Knowledge of political interpretation
Vol 5, No 18, Winter 2023
ppt 35-55
Received: 20, JUL, 2023
Accepted: 25, OCT, 2023

Examining the category of security in the light of artificial intelligence

Jalal salimi [1]

saeed seyed agha banihashemi[2]

Abstract

With the rapid developments of artificial intelligence, the importance of the security of individuals and institutions has been greatly appreciated. In this research, the main goal is to investigate the different aspects of security with an emphasis on artificial intelligence technology. The main question is, what effect will artificial intelligence have on global security? The findings show that with the uncontrollable progress of technology and artificial intelligence, it seems that security will be affected, so that some consider it a new global threat, but on the other hand, others believe that artificial intelligence despite all Aspects of threat can be useful in ego enhancement. The most important emphasis of the threat actors include increasing the accuracy of weapons, penetration and accessing information faster with this technology. From the point of view of those who consider artificial intelligence as an opportunity to improve security, it is important to emphasize issues such as accurate identification, prediction and use of artificial intelligence in eliminating threats with a significant reliability factor and away from human error.

[1]PhD student in International Relations; science and research Branch; Islamic Azad university; Tehran; iran**.** **Jalal.saalimii@gmail.com**

[2] Member of the Faculty of International Relations, Ministry of Foreign Affairs, Tehran, Iran. **s.banihashemi@mfa.gov.ir**

تاریخ دریافت: ۱۴۰۲/۰۴/۲۹ | تاریخ پذیرش: ۱۴۰۲/۰۸/۰۳

دانش تفسیر سیاسی | Knowledge of political interpretation

سال پنجم، شماره ۱۸، زمستان ۱۴۰۲ | Vol 5, No 18, Winter 2023

صفحات ۵۵-۳۵ | ppt 35-76

بررسی مقوله امنیت در پرتو هوش مصنوعی

جلال الدین سلیمی[۱]

سعید سید آقا بنی هاشمی[۲]

چکیده

با پیشرفت‌های سریع هوش مصنوعی اهمیت امنیت اشخاص و نهادها بسیار مورد توجه قرار گرفته است. در این پژوهش هدف اصلی بررسی ابعاد مختلف امنیت با تاکید بر فناوری هوش مصنوعی است.

سوال اصلی این است که هوش مصنوعی چه تاثیری بر امنیت جهانی خواهد گذاشت؟ یافته ها نشان میدهد که با روند غیر کنترل پیشرفت فناوری و هوش مصنوعی به نظر می رسد که امنیت تحت تاثیر قرار خواهد گرفت به طوری که برخی آن را تهدید نوین جهانی به حساب می آورند اما در مقابل برخی دیگر معتقدند که هوش مصنوعی علی رغم تمام جنبه های تهدید می تواند در ارتقا منیت مفید واقع شود. مهمترین تاکیدات تهدیدانگاران شامل افزایش دقت تسلیحات، نفوذ و دسترسی به اطلاعات به صورت سریع تر با این

[۱] دانشجوی دکتری روابط بین الملل، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران، ایران (نویسنده مسئول) **Jalal.saalimii@gmail. .**

[۲] عضو هیئت علمی دانشکده روابط بین الملل وزارت امور خارجه، تهران، ایران

فناوری است. از دیدگاه کسانی که هوش مصنوعی را فرصتی برای ارتقای امنیت می انگارند تاکید بر موضوعاتی چون شناسایی دقیق، پیش بینی و استفاده از هوش مصنوعی در رفع تهدیدات با ضریب اطمینان قابل توجه و دور از خطای انسانی است.

واژگان کلیدی: هوش مصنوعی، امنیت، فناوری، تهدیدات امنیتی

مقدمه

هوش مصنوعی که به عنوان چهارمین انقلاب صنعتی در نظر گرفته می شود، در دنیای امروز به ویژه با رشد فناوری و دسترسی آحاد افراد به دستگاه ها ارتباطی به یکی از مهمترین دغدغه های نوین تبدیل شده است. رشد این فناوری و احتمال تسخیر جهان آینده و تاثیرگذاری بر آن موجب شده است که آن را به یک واقعیت ملموس در صحنه زندگی و روابط تبدیل کند. از گذشته های دور هرچند با ظهور فناوری های ارتباطی کارشناسان و دانشگاهیان بر اهمیت ربات ها و هوش مصنوعی تأکید کرده اند اما با توجه به پتانسیل بالای هوش مصنوعی برای استفاده در حوزه های حساس مانند سامانه های نظامی، سلامت، امور مالی و غیره، امنیت اطلاعات و داده ها بسیار حائز اهمیت است به عبارت دقیق تر وجه جدید توجه ها به مقوله امنیت و پارامترهای تهدید نوین ناشی از آن معطوف شده است.

باید گفت با اینکه هوش مصنوعی یک فناوری نوین و قدرتمند است که می‌تواند مزایای بسیاری برای بشریت به ارمغان بیاورد ولی هوش مصنوعی می‌تواند با تبدیل شدن به یک ابزار و سلاح تغییراتی شگرفی را در سیاست ها و رقابت ها بگذارد. به عبارت دقیق تر می توان پیش بینی کرد که هوش مصنوعی به افزایش قدرت و نفوذ کشورهایی که از این فناوری به طور پیشرفته استفاده می‌کنند، منجر می شود.این فناوری به یک ابزار قدرتمند در رقابت جهانی تبدیل شده است و کشورهایی که در این زمینه سرمایه‌گذاری بیشتری می‌کنند، در آینده از مزیت‌های رقابتی بیشتری برخوردار خواهند بود. با توجه به اهمیت موضوع هوش مصنوعی و تاثیرات آن بر امنیت جهانی، لازم است که این موضوع به طور جدی مورد بررسی و تحلیل قرار بگیرد. این مقاله به هوش مصنوعی و تاثیر آن بر امنیت می پردازد بنابراین هوش مصنوعی چه تاثیری بر امنیت جهانی خواهد گذاشت؟ فرضیه پژوهش این است که هوش مصنوعی موجب بروز تهدیدات درحوزه امنیتی، اطلاعاتی

شده و بر روابط بین کشورها تاثیر گذار خواهد بود به طوری که جنبه مثبت آن تنها با وضع قوانین تقویت می شود. روش پژوهش توصیفی-تحلیلی و گردآوری داده ها از منابع کتابخانه ای بوده است.۰

مبانی نظری پژوهش

هوش مصنوعی

با نسل جدید از فناوریهای مخرب و هوش مصنوعی ما در حال ورود به انقلاب صنعتی چهارم هستیم. سه انقلاب قبل به ما ماشینی کردن بر مبنای بخار، برق رسانی و تولید جرم، سپس الکترونیک، فناوری اطلاعات و فرایند مکانیزه کردن کارها را عرضه کرد. این دورهی جدید چهارم با دستگاههای هوشمندش با بهبود پتانسیل و همگرایی چند زمینه ی علمی و فناوری تقویت شده است، مانند کلان داده، هوش مصنوعی، اینترنت اشیاء (IoT)، سخت افزار فوق محاسباتی، ارتباطات مفرط، رایانش ابری، ارزهای دیجیتال، بلاکچین سیستمهای دفتر حساب توزیع شده و محاسبات همراه. نتایج میان دت و طولانی مدت این فناوریهای نمایی همگرا برای افراد،جامعه، تجارت، دولت و امنیت فناوری اطلاعات اصلا واضح نیستند (۹.)سرعت پیشرفت هوش مصنوعی رو به افزایش است و این حتی برای کسانی که در این بخش هستند هم حیرت انگیز است. در ماه مارس سال۲۰۱۶، سیستم دیپمایند آلفاگو گوگل۱با نشان دادن سرعت پیشرفت در ماشین یادگیری، قهرمانGoجهان را شکست داد-فناوری هوش مصنوعی مرکزی. در بازی تختهایGoبیش از۵۶۰میلیون حرکت امکان پذیر است-نمیتوانید به سیستم تمام قوانین و جایگشتها را آموزش دهید(۷.)در عوض، آلفاگو به یک الگوریتم ماشین یادگیری مجهز شده بود که با استفاده از آن میتوانست قوانین و حرکات ممکن را با مشاهدهی هزاران بازی استنباطکند. همین فناوری امروزه میتواند در امنیت فناوری اطلاعات در برنامههای

کاربردی از شناسایی تهدیدات خارجی و جلوگیری از آن تا مشخص کردن ماده متشکلههای رفتارهای غیرقانونی بالقوه در میان کارمندان استفاده شود (محمدی، ۱۶:۱۴۰۲)

در تعریف هوش مصنوعی بیان می گردد که : " هر سیستم مصنوعی که وظایف خود را تحت شرایط مختلف و غیرقابل پیش بینی بدون نظارت چشمگیر انسان انجام دهد ، ، یا از تجربه خود بیاموزد و عملکرد آنها را بهبود بخشد .... آنها ممکن است کارهایی را انجام دهند که نیاز به درک مانند انسان از جمله شناخت. ، برنامه ریزی ، یادگیری ، ارتباطات یا فعالیت های بدنی دارند"(Congressional Research Service,2018:1).

کارویژه های هوش مصنوعی

هوش مصنوعی یک فناوری مبتنی بر رشته های مختلفی چون علوم کامپیوتر،زیست شناسی،روانشناسی،زبان شناسی،ریاضیات و مهندسی است.از این رو کاربرد ها و کارویژه های فراوانی می تواند داشته باشد

۱.بازی[۱]

شاید یکی از رایج ترین کاربرد های هوش مصنوعی در زمینه بازی باشد.بدین معنی که نقش مهمی در بازی های استراتژیک مانند شطرنج ، پوکر و غیره ایفا می کند ، جایی که دستگاه می تواند بر اساس دانش اکتشافی تعداد زیادی از موقعیت های ممکن را تصور کرده و بر اساس آن بازی را به پیش ببرد.

۲.پردازش زبان[۲]

[۱] Gaming

[۲] Natural Language Processing

این کاربرد بدین معنی است که هوش مصنوعی تعامل با رایانه ای را که به زبان طبیعی و توسط انسان صحبت می شود را امکان پذیر می کند.

٣.سیستم های متخصص[١]

برخی از برنامه ها وجود دارد که دستگاه ، نرم افزار و اطلاعات ویژه را برای ارائه استدلال و مشاوره در اختیار شما قرار می دهد. آنها توضیحات و توصیه هایی را به کاربران ارائه می دهند.

٤.سیستم های دیداری[٢]

این سیستم ها ورودی بصری را برای رایانه قابل درک،تفسیر و تحلیل می کنند.به عنوان مثال می توان از این مورد در سه موقعیت مختلف استفاده نمود و کاربرد های ان را شاهد بود: الف) یک هواپیمای جاسوسی عکس می گیرد ، که برای مشخص کردن اطلاعات مکانی یا نقشه مناطق مورد استفاده قرار می گیرد.این عکس برداری توسط هواپیماها و نیز پهپاد های جاسوسی به کمک هوش مصنوعی انجام می شود. ب) پزشکان برای تشخیص بیمار از سیستم متخصص بالینی استفاده می کنند. ج) پلیس از نرم افزار رایانه ای استفاده می کند که می تواند چهره جنایتکار را با پرتره ذخیره شده ساخته شده توسط پزشکی قانونی تشخیص دهد.

٥.تشخیص گفتار[٣]

[١] Expert Systems

[٢] Vision Systems

[٣] Speech Recognition

برخی از سیستم های هوشمند در حالی که یک انسان با آن صحبت می کند قادر به شنیدن و درک زبان از نظر جملات و معانی آنها هستند. این می تواند لهجه های مختلف ، کلمات عامیانه ، سر و صدا در پس زمینه ، تغییر صدای انسان به دلیل سرما و غیره را کنترل کند.

٦.تشخیص دست نوشته[۱]

نرم افزار تشخیص دست نویس متن نوشته شده روی کاغذ توسط قلم یا صفحه را توسط قلم می خواند. این می تواند اشکال حروف را تشخیص داده و آن را به متن قابل ویرایش تبدیل کند.

۷.روبات های هوشمند[۲]

روبات ها قادر به انجام وظایفی هستند که توسط یک انسان برنامه ریزی شده اند. آنها سنسورهایی برای شناسایی داده های فیزیکی از دنیای واقعی مانند نور ، گرما ، دما ، حرکت ، صدا ، ضربات و فشار دارند. آنها برای نمایش هوش از پردازنده های کارآمد ، سنسورهای متعدد و حافظه عظیم برخوردار هستند. علاوه بر این ، آنها قادر به یادگیری از اشتباهات خود هستند و می توانند با محیط جدید سازگار شوند(Tutorialspoint.com,2020).

بررسی امنیت در پرتو هوش مصنوعی

هوش مصنوعی (AI) به عنوان یک فناوری نوین و قدرتمند، تاثیرات عمیقی بر امنیت در سطوح مختلف، از جمله امنیت ملی، سایبری و اطلاعاتی خواهد داشت.

---

[۱] Handwriting Recognition

[۲] Intelligent Robots

۱- تاثیرگذاری بر محتوا و کیفیت اطلاعات:

سیستم های هوش مصنوعی همچنین به دلایل متعدد میتوانند ابزارهایی کارآمد برای مدیریت بحرانهای دیپلماتیک در عصر دیجیتال باشند؛ آنها میتوانند به سفارتخانهها و وزارتخانههای امور خارجه کمک کنند تا ماهیت و شدت حوادث را در زمان واقعی درک کنند، روند تصمیمگیری را سادهتر سازند، انتظارات مردم را مدیریت و خاتمه بحران را تسهیل کنند. بنابراین با وجود پیچیدگیهای فنی و ماهیت دشوار مذاکرات بینالمللی، هوش مصنوعی طی سالهای اخیر در این زمینه ورود کرده است؛ رباتیبه نام»مشاور تجاری شناختی«۱ توسط شرکت»آیبیام«تهیه شده تا با بررسی قوانین پایه ای، به سؤالات و ابهامات مربوط به توافقنامه های تجاری موجود پاسخ دهد، امور گمرکی و حتی دسترسی به پروفایل طرف مذاکرهکننده را تسهیل کند. این ربات از تجزیه و تحلیلهای توصیفی برای ارائه بینش بهموقع و قابل اعتماددر مورد موضوعات فنی پیچیدهای استفاده میکند که دستیابی به آنها توسط یک تیم باتجربه نیز نیاز به روزها یا احتمالاً چند هفته زمان دارد. البته این ربات حداقل تا کنون در فرایند تصمیمگیری جایگزین مذاکرهکننده انسانی نشده و مذاکرات را نیز به تنهایی انجام نمیدهد.، با این حال حضور و فعالیت چنین رباتهایی در کنار تیم مذاکرهکننده تا حد زیادی به آنها کمک میکند تا با کاهش شکافهای مهم اطلاعاتی، بهترین استراتژی مذاکره را به کار بگیرند (ملایی و کافی، ۳۱۸:۱۴۰۱).

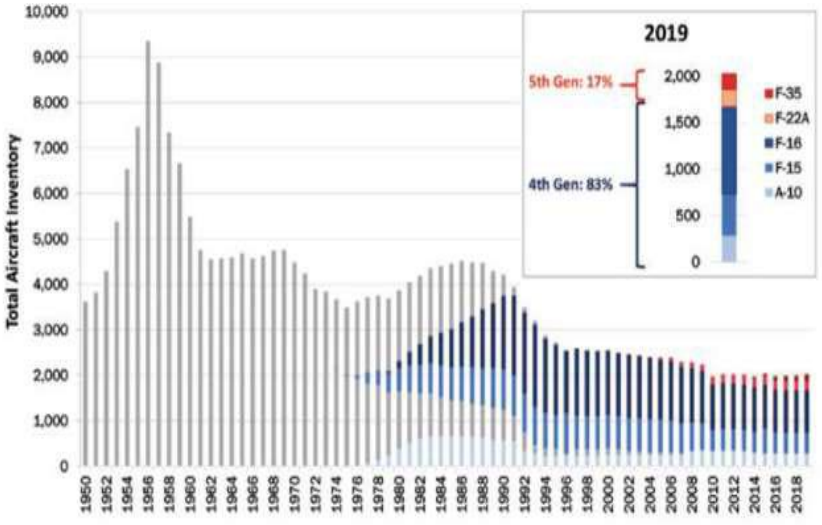
هوش مصنوعی می‌تواند توازن قدرت در جنوب آسیا را به نفع کشورهایی که به این فناوری دسترسی دارند و می‌توانند از آن به طور موثر استفاده کنند، تغییر دهد. برای مثال در رقابت هند و پاکستان قابلیت بازیابی اطلاعات هوش مصنوعی در هدف گیری زرادخانه های حریف، احساس ترس از حمله پیشگیرانه را در محیط افزایش میدهد که این

خود عاملی برای ایجاد بی ثباتی خواهد شد. جنگ سایبری که در سایه گسترش هوش مصنوعی مطرح میشود میتواند بر ثبات استراتژیک تأثیر بگذارد. جعل خبر و اطلاعات دروغ» از طریق پلتفرم های مختلف شبکه های اجتماعی پدیده ای است که در جریان جنگ سایبری مطرح میشود و پیامدهای آن میتواند به آغاز بحرانی جدی برای منطقه ای مانند جنوب آسیا منجر شود واضح ترین مثالی که در این باره مطرح میشود دست کاری اطلاعاتی بود که در ۱۴ فوریه ۲۰۱۹ در جریان حملات به شهر پولوامای کشمیر تحت مدیریت هند بود که نشان داد چگونه دستکاری اطلاعات می تواند منجر به تشدید تنش شود. (عباسیان، ۳:۱۴۰۰).

۲- ایجاد تحول و هوشمند سازی توان نظامی:

برخی از کارشناسان معتقدند که هوش مصنوعی می‌تواند به رقابت تسلیحاتی جدید منجر شود، زیرا کشورها برای توسعه سلاح‌های خودکار و پیشرفته‌تر رقابت می‌کنند. کلارک در یادداشت تحلیلی خود اشاره می‌کند که کشورهای پیشرفته در حال ایجاد سامانه‌های متنوع دایره‌راهبری جامع برای فرماندهی و کنترل نیروهای نظامی هستند. این سامانه‌ها امکان اجرای اقدامات نظامی در حوزه‌های هوایی، فضایی، سایبر، دریا و زمین را ارائه می‌دهند. کنیس نیز بیان می‌کند که کشورهای پیشرفته در تلاش برای استفاده از هوش مصنوعی در وسایل نقلیه نیمه‌خودکار و خودکار از جمله هواپیماهای جنگنده، پهپادها و وسایل نقلیه زمینی و دریایی قرار دارند. این نوع هوش مصنوعی به تشخیص محیط، تشخیص موانع، ترکیب داده‌های حسگرها، ناوبری براساس نقشه و حتی ارتباط با سایر وسایل نقلیه کمک می‌کند(احمدی و همکاران، ۱۴۷:۱۴۰۰).

در زیر به عنوان نمونه روند موجودی جنگنده های مبتنی بر هوش مصنوعی نیروی هوایی ایالاتمتحده نشان داده میشود:



جنگ هوایی آینده بر تسلط اطلاعات از طریق شبکه‌ای از حسگرهای مبتنی بر هوا، فضا و فضای سایبری متمرکز خواهد بود .این تسلط با مشارکت در همه حوزه‌های فضاینبرد تقویت می‌شود .همانطور که در طرح پرواز برتری هوایی ۲۰۳۰ ایالات متحده تأکید شده است، یافتن راه بهینه برای ترکیب داده‌ها از حسگرهای مبتنی بر ابر و ترجمه ورودی‌ها به اطلاعات با کیفیت، کلید موفقیت در سطوح عملیاتی و تاکتیکی خواهد بود (فیروز آبادی و چهرآزاد، ۲۲۷:۱۴۰۲).

در سال ۲۰۲۰، یک سایت کسب و کار مبتنی بر فناوری اطلاعات در آمریکا، ده روند محرک فناوری اطلاعات آینده را معرفی کرد که عبارتند از:

۱. **معماری پلتفرم :**استفاده از پلتفرم‌های قدرتمند و انعطاف‌پذیر برای ارائه خدمات و محصولات به مشتریان
۲. **پلتفرم‌های اجتماعی :**استفاده از پلتفرم‌های اجتماعی برای تعامل با مشتریان، بازاریابی و تبلیغات
۳. **رایانش ابری :**استفاده از خدمات ابری برای ذخیره‌سازی داده‌ها، پردازش و توسعه برنامه‌ها
۴. **امنیت داده‌ها :**حفظ امنیت داده‌های مشتریان و جلوگیری از حملات سایبری
۵. **محرمانگی داده‌ها :**احترام به حریم خصوصی مشتریان و استفاده مسئولانه از داده‌های آنها
۶. **علم تجزیه و تحلیل :**استفاده از داده‌ها برای تصمیم‌گیری بهتر و ارائه خدمات و محصولات شخصی‌سازی‌شده
۷. **معماری و تجربه کاربر :**طراحی رابط کاربری ساده و جذاب برای مشتریان
۸. **هوش مصنوعی :**استفاده از هوش مصنوعی برای خودکارسازی وظایف، پیش‌بینی رفتار مشتریان و ارائه خدمات بهتر
۹. **یادگیری ماشین :**استفاده از یادگیری ماشین برای بهبود عملکرد سیستم‌ها و ارائه خدمات شخصی‌سازی‌شده
۱۰. **اینترنت اشیاء :**استفاده از دستگاه‌های متصل به اینترنت برای جمع‌آوری داده‌ها و ارائه خدمات جدید

در راستای این مطالعات، سازمانهای نظامی هم کاربردهای این فناوریها را در بخشهای مختلف خود بررسی کرده اند که به برخی از آنها اشاره میشود:

فناوری	کاربردهای دفاعی نظامی
هوش مصنوعی و شاخه های آن	صرفه اقتصاادی پهبادهاا و دفااع حمالات ساایبری، داده کاوی، رباتیک و پردازش زبان طبیعی فراتر رفته و حیطههایی همانند مراقبت نظامی، شناسایی، ارزیاابی تهدید، مینگذاری زیار آب، امنیات ساایبری، آناالیز هوشمند، فرمانادهی و کنتارل، و آماوزش، کنتارل و رصد بیماری، میتواند قابلیتهای تحرک یگان نظامی را از طریااق تشااخیص هاادف، سیسااتم هاای ساالاح خودکار، ابزارهای حمایتی و برنامهریزی، حل چاالش - های لجستیکی، حمایت از بازیهای جناگ، مکاانیزه کردن نبرد از طریق حذف عامل انسانی، بهینهساازی و توسعه سرعت سلاحها و تشخیص کلیه پدیاده هاای منطقه نبرد، کمک به رزم، کشاف تهدیادات، ارتقااای عملکرد رادار و تشخیص و طبقهبنادی ناویز، شابیه - سازی رزم و سلاحها، کشف شکااف مهارتی در تعمیار و نگهاداری، تحلیال هاای بارخط، حمالات ساایبری، آشکارسازی فریاب و هادایت خودکاار پهباااد، جناگ الکترونیک، حمله سایبری، همکااری انساان ماشاین، - بصریسازی رایانهای برای کمک به تصمیمات بهتار و سریعتر، سلاحهای خودکار و مبتنی بر شبکه، پلتفرم- های بادون انساان و باا انساان، باازی جناگ، ارتقااء لجستیک، پایش ماهوارهها و سفینه فضایی، رباتیاک،

	مدیریت ترافیک، کشتیها و زیردریایی، خودکارسازی وسایل نقلیه،
کلان داده ها	بهینه سازی کارآیی تجهیزات، هدایت نیروها، کنترل ماشین هوشمند بدون سرنشین، معادل سازی و پیش بینی، کسب دانش و بینش نظامی، افزایش توان عملیاتی، کمک به تصمیمات راهبردی، تحلیل داده های مربوط به امکانات نظامی، محل استقرار سربازان، خدمات درمانی، عملیات ضد تروریستی، تدارکات نظامی، توسعه فناوری نظامی، پزشکی قانونی نظاامی، سامانه های اطلاعاتی جغرافیایی، تصاویر عملیاتی مشترک، تصمیم سازی نظامی، توسعه هوش نظامی
اینترنت اشیا	شبیه سازی زندهِ نظامی و غلبه بر چالش های امنیتی ، تامین مالی الکترونیکی، کمک به آموزش حین نبارد، تحلیل اعتمادپذیری، پیشبینای شکست در جنگ، پایش فضای نبرد، آشکارسازی ورودهای غیرقانونی به منطقه خودی، کنترل مرزهای جغرافیایی، هوافضا
رایانش ابری	افرایش انعطاف پذیری، چابکی و صرفه جویی، بهره وری، ذخیره سازی داده ها، کمک به ابزارهای تحلیل پلتفرم های بصری سازی، یکپارچگی زیرساخت فناوری

منبع: (محمدی فاتحو ابراهیمی، ۱۳۹۹:۱۵۶-۱۵۵)

سیاستمداران جهان ، از جمله اوباما ، ترامپ ، شی و پوتین ؛ همه اظهارات مهمی را ارائه داده اند که نشان دهنده اهمیت هوش مصنوعی است که می تواند با آنچه پوتین در سپتامبر سال ۲۰۱۷ اعلام کرد خلاصه شود: هر کس رهبر هوش مصنوعی شود ، بر جهان حکمرانی خواهد کرد(ÖZDEMIR.2019:7).

۳- تاثیرگذاری دیپ فیک ها بر امنیت:

دیپ‌فیک به تکنیکی نوین در هوش مصنوعی اشاره دارد که به واسطه آن می‌توان تصاویر و ویدئوهای جعلی با ظاهری بسیار واقعی و متقاعدکننده تولید کرد. این تکنولوژی، می تواند در امنیت اطلاعات و سپس بر تصمیم گیری و سیاستگذاری تاثیرگذار بشود. بنابراین یکی از بزرگترین نگرانی‌ها در خصوص دیپ‌فیک، سوءاستفاده از آن در زمینه اخبار جعلی و فریب افکار عمومی و روندهای سیاستگذاری صحیح است.؛ این تکنولوژی، اگرچه در برخی زمینه‌ها مانند سرگرمی و آموزش کاربردهای خلاقانه دارد، اما خطرات و چالش‌های متعددی را نیز به همراه آورده است. یکی از بزرگترین نگرانی‌ها در خصوص دیپ‌فیک، سوءاستفاده از آن در زمینه امنیت سایبری است. مجرمان سایبری می‌توانند از دیپ‌فیک برای دور زدن سیستم‌های امنیتی و دسترسی به اطلاعات و سیستم‌های حساس استفاده کنند. برای مثال، آنها می‌توانند از دیپ‌فیک برای جعل چهره یا اثر انگشت افراد و دسترسی به حساب‌های کاربری آنها استفاده کنند؛ استفاده از دیپ فیک ها به عنوان یک ابزار در جنگ سایبری برای تخریب زیرساخت‌های حیاتی، مختل کردن عملیات دولتی و ایجاد نوسانات در بازارهای مالی بسیار خطرناک است. برای پیشگیری از حملات سایبری مرتبط با دیپ فیک، ضرورت آگاه سازی سازمان‌های دولتی و ارائه‌دهندگان زیرساخت‌های حیاتی، توسعه پروتکل‌های شناسایی و واکنش موثر، و تقویت همکاری‌های بین‌المللی است. دیپ فیک نیز می تواند به روابط دیپلماتیک آسیب برساند و/یا مذاکرات پیمان را به تاخیر بیندازد. استراتژی‌های کاهش شامل توسعه فناوری تشخیص عمیق دیپ‌فیک موثر برای ارتباطات دیپلماتیک، افزایش سواد رسانه‌ای برای دیپلمات‌ها و مقامات دولتی، و ایجاد کانال‌های ارتباطی شفاف برای پاسخ به حوادث

دیپلماتیک مرتبط با دیپ‌فیک است. سازمان های تروریستی مطمئناً پتانسیل استفاده از دیپ فیک ها در گسترش تبلیغات و هماهنگی حملات را تشخیص می دهند. حتی در غیاب دیپ فیک، تروریسم امنیت جان بیگناهان و ثبات زیرساخت های حیاتی را به خطر می اندازد. بنابراین، افزایش آگاهی از تهدیدات تروریستی مرتبط با دیپ فیک در میان مجریان قانون و سازمان های اطلاعاتی، توسعه پروتکل های شناسایی و واکنش موثر، و تعهد قاطع به همکاری بین المللی برای مقابله با این استفاده شرورانه از دیپ فیک حیاتی است (Canada,2023).

در این مورد از یک سو نقض حریم خصوصی را داریم و از سوی دیگر انتساب برخی فیک محتواها به شخصیت های تاثیرگذار و سیاستمداران. بنابراین از یک سو جمع‌آوری و استفاده از داده‌های شخصی توسط سامانه‌های هوش مصنوعی ممکن است به نقض حریم خصوصی افراد منجر شود. از همین رو در حکمرانی هوش مصنوعی برخی کشورها چون چین در حال تحقیق و معرفی استانداردها و اخلاق هوش مصنوعی برآمده اند که برخی از پیشرفت ها در مورد حفاظت از حریم خصوصی و داده ها و همچنین اخلاق هوش مصنوعی شامل موارد زیر شده است :

۱- قانون مدنی چین در سال ۲۰۲۰ با اشاره خاص به حفاظت از حریم خصوصی و اطلاعات شخصی تصویب شد.

۲- دستورالعملی برای خود ارزیابی ۲۹ در سال ۲۰۲۰ تهیه شد تا سؤالات خاصی در مورد جمع آوری و استفاده اطلاعات شخصی توسط برنامه های تلفن همراه ارائه شود.

۳- قانون جدید امنیت داده ها در سال ۲۰۲۱ برای ارتقای امنیت داده ها و حقوق فردی و سازمانی تصویب شد.

۴- کتاب راهنما یا وایت پیپر) در مورد حفاظت از اطلاعات شخصی اپلیکیشنهای موبایل در نوامبر ۲۰۲۱ شد که اقدامات لازم را برای بهبود مکانیسمهای حاکمیتی برنامه های تلفن همراه ارائه میکند.

۵- قانون حفاظت از اطلاعات شخصی در سال ۲۰۲۱ برای تعیین قوانین سختگیرانه در مورد جمع آوری و استفاده از اطلاعات شخصی صادر شد.

۶- راهنمای اخلاق هوش مصنوعی در سال ۲۰۲۰ با اشاره به تحقیق طراحی کاربرد و استفاده از هوش مصنوعی پیشنهاد شد.

۷- هنجارهای اخلاقی برای نسل جدید هوش مصنوعی در سال ۲۰۲۱ منتشر شد تا اخلاق را در توسعه هوش مصنوعی بگنجاند و راهنماییهای اخلاقی ارائه دهد.

۸- راهنما یا وایت پیپر در مورد هوش مصنوعی قابل اعتماد در سال ۲۰۲۱ منتشر شد که اهمیت اعتماد مسئولیت پذیری و شفافیت توسعه هوش مصنوعی را برجسته میکند و به دولت شرکتها و صنایع توصیه کند که چگونه هوش مصنوعی را قابل اعتماد کنند (سکینه ببری گنبد، ۳۱:۱۴۰۲).

جمع بندی

هوش مصنوعی (AI) یکی از پیشرفت‌های مهم در علوم کامپیوتر و فناوری اطلاعات است و به سرعت در حال تغییر جهان است. از کاربردهای هوش مصنوعی می‌توان به خودروهای بدون راننده، سیستم‌های تشخیص چهره، موتورهای جستجو، و ترجمه زبان‌ها اشاره کرد. این فناوری در حال توسعه و رشد قابل توجهی است و پتانسیل بسیاری برای تغییرات زیاد در جوامع و صنایع مختلف دارد. و حوزه نظامی نیز از این قاعده مستثنی نیست. ظهور هوش مصنوعی، چالش‌ها و فرصت‌های جدیدی را برای امنیت به وجود می‌آورد. پیشرفت‌های سریع در حوزه فناوری، به‌ویژه در زمینه هوش مصنوعی، نگاه‌ها را به سوی آینده‌ای معطوف کرده که در آن، امنیت ملی به طور فزاینده‌ای تحت تاثیر این فناوری نوین قرار خواهد گرفت. این باور نه تنها بر فرضیه‌ها و گمانه‌زنی‌های پژوهشگران و مقامات عالی رتبه استوار است، بلکه با بررسی برنامه‌های توسعه کشورها برای سال‌های آینده و سرمایه‌گذاری‌های هنگفت کشورهای پیشرو در این زمینه، مانند ایالات متحده آمریکا، چین و روسیه، به وضوح قابل اثبات است.

هوش مصنوعی، با اتوماسیون و افزایش دقت در جنگ، چالش‌های جدیدی را برای امنیت ملی به وجود خواهد آورد. استفاده از هوش مصنوعی برای جمع‌آوری اطلاعات و نظارت بر شهروندان، نگرانی‌هایی را در مورد حریم خصوصی و آزادی‌های مدنی ایجاد می‌کند. یکی از نگرانی‌های جدید در خصوص دیپ‌فیک، سوءاستفاده از آن در عملیات اطلاعاتی است .دیپ‌فیک‌ها می‌توانند به عنوان سلاح‌های مخفی عمل کنند و به عملیات‌های مخفی اجازه می‌دهند بدون شناسایی انجام شوند .

ایجاد شواهد نادرست یا دستکاری فیلم‌های نظارتی و انتشار اطلاعات نادرست و پروپاگاندا می‌تواند به منظور ایجاد تفرقه و آشوب در جامعه یا برای تخریب وجهه افراد یا سازمان‌ها و روابط بین کشورها بکار گرفته شود. باید گفت هوش مصنوعی می‌تواند به افزایش رقابت بین کشورها برای تسلط بر این فناوری منجر شود. همچنین، هوش مصنوعی می‌تواند قدرت و نفوذ کشورهایی را که از این فناوری به طور پیشرفته استفاده می‌کنند، افزایش دهد. در نهایت، وضع قوانین و مقررات بین‌المللی برای استفاده مسئولانه از هوش مصنوعی ضروری است. این قوانین باید به گونه‌ای باشند که مزایای هوش مصنوعی را برای بشریت تضمین کرده و از سوءاستفاده از این فناوری برای مقاصد مخرب جلوگیری کنند.

منابع

احمدی، علی؛ زرگر،افشین, آدمی، علی (۲۰۲۲). نقش فناوری‌های نوظهور در امنیت و قدرت ملی کشورها؛ فرصت‌ها و تهدیدها. مطالعات بین المللی، سال ۱۸، شماره ۷۲، صص ۱۳۹-۱۶۰.

دهقانی فیروزآبادی ,، سید جلال، چهرآزاد، سعید (۱۴۰۲). هوش مصنوعی و مسئله دار کردنِ درون مایه های امنیت ملی .پژوهش های راهبردی سیاس، دوره ۱۲، شماره ۴۶، صص ۲۴۴-۲۰۹.

سکینه ببری گنبد(۱۴۰۲)،رانی چین درعرصه هوش مصنوعی ، چشم انداز و راهبردها در غرب آسیا، فصلنامه غرب آسیا، سال ول، شاه سوم، صص۳۷-۲۳

عباسیان، ساناز (۱۴۰۰)، امنیت نطقه ای در جنوب آسیا در پرتو هوش مصنوعی، نشریه آینده پژوهی جهان اسلام،

محمدی، شهرام (۱۴۰۲)، کاربرد هوش مصنوعی و اهمیت آن د رامنیت IT، نشریه علوم رایانه، شماره ۲۹، صص ۲۲-۱۴

ملایی، اعظم؛ کافی، مجید (۱۴۰۱)، جایگاههوش مصنوعی در دیپلماسی؛ ملاحظاتی برای جمهوری اسلامی ایران،لنامه مطالعات راهبردی، سال ۲۵، شماره ۴، صص ۳۳۱-۳۱۱

Canada(2023),Implications of Deepfake Technologies on National Security, https://www.canada.ca/en/security-intelligence-service/corporate/publications/the-evolution-of-disinformation-a-deepfake-future/implications-of-deepfake-technologies-on-national-security.html

Congressional Research Service ,(2018), "Artificial Intelligence and National Security", www.crs.gov

Özdemir, gloria shkurti,(2019), "artificial intelligence application in the military the case of united states and china", seta | siyaset, ekonomi ve toplum araştirmalari vakfi

Tutorialspoint (2020), Artificial Intelligence , can be found at: www.tutorialspoint.com , https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_overview.htm