ماهیت جنگ و امنیت ملی کشورها را متحول کرده‌اند.

هرچند مفهوم سلاح‌های خودکار سابقه‌ای طولانی دارد و نمونه‌های اولیه آن شامل مین‌ها، اژدرها، بمب‌های هدایت‌شونده رادیویی مانند FX۱۴۰۰ و سامانه‌های دفاع دریایی خودکار بوده‌اند، اما نسل جدید سلاح‌های خودمختار با تکیه بر الگوریتم های پیشرفته هوش مصنوعی، قادر به اجرای عملیات پیچیده با حداقل نظارت انسانی هستند.

روند جهانی توسعه سلاح‌های خودمختار

ایالات متحده: وزارت دفاع آمریکا به سرعت در حال توسعه و ادغام هوش مصنوعی در پهپادهای خودران، سیستم‌های شناسایی و وسایل نقلیه زمینی بدون سرنشین است. هدف اصلی، افزایش کارایی عملیاتی، ارتقاء سرعت واکنش، و کاهش خطرات جانی برای پرسنل نظامی است.

رژیم صهیونیستی: با سامانه‌هایی نظیر پهپادهای هارپی و هاروپ، قابلیت‌های هدف‌گیری خودکار رادارهای دشمن و عملیات‌های پرسه‌زن مرگبار را تثبیت کرده است. استفاده از این فناوری‌ها علیه ایران در حملات اخیر، نشان‌دهنده تمرکز استراتژیک این رژیم بر ترکیب هوش مصنوعی و تسلیحات خودران برای افزایش قدرت بازدارندگی و تهاجم سریع است.

کره جنوبی: ربات نگهبان SGR-A۱ در مرز DMZ با کره شمالی مستقر شده است. این سامانه می‌تواند به‌صورت خودکار اهداف را شناسایی و با آن‌ها درگیر شود، هرچند طبق گزارش‌ها همچنان تحت کنترل انسانی عمل می‌کند.

فرصت‌های راهبردی برای ایران

توسعه و بومی‌سازی سلاح‌های خودمختار، توان بازدارندگی کشور را به‌طور کیفی ارتقاء می‌دهد و امکان دفاع سریع، دقیق و بدون ریسک انسانی را فراهم می‌سازد.

بهره‌گیری از سلاح‌های خودمختار در مأموریت‌های شناسایی مرزی و دفاع زیرساخت‌های حیاتی، امنیت ملی پایدارتر و پاسخ‌گویی موثرتر به تهدیدات منطقه‌ای را ممکن می‌کند.

سرمایه‌گذاری هدفمند در این حوزه، قدرت چانه‌زنی امنیتی ایران را در سطح منطقه ای و بین‌المللی تقویت خواهد کرد.

تهدیدهای راهبردی و پیامدهای آن

تشدید درگیری‌ها بدون فرصت مداخله انسانی: سیستم‌های خودران با سرعت ماشین تصمیم می‌گیرند و می‌توانند باعث تشدید ناگهانی جنگ شوند.

ابهام در پاسخگویی اخلاقی و حقوقی: مشخص نیست مسئولیت عملیات‌های سلاح‌های خودمختار بر عهده برنامه‌نویس، تولیدکننده، فرمانده نظامی یا سیستم خودران است.

اشاعه به بازیگران غیردولتی و تروریستی: هزینه پایین‌تر و سهولت دسترسی به فناوری‌های هوش مصنوعی امکان بهره‌برداری گروه‌های غیردولتی از سلاح‌های خودمختار سبک را افزایش می‌دهد که تهدیدی مستقیم برای امنیت ملی است.

آسیب‌پذیری سایبری و جنگ الکترونیک: اتکای سلاح‌های خودمختار به شبکه‌های ارتباطی و نرم‌افزارهای پیشرفته، آن‌ها را در برابر حملات سایبری، هک، پارازیت و امثال آن بسیار آسیب‌پذیر می‌سازد.

پیشنهادهای سیاستی برای رفع شکاف فناورانه کشور

تجربه جنگ اخیر رژیم صهیونیستی علیه ایران نشان داد که فاصله فناوری‌های نظامی خودمختار میان ایران و دشمنان منطقه‌ای در حال گسترش است. در حالی که سلاح‌های خودمختار رژیم صهیونیستی به سطح عملیاتی رسیده، ایران همچنان فاقد سامانه‌های دفاعی متقارن یا تهاجمی بومی با قابلیت‌های مشابه است. در غیاب توسعه سامانه‌های خودمختار بومی و فناوری‌های دفاعی متقارن، ایران در معرض تهدید فزاینده سلاح‌های خودمختار دشمنان قرار خواهد داشت. تدوین سیاست جامع توسعه و حکمرانی سلاح‌های خودمختار، اقدامی فوری برای حفظ امنیت ملی، بازدارندگی هوشمند و پیشگیری از افزایش شکاف فناورانه نظامی کشور است. راهبردهای پیشنهادی:

• تشکیل کارگروه ملی توسعه هوش مصنوعی نظامی و دفاعی با ماموریت تدوین راهبرد، برنامه عملیاتی و پروژه های اولویت دار با مشارکت وزارت دفاع، وزارت ارتباطات و پژوهشگاه های مرتبط.

• ارزیابی آسیب‌پذیری‌های زیرساختی کشور در برابر سلاح‌های خودمختار مهاجم.

میان مدت:

• توسعه نمونه‌های اولیه سامانه‌های دفاعی ضد سلاح‌های خودمختار و فناوری‌های خنثی‌سازی پهپادهای خودران دشمن.

بلند مدت:

• سرمایه‌گذاری در تحقیقات بنیادی هوش مصنوعی نظامی و توسعه سلاح‌های خودمختار بومی مقاوم در برابر جنگ‌های الکترونیک و سایبری.

• دیپلماسی فعال دفاعی در سطح منطقه و بین‌الملل برای تدوین معاهدات محدودکننده توسعه تسلیحات خودمختار تهاجمی به منظور کاهش ریسک تهدیدات.

هوش مصنوعی در نبردهای هوایی:

بازآرایی موازنه قدرت و الزامات دفاعی ایران

بکارگیری هوش مصنوعی در نبردهای هوایی، به‌عنوان یکی از تحولات راهبردی نظامی، ابعاد قدرت‌افزایی و بازدارندگی را در ارتش‌های پیشرفته متحول ساخته است. هوش مصنوعی پیشرفته می‌تواند انقلابی در ساختار نیروی هوایی کشورها ایجاد کند؛ به‌ویژه از طریق توسعه هواپیماهای بدون سرنشین و پهپادهای خودران مجهز به الگوریتم‌های هوشمند که بدون نیاز به خلبان انسانی، وظایف پیچیده شناسایی، هدف گیری و حمله را انجام می‌دهند. بر اساس تجربیات جهانی، بکارگیری هوش مصنوعی در طراحی هواپیماهای خودران موجب افزایش تعداد هواپیماهای رزمی، کاهش وزن، هزینه و نیاز به زیرساخت‌های پشتیبانی انسانی شده است. این تغییر پارادایمی به ارتش‌ها امکان می‌دهد در مقایسه با جنگنده‌های سرنشین دار، ناوگان بزرگ‌تر، ارزان‌تر و با قابلیت مانور بالاتر ایجاد کنند. در جنگ اخیر رژیم صهیونیستی علیه ایران نیز، استفاده از پهپادهای انتحاری خودران و الگوریتم‌های هدف‌زن خودکار، سرعت و دقت عملیات‌های هوایی مهاجم را به‌طور محسوسی افزایش داد.

چالش‌های راهبردی ایران

- محدودیت‌های مالی و تحریم‌های بین‌المللی توسعه فناوری‌های هوایی مبتنی بر هوش مصنوعی را در کشور با چالش مواجه ساخته است. توسعه این فناوری‌ها نیازمند سرمایه‌گذاری کلان در تحقیق و توسعه، آزمایش‌های میدانی و ساخت نمونه‌های اولیه است.

- نبود زیرساخت‌های ملی در طراحی مدل‌های هوش مصنوعی هوافضا، ضعف در پردازنده‌های پیشرفته، حسگرهای دقیق و تجهیزات مخابراتی ایمن برای عملیات هوایی بدون سرنشین، عملاً ایران را در این حوزه وابسته نگاه داشته است.

- شکاف فناورانه نسبت به دشمنان منطقه‌ای به‌ویژه رژیم صهیونیستی که سرمایه‌گذاری گسترده‌ای بر هوش مصنوعی نظامی داشته، روزبه‌روز در حال افزایش است.

فرصت‌های راهبردی برای ایران

- توسعه هواپیماهای بدون سرنشین هوش مصنوعی‌محور می‌تواند توان پاسخ سریع و مقابله هوشمندانه با تهدیدات هوایی را برای کشور فراهم آورد.

- حذف خلبان، علاوه بر کاهش هزینه‌های آموزش نیروی انسانی و پشتیبانی، امکان ساخت هواپیماهای کوچک‌تر، سبک‌تر و ارزان‌تر را فراهم می‌کند که در «سناریوهای نبرد انبوه پهپادی » کاربرد حیاتی دارد.

- توسعه بومی این فناوری‌ها می‌تواند وابستگی به واردات تجهیزات و فناوری‌های هوایی خارجی را کاهش دهد و صنایع دفاعی و فناوری‌محور کشور را تقویت کند.

- در کنار کاربردهای نظامی، این فناوری‌ها می‌توانند در ماموریت‌های غیرنظامی همچون امدادرسانی، نظارت مرزی، پایش محیطی و حمل‌ونقل هوایی مسافر نیز مورد بهره‌برداری قرار گیرند.

پیامدهای راهبردی و پیشنهادهای سیاستی برای کشور

با توجه به سرعت تحولات هوش مصنوعی در نبردهای هوایی و کاربرد آن توسط رژیم صهیونیستی علیه ایران، هرگونه تأخیر در توسعه زیرساخت‌های هوش مصنوعی هوافضا، موجب افزایش آسیب پذیری دفاعی کشور و کاهش قدرت بازدارندگی هوایی ایران خواهد شد. توسعه بومی هواپیماها و پهپادهای رزمی هوشمند باید به‌عنوان یک اولویت ملی در دستورکار فوری قرار گیرد.

راهبردهای پیشنهادی:

کوتاه مدت:

• ایجاد کارگروه ملی توسعه هوش مصنوعی هوافضا با مشارکت وزارت دفاع، شورای عالی فضایی، وزارت ارتباطات و فناوری اطلاعات، سازمان هواپیمایی و پژوهشگاه‌های تخصصی.

• شناسایی فوری نیازهای فناورانه نیروی هوایی برای توسعه پهپادهای رزمی هوشمند شامل پردازنده‌ها، حسگرها، زیرساخت‌های آزمایشگاهی و دانش فنی مورد نیاز.

میان مدت:

• تدوین نقشه راه ملی توسعه پهپادهای رزمی هوشمند با تعیین اهداف فناورانه، پروژه‌های اولویت‌دار و زمان‌بندی اجرا.

• سرمایه‌گذاری مشترک وزارت دفاع و وزارت ارتباطات برای ایجاد آزمایشگاه‌ها و مراکز نوآوری هوش مصنوعی هوافضا.

بلندمدت:

• توسعه سامانه‌های هماهنگی پهپادهای انبوه رزمی با الگوریتم‌های تصمیم‌گیری غیرمتمرکز.

• تدوین دکترین ملی نبرد هوایی هوش مصنوعی محور .

هوش مصنوعی و تاب‌آوری زیرساخت‌های حیاتی ایران در بحران‌ها و جنگ‌های

ادغام هوش مصنوعی در مدیریت و بهره‌برداری زیرساخت‌های حیاتی کشور، تحولی بنیادین در افزایش کارایی، دقت تصمیم‌گیری و پاسخگویی به بحران‌ها ایجاد کرده است. با این حال، اتکای شدید این سامانه‌ها به اتصال دائم اینترنت و منابع ابری خارجی، تهدیدی جدی برای امنیت ملی در شرایط جنگ ترکیبی و بحران‌های گسترده محسوب می‌شود.

فرصت‌های راهبردی

- افزایش سرعت شناسایی و واکنش به تهدیدات زیرساختی: الگوریتم‌های هوش مصنوعی می توانند وقوع اختلالات در شبکه‌های انرژی، ارتباطات و حمل‌ونقل را پیش‌بینی کنند و هشدارهای پیشگیرانه صادر نمایند.

- افزایش کارایی و کاهش نیاز به نیروی انسانی در شرایط اضطراری: خودکارسازی وظایف حیاتی توسط هوش مصنوعی، امکان تداوم عملکرد حتی در شرایط بحران را فراهم می‌سازد.

- ظرفیت شبکه ملی اطلاعات برای توسعه Edge AI : زیرساخت شبکه ملی اطلاعات، بستر مناسبی برای استقرار پردازش‌های لبه‌ای بومی فراهم آورده است که باید در سیاست‌های مقاوم‌سازی استفاده شود.

تهدیدهای راهبردی

- وابستگی به منابع پردازشی ابری خارجی: در شرایط قطع اینترنت بین‌المللی، بسیاری از الگوریتم های هوش مصنوعی کشور از کار می‌افتند.

- آسیب‌پذیری در برابر حملات سایبری و جنگ الکترونیک: هک یا اختلال در سامانه‌های هوشمند می‌تواند کل زیرساخت حیاتی کشور را فلج کند.

- ضعف زیرساخت‌های Edge AI : تمرکز زیرساخت‌های پردازشی در کلان‌شهرها و توزیع نامتوازن آن در کشور، تاب‌آوری ملی را کاهش می‌دهد.

- نبود چارچوب استاندارد طراحی مقاوم: پروژه‌های زیرساختی هوشمند فاقد الزامات فنی برای ذخیره‌سازی آفلاین و عملکرد مستقل هستند.

حملات سایبری گسترده به سامانه‌های توزیع سوخت و مراکز داده کشور

در سال‌های اخیر، نشان داد که نبود پردازش لبه و الگوریتم‌های مقاوم‌ساز، ریسک توقف خدمات حیاتی را افزایش داده و مدیریت بحران را با چالش‌های جدی مواجه می‌سازد.

همچنین حملات سایبری اخیر به سامانه‌های بانکی کشور در جریان جنگ ۱۲ روزه و ایجاد اختلال در خدمات مالی، اهمیت توسعه Edge AI، الگوریتم‌های پیش‌بینی حمله و معماری مقاوم زیرساخت‌های حیاتی کشور را بیش از پیش آشکار ساخت.

سیاست های پیشنهادی

کوتاه‌مدت:

- تدوین چارچوب مقرراتی الزامی برای تاب‌آوری سامانه‌های هوش مصنوعی زیرساختی با هدف الزام پروژه‌های ملی به طراحی مقاوم در برابر قطع ارتباطات خارجی و حملات سایبری.

- تشکیل کارگروه ملی تاب‌آوری هوش مصنوعی .با مشارکت وزارت ارتباطات، سازمان پدافند غیرعامل و پژوهشگاه‌ها با ماموریت شناسایی فوری نقاط آسیب‌پذیر زیرساخت‌های حیاتی در برابر تهدیدات هوش مصنوعی محور.

میان‌مدت:

- توسعه پلتفرم‌های Edge AI برای زیرساخت‌های حیاتی (انرژی، آب، ارتباطات، بانکداری) با هدف امکان پردازش و ادامه عملکرد سامانه‌های حیاتی بدون نیاز به اینترنت خارجی.

- تربیت نیروی انسانی تخصصی در حوزه تاب‌آوری هوش مصنوعی از طریق برنامه‌های آموزشی مشترک میان وزارت ارتباطات، سازمان پدافند غیرعامل و دانشگاه‌ها.

- راه‌اندازی پایلوت‌های ملی تاب‌آوری هوشمند در حوزه‌های برق، حمل‌ونقل، ارتباطات سیار و بانکداری با هدف تست و بهینه‌سازی زیرساخت‌های مقاوم قبل از توسعه سراسری.

بلندمدت:

- ایجاد بانک ملی سناریوهای بحرانی زیرساختی برای آموزش مدل‌های هوش مصنوعی تاب‌آور با داده‌های واقعی و شبیه‌سازی‌شده.

- تدوین سند ملی الزامات تاب‌آوری زیرساخت‌های حیاتی مبتنی بر هوش مصنوعی.

در غیاب توسعه زیرساخت‌های هوشمند مقاوم و تاب‌آور، هرگونه پیشرفت در دولت الکترونیک و خدمات حیاتی کشور در شرایط بحران و جنگ هوش مصنوعی محور، به نقطه‌ضعف راهبردی و تهدیدی علیه امنیت ملی تبدیل خواهد شد.

سرمایه‌گذاری فوری در Edge AI و تربیت نیروهای تخصصی درحوزه تاب‌آوری هوش مصنوعی، اقدام ضروری برای تضمین اقتدار ملی در عصر جدید تهدیدات فناورانه است.

هوش مصنوعی و تاب‌آوری دولت الکترونیک ایران

در شرایط بحران و جنگ ترکیبی

هوش مصنوعی و تاب‌آوری دولت الکترونیک ایران در شرایط بحران و جنگ ترکیبی

گسترش دولت الکترونیک در ایران طی سال‌های اخیر، با دیجیتالی‌سازی گسترده خدمات حیاتی از جمله سلامت، احراز هویت، آموزش، پرداخت یارانه و خدمات شهری همراه بوده است. هرچند این تحول دیجیتال فرصت‌های قابل توجهی برای ارتقاء بهره‌وری و کیفیت زندگی مردم ایجاد کرده، اما اتکای شدید آن به اتصال مداوم اینترنت، زیرساخت‌های ملی را در شرایط بحران، جنگ سایبری و جنگ ترکیبی به شدت آسیب‌پذیر ساخته است.

ظرفیت‌های هوش مصنوعی برای تاب‌آوری دولت الکترونیک

- پردازش لبه: هوش مصنوعی با تحلیل داده‌های ذخیره‌شده به‌صورت محلی، امکان ارائه خدمات پایه را حتی در زمان قطع ارتباط فراهم می‌کند.
- پیش‌بینی رفتار کاربران: با استفاده از مدل‌های یادگیری ماشین، دولت می‌تواند نیازهای کاربران را پیش‌بینی کرده و همچنین، خدماتی هوشمند و شخصی‌سازی شده ارائه دهد.
- پشتیبانی از مدیریت بحران: هوش مصنوعی می‌تواند در شرایط اختلال یا تخریب زیرساخت ها، به عنوان «مغز جایگزین» برای اتخاذ تصمیمات سریع مدیریتی عمل کند.

تجربه بین‌المللی در تاب‌آوری دولت الکترونیک با هوش مصنوعی

- هند: سامانه سلامت الکترونیک با قابلیت عملکرد آفلاین در مناطق فاقد اینترنت،
- اوکراین: حفظ خدمات حیاتی دیجیتال در دوران جنگ با روسیه از طریق پلتفرم Diia و توسعه برنامه های مبتنی بر هوش مصنوعی برای ثبت‌نام و احراز هویت،
- استونی: راهبرد KRATT AI برای تداوم خدمات دولتی حتی در زمان قطع ارتباطات بین‌المللی.

چالش‌های راهبردی ایران در تاب‌آوری دولت الکترونیک

- وابستگی مدل‌های هوش مصنوعی به منابع ابری خارجی: بسیاری از خدمات هوش مصنوعی محور ایران به سرویس‌های ابری متصل هستند و قطع اینترنت، عملکرد آن‌ها را به صفر می‌رساند.
- نبود زیرساخت‌های سخت‌افزاری مناسب در مناطق کمتر برخوردار: به‌ویژه در استان‌های مرزی و روستایی، زیرساخت لازم برای پردازش لبه وجود ندارد.
- فقدان استانداردهای فنی مشخص برای طراحی پلتفرم‌های دولت دیجیتال آفلاین‌محور: نبود چارچوب‌های معماری و الزامات طراحی، اجرای پروژه‌ها را با ریسک شکست بالا مواجه می‌سازد.

فرصت‌های راهبردی ایران در این حوزه

- شبکه ملی اطلاعات به‌عنوان بستر مستقل داخلی: ظرفیت مهمی برای توسعه پلتفرم‌های هوش مصنوعی محور داخلی فراهم کرده است.

- داده‌های غنی دولتی: حجم بالای داده‌های ملی، امکان آموزش مدل‌های هوش مصنوعی بومی و بهینه‌سازی خدمات را مهیا می‌سازد.

- وجود ضرورت‌های امنیت ملی: بحران‌ها و تهدیدهای واقعی اخیر، عزم ملی برای مقاوم‌سازی خدمات حیاتی دیجیتال را افزایش داده است.

- ظرفیت شرکت‌های دانش‌بنیان: این شرکت‌ها توان توسعه راهکارهای بومی با هزینه کمتر و سرعت بالاتر را دارند.

- پشتیبانی قانونی از کاهش وابستگی به فناوری خارجی: اسناد بالادستی کشور توسعه ظرفیت های بومی در این حوزه را الزام‌آور ساخته‌اند.

پیشنهادهای سیاستی

کوتاه مدت:

• تدوین الزامات فنی طراحی پلتفرم‌های دولت الکترونیک آفلاین‌محور،

• تشکیل کارگروه دولت الکترونیک مقاوم مبتنی بر هوش مصنوعی با مشارکت سازمان های خدمت رسان در حوزه خدمات دولت الکترونیک و با ماموریت تعیین اولویت‌های مقاوم‌سازی خدمات حیاتی.

میان مدت:

• توسعه مدل‌های سبک هوش مصنوعی بومی برای خدمات دولتی با هدف عملکرد بدون نیاز به منابع ابری خارجی،

• ایجاد مراکز داده محلی در سطوح استانی با بهره‌گیری از الگوریتم‌های خودکار برای حفظ حداقلی خدمات در زمان قطع ارتباط.

بلندمدت:

• توسعه پلتفرم جامع دولت الکترونیک مقاوم مبتنی بر هوش مصنوعی،

• تدوین چارچوب راهبردی ملی تاب‌آوری دولت الکترونیک و خدمات دیجیتال در سناریوهای بحران.

فقدان زیرساخت‌های هوشمند مقاوم و معماری آفلاین‌محور در دولت الکترونیک، تهدیدی بزرگ برای امنیت ملی، ثبات اجتماعی و اعتبار حاکمیتی در شرایط بحران محسوب می‌شود. توسعه سریع مدل‌های بومی هوش مصنوعی و طراحی معماری مقاوم، از الزامات فوری حفظ تاب‌آوری حکمرانی دیجیتال ایران است.

هوش مصنوعی و جنگ روایت‌ها

هوش مصنوعی و جنگ روایت‌ها:
تهدیدات اطلاعات جعلی و راهبردهای مقابله ایران

جنگ ۱۲ روزه اخیر رژیم صهیونیستی علیه ایران، نقطه عطفی در بهره‌گیری نظامی و امنیتی از هوش مصنوعی برای هدایت جنگ روایت‌ها و تولید گسترده اطلاعات جعلی بود.

استفاده از فناوری‌های هوش مصنوعی محور در عملیات روانی، به دشمن امکان داد روایت‌های هدفمند، هماهنگ و شخصی‌سازی‌شده علیه افکار عمومی ایران و منطقه ایجاد کند و بر ادراک مخاطبان اثر فوری بگذار: انتشار اخبار دروغین گسترده درباره ضعف پاسخ ایران و شکست دفاعی، تمرکز بر القای نا امیدی و بی‌اعتمادی به توان دفاعی کشور، تاکید بر اقتدار ارتش رژیم صهیونیستی و مدیریت جنگ و بکارگیری شبکه‌های رباتی توییتری برای انتشار پیام‌های خاص در حجم انبوه.

تهدیدهای راهبردی

- تولید انبوه اطلاعات جعلی با مدل‌های زبانی بزرگ (LLM): دشمن با استفاده از هوش مصنوعی، حجم وسیعی از خبرهای جعلی، تحلیل‌های امنیتی ساختگی و محتوای تحریک‌آمیز تولید و منتشر کرد.

- دیپ‌فیک‌های صوتی و تصویری: استفاده از تصاویر و ویدیوهای جعلی برای تخریب روحیه داخلی و تضعیف اعتماد عمومی.

- عملیات روانی هدفمند : عملیات‌های روانی مبتنی بر هوش مصنوعی برای شخصی‌سازی پیام‌ها و القای ناامیدی، بی‌ثباتی و ناکارآمدی حکمرانی.

- حمله به اعتبار رسانه‌های رسمی: انتشار روایت‌های جعلی برای ایجاد سردرگمی خبری و کاهش اعتماد عمومی به رسانه‌های ملی.

فرصت‌های راهبردی

- توسعه مدل‌های شناسایی اطلاعات جعلی: بومی‌سازی الگوریتم‌های شناسایی و مقابله سریع با محتوای جعلی در شبکه‌های اجتماعی،
- هوش مصنوعی برای ارتقاء قدرت روایت ملی: استفاده از هوش مصنوعی برای تولید محتوای بومی باکیفیت و تقویت دیپلماسی عمومی،
- آموزش عمومی سواد رسانه‌ای هوش مصنوعی محور: ارتقاء تاب‌آوری شناختی جامعه در برابر حملات روایت‌محور دشمن.

سیاست‌های پیشنهادی

کوتاه‌مدت:

• ایجاد کارگروه ملی مقابله با اطلاعات جعلی با محوریت مرکز ملی فضای مجازی، مشارکت وزارت ارتباطات و فناوری اطلاعات، صداوسیما، مراکز امنیتی و سایر سازمان‌های مربوطه با ماموریت: شناسایی الگوهای تولید محتوای جعلی در جنگ اخیر و طراحی پاسخ سریع.

• راه‌اندازی مرکز هشدار سریع انتشار اطلاعات جعلی هوش مصنوعی محور با هدف رصد شبانه روزی محتوای رسانه‌های اجتماعی داخلی و خارجی.

میان‌مدت:

• توسعه مدل‌های بومی شناسایی دیپ‌فیک و محتوای جعلی،

• برنامه ملی ارتقاء سواد رسانه‌ای شناختی در برابر هوش مصنوعی آموزش عمومی برای مقابله با روایت‌های جعلی شخصی‌سازی‌شده.

بلندمدت:

• توسعه پلتفرم‌های تولید روایت هوشمند ملی استفاده از هوش مصنوعی برای تولید محتواهای جذاب، واقعی و قدرت‌افزا در روایت ملی ایران.

جنگ اخیر نشان داد که هوش مصنوعی به سلاحی قدرتمند در جنگ روایت‌ها تبدیل شده است. بدون توسعه زیرساخت‌های شناسایی دیپ‌فیک و اطلاعات جعلی، تربیت نیروی انسانی متخصص و تدوین راهبردهای ملی مقابله، جنگ‌های شناختی هوش مصنوعی محور آینده تهدیدی جدی علیه انسجام اجتماعی، اعتماد عمومی و اقتدار حکمرانی کشور خواهند بود.

مدل‌های زبانی بزرگ و هوش مصنوعی مولد در امنیت سایبری:

فرصت‌ها، تهدیدها و الزامات ایران

امنیت سایبری به‌عنوان یکی از حوزه‌های پرچالش حکمرانی دیجیتال، با تهدیداتی مواجه است که روزبه‌روز پیچیده‌تر و پیشرفته‌تر می‌شوند. مقیاس، تنوع و سرعت حملات سایبری، نیازمند راهکارهای دفاعی نوآورانه و مبتنی بر فناوری‌های تحول‌آفرین است. در این میان، مدل‌های زبانی بزرگ و هوش مصنوعی مولد ظرفیت‌های بی‌سابقه‌ای برای ارتقاء امنیت سایبری ایجاد کرده‌اند.

کاربردهای کلیدی مدل‌های زبانی بزرگ در امنیت سایبری

• شناسایی و تحلیل تهدیدات: تحلیل بلادرنگ حجم گسترده‌ای از داده‌های شبکه و شناسایی ناهنجاری‌ها، بدافزارها، تلاش‌های فیشینگ و ترافیک غیرعادی،

• اتوماسیون وظایف امنیتی: خودکارسازی وظایف تکراری نظیر مدیریت وصله‌ها، ارزیابی آسیب‌پذیری‌ها و بررسی‌های انطباق برای کاهش بارکاری تیم‌های امنیت،

• شناسایی فیشینگ پیشرفته: تحلیل دقیق متن ایمیل‌ها و شناسایی حملات فیشینگ با ارائه هشدار و اقدامات‌پیشگیرانه،

• تحلیل جرم‌شناسی سایبری: بررسی سریع داده‌ها و گزارش‌ها برای شناسایی روش حمله، نقاط نفوذ و ارائه‌راهکارهای‌پیشگیرانه،

• آزمایش نفوذ: کمک به تولید و ویرایش اسکریپت‌ها برای خودکارسازی بخش‌هایی از تست نفوذ،

• راستی‌آزمایی پروتکل‌های امنیتی: شناسایی نقص‌ها و آسیب‌پذیری‌های احتمالی در پروتکل‌هایی نظیر TLS/SSL و IPSec،

• پاسخ به رخدادها: تحلیل سریع وضعیت در حین حملات سایبری و پیشنهاد پاسخ‌های فوری یا خودکار،

• چت‌بات‌های امنیتی: ارتقاء توان چت‌بات‌ها برای پاسخ به سوالات پرتکرار، آموزش امنیتی و مدیریت رخدادها در زمان واقعی

• آموزش امنیت سایبری: تولید محتوای آموزشی متناسب با نیازهای هر سازمان و شبیه‌سازی حملات برای افزایش آمادگی کارکنان.

چالش‌های راهبردی مدل‌های زبانی بزرگ در امنیت سایبری ایران

• سازگاری با حملات فیشینگ پیشرفته مبتنی بر هوش مصنوعی: نیازمند به‌روزرسانی مداوم مدل‌ها برای مقابله با حملات پیچیده دشمنان.

• مدیریت حجم انبوه داده‌های سازمانی: توانمندی مدل‌های زبانی بزرگ در پردازش داده‌های گسترده، وابسته به زیرساخت‌های سخت‌افزاری و شبکه‌ای قدرتمند است.

• کمبود داده‌های آموزشی بومی با کیفیت: محدودیت در دسترسی به داده‌های واقعی امنیت سایبری به دلیل ملاحظات محرمانگی.

• نیاز به مدل‌های تخصصی امنیت سایبری: بسیاری از مدل‌های زبانی بزرگ عمومی توان درک واژگان و ساختارهای فنی حوزه امنیت را ندارند.

• لزوم پاسخ بلادرنگ: کوچک‌ترین تأخیر یا خطا در خروجی مدل‌ها می‌تواند منجر به آسیب‌های جبران‌ناپذیر شود.

فرصت‌های راهبردی ایران در این حوزه

• توسعه مدل‌های زبانی بزرگ بومی با تمرکز بر امنیت سایبری فارسی‌زبان،

• ایجاد دستیارهای امنیت سایبری برای تیم‌های دفاع سایبری،

• استفاده از مدل‌های زبانی برای تحلیل تهدیدات، تشخیص نفوذ و آموزش پرسنل امنیتی کشور.

پیشنهادهای سیاستی

کوتاه‌مدت:

• تشکیل کارگروه توسعه مدل‌های زبانی بزرگ در حوزه امنیت سایبری بومی با مشارکت پژوهشگاه ارتباطات، مرکز افتا و دانشگاه‌های پیشرو.

• شناسایی فوری نیازهای داده‌ای ملی برای آموزش مدل‌های امنیتی هوش مصنوعی.

میان‌مدت :

• توسعه کمک‌یارهای امنیتی فارسی‌زبان برای پشتیبانی تیم‌های SOC و CERT ملی.

• ایجاد پایگاه داده تهدیدات ملی با امکان اشتراک‌گذاری کنترل‌شده برای آموزش و به روزرسانی مدل‌ها.

• راه‌اندازی آزمایشگاه‌های امنیت سایبری مبتنی بر هوش مصنوعی برای توسعه، تست و ارزیابی مدل‌ها.

بلندمدت:

• طراحی مدل‌های زبانی بزرگ تخصصی امنیت سایبری با معماری‌های بومی.

عدم توسعه سریع مدل‌های زبانی بومی برای حوزه امنیت سایبری، کشور را در برابر تهدیدات فزاینده مبتنی بر هوش مصنوعی، آسیب‌پذیر و منفعل خواهد ساخت. بهره‌گیری هوشمندانه از مدل‌های زبانی بزرگ نه تنها قدرت دفاع سایبری ایران را ارتقاء می‌دهد، بلکه زیرساخت حکمرانی امنیت دیجیتال را نیز برای آینده مقاوم می‌سازد.

ابعاد اخلاقی و حقوقی استفاده نظامی از هوش مصنوعی:

الزامات حکمرانی و امنیت ملی ایران

بکارگیری هوش مصنوعی در حوزه نظامی، علاوه بر پیامدهای فناورانه و امنیتی، چالش‌های عمیق اخلاقی و حقوقی در سطح ملی و بین‌المللی ایجاد کرده است. نبود پاسخ روشن به این چالش‌ها، می‌تواند مانعی برای توسعه مسئولانه فناوری و همچنین عاملی برای سوءاستفاده دشمنان از خلاءهای حکمرانی باشد. استفاده گسترده از پهپادهای خودران و سامانه‌های هدف‌زن خودکار علیه اهداف ایرانی توسط رژیم صهونیستی در جنگ اخیر و به شهادت رسیدن افراد غیرنظامی، نمونه‌ای از بکارگیری فناوری بدون چارچوب های بازدارنده اخلاقی است که می‌تواند در آینده، زمینه‌ساز بحران‌های حقوق بشری و انسانی شود.

چالش‌های اخلاقی استفاده نظامی از هوش مصنوعی

• مسئولیت‌پذیری تصمیم‌های مرگبار هوش مصنوعی: اگر سامانه‌های نظامی مبتنی بر هوش مصنوعی به‌طور خودمختار منجر به مرگ غیرنظامیان شوند، مسئولیت حقوقی متوجه چه کسی خواهد بود؟ برنامه‌نویس، فرمانده، تولیدکننده یا خود سیستم؟

• تشدید سرعت و شدت جنگ‌ها: تصمیم‌گیری هوش مصنوعی با سرعت بسیار بالاتر از توان انسانی، خطر وقوع درگیری‌های غیرقابل‌کنترل را افزایش می‌دهد.

• تبعیض و جانبداری الگوریتمی: داده‌های آموزشی نامتوازن می‌توانند منجر به تصمیم‌گیری‌های تبعیض آمیز و غیرمنصفانه علیه گروه‌هایی خاص شوند.

• غیاب اختیار انسانی: حذف کامل انسان از چرخه تصمیم‌گیری می‌تواند ارزش‌های اخلاقی جنگ منصفانه را تضعیف کند.

• دسترسی گروه‌های تروریستی به هوش مصنوعی نظامی: ارزان شدن فناوری‌های هوش مصنوعی امکان سوءاستفاده گروه‌های غیردولتی و تروریستی از سلاح‌های هوشمند را فراهم می‌سازد.

چالش‌های حقوقی در استفاده نظامی از هوش مصنوعی

• خلاء قوانین ملی و بین‌المللی: هیچ معاهده بین‌المللی جامع درباره سلاح‌های خودمختار کشنده وجود ندارد. بحث‌های طولانی در UN و CCW هنوز به نتیجه نرسیده است.

• ابهام در انطباق با حقوق بشردوستانه بین‌المللی: به‌ویژه اصل تفکیک و تناسب در حملات نظامی، که هوش مصنوعی هنوز در اجرای دقیق آن‌ها ضعف دارد.

• قابلیت پیگیری قضایی نقض‌ها: نبود شفافیت در فرآیندهای تصمیم‌گیری هوش مصنوعی، امکان پاسخگویی حقوقی را دشوار می‌کند.

فرصت‌های راهبردی ایران در حوزه اخلاق و حقوق AI نظامی

پیشتازی در تدوین چارچوب حکمرانی اخلاقی هوش مصنوعی نظامی در منطقه: تدوین چنین چارچوبی می‌تواند ایران را به مرجع اخلاقی و حقوقی در حوزه هوش مصنوعی نظامی در سطح منطقه‌ای و بین‌المللی تبدیل کند.

ایجاد مزیت بازدارندگی اخلاقی: نمایش تعهد ایران به اصول اخلاقی جنگ می‌تواند هزینه‌های سیاسی و حقوقی دشمنان در استفاده بی‌پروا از هوش مصنوعی علیه ایران را افزایش دهد.

ظرفیت‌های علمی کشور در فقه، اخلاق و حقوق: بهره‌گیری از دانش حوزه‌های دینی و حقوقی ایران می‌تواند چارچوبی منسجم و بومی برای حکمرانی اخلاقی هوش مصنوعی ایجاد کند.

پیشنهادهای سیاستی

کوتاه‌مدت:

• تشکیل کمیته اخلاق و حقوق هوش مصنوعی نظامی با مشارکت وزارت دفاع، وزارت ارتباطات، پژوهشگاه‌ها، مرکز ملی فضای مجازی، حوزه علمیه و دانشگاه‌های حقوق.

• شناسایی خلاءهای اخلاقی و حقوقی موجود در اسناد ملی و بین‌المللی مرتبط با هوش مصنوعی نظامی.

میان‌مدت:

• تدوین چارچوب ملی اخلاقی و حقوقی استفاده نظامی از هوش مصنوعی با تاکید بر اصول اسلامی، انسانی و حقوق بشردوستانه.

• برگزاری کنفرانس ملی و منطقه‌ای هوش مصنوعی نظامی و اخلاق جنگ برای گفتمان‌سازی و ارائه ابتکار ایران در سطح منطقه.

بلندمدت :

• توسعه سند ملی حکمرانی هوش مصنوعی نظامی شامل ابعاد اخلاقی، حقوقی، امنیتی و عملیاتی.

• دیپلماسی فعال در سازمان‌های بین‌المللی برای تدوین معاهدات محدودکننده استفاده بی ضابطه از سلاح‌های خودمختار کشنده.

تدوین سیاست‌های اخلاقی و حقوقی هوش مصنوعی نظامی، اقدام راهبردی ضروری برای تقویت بازدارندگی اخلاقی و امنیت پایدار کشور است.

فهرست منابع:

[۱]. U.S. Department of Defense (۲۰۲۲). National Defense Strategy

[۲]. National AI Initiative Office (۲۰۲۱). Strategic Plan: The National Artificial Intelli-gence Research and Development

[۳]. DARPA (۲۰۲۰). GARD Program Overview

[۴]. U.S. Department of Energy (۲۰۲۳). AI for Infrastructure Resilience Projects

[۵]. State Council of China (۲۰۲۱). New Generation Artificial Intelligence Develop-ment Plan

[۶]. Tencent AI Lab & Alibaba DAMO Academy Reports (۲۰۲۲)

[۷]. Ministry of Science and Technology of China (۲۰۲۳). AI Infrastructure Whitepa-per

[۸]. Government of India, Ministry of Health. (۲۰۲۲). eSanjeevani Telemedicine Plat-form.

[۹]. OECD (۲۰۲۳). Digital Government in Ukraine: Strengthening Resilience in Crisis

[۱۰]. Ministry of Digital Transformation of Ukraine –Digital resilience of Ukraine dur-ing war Technical Annex.

[۱۱]. Estonian Information System Authority. (۲۰۲۳). Ensuring continuity of digital government in crisis situations .Cyber Resilience of e-Governance in Estonia

[۱۲]. Adrian Pokharel(۲۰۲۵),AI in Warfare: The Rise of Autonomous Weapons and the Future of Global Security https://www.linkedin.com/pulse/ai-warfare-rise-autonomous-weapons-future-global-adrian-pokharel-zg۳ee

[۱۳]. Bipartisan Policy Center. (۲۰۲۰). Artificial Intelligence and National Security. Re-trieved from https://bipartisanpolicy.org/wp-content/uploads/۲۰۲۰/۰۷/BPC-Artificial-Intelligence-and-National-Security_Brief-Final-۱.pdf

[۱۴]. Carnegie Endowment for International Peace. (۲۰۲۴). Governing Military AI Amid a Geopolitical Minefield. Retrieved from https://carnegieendowment.org/research/۲۰۲۴/۰۷/governing-military-ai-amid-a-geopolitical-minefield

[۱۵]. Center for Strategic and International Studies (CSIS). (۲۰۲۳). Addressing Na-tional Security Implications of AI. Retrieved from https://www.csis.org/analysis/addressing-national-security-implications-ai

[۱۶]. Foreign Policy. (۲۰۱۴). Lethal Autonomy: A Short History. Retrieved from https://foreignpolicy.com/۲۰۱۴/۰۷/۲۴/lethal-autonomy-a-short-history

[۱۷]. International Committee of the Red Cross (ICRC). (۲۰۲۳). What You Need to Know About Autonomous Weapons. Retrieved from https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons

[۱۸]. Stop Killer Robots. (۲۰۲۴). Military and Killer Robots: The Growing Risk. Re-trieved from https://www.stopkillerrobots.org/military-and-killer-robots

[۱۹]. Third Way. (۲۰۲۳). Lethal Autonomous Weapons ۱۰۱. Retrieved from https://www.thirdway.org/memo/lethal-autonomous-weapons-۱۰۱

[20]. United Nations Office for Disarmament Affairs. (2024). Discussions on the Regulation of Autonomous Weapons Systems under the CCW. Retrieved from https://www.un.org/disarmament/ccw/autonomous-weapons

[21]. Elke Schwarz(2025),The ethical implications of AI in warfare https://www.qmul.ac.uk/research/featured-research/the-ethical-implications-of-ai-in-warfare/

[22]. Artificial intelligence as a tool in war and a weapon for peace - the power of dis-information.

[23]. Mohamed Amine Ferrag, Fatima Alwahedi, Ammar Battah, Bilel Cherif, Abdechakour Mechri,and Norbert Tihanyi، arXiv [cs.CR] 21 May 2024»Generative AI and Large Language Models for Cyber Security: All Insights You Need«

[24]. Z. Burdette, D. Phillips, J. L. Heim, E. Geist, D. R. Frelinger, C. Heitzenrater, and K. P. Mueller, An AI Revolution in Military Affairs? How Artificial Intelli-gence Could Reshape Future Warfare, Santa Monica, CA: RAND Corporation, 2025. Available:https://www.rand.org/pubs/working_papers/WRA4004-1.html.

[25]. Bolgov. (2023). Artificial Intelligence Politics and Sanctions: Comparing the Cases of Russia and Iran. In Digital International Relations. https://link.springer.com/chapter/10.1007/978-981-99-3467-6_4(Vinnykova, 2021).

[26]. ZS Sabouri & B Mehrdel. (2024). New Geopolitics of Artificial Intelligence and the Challenges of Global Governance. In CIFILE Journal of International Law. https://www.cifilejournal.com/article_193438.html

[27]. Emery-Xu et al., (2024). International governance of advancing artificial Pub-lished: 19 September 2024

[28]. Vanberghen & Vanberghen, (2021). AI & SOCIETY Journal of Knowledge, Cul-ture and Communication

[29]. M Abdolhamid, M Lari, & H Najafi Rastaghi. (2024). A Comparative Study of Global Experiences in the Application of Artificial Intelligence in Public Admin-istration: Implications for Enhancing Smart Governance in Iran. https://www.jipas.ir/&url=http:/www.jipas.ir/article_219967.html?lang=en

[30]. Robyn Williams & Lisa Otto. (2022). Artificial intelligence as a tool of public di-plomacy. In The Thinker. https://www.semanticscholar.org/paper/b5577dfd815672872891d90b5f9e0512e06fd458

[31].Pashentsev & Kuznetsov (2022). Malicious Use of AI and Challenges to Psycho-logical Security of BRICS Countries Malicious Use of AI and Challenges to Psy-chological Security of BRICS Countries Report

[32]. N Zahra. (2025). AI at the Crossroads: The India-Israel Defense Cooperation and Its Strategic Implications for Iran. In ASSAJ. https://assajournal.com/index.php/36/article/view/490

[33]. A Haroon. (2024). AI and Cyber Drove Warfare in the Israeli-Iran Conflict and its Impact on Gulf States' Security. In Journal of Politics and International Stud-ies. https://jpis.pu.edu.pk/45/article/view/1387

[۳۴]. MR Hosseini & M Azizi Mehmandoost. (۲۰۲۵). Comparative Study of Artificial Intelligence Laws and Policies in Advanced Countries and Proposing Recom-mendations for Iran. In ModernTechnologies Law. https://mtlj.usc.ac.ir/article_۲۱۴۶۹۴.html?lang=en

[۳۵]. Mehdi Rezaei Qadi & Morteza Alavian. (۲۰۲۲). Evaluation and evaluation of public policy in the Islamic Republic of Iran based on the theory of good govern-ance. In International journal of health sciences. https://www.semanticscholar.org/paper/۰d۲۰۸b۴۷d۹dd۳b۰۹aeed۶۷۷۸f۶۲bba۴fb۴aeb۶۳۳۸

[۳۶]. mohebbi. n.d. Futures Studies on Artificial Intelligence Development in Iran

[۳۷]. MA Torabi & H Eghbal. (۲۰۲۵). Proposing an Artificial Intelligence Governance Model for State Administration in the Islamic Republic of Iran. In State Studies of Contemporary Iran. https://irsj.ihu.ac.ir/article_۲۰۹۵۹۴.html?lang=en

[۳۸]. obyn Williams & Lisa Otto. (۲۰۲۲). Artificial intelligence as a tool of public di-plomacy. In The Thinker. https://www.semanticscholar.org/paper/b۵۵۷۷dfd۸۱۵۶۷۲۸۷۲۸۹۱d۹۰b۵f۹e۰۵۱۲e۰۶fd۴۵۸

[۳۹]. Peiyu Gu. (۲۰۲۳). Global Artificial Intelligence Governance: Challenges and Complications. In Science Insights. https://bonoi.org/index.php/si/article/view/۱۰۷۸

[۴۰]. ZS Sabouri & B Mehrdel. (۲۰۲۴). New Geopolitics of Artificial Intelligence and the Challenges of Global Governance. In CIFILE Journal of International Law. https://www.cifilejournal.com/article_۱۹۳۴۳۸.html

[۴۱]. Mingting Zhu & Chongli Xu. (n.d.). International soft law governance of artifi-cial intelligence ethics: International soft law governance of artificial intelligence ethics: Current situation, challenges and countermeasures Current situation, challenges and countermeasures. https://www.semanticscholar.org/paper/fa۷۸e۴۴۲b۳e۵۹cb۸۳b۱۹۳۷۳d۵b۴۷c۰f۱۴۰۵۷c۷۵۲

[۴۲]. What's Next for AI Ethics, Policy, and Governance? A Global Overview, https://www.semanticscholar.org/paper/c۱۲۹d۷۱۲fa۳۱۵۸۹۴۵۴۵ca۱d۲ad۳۲bdaf۳bade۹۷d

[۴۳]. Worldwide AI ethics: A review of ۲۰۰ guidelines and recommendations for AI governance, https://linkinghub.elsevier.com/retrieve/pii/S۲۶۶۶۳۸۹۹۲۳۰۰۲۴۱۶

پژوهشگاه ارتباطات
و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)