The Diplomatic Interactions Quarterly
Vol. 3, No. 10, Summer 2025, Pp: 301-339
Http: www.dpiq.ir

Smart Diplomacy and International Security in the Age of Digital Transformation: An Analysis of the Role of Artificial Intelligence in Countering Cyberterrorism

Seyedeh Latifeh Hosseini[1]
Mohammad Arab Tat[2]
Mohammad Hosseinmardi[3]

(Received: 20/02/2025 - Accepted: 14/06/2025)
DOI: 10.22034/dpiq.2026.555275.1057

Extended Abstract

Introduction

The rapid expansion of Artificial Intelligence (AI) over the last decade has profoundly reshaped the foundations of governance, international politics,

1. Assistant Professor, Department of Law, Faculty of Social Sciences and Economics, Alzahra University, Tehran, Iran. (L.hosseini@Alzahra.ac.ir)
Orcid Code: https://orcid.org/0000-0002-7882-331X
2. Ph.D. Student, Department of International Law, University lecturer and researcher in International Law, Mashhad, Iran. (Mohamadarabtat1997@gmail.com)
Orcid Code: https://orcid.org/0009-0004-6773-4065
3. Assistant Professor, Department of Islamic Studies, Payame Noor University, Tehran, Iran (Mohamadarabtat1997@gmail.com) Corresponding Author
Orcid Code: https://orcid.org/000-000-4968-4186

and global security. Beyond its technical dimension, AI has increasingly become a strategic tool that transforms decision-making processes, enhances predictive capabilities, and restructures state interactions in the digital environment. Within this context, diplomacy has entered a new phase commonly conceptualized as Smart Diplomacy, in which algorithmic analysis, big data processing, automated risk assessment, and AI-supported forecasting play a central role in foreign policy formulation and international negotiations. At the same time, the international security environment has undergone significant transformation. Traditional security threats have been complemented—and in many cases replaced—by network-based and transnational threats rooted in cyberspace. Among these emerging challenges, cyberterrorism has gained particular importance due to its ability to target critical infrastructures, manipulate public opinion through disinformation, recruit individuals through digital platforms, and destabilize political systems without physical confrontation. This study argues that cyberterrorism is no longer a purely technical or domestic security issue; rather, it represents a global security concern requiring coordinated diplomatic strategies, multilateral cooperation, and international governance mechanisms. The main research question is: How can AI, through the framework of smart diplomacy, enhance states' capacity to counter cyberterrorism and strengthen international security in the era of digital transformation? The study hypothesizes that AI-driven smart diplomacy strengthens international security by improving threat detection, enabling predictive analysis, facilitating international cooperation, and enhancing diplomatic negotiation capacities, while also acknowledging that the unregulated use of AI may generate new risks and destabilizing dynamics.

Literature Review

The literature on AI and diplomacy has expanded considerably but remains fragmented across distinct strands. A first strand focuses on AI as a disruptive force in international relations and foreign policy decision-making. Cummings et al. (2018) argue that AI-driven technologies can

reshape strategic planning and crisis prediction by transforming diplomacy into a data-driven process, while Bjola (2019) emphasizes that AI is not merely a technical tool but an influential factor in diplomacy, particularly in negotiation support, crisis management, and public diplomacy. A second strand addresses cybersecurity and emerging threats, including cyberterrorism, focusing mainly on technical and operational dimensions of cyberattacks and the growing vulnerability of critical infrastructures. In this strand, AI is often treated primarily as a defensive cybersecurity instrument rather than a diplomatic tool. A third strand focuses on ethical, legal, and governance implications of AI. Roff (2023) highlights the absence of enforceable international accountability mechanisms in algorithmic decision-making in security and foreign policy, warning that unregulated AI deployment may undermine fundamental rights and international stability. Bjola and Manor (2025) further argue that generative AI can intensify information manipulation, reduce trust, and challenge the legitimacy of diplomatic engagement. Despite these contributions, a significant research gap remains: the relationship between smart diplomacy and the security functions of AI in addressing cyberterrorism has not been systematically examined. This study seeks to fill this gap through policy analysis and conceptual evaluation within the post-2015 digital security environment.

Methodology

This research adopts a qualitative descriptive–analytical approach based on document and policy analysis. Data are drawn from international policy documents, cybersecurity governance reports, academic literature, and institutional publications related to AI governance, cybersecurity, and counterterrorism. The analytical framework is based on thematic content analysis, enabling the identification of key mechanisms through which AI contributes to smart diplomacy and counter-cyberterrorism strategies. This approach provides a conceptual understanding of AI as both a diplomatic instrument and a security-enhancing technology. The study does not rely

on quantitative modeling and prioritizes interpretive and comparative analysis.

Results

The findings demonstrate that AI can strengthen smart diplomacy in countering cyberterrorism through four main mechanisms:
First, cyberattack detection and predictive threat assessment, where AI enables early warning systems by identifying abnormal cyber patterns, detecting malicious networks, and forecasting potential attack scenarios.
Second, countering online radicalization and terrorist recruitment, where AI supports states by monitoring extremist narratives, analyzing behavioral patterns, and identifying vulnerable individuals exposed to digital recruitment strategies.
Third, combating disinformation and information operations, where AI-based systems enhance the detection of coordinated disinformation campaigns, fake news dissemination, and manipulative digital propaganda aimed at destabilizing societies.
Fourth, strengthening multilateral cooperation and diplomatic coordination, where AI facilitates cybersecurity diplomacy through improved data-sharing systems, joint threat analysis, and international norm-building initiatives. Overall, AI contributes not only to technical cybersecurity but also to diplomatic effectiveness by enabling faster responses, improved situational awareness, and structured international cooperation against cyberterrorism.

Discussion

The findings indicate that the relationship between smart diplomacy and cyberterrorism is structurally interconnected. Since cyberterrorism is transnational, its containment requires international coordination, information exchange, and cooperative security frameworks. In this context, smart diplomacy serves as a bridge between technological security tools and international political cooperation. However, the integration of AI into diplomacy and security governance introduces serious challenges.

Algorithmic bias may distort threat perception and lead to discriminatory or politically motivated targeting. The opacity of AI decision-making can weaken accountability and reduce trust among states. Data vulnerability and cyber exploitation risks may also undermine system effectiveness. Furthermore, the concentration of AI capabilities in a limited number of technologically advanced states and private corporations may intensify geopolitical inequality and create new forms of technological hegemony. Thus, AI-enabled smart diplomacy carries a dual nature: while it enhances counterterrorism capacity and international security, it may also generate instability if deployed without regulation, ethical safeguards, and meaningful human oversight.

Conclusion

This study concludes that AI represents a strategic driver of smart diplomacy and an influential factor in reshaping international security in the digital age. It enhances the capacity of states and international organizations to counter cyberterrorism through predictive analytics, threat detection, disinformation management, and multilateral cooperation. However, without effective governance mechanisms, AI-driven diplomacy may increase security dilemmas, deepen distrust among international actors, and produce risks related to bias, privacy violations, and reduced transparency. Therefore, effective smart diplomacy in countering cyberterrorism requires international legal and ethical frameworks, robust data governance, transparency standards, and meaningful human control over critical security decisions.

Recommendations for Further Research

Future research should expand the scope of AI-enabled smart diplomacy in international security by addressing several key areas that remain underexplored in the current literature. First, comparative studies between developed and developing countries are necessary to better understand how differences in technological capacity, digital infrastructure, and institutional readiness shape the effectiveness of AI-driven diplomatic and

security strategies. Such comparisons can also highlight emerging inequalities in global cybersecurity governance.

Second, greater attention should be given to the legal and ethical dimensions of AI-based counterterrorism policies, particularly in relation to international human rights law, data protection standards, and accountability mechanisms in algorithmic decision-making. This is essential for ensuring that the use of AI in security contexts remains transparent, legitimate, and normatively grounded.

Third, future studies should investigate the role of AI in either escalating or mitigating cyber conflicts, with a specific focus on its influence on crisis dynamics, deterrence mechanisms, and the risk of unintended escalation between states in cyberspace.

Finally, further research is needed to explore the interaction between AI systems, non-state cyber actors, and terrorist networks, including how terrorist organizations may adapt to or exploit AI technologies for recruitment, propaganda, and cyber operations. Understanding this triangular interaction is crucial for developing more effective and adaptive counterterrorism strategies in the digital age.

Keywords: Smart diplomacy, Artificial intelligence, International security, Cyber terrorism

How to Cite: Hosseini's. L. , Arab Tat,M. and Hosseinmardi,M. (2025). Smart Diplomacy and International Security in the Era of Digital Transformation: An Analysis of the Role of Artificial Intelligence in Countering Cyber Terrorism. (e242744). *Diplomatic Interactions*, 3(10), e242744, 301- 339. doi: 10.22034/dpiq.2026.555275.1057

فصلنامه تعاملات دیپلماتیک

سال سوم، شماره ۱۰، تابستان ۱٤۰٤، صفحات ۳۳۹-۳۰۱

Http: www.dpiq.ir

دیپلماسی هوشمند و امنیت بین‌المللی در عصر تحول دیجیتال: تحلیل نقش هوش مصنوعی در مقابله با تروریسم سایبری

سیده لطیفه حسینی[۱] - محمد عرب طاط[۲] - محمد مهدی حسینمردی[۳]

(تاریخ دریافت:۱۴۰۳/۱۲/۰۲- تاریخ تصویب: ۱۴۰۴/۰۳/۲۴)

DOI: 10.22034/dpiq.2026.555275.1057

چکیده

ظهور هوش مصنوعی به‌عنوان یکی از مهم‌ترین تحولات فناورانه دهه اخیر، نه تنها ابزارهای حکمرانی دیجیتال را متحول ساخته، بلکه دیپلماسی را نیز وارد مرحله‌ای جدید موسوم به «دیپلماسی هوشمند» کرده است؛ مرحله‌ای که در آن تحلیل کلان‌داده‌ها، پیش‌بینی تهدیدات و تصمیم‌سازی مبتنی بر الگوریتم‌ها به مؤلفه‌ای تعیین‌کننده در سیاست خارجی و امنیت بین‌المللی تبدیل شده‌اند. با این حال، بخش قابل توجهی از پژوهش‌های موجود، یا بر ابعاد فناورانه هوش مصنوعی تمرکز دارد یا بر تهدیدات امنیت سایبری؛ در حالی که پیوند میان دیپلماسی هوشمند و کارکردهای امنیتی هوش مصنوعی در مدیریت «تروریسم سایبری» هنوز از انسجام نظری و تحلیل سیاستی کافی برخوردار نیست. مقاله حاضر با تمرکز بر نظم جهانی در عصر تحول دیجیتال و با بهره‌گیری از روش تحلیل کیفی اسناد و تحلیل سیاستی، نقش هوش مصنوعی را در ارتقای ظرفیت‌های دیپلماسی دولت‌ها برای مقابله با تروریسم سایبری بررسی می‌کند. یافته‌ها نشان می‌دهد که هوش مصنوعی از طریق چهار سازوکار اصلی شامل: (۱) شناسایی و پیش‌بینی الگوهای حملات سایبری، (۲) مقابله با افراط‌گرایی و جذب نیرو در فضای مجازی، (۳) مدیریت عملیات اطلاعاتی و انتشار اخبار جعلی، و (۴) تقویت همکاری‌های چندجانبه در حوزه امنیت سایبری، می‌تواند کارآمدی دیپلماسی را در مواجهه با تهدیدات تروریستی دیجیتال افزایش دهد. با وجود این، پیامدهایی همچون سوگیری الگوریتمی، آسیب‌پذیری داده‌ها، فقدان شفافیت تصمیمات ماشینی و تمرکز قدرت فناورانه، موجب می‌شود که دیپلماسی هوشمند بدون چارچوب‌های تنظیم‌گرانه، خود به عامل بی‌ثباتی در امنیت بین‌المللی تبدیل گردد. موفقیت دیپلماسی هوشمند در مقابله با تروریسم سایبری مستلزم توسعه حکمرانی داده، ایجاد رژیم‌های حقوقی و اخلاقی بین‌المللی و حفظ نقش نظارت انسانی بر تصمیمات امنیتی است.

واژگان کلیدی: دیپلماسی هوشمند، هوش مصنوعی، امنیت بین‌المللی، تروریسم سایبری.

---

۱. استادیار، گروه حقوق، دانشکده علوم اجتماعی و اقتصاد، دانشگاه الزهرا، تهران، ایران. (L.hosseini@Alzahra.ac.ir)

Orcid Code: https://orcid.org/0000-0002-7882-331X

۲. دانشجوی دکتری گروه حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی دانشگاه فردوسی، مشهد، ایران. (Mohamadarabtat1997@gmail.com)

Orcid Code: https://orcid.org/0009-0004-6773-4065

۳. استادیار گروه معارف اسلامی دانشکدهٔ الهیات و معارف اسلامی دانشگاه پیام نور، تهران، ایران (Mohamadarabtat1997@gmail.com)- نویسنده مسئول

Orcid Code: https://orcid.org/000-000-4968-4186

مقدمه

در دهه اخیر و به‌ویژه پس از ۲۰۱۵، هم‌زمان با گسترش فناوری‌های یادگیری ماشین، پردازش کلان‌داده و هوش مصنوعی مولد، سیاست خارجی دولت‌ها و سازوکارهای دیپلماسی بین‌المللی با تحولاتی بنیادین مواجه شده است. در این چارچوب، مفهوم «دیپلماسی هوشمند» به‌عنوان یکی از جلوه‌های دیپلماسی دیجیتال، به رویکردی اطلاق می‌شود که در آن تصمیم‌سازی و مدیریت تعاملات بین‌المللی، بیش از پیش بر تحلیل داده محور، ابزارهای الگوریتمی و قابلیت‌های پیش‌بینی کننده فناوری متکی است. این تحول نه‌تنها کارآمدی دیپلماسی را در مدیریت بحران‌ها افزایش داده، بلکه ماهیت تهدیدات امنیتی را نیز دگرگون کرده است؛ به‌گونه‌ای که بخش مهمی از تهدیدات جدید، ماهیتی فراملی، شبکه‌ای و مبتنی بر زیرساخت‌های دیجیتال یافته‌اند.

در این میان، «تروریسم سایبری» به‌عنوان یکی از پیچیده‌ترین تهدیدات نوظهور، با بهره‌گیری از ابزارهای دیجیتال و فضای مجازی، از مرزهای کلاسیک امنیت ملی عبور کرده و امنیت بین‌المللی را در معرض مخاطرات کیفی قرار داده است. حملات سایبری علیه زیرساخت‌های حیاتی، انتشار سازمان‌یافته اطلاعات جعلی، جذب نیرو از طریق شبکه‌های اجتماعی و هدایت عملیات روانی و تبلیغاتی در بستر اینترنت، نشان می‌دهد که مقابله با تروریسم سایبری دیگر صرفاً یک مسئله امنیت داخلی نیست، بلکه مستلزم هماهنگی بین‌المللی و دیپلماسی فعال در سطح جهانی است. همکاری‌های منطقه‌ای به‌عنوان یکی از عناصر مهم در مقابله با تروریسم سایبری و تأمین امنیت سایبری محسوب می‌شود(شهیدانی، مهدی، ۱۴۰۴:۲۴).

با وجود این، بخش عمده پژوهش‌های موجود درباره هوش مصنوعی در سیاست خارجی، عمدتاً بر موضوعاتی مانند کارایی تصمیم‌سازی یا دیپلماسی دیجیتال تمرکز دارد و از سوی دیگر، ادبیات مربوط به تروریسم سایبری نیز غالباً به ابعاد فنی و امنیتی حملات سایبری پرداخته است. بنابراین، خلأ اصلی پژوهشی در این حوزه، فقدان تحلیل منسجم از این مسئله است که چگونه هوش مصنوعی می‌تواند به‌عنوان ابزار دیپلماسی هوشمند،

ظرفیت دولت‌ها و سازمان‌های بین‌المللی را برای مدیریت تهدید تروریسم سایبری و تقویت امنیت بین‌المللی افزایش دهد.

مقاله حاضر با تمرکز بر نظم جهانی پس از ۲۰۱۵، درصدد پاسخ به این پرسش اصلی است که هوش مصنوعی چگونه و از طریق چه سازوکارهایی می‌تواند دیپلماسی هوشمند را در جهت مقابله با تروریسم سایبری تقویت کرده و بر امنیت بین‌المللی اثرگذار باشد؟ فرضیه پژوهش بر این مبنا استوار است که هوش مصنوعی از طریق افزایش ظرفیت‌های شناسایی تهدید، تحلیل داده محور، پیش‌بینی عملیات تروریستی دیجیتال و تسهیل همکاری‌های چندجانبه در حوزه امنیت سایبری، می‌تواند نقش مهمی در تقویت امنیت بین‌المللی ایفا کند؛ هرچند این فرایند در صورت فقدان چارچوب‌های تنظیم‌گرانه و اخلاقی، با مخاطراتی چون سوگیری الگوریتمی، تهدید حاکمیت داده و کاهش پاسخگویی تصمیمات امنیتی همراه خواهد بود.

این مقاله با رویکرد کیفی و با بهره‌گیری از روش تحلیل اسناد و تحلیل سیاستی انجام شده است. در این چارچوب، اسناد رسمی بین‌المللی، گزارش‌های معتبر درباره حکمرانی هوش مصنوعی و امنیت سایبری و ادبیات علمی مرتبط مورد تحلیل قرار گرفته و داده‌های حاصل به‌صورت تحلیلی و مقایسه‌ای تبیین شده‌اند.

در همین راستا در بخش نخست، تحول پارادایم دیپلماسی در عصر هوش مصنوعی و تحول دیجیتال از منظر نظری مورد تحلیل قرار می‌گیرد. بخش دوم به بررسی نقش هوش مصنوعی در مذاکرات دیپلماتیک مرتبط با تروریسم سایبری اختصاص دارد. در بخش سوم، خدمات و ظرفیت‌های بالقوه هوش مصنوعی در حوزه دیپلماسی تبیین می‌شود. بخش چهارم به کارکردهای اجرایی هوش مصنوعی در مقابله با تروریسم سایبری پرداخته و در ذیل آن، کاربردهای این فناوری در پیش‌بینی اقدامات تروریستی، شناسایی افراد آسیب‌پذیر در برابر جذب گروه‌های تروریستی، مقابله با اطلاعات جعلی و کنترل محتوای تهاجمی در فضای مجازی بررسی می‌گردد. در بخش پنجم، چالش‌های امنیت بین‌الملل در مواجهه با دیپلماسی مبتنی بر هوش مصنوعی تحلیل می‌شود و در نهایت، بخش ششم

به‌ضرورت بهره‌گیری دولت‌ها از دیپلماسی هوش مصنوعی در تقویت امنیت ملی اختصاص می‌یابد.

پیشینه پژوهش

مطالعات مربوط به نقش هوش مصنوعی در سیاست خارجی و امنیت بین‌المللی، در سال‌های اخیر رشد چشمگیری یافته و به‌تدریج از سطح تحلیل‌های فناورانه صرف، به حوزه‌های دیپلماسی دیجیتال، حکمرانی داده و امنیت سایبری گسترش یافته است. با این حال، بررسی ادبیات موجود نشان می‌دهد که پژوهش‌ها را می‌توان در سه دسته کلی طبقه‌بندی کرد:

نخست، پژوهش‌هایی که بر هوش مصنوعی و تحول دیپلماسی و تصمیم‌سازی سیاست خارجی تمرکز دارند. در این دسته، گزارش چتم هاوس(Cummings et al., 2018) با تبیین پیامدهای هوش مصنوعی بر روابط بین‌الملل، بر این نکته تأکید می‌کند که فناوری‌های مبتنی بر داده، ساختار تصمیم‌گیری دیپلماتیک را دگرگون کرده و دولت‌ها را به سمت سیاست‌گذاری پیش‌نگرانه سوق داده است. همچنین بجولا[1] (2019) با طرح مفهوم «دیپلماسی در عصر هوش مصنوعی»، هوش مصنوعی را نه صرفاً یک ابزار فنی، بلکه به‌عنوان عاملی اثرگذار در کیفیت تعاملات دیپلماتیک معرفی می‌کند و نقش آن را در تحلیل محیط بین‌المللی، دیپلماسی عمومی و مدیریت بحران برجسته می‌سازد.

دوم، پژوهش‌هایی که بر امنیت سایبری و تهدیدات نوظهور در نظم بین‌المللی تمرکز دارند. این مطالعات عمدتاً از منظر امنیتی و فنی به موضوع نگاه کرده و تروریسم سایبری را به‌عنوان تهدیدی فراملی علیه زیرساخت‌های حیاتی و ثبات سیاسی بررسی کرده‌اند. در این چارچوب، ادبیات امنیت سایبری نشان می‌دهد که ماهیت شبکه‌ای تهدیدات سایبری موجب شده است که دولت‌ها ناگزیر از توسعه همکاری‌های چندجانبه و تنظیم‌گری بین‌المللی شوند. با این حال، در این دسته از پژوهش‌ها، هوش مصنوعی بیشتر به‌عنوان ابزار

1 Bjola

دفاع سایبری یا فناوری امنیتی معرفی شده و نقش آن در «دیپلماسی» و مدیریت همکاری‌های بین‌المللی کمتر مورد توجه قرار گرفته است.

سوم، پژوهش‌هایی که به ابعاد حقوقی، اخلاقی و حکمرانی هوش مصنوعی پرداخته‌اند. در این حوزه روف[1] (2023) بر فقدان چارچوب‌های الزام‌آور بین‌المللی در زمینه پاسخگویی دولت‌ها نسبت به تصمیمات الگوریتمی تأکید کرده و هشدار می‌دهد که استفاده بی‌ضابطه از هوش مصنوعی در سیاست خارجی می‌تواند زمینه‌ساز نقض حقوق بنیادین و بی‌ثباتی در نظم بین‌المللی گردد. علاوه بر این، منور [2] و بجولا (2025) با تمرکز بر هوش مصنوعی مولد، دیپلماسی دیجیتال را در معرض خطراتی همچون دست‌کاری اطلاعات، بی‌اعتمادی عمومی و بحران مشروعیت قرار می‌دهند.

با وجود ارزش تحلیلی این پژوهش‌ها، خلأ اصلی در ادبیات موجود آن است که پیوند میان دیپلماسی هوشمند و کارکردهای امنیتی هوش مصنوعی در مدیریت تهدید تروریسم سایبری هنوز به‌صورت منسجم و نظام‌مند مورد واکاوی قرار نگرفته است. بخش قابل‌توجهی از مطالعات، یا بر دیپلماسی هوشمند تمرکز کرده و تهدیدات سایبری را در حاشیه قرار داده‌اند، یا بر تروریسم سایبری متمرکز بوده و نقش دیپلماسی و ابزارهای سیاست خارجی در مدیریت این تهدید را کمتر بررسی کرده‌اند. از این رو، پژوهش حاضر با تمرکز بر نظم جهانی پس از ۲۰۱۵ و با رویکرد تحلیل سیاستی و اسنادی، درصدد است این شکاف تحلیلی را پر کرده و نشان دهد که هوش مصنوعی چگونه می‌تواند به‌عنوان ابزار دیپلماسی هوشمند، ظرفیت‌های همکاری بین‌المللی و مدیریت تهدیدات تروریستی دیجیتال را تقویت کند.

چارچوب مفهومی و نظری دیپلماسی هوشمند در عصر تحول دیجیتال

سیاست خارجی بخشی از حاکمیت سیاسی است(کوهکن، ۱۴۰۳: ۱۲۵). در دهه اخیر، فناوری‌های ارتباطی و اطلاعاتی به عاملی تعیین‌کننده در شکل‌دهی سیاست خارجی،

1 Roff
2 Manor

دیپلماسی و امنیت بین‌المللی تبدیل شده‌اند. تأثیر این فناوری‌ها بر روابط میان دولت‌ها که در ابتدا مسئله‌ای نوظهور تلقی می‌شد، به‌تدریج به یکی از محورهای اصلی برنامه‌ریزی سیاست خارجی بدل شده است. تأکید وزیر امورخارجه وقت ایالات‌متحده در سال ۲۰۱۰ بر آزادی اینترنت و نقش آن در سیاست دولت‌ها، نقطه عطفی در به رسمیت شناختن اهمیت فضای مجازی در دیپلماسی معاصر به شمار می‌رود(Clinton, 2010) . در نتیجه این تحول، بسیاری از کشورها بخش‌هایی را در وزارت امورخارجه به دیپلماسی سایبری اختصاص داده‌اند. دیپلماسی سایبری، به‌عنوان گونه‌ای از دیپلماسی عمومی، مبتنی بر اینترنت و فضای مجازی است و مدیریت و انتشار اطلاعات در رسانه‌های آنلاین را به ابزاری کلیدی برای تقویت روابط بین‌دولتی و مقابله با تهدیدات فراملی، از جمله تروریسم سایبری، تبدیل کرده است (حاج زرگرباشی، ۱۳۹۷: ۹).

هم‌زمان، هوش مصنوعی به‌عنوان فناوری نوین، تأثیرات عمیقی بر حوزه‌های امنیتی و دیپلماتیک بر جای گذاشته است. ظرفیت این فناوری در تحلیل داده‌های کلان، مدیریت بحران‌ها و پیش‌بینی رویدادهای بین‌المللی، آن را به ابزاری راهبردی در سیاست خارجی بدل کرده است (Spike Back, 2018: 3). بهره‌گیری دیپلمات‌ها از سامانه‌های هوشمند نه‌تنها الگوهای سنتی تصمیم‌گیری را متحول ساخته، بلکه به شکل‌گیری «دیپلماسی هوشمند» انجامیده است؛ دیپلماسی‌ای که با تحلیل سریع داده‌ها و پیش‌بینی رفتار بازیگران، امکان واکنش مؤثرتر به تهدیدات نوظهور، به‌ویژه در فضای سایبری، را فراهم می‌کند (خرازی آذر، ۱۳۹۲: ۵). دیپلماسی هوش مصنوعی، به‌عنوان شاخه‌ای نوظهور از دیپلماسی علمی و فناورانه، بر تنظیم، نظارت و استفاده مسئولانه از فناوری‌های مبتنی بر هوش مصنوعی تمرکز دارد و تلاشی برای پر کردن شکاف میان شتاب پیشرفت فناوری و کندی فرایندهای تنظیم‌گری بین‌المللی است. از منظر نظری، این نوع دیپلماسی ابزاری برای مدیریت ریسک‌های فراملی ناشی از هوش مصنوعی، از جمله نظارت انبوه، تبعیض الگوریتمی و سوءاستفاده گروه‌های تروریستی از فضای سایبری، محسوب می‌شود (Bjola, 2023: 21–38). در این چارچوب، قدرت‌های بزرگ رویکردهای متفاوتی اتخاذ کرده‌اند: ایالات‌متحده بر نوآوری و بازار آزاد، اتحادیه اروپا بر تنظیم گرایی و

حفاظت از حقوق بنیادین، و چین بر امنیت ملی و کنترل داده‌ها تأکید دارد (Cave, 2022: 45).

در دیپلماسی مدرن، الگوهای هوشمند تصمیم‌گیری با تحلیل داده‌های متنوع، از شبکه‌های اجتماعی تا تصاویر ماهواره‌ای، امکان شناسایی زودهنگام تهدیدات سایبری و تروریستی را فراهم می‌کنند و بدین ترتیب توان پاسخگویی دولت‌ها و شفافیت روابط بین‌المللی را افزایش می‌دهند (Gavriloric, 2020: 12). هوش مصنوعی همچنین در مدیریت بحران‌ها، عملیات صلح سازی و ارتقای امنیت اطلاعات نقش مؤثری ایفا می‌کند و از طریق پیش‌بینی ناهنجاری‌ها و پایش فضای دیجیتال، به مقابله با فعالیت‌های تروریستی در فضای سایبری یاری می‌رساند (Anastassia Lauterbach, 2017: 13).

در سطح چندجانبه، سازمان‌هایی مانند یونسکو، اتحادیه اروپا و سازمان همکاری و توسعه اقتصادی در تدوین چارچوب‌های اخلاقی و حقوقی هوش مصنوعی فعال بوده‌اند. تصویب «توصیه‌نامه اخلاق هوش مصنوعی یونسکو» در سال ۲۰۲۱ نشان‌دهنده تأکید جامعه بین‌المللی بر همکاری چندجانبه برای جلوگیری از رقابت مخرب فناورانه و سوءاستفاده امنیتی از این فناوری است (UNESCO, 2021: 3–7).

از منظر امنیت بین‌الملل، دیپلماسی هوش مصنوعی همچنین ابزاری برای مهار مسابقه تسلیحاتی و مدیریت تهدیدات سایبری تلقی می‌شود، هرچند نبود اعتماد متقابل و ضعف سازوکارهای نظارتی، تحقق یک رژیم مؤثر کنترل را با چالش مواجه ساخته است. (Brundage, 2023: 742). در این میان چندجانبه گرایی، افزایش نقش بازیگران غیردولتی در بازی‌های دیپلماتیک و قدرت نرم از جمله عوامل تغییرات در دیپلماسی عصر حاضر هستند (کوهکن، ۱۴۰۳: ۷).

در مجموع، تحول دیپلماسی در عصر هوش مصنوعی را می‌توان تغییر پارادایمی در فهم سنتی از امنیت بین‌المللی دانست. همان‌گونه که بوتروس غالی بر اهمیت پیشگیری، دیپلماسی پیش‌دستانه و هشدار زودهنگام تأکید می‌کند(Boutros-Ghali, 1992) . هوش مصنوعی این ظرفیت را دارد که شناسایی تهدیدات، از جمله تروریسم سایبری، را از سطح منطقه‌ای به مقیاس جهانی ارتقا دهد. در پرتو دیدگاه صلح مثبت گالتونگ نیز،

این فناوری می تواند با کاهش خطاهای انسانی، افزایش شفافیت اطلاعاتی و پیشگیری از خشونت ساختاری، به تحکیم امنیت بین‌المللی یاری رساند(Galtung, 1996: 270) و فناوری‌های نوینی همچون هوش مصنوعی می توانند با کاهش خطاهای انسانی، پیش‌بینی منازعات، و بهبود شفافیت اطلاعاتی، به تحقق این نوع امنیت یاری رسانند. از این‌رو، دیپلماسی هوشمند نه‌تنها ابزاری فناورانه، بلکه سازوکاری نرم برای تحکیم امنیت بین-المللی، اعتمادسازی میان ملت‌ها و تقویت چندجانبه گرایی در نظام‌بین‌الملل محسوب می‌شود.

نقش هوش مصنوعی در مذاکرات دیپلماتیک مرتبط با تروریسم سایبری

در سال‌های اخیر، هوش مصنوعی به‌طور فزاینده‌ای وارد عرصه مذاکرات دیپلماتیک بین‌المللی شده و با فراهم‌سازی ابزارهای تحلیلی پیشرفته، به ارتقای توان تصمیم‌سازی تیم‌های مذاکره‌کننده کمک کرده است. این فناوری از طریق تحلیل کلان‌داده‌ها، شناسایی الگوهای رفتاری بازیگران و پیش‌بینی سناریوهای محتمل، فرآیند دستیابی به توافق را تسهیل می‌کند. برای نمونه، شرکت بین‌المللی ماشین‌های تجاری پلتفرمی شناختی تحت عنوان «مشاور تجاری شناختی» طراحی کرده است که با کنکاش در مقررات و اسناد حقوقی حوزه تجارت، به پرسش‌ها و ابهامات مربوط به توافقنامه‌ها پاسخ می‌دهد و بینش‌های تحلیلی به‌موقع در اختیار مذاکره‌کنندگان قرار می‌دهد؛ هرچند این سامانه فاقد اختیار تصمیم‌گیری مستقل بوده و جایگزین مذاکره انسانی نمی‌شود (Brundag & Avin, Same,2018: 14). بر این اساس، هوش مصنوعی نه جایگزین دیپلمات، بلکه ابزاری مکمل برای افزایش دقت راهبردی و توان تحلیلی مذاکرات است. به‌ویژه در مذاکرات حساس و نیمه ساختاریافته مانند امنیت بین‌المللی، مسائل اقلیمی و کنوانسیون‌های دیجیتال، قضاوت انسانی همچنان نقش محوری دارد؛ زیرا داده‌ها اغلب در معرض تفسیرهای متعارض قرار می‌گیرند و انتخاب تفسیر برتر مستلزم داوری انسانی است (حسینی، ۱۴۰۳: ۱۱) مسئله دشوار در این خصوص برای هوش مصنوعی می‌تواند ناشی از آن باشد که میزان صحت و استحکام داده‌ها در موضوعاتی که به‌راحتی در معرض تفسیرها

و مباحثه‌های تخصصی قرار می‌گیرند، در سطح پایین‌تری قرار دارد. از این رو، وجود تخصص انسانی در برنامه‌ریزی و داوری ضروری‌تر است زیرا انسان می‌تواند از میان گستره متنوعی از تفاسیر موجود درباره یک مسئله، برداشت برتر یا مناسب‌تر را برگزیده و روند تصمیم‌گیری و مذاکره را بر محور آن هدایت کند (Mintz, 2010:15).در عین حال، سامانه‌های هوشمند می‌توانند با تحلیل سریع داده‌ها، شناسایی تهدیدات بالقوه و پیش‌بینی روندهای بحرانی، آمادگی تیم‌های مذاکره‌کننده را در شرایط پیچیده افزایش دهند، مشروط بر آن‌که کنترل نهایی فرآیند تصمیم‌گیری در اختیار انسان باقی بماند (Bjola, 2021:22).

تحول دیپلماسی در بستر دیجیتال، موجب فاصله گرفتن آن از ساختار سلسله‌مراتبی سنتی شده است. در دیپلماسی برخط، بازیگران دیپلماتیک از دسترسی تقریباً برابر به ابزارهای ارتباطی برخوردارند و ارزیابی اثربخشی کنش‌های دیپلماتیک عمدتاً از طریق تحلیل داده‌های فضای مجازی صورت می‌گیرد. در این زیست‌بوم، زبان دیپلماتیک کلاسیک جای خود را به زبانی فناورانه، دیداری و نشانه‌ای داده است که از ظرفیت ارتباطی و اقناعی بالاتری برخوردار است (David Valle-Cruz, 2019:5) . در الگوی دیپلماسی فاقد هوش مصنوعی، تمامی اعضای یک هیئت دیپلماتیک از کارکنان رده پایین تا وزیر امورخارجه از دسترسی تقریباً برابر به ابزارهای ارتباطی و رسانه‌ای برخوردارند و هر یک می‌توانند به‌صورت مستقل، صفحه یا وبگاه رسمی خود را ایجاد و مدیریت کنند. در چنین بستری، ارزیابی کمی و کیفی محتوای تولید شده تنها از رهگذر تحلیل داده‌ها در فضای مجازی ممکن است؛ به گونه‌ای که تعداد و تعامل دنبال کنندگان را می‌توان از شاخص‌های برجسته اعتبار و اثربخشی ارتباطی به شمار آورد. از سوی دیگر، در این زیست‌بوم دیجیتالی، زبان دیپلماتیک کلاسیک جای خود را به گونه‌ای تازه از زبان فناورانه داده است؛ زبانی که بر پایه‌ی عناصر دیداری و نشانه‌ای نظیر تصویر متحرک، نگاره، برچسب تصویری و پیام مستقیم شکل می‌گیرد. این شکل نوین از بیان، در مقایسه با زبان رسمی و ساده، از ظرفیت بیانی و ارتباطی بسیار عمیق‌تری برخوردار است و به دلیل

وضوح، اختصار و بار معنایی بالا جایگاه ممتاز در تعاملات دیپلماتیک دیجیتال یافته است (Unever, 2020:9).

در همین چارچوب، پیوند میان مذاکرات دیپلماتیک، امنیت بین‌المللی و مقابله با تروریسم سایبری آشکار می‌شود؛ زیرا هوش مصنوعی از یک‌سو ابزار تحلیلی مذاکرات امنیتی و سایبری را تقویت می‌کند و از سوی دیگر، از طریق شناسایی حملات سایبری، مقابله با اطلاعات جعلی و تحلیل شبکه‌های افراطی در فضای مجازی، به مهار تهدیدات تروریستی سایبری یاری می‌رساند. با توجه به تبدیل‌شدن حملات سایبری به تهدیدی راهبردی علیه حاکمیت و ثبات دولت‌ها (اسلامی، ۱۳۹۳: ۲)، بهره‌گیری دیپلماتیک از هوش مصنوعی به بخشی جدایی‌ناپذیر از راهبردهای امنیت بین‌المللی بدل شده است.

در عصر داده محور کنونی، رقابت دولت‌ها و شرکت‌های بزرگ فناوری بر سر دسترسی و کنترل داده‌ها، جایگزین رقابت‌های منابع محور سنتی شده است؛ به‌گونه‌ای که داده‌ها نقشی مشابه منابع هیدروکربنی قرن بیستم یافته‌اند (Fernando Filgueiras, 2022:7).از این رو، دیپلمات‌ها ناگزیرند با اتکا به دانش فنی و چارچوب‌های حقوقی بین‌المللی، قواعد حاکم بر فعالیت شرکت‌های فناوری، بهره‌برداری از داده‌های شخصی و کاربردهای امنیتی هوش مصنوعی را در مذاکرات بین‌المللی تنظیم کنند(حسنی،۱۴۰۳: ۱۲).

در مجموع، هوش مصنوعی در مذاکرات دیپلماتیک، با ایفای نقش تحلیلی، پیش‌بینی و پشتیبان تصمیم‌گیری، توان دیپلماسی انسانی را در مدیریت بحران‌ها، کاهش تنش‌ها و مقابله با تهدیدات نوظهور از جمله تروریسم سایبری افزایش می‌دهد و از این رهگذر، به تقویت صلح و امنیت بین‌المللی کمک می‌کند (Bjola, 2021:22).

با وجود ظرفیت‌های قابل‌توجه هوش مصنوعی در ارتقای کیفیت تحلیل و پشتیبانی از تصمیم‌سازی در مذاکرات دیپلماتیک، اتکای فزاینده به این فناوری بدون طراحی سازوکارهای حقوقی و نهادی مناسب، می‌تواند به بازتولید عدم تقارن قدرت میان دولت‌ها و تعمیق شکاف دیجیتال در نظام‌بین‌الملل منجر شود. دولت‌هایی که از زیرساخت‌های داده‌ای پیشرفته، شرکت‌های فناوری بومی و دسترسی گسترده به الگوریتم‌های تحلیلی

برخوردارند، در عمل از مزیت ساختاری در فرآیندهای مذاکره بهره‌مند می‌شوند؛ امری که اصل برابری حاکمیت‌ها در دیپلماسی چندجانبه را با چالش مواجه می‌سازد. افزون بر این، ماهیت غیر شفاف برخی الگوریتم‌ها، خطر انتقال سوگیری‌های سیاسی، فرهنگی و امنیتی به فرآیند تصمیم‌سازی دیپلماتیک را در پی دارد و می‌تواند مسئولیت‌پذیری و پاسخگویی تصمیمات اتخاذشده را تضعیف کند. از این منظر، هوش مصنوعی نه صرفاً یک ابزار فنی، بلکه پدیده‌ای هنجاری و قدرت ساز است که استفاده از آن در مذاکرات دیپلماتیک مستلزم تثبیت اصل «کنترل انسانی معنادار»، شفافیت الگوریتمی و تنظیم قواعد حقوقی بین‌المللی است. تنها در چنین چارچوبی می‌توان اطمینان یافت که دیپلماسی هوشمند، به جای تهدید، به عاملی برای تقویت اعتماد، ثبات و امنیت پایدار در نظام بین‌المللی بدل شود.

نقش هوش مصنوعی در تقویت دیپلماسی هوشمند برای مدیریت تهدیدات سایبری

در چشم‌انداز دیپلماسی هوشمند، بسیاری از کارکردهای مرتبط با سیاست خارجی و حاکمیت ملی دولت‌ها -از جمله مشاوره حقوقی، نگارش، ترجمه، تحلیل، طبقه‌بندی و سازمان‌دهی اسناد دیپلماتیک- به‌تدریج مشمول فرایندهای اتوماسیون و هوشمند سازی خواهند شد و این تحول، به‌طور مستقیم بر سازوکارهای تصمیم‌گیری و کنش دیپلماتیک دولت‌ها اثرگذار خواهد بود (Magdin, 2019:20).در همین راستا، سفارتخانه‌ها به پایگاه‌های داده‌ای گسترده، به‌ویژه در ارتباط با دیاسپورا، تبدیل می‌شوند و از داده‌های طبقه‌بندی‌شده برای پیشبرد منافع ملی و امنیتی خود بهره می‌گیرند (Ben Scott, 2018:19).

پیشرفت ربات‌های مذاکره‌کننده و سامانه‌های هوشمند نشان می‌دهد که هوش مصنوعی می‌تواند با پردازش حجم عظیمی از داده‌های سیاسی، امنیتی و سایبری، فرآیندهای چانه‌زنی و مذاکره را تسهیل و از بن‌بست‌های دیپلماتیک جلوگیری کند (کرمی، ۱۴۰۳: ۱).

با این حال، در حوزه‌هایی چون صلح، حاکمیت ملی و امنیت بین‌المللی، نقش قضاوت انسانی همچنان تعیین‌کننده است؛ زیرا تصمیم‌گیری‌های سیاسی به‌طور ماهوی وابسته به تجربه، مهارت و درک انسانی از زمینه‌های پیچیده اجتماعی و ارزشی‌اند (کرمپور، ۱۴۰۳: ۱۲). به‌عنوان نمونه، یک ربات دیپلمات که در حال مذاکره درباره توافق‌نامه‌ای سیاسی با هدف تقویت حاکمیت ملی دولت‌ها در جهت تأمین صلح و امنیت بین‌المللی است، به اکثریت داده‌های سیاسی، اجتماعی، امنیتی، اطلاعاتی و سایبری موجود، دسترسی به‌موقع دارد. چنین سامانه‌ای این قابلیت را دارد که با صرف هزینه‌های مالی و زمانی کمتر نسبت به دیپلمات‌های انسانی، با ربات دیپلمات رقیب خود پیرامون مجموعه‌ای از پیشنهادهای متقابل به مباحثه و مذاکره بپردازد. راندمان اجرایی ربات‌های دیپلماتیک در مذاکرات چندجانبه‌ای همچون توافق‌نامه تغییرات اقلیمی پاریس، منجر به صرفه‌جویی و بهینه‌سازی قابل‌توجهی در زمان می‌گردد. افزون بر این، ربات‌های مزبور با ارائه مجموعه‌ای از راهکارهای متنوع، مانع از به بن‌بست رسیدن مذاکرات سیاسی و رکود در روندهای دیپلماتیک می‌شوند. با این حال، این امر به معنای حذف کامل دیپلمات‌های انسانی از فرایند مذاکرات مرتبط با اعمال حاکمیت‌های ملی نیست؛ زیرا امور وابسته به جهان سیاست به‌گونه‌ای ماهوی، قائم به انسان هستند و نقش شخصیت، تجربه و مهارت‌های فردی در این عرصه همواره حائز اهمیت باقی می‌ماند(کیریلینکا اینا، ۱۴۰۳: ۹) .ازاین‌رو، الگوی مسلط آینده نه حذف دیپلمات‌های انسانی، بلکه واگذاری وظایف فنی و فرعی به سامانه‌های هوشمند و تمرکز انسان بر تصمیمات راهبردی خواهد بود (Andrea Renda, 2019:112).

در سطح نظری، دیپلماسی مبتنی بر هوش مصنوعی از یک‌سو با کاهش خطاهای انسانی و تصمیم‌گیری‌های هیجانی می‌تواند به افزایش کارآمدی مذاکرات و همکاری میان دولت‌ها منجر شود، و از سوی دیگر، به دلیل احتمال بازتولید سوگیری‌های انسانی در الگوریتم‌ها، با چالش‌هایی جدی در زمینه بی‌طرفی و مشروعیت مواجه است (میرکوشش، ۱۴۰۳ : ۸-۹). این وضعیت، عدم اطمینان در عرصه دیپلماسی مدرن را تشدید کرده و

ضرورت برخورداری از ظرفیت‌های محاسباتی پیشرفته و چارچوب‌های تنظیم‌گر مناسب را برجسته می‌سازد (Unever,2020:15).

در همین راستا، توجه به این نکته ضروری است که با توجه به گسترش روزافزون فناوری‌های نوین، مفهوم امنیت دیگر محدود به عرصه‌های فیزیکی و تکوینی نیست؛ بلکه در ابعاد سایبری و غیرملموس نیز امکان بروز ناامنی به‌صورت مداوم وجود دارد. در چنین بستری، پیوند دیپلماسی هوشمند با مقابله با تروریسم سایبری و امنیت بین‌المللی آشکار می‌شود؛ زیرا هوش مصنوعی با تحلیل پیش‌بینی کننده داده‌های کلان، پایش تهدیدات سایبری و شناسایی الگوهای افراط‌گرایانه در فضای دیجیتال، امکان پیشگیری از بحران‌ها و ناامنی‌های نوظهور را فراهم می‌سازد. این ظرفیت‌ها به دولت‌ها و سازمان‌های بین‌المللی اجازه می‌دهد پیش از تبدیل تهدیدات سایبری به بحران‌های امنیتی، از ابزارهای دیپلماتیک، میانجی‌گری و تنظیم‌گری بهره گیرند و بدین‌سان، امنیت و ثبات بین‌المللی را تقویت کنند؛ هرچند نظارت و داوری انسانی همچنان شرط لازم مشروعیت و اخلاق‌مندی این فرایندها باقی می‌ماند. بر همین اساس، تمرکز بر سازوکارهای هوش مصنوعی در مقابله با تهدیدات و تروریسم سایبری، گام بعدی و منطقی این پژوهش را تشکیل می‌دهد.

سازوکارهای عملی هوش مصنوعی در مقابله با تروریسم سایبری

تهدیدات بالقوه ناشی از فعالیت گروه‌های تروریستی و نیز آشنایی گسترده این گروه‌ها با فضای مجازی، پژوهشگران و فعالان حوزه هوش مصنوعی را بر آن داشته است تا از ظرفیت‌های این فناوری در مبارزه با تروریسم سایبری بهره گیرند. چنین رویکردی می‌تواند تأثیرات قابل‌توجهی در تقویت امنیت ملی و منطقه‌ای بر جای گذارد و به شکل‌گیری نظام‌های پیشگیرانه و پاسخ‌گو در برابر حملات دیجیتالی منجر شود.

در همین زمینه، آنتونیو گوترش، دبیر کل وقت سازمان ملل متحد، در چارچوب «اختیارات استراتژیک دبیر کل در حوزه فناوری‌های نوین»، بر اهمیت کنترل هوشمندانه این فناوری تأکید کرده و اظهار داشت:

«اگر هوش مصنوعی به‌درستی مدیریت شود و ارزش‌ها و تعهدات مندرج در منشور ملل متحد و اعلامیه جهانی حقوق بشر مورداحترام قرار گیرند، این فناوری می‌تواند نقش مؤثری در تحقق توسعه پایدار از طریق پایان دادن به فقر، حفاظت از سیاره زمین و تضمین صلح و رفاه برای همگان ایفا کند. به همین نحو، هوش مصنوعی قادر است به ابزاری قدرتمند برای مقابله با تروریسم سایبری و اخلالگران امنیت در فضای مجازی تبدیل شود» (Guterres, 2023:2). با توجه به مطالب فوق، می‌توان هوش مصنوعی را از جنبه‌های گوناگون بر ابعاد مختلف امنیت بین‌المللی مؤثر دانست؛ تأثیری که در ادامه، مهم‌ترین ابعاد و کارکردهای آن به‌صورت مختصر موردبررسی قرار می‌گیرد.

الف) پیش‌بینی حملات و هشدار سریع

سازمان‌های امنیتی با بهره‌گیری از قابلیت‌های هوش مصنوعی می‌توانند از طریق پیش‌بینی حملات تروریستی و اتخاذ اقدامات پیشگیرانه یا ارائه هشدار به مراجع ذی‌صلاح، از بروز خسارات جبران‌ناپذیر ناشی از این اقدامات جلوگیری کنند. به‌عنوان نمونه، یکی از مدل‌های برجسته پیش‌بینی به نام استون[1] وجود دارد که به نحوی طراحی شده است تا بتواند پیش‌بینی کند در صورت بازداشت هر یک از اعضای شبکه تروریستی، کدام عضو جانشین او خواهد شد و همچنین، نحوه بازسازی و احیای شبکه و مقاومت آن در برابر تهدیدهای بعدی را تحلیل نماید (Karabiyik, 2016: 5).

علاوه بر این، شرکت نوپای فعال در حوزه هوش مصنوعی به نام هوش حشره‌ای نیز با استفاده از مدل‌های متنوع یادگیری ماشین، موفق به پیش‌بینی تهدیدات آنلاین در شبکه‌های اجتماعی، از جمله فعالیت‌های تروریستی، شده است.[2]

ب) شناسایی شبکه‌های افراطی و جذب نیرو

مجریان قانون و سازمان‌های ضد تروریستی با بهره‌گیری از تکنیک‌هایی مانند استون و مدل‌های مشابه، قادرند با شناسایی کلمات و عبارات کلیدی که معمولاً توسط افراط‌گرایان

1 stone
2 INSIKT Intelligence.

تروریست به کار می‌رود، احتمال گرایش افراد به اقدامات تروریستی و جذب در این گروه‌ها را پیش‌بینی و تحلیل کنند. به‌عنوان نمونه، می‌توان به پروژه اتحادیه اروپا در سال ۲۰۲۰ تحت عنوان سیستم تشکیل و هشدار زودهنگام محتوای تروریستی آنلاین اشاره نمود[1] این پروژه از جمله ابزارهایی است که هدف اصلی آن شناسایی و تشخیص گرایش به افراط‌گرایی در مراحل اولیه و مقدماتی است.[2]

ج) مقابله با اطلاعات جعلی و عملیات روانی

تحریف یا جعل اطلاعات می‌تواند در گسترش رفتارهای خشونت‌آمیز و تحریک اقدامات تروریستی نقش داشته باشد. در این زمینه، شناسایی حساب‌های کاربری جعلی به‌عنوان گامی مؤثر در مقابله با انتشار اطلاعات نادرست مطرح است.برای مثال، سازمان اطلاعات و امنیت بریتانیا با بهره‌گیری از قابلیت‌های هوش مصنوعی توانسته است حساب‌های جعلی را شناسایی کند (Smith, 2021:3).به همین ترتیب، در سریلانکا نیز از الگوریتم‌ها و روش‌هایی مانند استون برای شناسایی و تشخیص اطلاعات نادرست استفاده شده است؛ این اقدام، گامی پیشرفته در محدودسازی فعالیت گروه‌های تروریستی و کاهش تهدیدات علیه امنیت بین‌المللی در حوزه‌های مختلف انتشار اطلاعات محسوب می‌شود.

د) مدیریت امنیت زیرساخت‌های حیاتی

یکی از رایج‌ترین اقداماتی که توسط شبکه‌های اجتماعی با هدف مقابله با تروریست‌ها، آشوبگران بین‌المللی و گروه‌های افراط‌گرا انجام می‌شود، استفاده از حذف خودکار محتواهای توهین‌آمیز و تهاجمی است. این فرایند عمدتاً با توسل به فناوری‌های هوش مصنوعی و مکانیسم‌های پیشرفته آن امکان‌پذیر می‌گردد. در این راستا، عقاید توهین‌آمیز و محتوای تهاجمی حذف شده و وب‌سایت‌ها یا حساب‌هایی که این محتواها را منتشر

1 Early Detection and Alert System for Online Terrorist Content (RED-Alert).

۲ در این زمینه می‌توان به سیستم نظارت دولت آلمان بر فعالیت‌های افراط‌گرایی با عنوان اختصاری(موترا) اشاره کرد، که ابزار نظارتی جامعی برای تحلیل داده‌های جمع‌آوری‌شده به‌منظور ارزیابی تحولات اجتماعی رخ داده در جوامع با قابلیت بالای پذیرش افراط‌گرایی است.

می‌کنند، مسدود می‌شوند. به‌عنوان مثال، فیس‌بوک برای اولویت‌بندی محتوا و شناسایی نقض‌کننده‌های خط‌مشی‌های خود، از یادگیری ماشین و مدل استون بهره می‌برد؛ به‌نحوی که پست‌های متخلف توسط فیلترهای یادگیری ماشین علامت‌گذاری می‌شوند (Saltman, 2020:1).

همچنین، وزارت کشور بریتانیا در سال ۲۰۱۸ اعلام کرد که به دنبال توسعه فناوری جدیدی است تا با استفاده از یادگیری ماشین استون، محتوای صوتی و تصویری موجود در فضای مجازی را تحلیل کرده و تبلیغات گروه‌های تروریستی، از جمله داعش، را شناسایی کند.

چالش‌های حقوقی، اخلاقی و امنیتی دیپلماسی هوشمند

گسترش و توسعه دیپلماسی مبتنی بر هوش مصنوعی، مزایایی نظیر تسهیل در آنالیز داده‌ها، پیش‌بینی رفتار و نگرش رقبا را برای مسئولان دستگاه‌های دیپلماسی فراهم می‌آورد. با این حال، الگوریتم‌ها و مدل‌های موجود در این حوزه، دستگاه‌های دیپلماسی و وزرای امورخارجه را با چالش‌های محاسباتی و اجرایی متعددی مواجه می‌سازند. یکی از نمونه‌های بارز این چالش، ظهور بازیگران جدید در حوزه دیپلماسی و روابط سیاسی است(افشار، ۱۳۹۹: ۲۴).

نمی‌توان این واقعیت را نادیده گرفت که با پیدایش و فعالیت دیپلماسی هوش مصنوعی، دیپلمات‌ها و مسئولان سیاسی شاهد پردازش آنی حجم قابل‌توجهی از داده‌های فضای سایبر توسط ربات‌ها خواهند بود. این ربات‌ها با ارائه راهکارهای تخصصی، می‌توانند اشراف و تسلط دولت‌ها بر مسائل مرتبط با امنیت بین‌الملل را تحت تأثیر قرار دهند. نتیجه این امر، کاهش اقتدار حاکمیتی دولت‌ها در زمینه‌های ملی و بین‌المللی و افزایش درصد ناامنی‌ها در چارچوب داخلی است که به‌نوبه خود می‌تواند امنیت بین‌الملل را دچار اختلال و ازهم‌گسیختگی نماید (Weiss,2015 :411-430).

در چارچوب دیپلماسی هوش مصنوعی، برنامه‌های اجرایی گسترده‌ای برای کنترل و تحلیل داده‌ها ایجاد می‌شود که می‌تواند در آینده، دولت‌ها را قادر سازد تا تعامل بهتری با

شهروندان در شبکه‌های اجتماعی و سایر فضاهای دیجیتال داشته باشند. با این حال، این امر نگرانی‌های جدی درباره حریم خصوصی افراد ایجاد می‌کند. همچنین، خطر سوءاستفاده برخی دولت‌ها از اطلاعات شخصی شهروندان وجود دارد که می‌تواند به مشروعیت بخشیدن به رفتارهای استبدادی و تضعیف حاکمیت سالم منجر شود و حاکمیت دولت را از وضعیت فاضله به فاسده تغییر دهد (Brundage, 2018: 20).

نگرانی جدی در این حوزه آن است که الگوهای کامپیوتری، که وظیفه بررسی اطلاعات شخصی افراد عادی و همچنین تحلیل اطلاعات سیاسی دیپلمات‌ها را بر عهده دارند، به‌صورت کاملاً برخط عمل می‌کنند و همین ویژگی، آن‌ها را در معرض حملات مکرر سایبری قرار می‌دهد. بدین ترتیب، الگوریتم‌های مورد استفاده در حوزه‌های حاکمیت دولت‌ها و سیاست خارجی نیز می‌توانند هدف تجاوز و دستکاری قرار گیرند. این امر زمینه را فراهم می‌کند تا دولت‌ها، در جهت تغییر تصمیمات اتخاذشده، داده‌ها و فرمت تحلیلی آن‌ها را دستکاری نمایند.از سوی دیگر، با گسترش عملکرد هوش مصنوعی در حوزه دیپلماسی و امنیت میان دولت‌ها و کاهش نقش انسان در فرآیند تصمیم‌گیری، عوامل و مجریان انسانی احساس می‌کنند که اشراف و کنترل خود بر اطلاعات به‌تدریج کاهش‌یافته و در معرض تزلزل قرار می‌گیرد. چالش مهم دیگر، رشد سریع و بی‌رویه اکوسیستم‌های نوآوری هوش مصنوعی است. با توجه به اینکه تاکنون هیچ نهاد ذی‌صلاحی برای استانداردسازی و ایجاد هماهنگی نسبی در پژوهش‌ها و توسعه هوش مصنوعی شکل نگرفته است، می‌توان علت اصلی این وضعیت را در هژمونی و تسلط قدرت‌های برتر، مانند ایالات‌متحده آمریکا و جمهوری خلق چین، دانست. این کشورها در حوزه دیپلماسی هوش مصنوعی پیشرو هستند و کمتر نیازی به هماهنگی، یکپارچگی و اتحاد بین‌المللی احساس می‌کنند، حتی اگر هدف، تضمین صلح جهانی فراگیر باشد(ببری گنبد، ۱۴۰۲: ۲).

از این رو، چالش‌هایی که هوش مصنوعی برای بشر ایجاد می‌کند، بسیار گسترده است. به همین دلیل، در سال ۲۰۱۵، جمعی از کارشناسان برجسته هوش مصنوعی، از جمله استیفن هاوکینگ و ایلان ماسک، با امضای یک نامه سرگشاده، خواستار تحقیقات عمیق‌تر

در خصوص ماهیت اتوماسیون و اثرات منفی آن شدند. یکی از نگرانی‌های اصلی مطرح شده در این نامه، مسائل اخلاقی مرتبط با ربات‌ها بود. امضاکنندگان نامه، نسبت به توسعه بی‌رویه و بدون نظارت هوش مصنوعی هشدار دادند و آن را به‌عنوان خطری جدی برای نسل بشر توصیف کردند (Singh Gill, 2019:4).

حائز اهمیت است که این نگرانی‌ها، به‌ویژه در زمینه رشد و عملکرد هوش مصنوعی و همچنین عدم وجود نظام حقوقی لازم‌الاجرا و مدون برای کنترل و نظارت بر فرآیندهای طراحی و بهره‌برداری از سیستم‌های هوش مصنوعی، کمیسیون اروپایی را بر آن داشت تا در آوریل ۲۰۲۱، پیش‌نویس قانونی با عنوان "قانون اتحادیه اروپا در همسان‌سازی قوانین حاکم بر هوش مصنوعی" ارائه دهد. هدف این پیش‌نویس، ایجاد نظام حقوقی واحد و هماهنگ در خصوص تولید، عرضه، بهره‌برداری و استفاده از سیستم‌های هوش مصنوعی در قاره اروپا است .در صورت تصویب، مقررات مذکور در چارچوب نظام حقوقی ۲۷ کشور عضو اتحادیه اروپا لازم‌الاجرا خواهد بود و طبق مفاد بند نخست ماده دوم پیش‌نویس، شامل عرضه‌کنندگان و ارائه‌دهندگان سیستم‌های هوش مصنوعی مستقر در کشورهای ثالث (خارج از اتحادیه) نیز می‌شود. به بیان دیگر، با تصویب این قانون، اتحادیه اروپا قصد دارد هم از توسعه هوش مصنوعی قابل‌اعتماد و اخلاق‌مدار حمایت کند و هم از رشد بی‌رویه و خطرناک آن جلوگیری نماید و همان‌طور که شورای اروپایی اعلام کرده، در این حوزه رهبری جهانی را در اختیار گیرد (رزمخواه، ۱۴۰۳: ۲).

گرچه تمرکز و توجه بسیاری از دولت‌ها بر طراحی و تولید برنامه‌ها و ماشین‌های رباتیک برای پیشبرد امور سیاسی، حاکمیتی، اقتصادی، امنیتی و قضایی، از منظر کاربردی سودمند است، اما با پیشرفت روزافزون این پدیده در عرصه‌های هنری و فرهنگی و نفوذ شتاب‌زده آن در دستاوردهایی از قبیل موسیقی، داستان، فیلم و سایر تولیدات، می‌بایست به پیامدها و خطرات احتمالی افراط‌گرایی در این تولیدات نیز توجه داشت (احمدیان، ۱۴۰۳: ۱۰).

نباید فراموش کرد که رعایت ملاحظات اخلاقی در دنیای هوش مصنوعی نقشی بسیار مهم ایفا می‌کند. واقعیت آن است که ماشین‌های رباتیک خودکار به‌وضوح جای خود را

در تمام ابعاد زندگی اجتماعی و حتی زندگی شخصی انسان‌ها باز کرده و افراد را به خود وابسته نموده‌اند. در چنین موقعیت‌هایی، تهدیداتی وجود دارد که سیستم‌های مبتنی بر هوش مصنوعی ممکن است تصمیماتی اتخاذ کنند که تأثیرات منفی بر افراد، ارگان‌ها و جوامع داشته باشد.

طراحی و ساخت الگوریتم‌ها و انتخاب و پالایش داده‌هایی که به‌عنوان پیش‌زمینه به ماشین‌ها ارائه می‌شود، می‌تواند حجم بالایی از تعصبات مذهبی، سیاسی، نژادی و... را پنهان نماید و به نفع طراحان برنامه عمل کند و موضع آن‌ها را تقویت کند. همین امر می‌تواند منجر به تبعیض‌های حاکمیتی علیه گروه‌های خاص شود و خط‌مشی سیاسی بسیاری از دولت‌ها در حوزه تمهیدات امنیت بین‌المللی را به حاشیه براند (Kulesz, 2018:20).

با توجه به چالش‌های مطرح‌شده در دیپلماسی مبتنی بر هوش مصنوعی، روشن است که افزایش اتکا به سامانه‌های خودکار می‌تواند ضمن بهبود توان تحلیل داده و پیش‌بینی رفتار بازیگران، مخاطرات جدی برای امنیت بین‌الملل نیز به همراه داشته باشد. وابستگی بیش از حد به هوش مصنوعی و کاهش نقش قضاوت انسانی در تصمیم‌گیری‌های حساس، ممکن است موجب سوءتفاهم، تشدید تنش‌های سیاسی و افزایش بی‌اعتمادی میان دولت‌ها شود. همچنین، خطر نفوذ و دستکاری داده‌ها توسط بازیگران دولتی یا غیردولتی، احتمال وقوع بحران‌های دیپلماتیک را افزایش می‌دهد و ثبات منطقه‌ای را تحت تأثیر قرار می‌دهد. در این زمینه، ضرورت تدوین چارچوب‌های حقوقی و اخلاقی بین‌المللی برای استفاده مسئولانه از هوش مصنوعی در دیپلماسی و امنیت، بیش از پیش احساس می‌شود. چنین چارچوب‌هایی می‌توانند با تعیین استانداردهای شفاف برای طراحی الگوریتم‌ها، کنترل سوگیری‌ها و حفاظت از حریم خصوصی، امکان بهره‌گیری هم‌زمان از ظرفیت‌های پیش‌بینی و تحلیل هوش مصنوعی و حفظ نقش حیاتی انسان در نظارت و تصمیم‌گیری استراتژیک را فراهم کنند. به این ترتیب، هوش مصنوعی می‌تواند به ابزاری مکمل در تقویت امنیت بین‌المللی و مقابله با تروریسم سایبری تبدیل شود، بدون آن‌که جایگزین

عنصر انسانی در فرآیندهای حساس و چندجانبه شود و زمینه‌ساز افزایش همکاری‌های بین‌المللی در مواجهه با تهدیدات پیچیده گردد.

ضرورت بهره‌گیری دولت‌ها از دیپلماسی هوش مصنوعی در تقویت امنیت ملی

به‌رغم این‌که برای تحقق اهداف کلان، پاسخ به نیازهای امنیتی، تأمین منافع و تحکیم حاکمیت دولت‌ها در عرصه سیاست خارجی، وجود عزم ملی، یکپارچگی ارکان حاکمیتی و شناخت دقیق از نقاط ضعف و قوت داخلی و خارجی اهمیت ویژه‌ای دارد، نمی‌توان از تأثیرات فعل و انفعالات خارج از اراده بین‌المللی و همچنین برخی ناهماهنگی‌ها در روابط سیاسی دولت‌ها و تصمیمات افسارگسیخته در سلسله‌مراتب قدرت که گاه منجر به کاهش راندمان امنیتی در سطح جهانی می‌شود، به‌سادگی چشم‌پوشی کرد (حسینی، ۱۴۰۳ :۱۷).

می‌توان اذعان داشت که با توجه به مدارک و شواهد موجود، قدرت‌های برتر در عرصه دیپلماسی بین‌المللی، بسط و نفوذ هوش مصنوعی را به‌منظور تقویت دیپلماسی امنیتی و تحکیم حاکمیت ملی خود، به‌طور چشمگیر توسعه خواهند داد. پرواضح است که در چنین شرایطی، دولتی که در این زمینه اقداماتی مستحکم و هدفمند اتخاذ نکند، تمامی اهداف و منافع آن در فضای بی‌رحم سیاست بین‌الملل تحت تأثیر قرار خواهد گرفت و مشکلات عدیده‌ای ناشی از عقب‌ماندگی در بهره‌گیری از هوش مصنوعی گریبان گیر آن خواهد شد (دانائی فرد ، ۱۴۰۲: ۸).

این نکته مهم است که امروزه فناوری‌های دیجیتال، رشد انفجاری حوادث سایبری و ارتقاء میزان و ماهیت تنش‌های بین‌المللی، از جمله عوامل کلیدی‌ای هستند که قدرت حاکمیت دولت‌ها و کارایی دیپلماسی در ابعاد امنیتی را به مخاطره انداخته و در نتیجه تبعات ناخوشایندی برای خود دولت‌ها و ملت‌های تحت تکفل آن‌ها به دنبال دارد. نقش‌آفرینی بازیگران غیردولتی و گاه سوءاستفاده آن‌ها از ابزارهای وابسته به امنیت سایبری و اعمال نفوذ پیشرفته در دستگاه‌های اجرایی کشورها، تساوی و تعادل قوا در مسیر هدفمند روابط بین‌الملل و نظام مبتنی بر حاکمیت دولت‌ها را دستخوش تغییر می‌کند. در

شرایطی که گروهی از افراد با بهره‌گیری از الگوریتم‌ها و هوش مصنوعی توانمند شوند و قابلیت‌هایی کسب کنند که کارایی و نفوذ دولت‌ها را کاهش داده یا آن‌ها را به انزوا بکشانند، دولت‌ها استقلال، ثبات مرزی و امنیت ملی و بین‌المللی خود را از دست خواهند داد (Timmers,2019 :11).

پدیده هوش مصنوعی، کانون اصلی موفق‌ترین شرکت‌های تاریخ بشریت، از جمله مایکروسافت، اپل و آمازون است که در بسیاری از زمینه‌ها، حتی در صنایع خودرو و سایر حوزه‌ها نفوذ کرده و در جذب توجه کاربران و مصرف‌کنندگان بسیار موفق بوده و در بازار سرمایه جایگاه برجسته‌ای برای خود ایجاد کرده‌اند. با توجه به این مباحث، هوش مصنوعی در کنار فناوری اطلاعات و ارتباطات، نقش محوری در تسهیل دسترسی جهانیان به دانش، اعتبار، اطلاعات و سایر مزایا و منافع جامعه جهانی در عصر معاصر ایفا می‌کند (احمدی، ۱۴۰۱ :۵).

قابل انکار نیست که این پدیده بر فرایند جامعه‌پذیری سیاسی، اعتقادات و نگرش‌های سیاسی، مذهبی و فرهنگی و به‌طورکلی بر هویت افراد جامعه تأثیرگذار است و با ایجاد تغییرات اساسی و بنیادین در عملکرد سیاسی افراد و دولت‌ها، یکپارچگی، هماهنگی و وحدت ملی را نیز تحت تأثیر قرار می‌دهد (Adam Thierer, 2017:10).

در عصر حاضر، از کشورهای کمتر توسعه‌یافته گرفته تا دولت‌های سازمان‌یافته و به تعبیری قدرت‌های جهانی، از جمله ایالات‌متحده آمریکا، جمهوری فدرال روسیه و جمهوری خلق چین، هوش مصنوعی را فراتر از امور غیر حاکمیتی، در زمینه‌های سیاسی نیز به کار گرفته‌اند. به گونه‌ای که چندی پیش دولت امارات متحده عربی، در راستای تحقق سیاست‌های تحول گرایانه خود در حوزه‌های مختلف امنیتی، نخستین وزیر هوش مصنوعی خود را منصوب و حکم صدارت آن را صادر نمود (Ryan Calo, 2017:4).

علاوه بر این، گاه و بیگاه اخبار و گزارش‌هایی منتشر می‌شود که بیانگر رشد سریع این حوزه است. به‌عنوان نمونه، طبق یکی از گزارش‌های اخیر موسسه پژوهشی "گروه داده‌های بین‌المللی"، حجم سرمایه‌گذاری در حوزه هوش مصنوعی در مناطق مختلف

خاورمیانه و آفریقا تا سال ۲۰۲۲ به میزان ۵۳۰ میلیون دلار خواهد رسید، که نشان‌دهنده انفجاری عظیم در حوزه هوش مصنوعی است (ملایی، ۱۴۰۲، :۱۵).

به همین دلیل، رغبت و تقاضای بسیار بالای هوش مصنوعی در سطح جهانی، در صورتی که یک دولت نتواند خود را با این جریان همراه سازد، می‌تواند عواقب و تبعات غیرقابل جبرانی برای آن دولت و زمامداران آن در پی داشته باشد (Zuiderveen .(Borgesius,2018:20

با توجه به اهمیت بهره‌گیری از هوش مصنوعی در تقویت دیپلماسی امنیتی، روشن است که این فناوری می‌تواند نه تنها قدرت حاکمیت ملی دولت‌ها را ارتقا دهد، بلکه نقش کلیدی در تحکیم امنیت و ثبات بین‌المللی نیز ایفا کند. توانمندی‌های هوش مصنوعی در تحلیل سریع و دقیق داده‌های امنیتی، پیش‌بینی تهدیدات منطقه‌ای و بین‌المللی و مدیریت بحران‌های پیچیده، امکان اتخاذ تصمیمات به‌موقع و هماهنگ در سطح جهانی را فراهم می‌آورد. این امر به کاهش تنش‌ها میان دولت‌ها، پیشگیری از تصاعد منازعات سایبری و ایجاد مکانیسم‌های مؤثر برای حل و فصل اختلافات کمک می‌کند. با این حال، در صورتی که استفاده از هوش مصنوعی به‌طور غیرمسئولانه یا با تمرکز بیش از حد بر اهداف داخلی و رقابت‌های قدرت‌های بزرگ صورت گیرد، احتمال بروز سوءتفاهم‌ها، رقابت‌های تسلیحاتی سایبری و افزایش بی‌اعتمادی بین دولت‌ها افزایش یافته و امنیت بین‌الملل تهدید می‌شود. بنابراین، بهره‌گیری هدفمند و اخلاق‌مدار از دیپلماسی هوش مصنوعی، همراه با چارچوب‌های حقوقی و استانداردهای بین‌المللی، می‌تواند تعادل میان توسعه ظرفیت‌های امنیت ملی و تقویت امنیت جهانی را حفظ نماید و دولت‌ها را قادر سازد تا با همکاری و هماهنگی، تهدیدات پیچیده عصر دیجیتال را مدیریت کنند.

نتیجه‌گیری

هوش مصنوعی به‌عنوان یکی از مؤلفه‌های اصلی تحول دیجیتال، نه صرفاً یک ابزار فناورانه، بلکه یک عامل ساختاری در بازتعریف الگوهای تعامل دیپلماتیک و امنیت بین‌المللی محسوب می‌شود. بر اساس یافته‌های مقاله، دیپلماسی هوشمند را باید چارچوبی

دانست که در آن تصمیم‌سازی سیاست خارجی و مدیریت تعاملات میان دولتی، بیش از گذشته بر داده محوری، تحلیل الگوریتمی و ظرفیت‌های پیش‌بینی‌گرانه استوار می‌گردد. این تحول سبب شده است که دیپلماسی از شکل سنتی مبتنی بر تجربه، شهود و گفت‌وگوهای محدود به‌سوی الگویی حرکت کند که در آن پردازش کلان‌داده‌ها و تحلیل لحظه‌ای محیط امنیتی و سیاسی، در کانون فرآیند تصمیم‌گیری قرار می‌گیرد.

یافته نخست مقاله آن است که هوش مصنوعی در چارچوب دیپلماسی هوشمند می‌تواند ظرفیت دولت‌ها را در تحلیل و مدیریت مذاکرات دیپلماتیک ارتقا دهد؛ زیرا ابزارهای مبتنی بر یادگیری ماشین و تحلیل داده، امکان شناسایی ترجیحات بازیگران، پیش‌بینی رفتارهای آینده، ارزیابی سناریوهای محتمل و کاهش عدم قطعیت در مذاکرات را فراهم می‌سازد. بدین ترتیب، مذاکرات دیپلماتیک در عصر هوش مصنوعی از یک کنش صرفاً مبتنی بر مهارت انسانی به‌سوی فرآیندی ترکیبی حرکت می‌کند که در آن فناوری نقش پشتیبان و تقویت‌کننده قدرت تصمیم‌سازی دارد. با این حال، این ارتقا صرفاً زمانی به نتایج مثبت منجر خواهد شد که تصمیمات راهبردی همچنان تحت کنترل انسانی باقی بماند و سازوکارهای پاسخ‌گویی و شفافیت الگوریتمی تضمین شود.

یافته دوم بیانگر آن است که تهدید تروریسم سایبری، به دلیل ماهیت شبکه‌ای، فراملی و مبتنی بر فناوری، مستقیماً امنیت بین‌المللی را تحت تأثیر قرار داده و ابزارهای سنتی دیپلماسی و امنیت را با محدودیت مواجه کرده است. در چنین شرایطی، هوش مصنوعی قادر است از طریق شناسایی الگوهای رفتاری در فضای دیجیتال، کشف فعالیت‌های غیرعادی، تحلیل پیام‌ها و محتواهای تبلیغاتی، رصد شبکه‌های جذب نیرو و پیش‌بینی نقاط آسیب‌پذیر، نقش مؤثری در مهار و کاهش تهدیدات تروریستی ایفا کند. بنابراین، کاربرد هوش مصنوعی در مقابله با تروریسم سایبری صرفاً در سطح دفاع فنی نیست، بلکه ابزاری برای تقویت حکمرانی امنیتی دولت‌ها و ارتقای ظرفیت‌های پیشگیری در سطح بین‌المللی محسوب می‌شود.

یافته سوم مقاله، آن است که «مذاکرات دیپلماتیک» و «تروریسم سایبری» در ظاهر دو حوزه مستقل به نظر می‌رسند، اما در چارچوب امنیت بین‌المللی دارای رابطه‌ای ساختاری

و مکمل‌اند. به بیان دقیق‌تر، مقابله با تروریسم سایبری در عمل نیازمند هماهنگی میان دولت‌ها، تبادل اطلاعات، ایجاد رژیم‌های همکاری امنیتی، تدوین هنجارهای بین‌المللی و تنظیم قواعد رفتاری در فضای سایبری است؛ اموری که بدون مذاکرات و توافقات دیپلماتیک تحقق نمی‌یابد. از این منظر، دیپلماسی هوشمند می‌تواند نقش واسط میان «تهدید امنیتی» و «راهکار سیاسی–حقوقی مقابله» را ایفا کند و زمینه را برای شکل‌گیری ترتیبات همکاری بین‌المللی در حوزه امنیت سایبری فراهم آورد. در نتیجه، پیوند میان این دو مفهوم، نه تصنعی و نامنسجم، بلکه برخاسته از ماهیت فراملی تهدیدات سایبری و ضرورت مدیریت چندجانبه آن است.

به این ترتیب دیپلماسی مبتنی بر هوش مصنوعی ماهیتی دوگانه دارد؛ بدین معنا که در کنار ظرفیت‌های مثبت برای ارتقای امنیت بین‌المللی، می‌تواند خود منشأ تهدیدات جدید نیز باشد. جانب‌داری الگوریتمی، فقدان شفافیت در تصمیم‌سازی ماشینی، امکان دست‌کاری داده‌ها، آسیب‌پذیری در برابر حملات سایبری و تمرکز قدرت فناورانه در دست دولت‌ها یا شرکت‌های محدود، از جمله عواملی است که ممکن است دیپلماسی هوشمند را به ابزاری برای تشدید بی‌اعتمادی و افزایش رقابت‌های ژئوپلیتیکی تبدیل کند. به‌ویژه در شرایطی که نظام بین‌المللی هنوز فاقد رژیم حقوقی الزام‌آور و سازوکارهای نظارتی مؤثر برای حکمرانی هوش مصنوعی در سیاست خارجی و امنیت سایبری است، احتمال تبدیل این فناوری به عامل بی‌ثباتی بین‌المللی افزایش می‌یابد.

پژوهش حاضر نشان داد که هوش مصنوعی در عصر تحول دیجیتال می‌تواند به‌عنوان عنصر کلیدی دیپلماسی هوشمند، در دو سطح مکمل عمل کند: نخست، ارتقای کارآمدی تصمیم‌سازی و مذاکرات دیپلماتیک از طریق تحلیل داده و پیش‌بینی رفتار بازیگران؛ و دوم، تقویت ظرفیت دولت‌ها برای پیشگیری و مقابله با تهدید تروریسم سایبری از طریق ابزارهای رصد، شناسایی و کنترل اطلاعات. با این حال، تحقق این ظرفیت‌ها مستلزم آن است که دولت‌ها به سمت طراحی چارچوب‌های حقوقی و نهادی روشن حرکت کنند، کنترل انسانی بر تصمیمات راهبردی را حفظ نمایند و همکاری‌های چندجانبه برای استانداردسازی امنیت سایبری و حکمرانی داده را توسعه دهند.

بر این اساس، می‌توان نتیجه گرفت که دیپلماسی هوشمند در عصر هوش مصنوعی نه یک گزینه فرعی، بلکه ضرورتی راهبردی برای حفظ و ارتقای امنیت بین‌المللی است؛ اما این ضرورت تنها زمانی به فرصت تبدیل می‌شود که هوش مصنوعی در چارچوب حکمرانی مسئولانه، شفافیت تصمیم‌سازی، پاسخ‌گویی حقوقی و همکاری بین‌المللی به کار گرفته شود. در غیر این صورت، همین فناوری می‌تواند به عاملی برای تعمیق شکاف‌های قدرت، افزایش رقابت‌های سایبری و تشدید ناامنی جهانی تبدیل گردد.

با توجه به تحلیل حاضر، اقدامات زیر برای بهره‌گیری مؤثر و امن ضروری است:

❖ ایجاد چارچوب‌های قانونی و نظارتی برای تولید و مدیریت هوش مصنوعی، مشابه پیش‌نویس قانون هماهنگی هوش مصنوعی اتحادیه اروپا، جهت پیشگیری از سوءاستفاده‌ها.

❖ توازن میان انسان و هوش مصنوعی؛ حفظ نظارت انسانی بر تصمیمات استراتژیک و استفاده از هوش مصنوعی به‌عنوان ابزار کمکی.

❖ سیاست‌های اخلاق محور و شفاف برای احترام به حقوق شهروندان و جامعه بین‌الملل.

❖ تقویت همکاری‌های بین‌المللی و استانداردسازی برای پیشگیری از هژمونی های فناوری و تهدید امنیت جهانی.

❖ نظارت مستمر و به‌روزرسانی الگوریتم‌ها برای پاسخگویی به تهدیدات نوظهور و تغییرات محیط دیجیتال.

❖ آموزش و توانمندسازی نیروی انسانی دیپلماتیک و امنیتی برای تحلیل نتایج هوشمندانه و اتخاذ تصمیمات راهبردی.

❖ پیشنهادهای پژوهشی آینده:

❖ بررسی مقایسه‌ای تأثیر دیپلماسی هوش مصنوعی بر امنیت ملی و منطقه‌ای در دولت‌های توسعه‌یافته و درحال‌توسعه.

❖ تحلیل اخلاقی و حقوقی استفاده از هوش مصنوعی در تصمیم‌گیری‌های امنیتی، با تمرکز بر حقوق بشر بین‌الملل.

❖ مطالعه نقش الگوریتم‌ها در کاهش یا افزایش تنش‌های بین‌المللی و اثرات آن بر صلح جهانی.

❖ تحقیق در زمینه مدیریت تعامل میان هوش مصنوعی و بازیگران غیر حکومتی در حوزه امنیت سایبری.

❖ توسعه مدل‌های پیش‌بینی تهدیدات سایبری و ایجاد نظام هشدار سریع بین‌المللی با همکاری چندجانبه.

در جمع‌بندی، دیپلماسی مبتنی بر هوش مصنوعی ابزار حیاتی برای افزایش امنیت، مقابله با تروریسم سایبری و تقویت اقتدار ملی است؛ اما بدون چارچوب‌های مدیریتی، نظارتی و اخلاق محور، می‌تواند به تهدیدی برای دولت‌ها و نظم بین‌المللی تبدیل شود. شناخت فرصت‌ها و تهدیدهای این فناوری و سیاست‌گذاری راهبردی، مسیر آینده صلح و امنیت بین‌المللی را شکل خواهد داد.

منابع

احمدیان، مهدی، حیدری، محدثه،طاووسی، مجتبی(۱۴۰۳)، سناریوهای آینده تأثیر هوش مصنوعی بر حکمرانی ملی و بین‌المللی در افق ۱۰ ساله. *سیاست‌نامه علم‌وفناوری*، دوره ۱۴، شماره ۳، شماره پیاپی ۴۸.

احمدی، علی، زرگر، افشین، آدمی، علی(۱۴۰۱)، نقش فناوری‌های نوظهور در امنیت و قدرت ملی کشورها؛ فرصت‌ها و تهدیدها. *مطالعات بین‌المللی*، دوره ۱۸، شماره ۴، پیاپی ۷۲.

افشار، محمدمهدی، برزگر، کیهان،کیانی، داود(۱۳۹۹)، شناسایی سناریوهای مؤثر بر آینده دیپلماسی عمومی تحت تأثیر فرا روندهای فضای سایبر با رویکرد تحلیل ساختاری. *تحقیقات سیاسی بین‌المللی*، شماره ۴۴.

اسلامی، روح‌الله (۱۳۹۳)، تکنولوژی اطلاعات و سیاست به‌مثابه متون متحول برای سیاست‌گذاری. *سیاست‌های راهبردی و کلان*، سال دوم، شماره ۶.

ببری‌گنبد، سکینه(۱۴۰۲)، تبیین حکمرانی چین در عرصه هوش مصنوعی؛ چشم‌انداز و راهبردها در غرب آسیا. *سیاست خارجی*، سال اول، شماره ۳.

حاج زرگرباشی، سید روح‌الله، موحدیان، احسان(۱۳۹۷)، سایبر دیپلماسی دولت آمریکا؛ تأثیر صفحه فیس‌بوک وزارت امورخارجه آمریکا بر نگرش کاربران ایرانی نسبت به جامعه ایران. *مطالعات رسانه‌های نوین*، سال چهارم، شماره ۱۵.

حسنی، حسین(۱۴۰۳)، سیاست‌گذاری هوش مصنوعی در اتحادیه اروپا؛ اصول بنیادین، سازوکار حکمرانی و اصول اخلاقی. *سیاست‌گذاری عمومی*، دوره ۱۰، شماره ۲

حسینی، سید امیرعلی، هاشمی زاده، سید علیرضا(۱۴۰۳)، هوش مصنوعی و صلح و امنیت بین‌المللی. *پژوهش‌های بین‌الملل*، دوره ۱۳، شماره ۲، پیاپی ۴۹.

حسینی، سید حامد(۱۴۰۳)، تأثیر فناوری هوش مصنوعی بر عرصه سیاست بین‌الملل. *سیاست خارجی*، دوره ۲، شماره ۳۸.

خرازی آذر، رها (۱۳۹۲)، سایبر دیپلماسی در محیط هوشمند نوین رسانه‌ای، *رسانه*، سال بیست و چهارم، شماره

دانایی‌فرد، حسن(۱۴۰۲)، هوش مصنوعی و کشورداری؛ واکاوی ساحت‌های تاریک. *مطالعات مدیریت دولتی ایران*، دوره ۶، شماره ۱.

رزمخواه، نجمه(۱۴۰۳)، نقدی بر پیش‌نویس قانون اتحادیه اروپا در همسان‌سازی قوانین حاکم بر هوش مصنوعی از منظر مقابله با تروریسم سایبری. *مطالعات حقوق عمومی*، دوره ۵۴، شماره ۳.

کرمی، علی؛ متقی‌دستنائی، افشین(۱۴۰۳)، آسیب‌شناسی تأثیر هوش مصنوعی بر دیپلماسی عمومی. *پژوهشنامه روابط جهانی*، دوره ۱، شماره ۳.

کرمپور، محمد، اسلامی، روح‌الله(۱۴۰۳)، حاکمیت هوش مصنوعی از دیدگاه پدیدارشناسی سیاسی. *پژوهش‌های فلسفی*، سال دوم، ۱۴۰۳..

کیریلینکا، اینا، کاروچکین، سرگئی(۱۴۰۳)، تأثیر گسترش هوش مصنوعی بر دیپلماسی نوین کشورهای جهان. *مطالعات کشورها*، سال سوم.

کوهکن، محمدمهدی (۱۴۰۳)، بررسی جایگاه مصلحت در روابط دیپلماتیک از منظر فقهی، *تعاملات دیپلماتیک*، سال دوم، شماره ۸، زمستان ۱۴۰۳، ۱۵۴-۱۱۵

کوهکن، علیرضا (۱۴۰۳)، دیپلماسی علمی در سیاست خارجی هند، *تعاملات دیپلماتیک*، سال دوم، شماره ۸، زمستان ۱۴۰۳، ۳۴-۱

ملایی، اعظم (۱۴۰۲)، سیاست خارجی الگوریتمی؛ نقش هوش مصنوعی در روند تصمیم‌گیری. *سیاست خارجی*، دوره ۳۷، شماره ۴.

میرکوشش، امیر هوشنگ، حسینی، محمدمهدی، شریف‌زاده، زهرا(۱۴۰۳)، بررسی آثار سیاست‌های توسعه فناوری‌های نوین و هوش مصنوعی در گسترش راهبردهای سیاسی کلان با رویکرد سیاست‌های کلی نظام. *سیاست‌های راهبردی و کلان*، دوره ۱۲، شماره ۴۵.

هدایتی شهیدانی، مهدی، مهدی‌زاده، هادی (۱۴۰۴)، چالش‌ها و فرصت‌های امنیت سایبری در روابط دیپلماتیک و تجاری ایران و ارمنستان، *تعاملات دیپلماتیک*، سال سوم، شماره ۹، بهار ۱۴۰۴، ۱-۳۲

References

Anastassia Lauterbach. (2017). Artificial Intelligence and Policy: Quo Vadis? Digital Policy, *Regulation and Governance*, 21(3), 13.

Beebeejaun, A.; Dulloo, L. (2021). Taxation of Bitcoin Transactions in Mauritius: A Comparative Study with the U.S. and Italy. *International Journal of Law*, Humanities and Social Science, 4.

Bjola, C. (2019). *Diplomacy in the Age of Artificial Intelligence*. Madrid: Real Instituto Elcano.

Bjola, C.; Manor, I. (2025). Digital Diplomacy in the Age of Technological Acceleration. *Place Branding and Public Diplomacy*, 21(3), 303-308.

Bjola, C.; Manor, I. (2023). A*I and Digital Diplomacy: Managing Disruptive Technologies in International Relations*. Oxford: Oxford University Press, pp. 21-38.

Brundage, S.; Avin, S.; et al. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute*, University of Oxford.

Boutros-Ghali, Boutros, (1992), *An Agenda for Peace: Preventive Diplomacy, Peacemaking and Peace-keeping*. New York: United Nations

Bjola, Corneliu & Manor, Ilan. (2023), *AI and Digital Diplomacy: Managing Disruptive Technologies in International Relations*. Oxford: Oxford University Press.

Calo, R. (2017). Artificial Intelligence Policy: A Primer and Roadmap. *International Policy*, 51, 4.

Cave, S.; ÓhÉigeartaigh, S. (2022). *AI Governance: A Research Agenda. Centre for the Study of Existential Risk*, University of Cambridge, 45-63.

Clinton, H. R. (2010, January 21). *Remarks on Internet Freedom. U.S. Department of State*. Retrieved from https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Filgueiras, F. (2022). Artificial Intelligence Policy Regimes: Comparing Politics and Policy to National Strategies for Artificial Intelligence. *Global Perspectives*, 4, 7.

Guterres, A. (2023, July 18). *Remarks to the Security Council – Artificial Intelligence.* United Nations. Retrieved from https://www.un.org/sg/en/content/sg/speeches/2023-07-18/secretary-generals-remarks-the-security-council-artificial-intelligence

Galtung, Johan, (1996), *Peace by Peaceful Means: Peace and Conflict, Development and Civilization*. Oslo: International Peace Research Institute (PRIO) and Sage Publications,

Karabiyik, U. (2016). A Survey of Social Network Forensics. *Journal of Digital Forensics*, Security and Law, 5, 5.

Kulesz, O. (2018). Culture-Platforms and Machines: The Impact of Artificial Intelligence on the Diversity of Cultural Expressions. *International Federation of Coalitions for Cultural Diversity*, 20.

Magdin, R. (2019). *The Great Game through an AI Lens*. [Publisher not specified].

Mintz, A.; DeRouen, K. (2010). *Understanding Foreign Policy Decision Making*. Cambridge: Cambridge University Press.

Renda, A. (2019). *Artificial Intelligence: Ethics, Governance and Policy Challenges*. Brussels: Centre for European Policy Studies (CEPS).

Roff, H. (2023). *AI Governance and Human Rights*. London: Chatham House Research Paper.

Scott, B.; Heumann, S.; Lorenz, P. (2018). *Artificial Intelligence and Foreign Policy*. Stiftung Neue Verantwortung Policy Brief, Intersection of Technology and Society, 19.

Singh Gill, A. (2019). Artificial Intelligence and International Security: The Long View. *Ethics & International Affairs*, 33, 169-179.

Smith, W. (2021). UK Intelligence Agency GCHQ Sets out AI Strategy and Ethics. *AI Strategy*, 1, 3.

Spike Back, N. [= Cardon, D.; Cointet, J.-P.; Mazières, A.] (2018). Neurons Spike Back: The Invention of Inductive Machines and the Artificial Intelligence Controversy. *Réseaux,* 211, 173-220.

Thierer, A.; Castillo O'Sullivan, A.; Russell, R. (2017). *Artificial Intelligence and Public Policy*. Mercatus Center, George Mason University, 10.

Timmers, P. (2019). *Ethics of AI and Cyber Security When Sovereignty Is at Stake*. Minds and Machines, 29, 635-645.

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO Publishing, 3-7.

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2021). *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO Publishing

Unever, A. (2020). *Computational Diplomacy: Foreign Policy Communication in the Age of Algorithms and Automation*. The Centre for Economics and Foreign Policy Studies (EDAM), 9.

Valle-Cruz, D.; Ruvalcaba-Gomez, E. A.; Sandoval-Almazan, R.; Criado, J. I. (2019). *A Review of Artificial Intelligence in Government and Its Potential from a Public Policy Perspective*. Proceedings of the 20th Annual International Conference on Digital Government Research, 8, 5.

Weiss, C. (2015). How Do Science and Technology Affect International Affairs? *Minerva*, 53(4), 411-430.

Zuiderveen Borgesius, F. (2018). *Discrimination, Artificial Intelligence and Algorithmic Decision Making. Council of Europe, Directorate-General of Democracy*, Institute for Information Law (IViR).

Translated References into English

Ahmadi, A., Zargar, A., & Adami, A. (2022). The role of emerging technologies in the security and national power of countries: Opportunities and threats. International Studies Quarterly, 18(4), Serial No. 72. [In Persian]

Ahmadian, M., Heydari, M., & Tavousi, M. (2024). Future scenarios of the impact of artificial intelligence on national and international governance

in a 10-year horizon. Science and Technology Policy Journal, 14(3), Serial No. 48. [In Persian]

Anastassia Lauterbach. (2017). Artificial intelligence and policy: Quo vadis? Digital Policy, Regulation and Governance, 21(3), 13.

Afshar, M. M., Barzegar, K., & Kiani, D. (2020). Identifying effective scenarios for the future of public diplomacy under the influence of cyberspace megatrends using a structural analysis approach. International Political Research Quarterly, No. 44. [In Persian]

Beebeejaun, A., & Dulloo, L. (2021). Taxation of Bitcoin transactions in Mauritius: A comparative study with the U.S. and Italy. International Journal of Law, Humanities and Social Science, 4.

Bebri-Gonbad, S. (2023). Explaining China's governance in the field of artificial intelligence: Outlook and strategies in West Asia. Foreign Policy Quarterly, 1(3). [In Persian]

Bjola, C. (2019). Diplomacy in the Age of Artificial Intelligence. Madrid: Real Instituto Elcano.

Bjola, C., & Manor, I. (2023). AI and Digital Diplomacy: Managing Disruptive Technologies in International Relations (pp. 21–38). Oxford: Oxford University Press.

Bjola, C., & Manor, I. (2025). Digital diplomacy in the age of technological acceleration. Place Branding and Public Diplomacy, 21(3), 303–308.

Boutros-Ghali, B. (1992). An Agenda for Peace: Preventive Diplomacy, Peacemaking and Peace-keeping. New York: United Nations.

Brundage, S., Avin, S., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Oxford: Future of Humanity Institute, University of Oxford.

Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. International Policy, 51(4).

Cardon, D., Cointet, J.-P., & Mazières, A. (2018). Neurons spike back: The invention of inductive machines and the artificial intelligence controversy. Réseaux, 211, 173–220.

Cave, S., & ÓhÉigeartaigh, S. (2022). AI Governance: A Research Agenda (pp. 45–63). Cambridge: Centre for the Study of Existential Risk, University of Cambridge.

Clinton, H. R. (2010, January 21). Remarks on internet freedom. U.S. Department of State. Retrieved from https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Danaei-Fard, H. (2023). Artificial intelligence and governance: Exploring the dark dimensions. Iranian Journal of Public Administration Studies, 6(1). [In Persian]

Filgueiras, F. (2022). Artificial intelligence policy regimes: Comparing politics and policy to national strategies for artificial intelligence. Global Perspectives, 4, 7.

Galtung, J. (1996). Peace by Peaceful Means: Peace and Conflict, Development and Civilization. Oslo: International Peace Research Institute (PRIO) & Sage Publications.

Guterres, A. (2023, July 18). Remarks to the Security Council – Artificial intelligence. United Nations. Retrieved from https://www.un.org/sg/en/content/sg/speeches/2023-07-18/secretary-generals-remarks-the-security-council-artificial-intelligence

Haj Zargarbashi, S. R., & Movahhedian, E. (2018). Cyber diplomacy of the U.S. government: The impact of the U.S. Department of State Facebook page on Iranian users' attitudes toward Iranian society. Journal of New Media Studies, 4(15). [In Persian]

Hedayati Shahidani, M., & Mahdi-Zadeh, H. (2025). Challenges and opportunities of cyber security in Iran–Armenia diplomatic and trade relations. Diplomatic Interactions Quarterly, 3(9), 1–32. [In Persian]

Hassani, H. (2024). Artificial intelligence policymaking in the European Union: Fundamental principles, governance mechanism, and ethical foundations. Public Policy Quarterly, 10(2). [In Persian]

Hosseini, S. A., & Hashemi-Zadeh, S. A. (2024). Artificial intelligence and international peace and security. International Studies Research Quarterly, 13(2), Serial No. 49. [In Persian]

Hosseini, S. H. (2024). The impact of artificial intelligence technology on the field of international politics. Foreign Policy Quarterly, 2(38). [In Persian]

Islami, R. (2014). Information technology and politics as transforming texts for policymaking. Strategic and Macro Policies Quarterly, 2(6). [In Persian]

Karabiyik, U. (2016). A survey of social network forensics. Journal of Digital Forensics, Security and Law, 5(5).

Karami, A., & Motaghi-Dastenaei, A. (2024). Pathology of the impact of artificial intelligence on public diplomacy. Global Relations Research Journal, 1(3). [In Persian]

Kermpour, M., & Islami, R. (2024). Artificial intelligence sovereignty from the perspective of political phenomenology. Philosophical Research Journal, 2. [In Persian]

Khorazi Azar, R. (2013). Cyber diplomacy in the modern intelligent media environment. Media Quarterly, 24. [In Persian]

Kirilenka, I., & Karochkin, S. (2024). The impact of the expansion of artificial intelligence on modern diplomacy in world countries. Countries Studies Quarterly, 3. [In Persian]

Kohkan, A. (2024). Scientific diplomacy in India's foreign policy. Diplomatic Interactions Quarterly, 2(8), 1–34. [In Persian]

استناد به این مقاله: حسینی، سیده لطیفه، عرب طاط، محمد و حسینمردی، محمد مهدی. (۱۴۰۴). دیپلماسی هوشمند و امنیت بین-المللی در عصر تحول دیجیتال: تحلیل نقش هوش مصنوعی در مقابله با تروریسم سایبری. *تعاملات دیپلماتیک*، ۲ (۷)، e242744، ۳۰۱ - ۲۲۸.

doi: 10.22034/dpiq.2026.555275.10