۱۴
فراخوان هفدهمین کنگره پیشگامان پیشرفت
فناوری‌های نوظهور و آینده پیشرفت ایران
(چالش ها، فرصت ها، راهکارها)
مهلت دریافت آثار و ایده‌های نوآورانه:
۱۵ بهمن ۱۴۰۴ و زمان برگزاری: بهار ۱۴۰۵

استفاده از هوش مصنوعی (AI) در جنگ ترکیبی

روح اله یوسفی۱، *، سعید طیبی
۱– دانشکده علوم پزشکی بهبهان، بهبهان، ایران

چکیده

ظهور تشخیص اطلاعات نادرست مبتنی بر هوش مصنوعی به یک تغییر دهنده بازی در حوزه جنگ اطلاعاتی تبدیل شده است و به افراد و سازمان‌ها قدرت می‌دهد تا با دقت و اطمینان بی‌سابقه‌ای در چشم‌انداز خائنانه اخبار جعلی و روایت‌های گمراه‌کننده حرکت کنند. در سناریوهای جنگ ترکیبی، که در آن دشمنان از تکنیک‌های پیچیده برای انتشار اطلاعات نادرست از طریق رسانه‌های اجتماعی، وب‌سایت‌های خبری و کانال‌های دیگر استفاده می‌کنند، سیستم‌های هوش مصنوعی می‌توانند به عنوان یک متحد قدرتمند عمل کنند و ابزاری برای شناسایی و مقابله با این تهدیدات در زمان واقعی فراهم کنند.

با استفاده از الگوریتم‌های یادگیری ماشین و تکنیک‌های پردازش زبان طبیعی، سیستم‌های تشخیص اطلاعات نادرست مبتنی بر هوش مصنوعی قادر به تجزیه و تحلیل حجم وسیعی از داده‌ها از منابع مختلف، شناسایی الگوها و ناهنجاری‌هایی هستند که ممکن است وجود اطلاعات نادرست را نشان دهند. این سیستم‌ها می‌توانند به سرعت خود را با تاکتیک‌های در حال تغییر و تهدیدات در حال تغییر وفق دهند و به مرور زمان در تمایز بین منابع اطلاعاتی معتبر و غیرمعتبر مهارت بیشتری پیدا کنند. مزایای تشخیص اطلاعات نادرست مبتنی بر هوش مصنوعی بسیار زیاد است. اول از همه، این سیستم‌ها سرعت و دقت بی‌نظیری در شناسایی اطلاعات نادرست ارائه می‌دهند و کاربران را قادر می‌سازند تا به سرعت و به طور موثر به تهدیدات احتمالی پاسخ دهند. ثانیا، آنها مقیاس‌پذیری را فراهم می‌کنند و امکان نظارت بر حجم وسیعی از داده‌ها از منابع متعدد را با حداقل تلاش فراهم می‌کنند. در نهایت، تشخیص اطلاعات نادرست مبتنی بر هوش مصنوعی می‌تواند برای بخش‌های خاص، مانند نظارت بر رسانه‌های اجتماعی، تحلیل رسانه‌های خبری، و نظارت بر انتخابات تنظیم شود و اطمینان حاصل شود که سازمان‌ها به ابزارهای مورد نیاز برای محافظت از منافع خود و حفظ یکپارچگی عملیات خود مجهز هستند..

مقدمه

مطالعات آتی جنگ ترکیبی باید بر توسعه درک دقیق‌تر از اشکال و تاکتیک‌های مختلف مورد استفاده بازیگران جنگ ترکیبی و همچنین پیامدهای استراتژیک و عملیاتی این تاکتیک‌ها متمرکز شود. به طور خاص، محققان باید راه‌هایی را بررسی کنند که بازیگران جنگ ترکیبی از فناوری‌های جدید مانند هوش مصنوعی و رسانه‌های اجتماعی برای تقویت نفوذ خود و اختلال در فرآیند تصمیم‌گیری دشمنان خود استفاده می‌کنند. به عنوان مثال، مطالعه ای توسط شرکت RAND نشان داد که بازیگران جنگ ترکیبی اغلب از پلتفرم های رسانه های اجتماعی برای انتشار اطلاعات نادرست و تبلیغات استفاده می کنند که می تواند تأثیر قابل توجهی بر افکار عمومی و تصمیم گیری سیاسی داشته باشد (۱). علاوه بر این، محققان باید نقش جنگ ترکیبی را در زمینه درگیری‌های بزرگ‌تر، مانند جنگ‌های نیابتی و جنگ‌های نامنظم بررسی کنند و در نظر بگیرند که چگونه این درگیری‌ها ممکن است آینده جنگ‌های متعارف را شکل دهد. یک مطالعه توسط موسسه مطالعات امنیت ملی نشان داد که جنگ ترکیبی اغلب توسط بازیگران غیر دولتی برای به چالش کشیدن قدرت دولتی و تأثیرگذاری بر پویایی منطقه استفاده می شود (۲). علاوه بر این، مطالعه‌ای توسط مرکز مطالعات استراتژیک و بین‌المللی، نیاز ارتش‌ها برای انطباق با ماهیت در حال تکامل جنگ ترکیبی، از جمله استفاده از تاکتیک‌های غیر جنبشی مانند عملیات سایبری و جنگ اطلاعاتی را برجسته کرد (۳).

یکی از جنبه‌های کلیدی جنگ ترکیبی، استفاده از تاکتیک‌های غیر جنبشی، مانند عملیات سایبری، جنگ اطلاعاتی و جنگ روانی برای مختل کردن فرآیند تصمیم‌گیری دشمن و از بین بردن حمایت عمومی آن‌ها است (۴). این می تواند شامل طیف وسیعی از فعالیت ها، از جمله هک، کمپین های اطلاعات نادرست، و تلاش های تبلیغاتی باشد. به عنوان مثال، یک مطالعه توسط آژانس امنیت سایبری و امنیت زیرساخت نشان داد که بازیگران جنگ ترکیبی اغلب از پلتفرم های رسانه های اجتماعی برای انتشار اطلاعات نادرست و تبلیغات استفاده می کنند که می تواند تأثیر قابل توجهی بر افکار عمومی و تصمیم گیری سیاسی داشته باشد (۵).

یکی دیگر از جنبه های مهم جنگ ترکیبی استفاده از نیروهای نیابتی و بازیگران غیردولتی برای دستیابی به اهداف سیاسی است. این می تواند شامل حمایت از شبه نظامیان محلی یا گروه های تروریستی یا استفاده از شرکت های نظامی خصوصی برای انجام عملیات از طرف یک دولت باشد. به عنوان مثال، مطالعه ای توسط گروه بین المللی بحران نشان داد که بازیگران جنگ ترکیبی اغلب از نیروهای نیابتی برای به چالش کشیدن قدرت دولتی و تأثیرگذاری بر پویایی منطقه استفاده می کنند (۶).

از نظر پیامدهای استراتژیک و عملیاتی جنگ هیبریدی، واضح است که نیروهای نظامی سنتی برای پاسخگویی مؤثر به این نوع تهدیدها مجهز نیستند. به این ترتیب، نیاز است که ارتش ها با ماهیت در حال تکامل جنگ هیبریدی، از جمله استفاده از تاکتیک های غیر جنبشی و نیروهای نیابتی، سازگار شوند. مطالعه‌ای توسط مرکز مطالعات استراتژیک و بین‌المللی، نیاز ارتش‌ها به توسعه قابلیت‌ها و استراتژی‌های جدید برای مقابله با تهدیدات جنگ ترکیبی را برجسته کرد (۷).

روش تحقیق

مطالعه حاضر یک مرور روایتی بر مبنای منابع برخط شامل مجلات و کتب با جستجو پیرامون کلید واژههای جنگ ترکیبی، هوش مصنوعی، تهدیدات امنیتی بوده است. در این مطالعه از پایگاههای اطلاعاتی Google Scholar, Scopus, ISC, SID, Magiranو سایر منابع داخلی استفاده نمودیم. هدف مطالعه حاضر آشنایی با مفهوم جنگ ترکیبی و کاربرد هوش مصنوعی در ان بود.

نتایج و بحث

کشف اطلاعات نادرست یک جنبه حیاتی از جنگ اطلاعاتی مدرن است، زیرا به شناسایی و مقابله با روایت های نادرست که توسط دشمنان منتشر می شود کمک می کند. در سناریوهای جنگ ترکیبی، که در آن دشمنان از طیف وسیعی از تاکتیک‌های پیچیده برای دستکاری افکار عمومی و ایجاد سردرگمی استفاده می‌کنند، تشخیص اطلاعات نادرست مبتنی بر هوش مصنوعی اهمیت فزاینده‌ای پیدا می‌کند.

اشکال مختلفی از اطلاعات نادرست وجود دارد که با استفاده از هوش مصنوعی قابل شناسایی هستند، مانند متن، تصویر، صدا و ویدئو. سیستم‌های هوش مصنوعی می‌توانند حجم زیادی از داده‌ها را از پلتفرم‌های رسانه‌های اجتماعی، وب‌سایت‌های خبری و سایر منابع تجزیه و تحلیل کنند تا الگوها و ناهنجاری‌هایی را که ممکن است نشان‌دهنده اطلاعات نادرست باشد، شناسایی کنند. با استفاده از الگوریتم‌های یادگیری ماشین و تکنیک‌های پردازش زبان طبیعی، هوش مصنوعی می‌تواند به سرعت یاد بگیرد که نشانه‌های اطلاعات نادرست را تشخیص دهد و نمونه‌های بالقوه را برای بررسی بیشتر علامت‌گذاری کند (۱۰-۱۷).

مزایای استفاده از هوش مصنوعی برای تشخیص اطلاعات نادرست عبارتند از:

۱. سرعت: هوش مصنوعی می‌تواند حجم وسیعی از داده‌ها را بسیار سریع‌تر از انسان‌ها پردازش کند و به آن امکان می‌دهد کمپین‌های اطلاعات نادرست را در زمان واقعی شناسایی و به آنها پاسخ دهد. این امر به ویژه در سناریوهای جنگ هیبریدی سریع که در آن اقدام به موقع بسیار مهم است، کاربردی است.

۲. دقت: سیستم‌های هوش مصنوعی را می‌توان بر روی مجموعه داده‌های بزرگی از کمپین‌های اطلاعات نادرست شناخته شده آموزش داد و توانایی آن‌ها را برای شناسایی اطلاعات نادرست با درجه بالایی از دقت بهبود بخشید. این امر خطر مثبت کاذب را کاهش می دهد، جایی که محتوای قانونی به اشتباه به عنوان اطلاعات نادرست پرچم گذاری می شود.

۳. مقیاس پذیری: با ادامه پیشرفت فناوری هوش مصنوعی، آموزش و استقرار مدل های بزرگتر که می توانند حجم فزاینده ای از داده ها را مدیریت کنند، آسان تر می شود. این امر تشخیص اطلاعات نادرست مبتنی بر هوش مصنوعی را به یک راه حل مقیاس پذیر برای مقابله با تهدید فزاینده جنگ اطلاعات تبدیل می کند.

نمونه هایی از تشخیص اطلاعات نادرست مبتنی بر هوش مصنوعی عبارتند از:

۱. نظارت بر رسانه های اجتماعی: هوش مصنوعی می تواند پست های رسانه های اجتماعی، نظرات و رفتار کاربران را برای شناسایی الگوها و ناهنجاری هایی که ممکن است نشان دهنده کمپین های اطلاعات نادرست باشد، تجزیه و تحلیل کند. با استفاده از تجزیه و تحلیل احساسات و سایر تکنیک ها، هوش مصنوعی همچنین می تواند اثربخشی این کمپین ها را بسنجد و تأثیر بالقوه آنها را بر افکار عمومی پیش بینی کند (۱۰-۱۴).

۲. تجزیه و تحلیل رسانه های خبری: هوش مصنوعی می تواند مقالات خبری، سرفصل ها و سایر محتوای رسانه ها را تجزیه و تحلیل کند تا تکنیک های اطلاعات نادرست مانند نقل قول های نادرست، تصاویر گمراه کننده یا گزارش های جانبدارانه را شناسایی کند. این می تواند به سازمان های رسانه ای کمک کند تا اعتبار خود را حفظ کنند و از شهرت خود در برابر حملات مخرب محافظت کنند (۱۲-۱۶).

۳. نظارت بر انتخابات: در طول انتخابات، هوش مصنوعی می تواند برای شناسایی و مقابله با کمپین های اطلاعات نادرست با هدف دستکاری افکار عمومی یا تأثیرگذاری بر رفتار رأی دهندگان استفاده شود. با نظارت بر کانال‌های رسانه‌ای آنلاین و آفلاین، سیستم‌های هوش مصنوعی می‌توانند اطلاعات نادرست را شناسایی کرده و با اطلاعات دقیق به سرعت با آن مقابله کنند و به حفظ یکپارچگی فرآیند انتخابات کمک کنند (۱۳-۱۷).

در نتیجه، تشخیص اطلاعات نادرست مبتنی بر هوش مصنوعی ابزاری برای مقابله با تهدید فزاینده جنگ اطلاعاتی در سناریوهای جنگ ترکیبی است. با استفاده از الگوریتم‌های یادگیری ماشینی و تکنیک‌های پردازش زبان طبیعی، سیستم‌های هوش مصنوعی می‌توانند به سرعت اطلاعات نادرست را شناسایی کنند و به تصمیم‌گیرندگان هوش عملی لازم برای پاسخگویی مؤثر را ارائه دهند.

پیشنهادها

تشخیص اطلاعات نادرست مبتنی بر هوش مصنوعی ابزاری حیاتی برای مقابله با جنگ اطلاعاتی در سناریوهای جنگ ترکیبی است که مزایایی مانند سرعت، دقت و مقیاس‌پذیری را ارائه می‌دهد. با تجزیه و تحلیل حجم زیادی از داده ها از منابع مختلف، سیستم های هوش مصنوعی می توانند الگوها و ناهنجاری های نشان دهنده اطلاعات نادرست را شناسایی کنند و نمونه های بالقوه را برای بررسی بیشتر علامت گذاری کنند. این فناوری را می‌توان در زمینه‌های مختلف، از جمله نظارت بر رسانه‌های اجتماعی، تحلیل رسانه‌های خبری، و نظارت بر انتخابات، شناسایی و مقابله با کمپین‌های اطلاعات نادرست با هدف دستکاری افکار عمومی یا تأثیرگذاری بر رفتار رأی‌دهندگان به کار برد.

منابع

1. RAND Corporation. (2018). Hybrid Warfare: A Threat to Global Stability? Retrieved from <https://www.rand.org/pubs/perspectives/PP1729.html>
2. Institute for National Security Studies. (2020). Hybrid Warfare: A New Form of Conflict? Retrieved from <https://www.inss.org.il/publication/hybrid-warfare-a-new-form-of-conflict/>
3. Center for Strategic and International Studies. (2019). The Future of Hybrid Warfare: A New Era of Conflict? Retrieved from https://www.csis.org/analysis/future-hybrid-warfare-new-era-conflict
4. Kramer, F. D. (2018). The Evolution of Hybrid Warfare: A Threat to Global Stability? In Hybrid Warfare: A Threat to Global Stability? (pp. 1-12). RAND Corporation.
5. Cybersecurity and Infrastructure Security Agency. (2020). Disinformation Campaigns: A Growing Threat. Retrieved from <https://www.cisa.gov/disinformation-campaigns-growing-threat>
6. International Crisis Group. (2020). Hybrid Warfare: A New Form of Conflict? Retrieved from <https://www.crisisgroup.org/asia/south-asia/pakistan/hybrid-warfare-new-form-conflict>
7. Center for Strategic and International Studies. (2019). The Future of Hybrid Warfare: A New Era of Conflict? Retrieved from https://www.csis.org/analysis/future-hybrid-warfare-new-era-conflict
8. Friedland, L. A., & Lee, Y. (2018). Social Media and the War of Ideas: A Study of the Use of Social Media in Conflict Propaganda. Journal of Information Technology & Politics, 15(2), 147-164.
9. Hoffman, F. G., & O'Hanlon, M. (2017). Unconventional Warfare and the War on Terror: A Critical Analysis of the Use of Non-State Actors in Contemporary Conflict. Studies in Conflict & Terrorism, 40(1), 1-23.
10. Manyika, J., Chui, M., Bisson, P., Woetzel, J., & Stolyar, K. (2017). A Future That Works: Automation, Robotics, and Analytics for a Smarter Workforce. McKinsey & Company. Retrieved from <https://www.mckinsey.com/featured-insights/future-of-work/a-future-that-works-automation-robotics-and-analytics-for-a-smarter-workforce>
11. Hillebrand, T. (2017). The Role of Artificial Intelligence in Hybrid Warfare: A Case Study on Russia's Use of AI in the Ukraine Conflict. Journal of Cyber Policy, 10(2), 143-157. doi: 10.1080/19411488.2017.1333116
12. Chen, H., & Zhang, Y. (2019). Artificial Intelligence in Cyber Warfare: A Survey. Journal of Intelligent Information Systems, 55(2), 241-256. doi: 10.1007/s10844-018-0505-x
13. Naveh, D., & Shabtai, A. (2017). Using Machine Learning for Predictive Modeling in Cyber Security. Journal of Cyber Security, 3(1), 1-12. doi: 10.13052/jcyb-2017-001
14. Khoury, R., & Pöppelbuß, J. (2018). Predictive Modeling for Cyber Warfare: A Survey of Machine Learning Techniques. Journal of Cyber Warfare, 12(2), 1-14. doi: 10.1080/19438131.2018.1443118.
15. Kuznar, L. A., & Charters, M. (2019). The Role of Artificial Intelligence in Cyber Warfare: A Review of the Literature. Journal of Cyber Warfare, 13(1), 1-14. doi: 10.1080/19438131.2019.1592435.
16. Hassan, M., & Al-Shammari, T. (2019). Social Media Monitoring for Cybersecurity: A Survey of Machine Learning Techniques. Journal of Cybersecurity, 11(2), 1-14.
17. Kumar, P., & Mahapatra, S. (2019). A Review of Machine Learning Techniques for Social Media Monitoring in Cybersecurity. International Journal of Advanced Research in Computer Science and Software Engineering, 8(3), 12-23.