INTERNATIONAL RELATIONS RESEARCHES
Homepage: https://iisajournals.ir/
Iranian International Studies Association

New reading of international peace and security in the light of the fight against cyber terrorism

Mohsen Khakzad Shahandashti *Corresponding Author*, Assistant Professor, Department of Law, Faculty of Literature and Humanities, University of Guilan, Rasht, Iran E-mail: mohsen.khakzad777@gmail.com
Leila Mirbod Instructor, Department of Law, Rasht Branch, Islamic Azad University, Rasht, Iran. E-mail: Leila_mirbod@yahoo.com

Article Info

Article Type:
Reserch Article

Keywords:
Cyber Security, International Peace, Human Security, Cyber Terrorism, Artificial Intelligence

ABSTRACT

Peace and security in the national and international dimensions had different meanings for states and the world community in successive periods, and due to this reason there are different approaches to them. With the arrival of new areas such as cyberspace and today artificial intelligence, these classic definitions have undergone changes. Terrorism is known as disrupting international order, peace and security. Considering the characteristics of the cyber space, cyber terrorism raises the need to recreate concepts such as digital security, regularizing the use of artificial intelligence technology. This research was written using library documents and sources on descriptive-analytical method.Cyber threat is one of the most serious threats against national interests and international security. Due to the serious destruction of vital infrastructure, some countries have declared that they consider it as a military attack and will respond to it militarily. Cyber space and artificial intelligence have questioned all common and traditional understandings of the concept of national security. Therefore, these concepts need to be redefined in the light of international custom resulting from the decisions of organizations such as the United Nations and NATO.The technological opportunities created by cyberspace and artificial intelligence shape the future, but do not determine it. In order to manage the challenges ahead, states should put a national strategy on how to use the benefits of cyberspace and artificial intelligence while reducing its harmful effects by adopting measures based on international cooperation.

Cite this Article: Khakzad Shahandashti, M. , & Mirbod, L. (2024). New reading of international peace and security in the light of the fight against cyber terrorism. International Relations Researches, 14(3), 179-204. doi: 10.22034/irr.2024.463239.2557

Publisher: Iranian Association of International Studies
DOI: 10.22034/irr.2024.463239.2557

پژوهش های روابط بین الملل
Homepage: https://iisajournals.ir/

خوانش نوین صلح و امنیت بین المللی در پرتو مبارزه با تروریسم سایبری

محسن خاکزاد شاهاندشتی *نویسنده مسئول*، استادیار گروه حقوق، دانشکده ادبیات و علوم انسانی، دانشگاه گیلان، رشت، ایران. رایانامه: mohsen.khakzad777@gmail.com

لیلا میربد مدرس گروه حقوق، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران.
رایانامه: Leila_mirbod@yahoo.com

درباره مقاله

نوع مقاله:
مقاله پژوهشی

کلیدواژه‌ها:
امنیت سایبری،
صلح بین المللی،
امنیت انسانی،
تروریسم سایبری،
هوش مصنوعی

تاریخچه مقاله
تاریخ دریافت: ۱۴۰۳/۶/۸
تاریخ پذیرش: ۱۴۰۳/۹/۲۵

چکیده

صلح و امنیت در بعد ملی و بین المللی در دوره های متوالی، تعابیر گوناگونی برای دولت ها و جامعه جهانی داشته است و به همین دلیل رویکردهای متفاوتی نیز در مورد آن وجود دارد. با ورود حوزه های نوینی چون تروریسم سایبری و نیز هوش مصنوعی، این تعاریف کلاسیک، دستخوش تغییر شده اند. تروریسم در دکترین حقوق بین الملل و حقوق بین الملل عرفی به مثابه برهم زننده نظم، صلح و امنیت بین المللی شناخته می شود. با توجه به ویژگی های فضای سایبر، تروریسم سایبری نیاز به بازآفرینی مفاهیمی چون امنیت دیجیتال، قاعده مند سازی استفاده از تکنولوژی هوش مصنوعی و از همه مهم تر امنیت انسانی را مطرح می کند. این پژوهش با استفاده از اسناد و منابع کتابخانه‌ای و به روش توصیفی ـــ تحلیلی نگارش یافته است و در پی آن است تا خوانش نوینی را از مفهوم صلح و امنیت بین المللی با توجه به اهمیت تهدید سایبری و اقدامات مخل امنیت، ارتکاب یافته با هوش مصنوعی ارائه دهد. فضای سایبر و هوش مصنوعی تمام برداشت‌های رایج و سنتی از مفهوم امنیت بین المللی و ملی را زیر سؤال برده است. فرصت های تکنولوژیکی که فضای سایبر و هوش مصنوعی ایجاد می کند آینده را شکل می دهد، اما آن را تعیین نمی کند. به منظور مدیریت چالش های پیش رو، دولت ها باید یک استراتژی ملی برای نحوه استفاده از مزایای فضای سایبر و هوش مصنوعی و در عین حال کاهش اثرات مخرب آن با اتخاذ تدابیر مبتنی بر همکاری بین المللی در دستور کارخود قرار دهند.

استناد به این مقاله: خاکزاد شاهاندشتی, محسن , & میربد, لیلا . (۱۴۰۳). خوانش نوین صلح و امنیت بین المللی در پرتو مبارزه با تروریسم سایبری. پژوهش های روابط بین الملل, ۱۴(۳), ۱۷۹-۲۰۴. doi: 10.22034/irr.2024.463239.2557

ناشر: **انجمن ایرانی روابط بین الملل**

مقدمه

برقراری صلح و امنیت امروزه غایت تلاش‌های بین المللی دولت‌ها و ملت‌هاست. از نگاه نظام وستفالیایی، صلح و امنیت به معنای رعایت اصول حق حاکمیت، برابری حقوق، رعایت مصونیت کشورها و نمایندگان آنان، احترام به تمامیت ارضی کشورها، عدم مداخله در امور داخلی آنان و حل و فصل مسالمت آمیز اختلافات تلقی می‌شده است. از این زاویه، حاکمیت و استقلال دولت‌ها مهم‌ترین رکن امنیت بین المللی بود. در این مفهوم اگر تهدیدی وجود داشت، عمدتاً تهدید نظامی و غالباً از طرف دولت‌های دیگر بود و مسئول اولیه تأمین امنیت نیز خود دولت‌ها یا متحدان آن‌ها تلقی می‌شدند. منظور از صلح و امنیت در روابط بین الملل، آرامش و ثبات در جامعه جهانی است. امنیت نیز عمدتاً به نوعی احساس روانی اطلاق می‌شود که در آن به علت فقدان ترس، وضعیت آرامش و اطمینان خاطر حاصل می‌شود. حوزه وابسته به صلح، امنیت است. امنیت مفهومی تجزیه ناپذیر و جهانی است و صلح جزئی از پهنه کلی امنیت است و هم در بعد زمان و هم مکان تعاریف و علل مختلفی دارد و به همین دلیل رویکردهای متفاوتی نیز در مورد آن وجود دارد، رویکردهایی که بر اساس مفاهیمی چون ساختار نظام بین الملل، قدرت و منافع ملی به مقوله امنیت می‌پردازند. عللی که ممکن است سبب ترس و اختلال در صلح و آرامش شوند بسیار متعدد و متنوعند و با گذر زمان تغییر می‌کنند. به طور مثال امروز اتفاقاتی همچون گرم شدن کره زمین و تغییرات آب و هوایی، امنیت بشر را بر هم می زند و باعث طرح دعوا علیه دولت ها نیز می شود. رای اخیر دیوان اروپایی حقوق بشر در دعوای زنان شهروند سوئیس و انجمن وِرِین کلیماسِنیورین[1] علیه دولت سوئیس، به سبب موثر دانستن گرمایش جهانی بر شرایط زندگی و به خطر افتادن حق بر سلامت و حیات، از این دسته است. شکایت بیش از ۲ هزار زن سوئیسی علیه دولت با این اعتقاد مطرح شد که دولت سوئیس اقدام کافی در مبارزه با تغییرات آب و هوایی انجام نداده و آنان را به سبب سن بالا و وضعیت بیماری های دوره سالخوردگی در معرض خطر مرگ قرار داده است. گرمایش ناشی از تغییرات آب و هوایی به کیفیت زندگی افراد لطمه می زند و آنان را حتی در معرض خطر مرگ قرار می دهد و این نقض امنیت روانی نه تنها یک ملت بلکه امنیت بین المللی می شود. در صورتی که پنجاه سال پیش، چنین امری متصور نبود و جزو دغدغه های امنیتی دولت ها نیز به شمار نمی رفت. این بدان

[1] Verein KlimaSeniorinnen

دلیل است که با گذر زمان، ساختار جوامع بشری پیچیده‌تر شده و وابستگی افراد بشر و جوامع مختلف به یکدیگر افزون‌تر شده و تقابل مباحث امنیتی با حوزه های نوین حقوق بشر نیز اهمیت یافته است.
یکی از این حوزه های نوین فضای سایبری و نمود نوین آن هوش مصنوعی است. کارشناسان حوزه امنیت، تروریسم سایبری را به عنوان یک خطر جدی برای امنیت ملی و بین المللی دانسته‌اند. خطر فضای سایبر و اینترنت تمام برداشت‌های رایج و سنتی از مفهوم امنیت ملی را زیر سؤال برده است. اگر تروریسم سایبری را به عنوان یک حمله و یا مجموعه‌ای از حملات که با انگیزه‌های سیاسی، مذهبی، و یا ایدئولوژیک و با هدف القا ترس و تخریب صورت می‌گیرد تعریف کنیم، بسیاری از حوادثی که در سال‌های اخیر اتفاق افتاده‌اند می‌توانند نمونه‌هایی از تروریسم سایبری باشند. بنابراین می‌توان به تحلیل گفتمان تروریسم سایبری از یک زاویه مطالعات امنیتی بپردازیم. پژوهش حاضر به شیوه توصیفی-تحلیلی با استفاده از منابع کتابخانه ای به تحلیل خوانش های جدید امنیت در پرتو تروریسم سایبری و هوش مصنوعی می پردازد. سؤال اصلی که در این پژوهش مطرح می‌شود آن است که ابعاد تهدید امنیت در حوزه سایبری چیست و تهدیدات و از همه مهم‌تر تروریسم سایبری چگونه بر امنیت ملی و بین المللی تأثیر می‌گذارد؟ به نظر می رسد با توجه به ماهیت فضای سایبری در سرعت، گستردگی و به روز بودن، مفاهیمی چون امنیت داده ها، امنیت نظامی مبتنی بر فضای سایبری، امنیت انسانی و چالش های نوین حاصل از هوش مصنوعی نیاز به رویکردهای نوین امنیتی در حوزه روابط بین الملل دارد. رویکردهایی که باید با اتخاذ سیاست های ملی دولت ها و همکاری های بین المللی میسور گردد.

۱. پیشینه پژوهش، مفاهیم و مبانی نظری

اگرچه تهدید امنیت در حوزه سایبری از دیدگاه حقوق و روابط بین الملل با رویکردهای مختلفی بررسی شده است، اما نسبت این تهدیدات با رویکردهای نوینی که در عرصه هوش مصنوعی به وجود آمده است و نیز اهمیت امنیت انسانی از نوآوری های این پژوهش است.
سامان افتخار در مقاله ای با عنوان تروریسم سایبری به عنوان یک تهدید جهانی: مروری بر پیامدها و اقدامات متقابل (۲۰۲۴) این گونه بحث نموده است: «تروریسم سایبری شامل استفاده از اینترنت و سایر اشکال فناوری اطلاعات و ارتباطات برای تهدید یا ایجاد آسیب بدنی برای به دست آوردن قدرت سیاسی یا ایدئولوژیکی از طریق تهدید یا ارعاب است. سرقت داده ها، دستکاری داده ها و اختلال در خدمات ضروری به عنوان زیرساخت دیجیتال، همه انواع حملات سایبری هستند که نقض امنیت سایبری، ملی و نیز بین المللی تلقی می شوند. کشف، واکنش و پیشگیری از این جرم چالش‌های منحصر به فردی را

برای مجریان قانون و دولت‌ها ایجاد می‌کند که نیازمند رویکردی چندوجهی است. تروریسم سایبری می تواند اثرات مخربی بر طیف وسیعی از افراد و سازمان ها داشته باشد. ثبات یک کشور ممکن است آسیب ببیند، خسارات مالی رخ دهد و در برخی موارد حتی ممکن است جان افراد از دست برود. در نتیجه حملات سایبری، زیرساخت های حیاتی مانند شبکه های برق، بیمارستان ها و سیستم های حمل و نقل می توانند مختل شود و امنیت ملی به مخاطره افتد. بررسی حوادث سایبری تروریسمی که در ده سال گذشته رخ داده است، تأثیرات آن ها بر اقتصاد کشور، بی ثباتی سیاسی و نیز اقدامات اتخاذ شده برای مقابله با آن حایز اهمیت است و می تواند به توسعه استراتژی ها و سیاست های بهتر برای مقابله با تروریسم سایبری کمک کند.»

سرنا بیانچی و همکاران در مقاله ای با عنوان هوش مصنوعی و مبارزه با تروریسم سایبری (۲۰۲۳) در حوزه اهمیت استفاده از هوش مصنوعی در تسهیل ارتکاب تروریسم سایبری آورده اند: «استفاده از هوش مصنوعی در رویکرد ارائه دهندگان خدمات میزبانی، مجریان قانون و پلیس در مبارزه با تروریسم سایبری اهمیت دارند. محتوای خشونت‌آمیز و تروریستی با بهره‌گیری از فرصت‌های ارائه‌شده توسط اینترنت، بیشتر و بیشتر به صورت آنلاین منتشر می‌شود. نهادهای اروپایی در سال ۲۰۲۱ مقرراتی را برای رسیدگی به سوء استفاده از خدمات میزبانی منتشر کردند، در مبارزه با فناوری‌های مخرب مبتنی بر هوش مصنوعی اجرای مقررات و پیامدهای قانونی و اخلاقی باید در نظر گرفته شود. چارچوب مبتنی بر هوش مصنوعی برای حمایت از ارائه دهندگان خدمات میزبانی در گزارش و حذف محتوای تروریستی آنلاین، از آن جمله است.» ***طبق نتایج مقاله حجت*** سبزواری نژاد و محمد رضازاده سلطان آباد ***با عنوان*** پیشگیری غیر کیفری از تهدیدات امنیت ملی در راستای ***تروریسم سایبری*** (۱۳۹۹)، «***تروریسم سایبری*** امروزه تهدیدی واقعی نسبت به پیشرفت سریع تکنولوژی محسوب می گردد. افزایش سریع کاربران اینترنت و اتکاء به آن به طرز نگران کننده ای ریسک های امنیتی را افزایش داده است علیرغم اینکه تدابیر امنیتی مناسبی برای کمک به پیشگیری از ریسک های امنیتی وجود داشته ولی کافی نبوده است. این تهدیدات می تواند به طور بالقوه، امنیت ملی ایران و زیرساخت حیاتی آن را مورد آسیب قرار دهد. ترکیبی از راهکارهای پیشگیرانه اجتماعی و موقعیت مدار می تواند مناسب باشد که شامل بهره گیری از خبرگان، جرم انگاری براساس پیشرفت های تکنولوژی، آگاه سازی و اطلاع رسانی همگانی، اقدامات آموزش محور، افزایش و ارتقای درجه رفاه همگانی و مهیا سازی زمینه و بستر عدالت اجتماعی است.»

مفهوم صلح و امنیت چه در بعد ملی و چه در حوزه بین المللی معانی متفاوتی برای دولت ها و جامعه جهانی داشته است. دیدگاه کلاسیک حقوق و روابط بین الملل، در سال ۱۹۴۵ و در زمان تشکیل ملل متحد، عمدتاً متوجه صلح و امنیت بین المللی بوده و در واقع اولین خط مقدمه منشور به ضرورت حفظ نسل‌های آینده از خطرات جنگ اشاره می‌کند. برای تحقق این هدف بود که مؤسسین سازمان، قدرت ایجاد نظام امنیت دسته جمعی را برای حفظ صلح و امنیت بین المللی به سازمان اعطا کردند. (اشرفی، ۲:۱۳۹۳) اما با توجه به شرایط فعلی حاکم بر روابط بین الملل دو نکته را در مورد مفهوم صلح و امنیت جهانی باید مد نظر قرار داد. اول اینکه در گذشته صلح و امنیت از مفاهیمی بود که صرفاً در حوزه نظامی و احیاناً سیاسی کاربرد داشت اما امروزه به خصوص اصطلاح امنیت در ابعاد وسیع سیاسی، فرهنگی، اقتصادی، تکنولوژیکی و جز آن معنی دارد. در هم تنیدگی و تداخل قلمروهای مزبور به عنوان یکی از پیامدهای پدیده «جهانی شدن» موجب شده که بحران و ناامنی در یکی از حوزه‌ها به دیگر قلمروها تسری یابد، بنابراین بحران اقتصادی، فناوری های نوین و مسائل فرهنگی می‌تواند به بحران سیاسی و احیاناً نظامی منجر شود.

دوم آن که صلح و امنیت بین المللی به معنای واقعی آن الزاماً با حفظ وضع موجود تأمین نمی‌شود، چرا که امکان دارد قوانین و ساختارهای حقوقی نظام حاکم بر روابط بین الملل ماهیت ظالمانه و تبعیض آمیز داشته باشد. در حالی که صلح از مفاهیمی است که با عدالت و مساوات عجین است، لذا پایداری آن بدون عدالت ممکن نیست. در این حوزه اشاره به نظریاتی که در مورد دست یابی به صلح در نظام بین الملل مطرح شده‌اند، خالی از فایده به نظر نمی‌رسد، ناگفته نماند که در این راستا ارتباط و وابستگی مفهوم صلح و امنیت باید در نظر گرفته شود، این نظریات را می‌توان در سه دسته کلی تقسیم کرد: الف) نظریات آرامان گرایانه که برتری دادن به اخلاق نسبت به قانون و تقدم سیاست بین الملل به سیاست داخلی و خیرخواهی و صلح طلبی را مدنظر دارند. خلع سلاح، تحقق صلح از طریق مودت، تأسیس جامعه ملل، امنیت دست جمعی و خود محدودیتی دولت‌ها از طریق پای بندی به قوانین جهانی از جمله راه حل‌های این گروه است. ب) در نظریات واقع گرایانه معتقدند نمی‌توان شکاف میان سیاست داخلی و بین المللی را کاهش داد و حتی از بین برد؛ واقع گرایی مدت ها اندیشه غالب در روابط بین الملل بود که به رقابت بی پایان دولت‌ها بر سر قدرت و امنیت تاکید دارد. نظریه بازدارندگی هسته‌ای، نظریه موازنه قوا ونظریه های دیپلماسی از برآیند این طرز تفکر است. ج) نظریات بینابین بر آن هستند که راه دیگری برای تفکر در مورد روابط بین الملل وجود دارد که تاحدودی با واقع گرایی و آرمان گرایی تداخل پیدا

می‌کند. تمام این مکاتب جایگاه خود را در نقطه مابین دو قطب افراطی آرمان گرایی و واقع گرایی حفظ کرده‌اند. اندیشه ایجاد صلح از طریق روابط بازرگانی وتفکر حاکم بر سازمان ملل متحد را می‌توان مرتبط با این اندیشه دانست. (شفیعی، ۱۳۸۹) در برآیند تمامی نظریات باید گفت هم صلح و هم امنیت، مفاهیمی چند وجهی هستند. دولت‌ها باید ابعاد جدیدی را در باب امنیت در نظر بگیرند. به طور مثال کانادایی‌ها دیگر نگران سوزاندن تورنتو توسط سربازان آمریکایی نیستند، بلکه نگرانند رایانه‌ای در تگزاس، تورنتو را با مشکل موجه کند. (نای، ۱۳۸۷: ۱۲۴). گذشته از مفهوم امنیت در زمینه داخلی و بین المللی، صلح نیز از جمله مفاهیم مورد مناقشه در حقوق و روابط بین الملل است. صلح را باید چیزی فراتر از فقدان جنگ دانست.[۱] صلح را می‌توان به شکل صلح مثبت و منفی تعریف کرد. صلح مثبت شامل حذف خشونت ساختاری است. اگر صلح به معنی عدم وجود تهدیدی برای وضع موجود یا عدم نقض آن یعنی صلح منفی تلقی شود، امنیت شامل بخش‌هایی خواهد بود که معولاً از آن به عنوان مفهوم صلح مثبت یاد می‌شود. (وکیل، ۱۳۹۱: ۱۱۸-۱۱۹)

حق بر صلح در نسل سوم حقوق بشر یا حقوق همبستگی جای دارد. که زمینه را برای تحقق دو نسل دیگر حقوق بشر فراهم می‌سازد. در مقدمه منشور ملل متحد به عنوان یک سند عام الشمول، اهمیت صلح در تحقق حقوق بشر و آزادی‌های اساسی ذکر شده است. می‌توان حق بر صلح را توسعه ماده سوم اعلامیه جهانی حقوق بشر دانست که حق همه افراد را به حیات، آزادی و امنیت فردی به رسمیت می‌شناسد. حق بر صلح را می‌توان، توسعه ماده سوم اعلامیه جهانی حقوق بشر دانست که حق همه افراد را به حیات، آزادی و امنیت فردی به رسمیت می‌شناسد. در پی ظهور این مفهوم در ادبیات حقوقی بین‌الملل، مجمع عمومی سازمان ملل متحد نیز با تصویب قطعنامه «آماده کردن جوامع برای زندگی در صلح» گام در مسیر نهادینه‌سازی حق بر صلح گذاشت. پس از آن در سال ۱۹۸۴ مجمع عمومی سازمان ملل متحد اقدام به صدور قطعنامه‌ای تحت عنوان اعلامیه حق مردم بر صلح کرد و در آن ضمن شناسایی حق بر صلح، به عنوان حقی مقدس دولت‌ها را مکلف به حفظ و ترویج آن در سطوح ملی و بین‌المللی دانست. حق بر صلح زمینه را برای تحقق دو نسل دیگر حقوق بشر فراهم می‌سازد.

رویکردهای متفاوتی که در مورد امنیت وجود دارد، بر اساس مفاهیمی چون ساختار نظام بین الملل، قدرت و منافع ملی به مقوله امنیت می‌پردازند. واقع گرایان امنیت ملی را همان امنیت بین المللی شناسایی

[۱] برخی صلح را یک "نهاد نظم مبتنی بر عدالت" دانسته‌اند. بر این اساس هر عملی که در تعارض با عدالت است، تهدید علیه صلح به شمار می‌آید.

نموده و در این راستا وجود ناامنی ویژگی بارز آن است. از نگاه واقع گرایان هرچیزی ممکن است بر امنیت تاثیرگذار باشد و از آن جایی که دولت‌ها بازیگران اصلی در نظام بین المللی هستند، بنابراین آن‌ها مرجع امنیت قرار خواهند گرفت. (عبدالله خانی، ۱۳۸۲: 70-۸۳) در مقابل در اندیشه لیبرالیست‌ها، برقراری صلح را نه با موازنه قدرت که از طریق حکومت‌های دموکراتیک قابل دسترسی می‌دانند. برای حفظ امنیت لگام زدن به رفتار دولت‌ها با ایجاد سازمان‌ها و رژیم‌های بین المللی راه حل است. (یزدان فام، ۱۳۸۶: ۷۳۲) مباحث عمیق در حوزه امنیت مربوط به مکتب کپنهاک است که عرصه مطالعات امنیتی را به پنج حوزه تقسیم بندی می‌کند: نظامی، سیاسی، اقتصادی، اجتماعی و تا مباحثی چون محیط زیست. اگرچه از تهدیدات سایبری سخنی به میان نمی‌آورد اما آثار و پیامدهای مخاطره آمیز این تهدیدات به حدی است که دیگر نمی‌تواند مورد غفلت رویکردهای نظری در روابط بین الملل باقی بماند. (خلیلی پور رکن آبادی و نورعلی وند، ۱۳۹۱: ۱۹۰) باید گفت تروریسم در تمامی اشکال آن ویرانگر نظم حقوقی، صلح و امنیت بین المللی است، تحولات تکنولوژیک اخیر، نشان داده است که صلح بیش از هر زمان دیگری در معرض تهدید و نقض می‌باشد و جامعه جهانی نیز به جای شناخت علت‌ها، بر سر معلول‌ها متمرکز شده است و همین عامل باعث شده پیشگیری لازم برای بحران‌های تروریستی صورت نگیرد. (بندک ومانگوپولوس، ۱۳۸۹: ۸-۱۱)

۲. تروریسم سایبری و ابعاد تهدید علیه امنیت و صلح

نگاه کلاسیک به مقوله امنیت، ناظر بر بعد نظامی آن است. اما بسیاری از متغیر های دیگر، امروزه چه بسیا آثار ضد امنیتی مخرب تری نسبت به حمله یا تهدید نظامی داشته باشد. یکی از این پدیده ها که ظهور تکنولوژیک هم دارد، تروریسم سایبری است. تروریسم در اسناد بین المللی و قطعنامه های سازمان ملل به عنوان ناقض صلح، امنیت و حقوق بشر معرفی شده و حتی دبیرکل سازمان ملل متحد و کمیسرعالی کمیسیون حقوق بشر آن را جنایت علیه بشریت دانسته اند.

در سال‌های اخیر به جز دولت های حامی تروریسم، شرکت‌های فراملی، جنبش‌های اجتماعی، گروه‌های افراطی و مهاجران سربرآورده اند که می‌توانند نقش موثری در تهدید امنیت به ویژه در حوزه سایبر بازی کنند. بنابراین از آن جایی که در تهدیدات سایبری با بازیگران غیردولتی بین المللی سرو کار داریم، این حوزه از امنیت تنها مربوط به امنیت ملی نمی‌شود، در واقع همین جاست که مبحث امنیت بین المللی مطرح می‌شود، زیرا مبارزه همه جانبه با حملات سایبری همکاری دولت‌ها و سایر تابعان حقوق بین الملل را می‌طلبد. (خلیلی پور رکن آبادی و نورعلی وند، ۱۳۹۱: ۱۸۹) هوش مصنوعی نیز به عنوان

عرصه ای سایبری از این مهم مستثنی نیست. در ادامه حوزه های فوق الذکر در پرتو مفهوم چند بعدی امنیت، مورد بررسی قرار می گیرند.

۱-۲. امنیت در حوزه سایبر

اگر تروریسم سایبری را به عنوان یک حمله و یا مجموعه‌ای از حملات با انگیزه‌های سیاسی، مذهبی و یا ایدئولوژیک و که با هدف القا ترس و تخریب صورت می‌گیرد تعریف کنیم، بسیاری از حوادثی که در سال‌های اخیر اتفاق افتاده‌اند می‌توانند نمونه‌هایی از تروریسم سایبری باشند. بنابراین می‌توان به تحلیل گفتمان تروریسم سایبری از یک زاویه مطالعات امنیتی بپردازیم. یکی از دلایل پیچیدگی مفهوم امنیت و ماهیت ابهام آمیز آن، چندوجهی بودن مفهوم امنیت است. یکی از متغیرهای پیچیده و نوپدید که در قلمرو امنیت بین المللی مطرح است، مقوله جهانی شدن است. جهانی شدن در این زمینه به معنی فرایندهایی است که به شکل گرفتن فضای جهانی واحد کمک می‌کند، این امر با ورود هوش مصنوعی نیز پیچیدگی های خاص خود را به دنبال دارد. امروزه سازمان‌های ارائه‌دهنده خدمات، سیستم‌های مالی و بانکداری، شبکه‌های ارتباطات اجتماعی، روزنامه‌نگاری و حتی پلیس، سازمان‌ها و تشکیلات امنیتی با طبقه‌بندی‌های حفاظتی به فضاهای مجازی ورود پیدا کرده و از این عرصه برای تسهیل ارتباطات و کارکردها بهره می‌گیرند. با توجه به این کارکردهای کلان، مسئله امنیت در فضای مجازی به قدری از اهمیت رسیده که اساساً مفاهیم کنترل امنیت در فناوری اطلاعات یکی از ارکان اساسی و حفاظتی سازمان‌ها و دستگاه‌های اداری را تشکیل داده است.

به امنیت فناوری اطلاعات، وابسته به سیاست دولت‌ها، امنیت سایبری گفته می‌شود. امنیت سایبری یا امنیت اینترنتی به جوانب امنیت شبکه و اصول سیاست‌گذاری شبکه‌ها مانند تعریف حریم خصوصی، جرائم سایبری، تجارت و ارتباطات جهانی اشاره دارند. امنیت فضای سایبری به خاطر اتکای بیش از حد تمامی بازیگران سیاسی به آن، بی تردید مقوله‌ای استراتژیک قلمداد می‌شود و به همین دلیل است که در ارزیابی از تهدیدات امنیت ملی و بین المللی، مفهوم امنیتی فضای سایبری، وارد اسناد پایه‌ای امنیتی شده است. (موسوی، حیدری و قنبری، ۱۳۹۲: ۸- ۹) توانایی استفاده از فضای سایبری، یکی از مهم‌ترین منابع قدرت در قرن ۲۱ به حساب می‌آید. بازیگران دولتی و غیردولتی از این قدرت استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود درفضای سایبری و دنیای واقعی دست یابند. از منظر امنیت ملی می‌توان گفت که در شرایط حاضر، دولت‌ها و ملت‌ها با زنجیره‌ای از تهدیدات نامشخص در محیط‌های مجازی مواجهند که امنیت آن ها را به چالش

کشـیده و ابزارهـای سـنتی تأمین کننده امنیت ملی دیگر توان مقابله با آن ها را ندارند (حسن بیگی، ۱۳۸۴: ۲۷۸). در حوزه امنیت سایبر باید به امنیت داده‌ها و مفهوم امنیت انسانی و نیز تهدید تروریسم سایبری در دو بعد امنیت ملی و بین المللی اشاره نمود.

الف) امنیت داده‌ها: هدف از امنیت داده‌ها حفظ محرمانگی، یک پارچگی و در دسترس بودن اطلاعات است. امنیت اطلاعات یا داده‌ها به معنای حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز می‌باشد. این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری. امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها مربوط است. داده رایانه‌ای توسط کنوانسیون جرائم اینترنتی در بند (ب) ماده ۱ تعریف می‌شود: «هر گونه ارائه ایی از حقایق، اطلاعات یا مفاهیم در یک فرم مناسب برای پردازش در یک سیستم کامپیوتری، از جمله یک برنامه مناسب برای انجام عملکرد یک سیستم کامپیوتری». (Budapest convention, 2001) به زعم نگارندگان از آن جا که دولت‌ها، مراکز نظامی، شرکت‌ها، مؤسسات مالی، بیمارستان‌ها، و مشاغل خصوصی مقادیر زیادی اطلاعات محرمانه در مورد کارکنان، مشتریان، محصولات، تحقیقات، و وضعیت مالی گردآوری می‌کنند و بسیاری از این اطلاعات در حال حاضر بر روی کامپیوترهای الکترونیکی جمع آوری، پردازش و ذخیره و در شبکه به کامپیوترهای دیگر منتقل می‌شود، اگر اطلاعات محرمانه در مورد مشتریان و یا امور مالی یا محصول جدید موسسه‌ای به دست رقیب بیفتد، این درز اطلاعات ممکن است به خسارات مالی به کسب و کار، پیگرد قانونی و یا حتی ورشکستگی منجر شود. حفاظت از اطلاعات محرمانه یک نیاز تجاری، و در بسیاری از موارد نیز نیاز اخلاقی و قانونی است. از آن جایی که امینت اطلاعات تاثیری معنادار بر حقوق بشر و به ویژه حریم خصوصی افراد دارد و نیز تعابیری متفاوت از آن عرضه شده است، باید به موضوعات تخصصی گوناگونی در این حیطه اهمیت داد. از جمله: تأمین امنیت شبکه و زیرساخت‌ها، تأمین امنیت برنامه‌های کاربردی و پایگاه داده‌ها، تست امنیت، حسابرسی و بررسی سیستم‌های اطلاعاتی، برنامه ریزی تداوم تجارت و بررسی جرائم الکترونیکی و غیره.

ب) امنیت انسانی: امنیت انسانی مسائل جدیدی را مطرح می‌کند که پیش از این به عنوان مسائل امنیتی مطرح نبوده‌اند، تروریسم سایبری در دو حوزه با مفهوم امنیت انسانی تلاقی می‌یابد یکی از آن جهت که با حمله یا تهدید به اعمال خشونت بار علیه زیر ساخت‌های حیاتی چون شبکه‌های آب، انتقال انرژی و

شبکه‌های مالی و بانکی یا حمل و نقل، مؤلفه‌های سازنده امنیت انسانی شامل امنیت اقتصادی، بهداشتی، فیزیکی و سیاسی را مختل می‌کند و دیگری اثری است که بر مفهوم حق بر توسعه به عنوان یکی از غایات امنیت انسانی می‌گذارد و تحقق آن را با مانع جدی مواجه می‌نماید. حق بر توسعه حقی جمعی شامل مجموع حقوق اقتصادی، اجتماعی و فرهنگی است و تا زمانی که این حق محقق و استیفا نشود، سایر حقوق نسل اول و دوم نیز محقق نخواهد شد.

برنامه توسعه سازمان ملل متحد مفهوم امنیت انسانی را این گونه تعریف کرده است: « امنیت انسانی دو بعد دارد، نخست امنیت از تهدیدات گسترده و مدامی مانند گرسنگی و بیماری و بعد دیگر حمایت در مقابل حوادث زیان بار و ناگهانی که در جریان زندگی عادی رخ می‌دهد. محدوده این تعریف گسترده است و عملاً هر درد و رنج ناخواسته‌ای می‌تواند امنیت انسانی را تهدید کند. ۷ عنصری که سازنده امنیت انسانی تلقی می‌شوند عبارتند از: امنیت اقتصادی، غذایی، بهداشتی، محیط زیستی، شخصی (امنیت فیزیکی)، امنیت اجتماعی و سیاسی. (قبادی، ۱۳۹۴: ۵۸). امنیت انسانی متضمن این اندیشه کانتی است که ما باید با مردم به عنوان هدف و نه ابزار نگاه کنیم، اما با دولت‌ها باید به عنوان ابزار و نه هدف رفتار کرد. (همپستون، ۱۳۹۰: ۳۵۳)

به نظر نگارندگان از آن جایی که مفهوم امنیت انسانی حاصل نزدیکی در دو زمینه مطالعات امنیتی و توسعه بین المللی است، بنابراین امنیت ارتباطات نیز از مؤلفه‌های امروزی امنیت انسانی است. طبق تعریف سلبی از امنیت انسانی، آن را نبود تهدید علیه ارزش‌های اساسی بشر دانسته و طبق تعریف ایجابی هدف آن را می‌توان پاسداری از هسته حیاتی همه انسان‌ها در برابر تهدیدات فراگیر جدی قلمداد کرد. پس مقصود از امنیت انسانی بر خلاف مفهوم سنتی آن امنیت دولت‌ها و حاکمیت در برابر تهدیدات خارجی یا داخلی نیست بلکه، امنیت انسان‌ها در برابر تهدیدات جدی است.

در اواسط دهه نود، شبکه‌ای موسوم به شبکه امنیت انسانی توسط یازده کشور شکل گرفت که اقدام به طرح ریزی نتایج سیاسی حاصل از سرشت تهدیدات علیه صلح و امنیت نموده‌اند. این دولت‌ها اعلام نموده‌اند که رویکرد امنیت انسانی می‌تواند از رهگذر این آگاهی مشخص گردد که، تاکید منحصر بر رویکرد سنتی نظامی نسبت به امنیت منسوخ و ناکافی است و دولت‌هایی که چنین رویکردی را در نظر داشته‌اند در حمایت از شهروندان از آسیب پذیری های نوینی چون تروریسم سایبری خود ناتوان خواهند بود. کانادا و ژاپن از جمله دولت‌هایی هستند که امنیت انسانی را جزو اصول سیاست خارجی خود قرار داده‌اند و آن را ایمنی مردم در دنیا در حال تغییر، رهایی از فقر، زیست در حال صلح و احترام به کرامت

انسانی دانسته‌اند. می‌توان گفت تحقق امنیت انسانی، از رهگذر تحقق کامل حق‌های بشری نمودار می‌گردد و بدون امنیت انسانی نیز توسعه انسانی نمی‌تواند وجود داشته باشد. (بندک و مانگوپولوس، ۱۳۸۹: ۲۳۱– ۲۳۳)

۲-۲. تروریسم سایبری تهدید علیه امنیت ملی

امروزه مسائل زیست محیطی، فقر، مهاجرت و تهدیدات فضای مجازی از جمله هوش مصنوعی بیش از تهدیدات نظامی امنیت دولت‌ها و نیز جامعه جهانی را به مخاطره می‌اندازد. امنیت سایبری در ارتباط مستقیم با امنیت ملی است. امروزه دیگر نمی‌توان امنیت را منحصراً در ارتباط با مرزها و حفاظت از جان شهروندان به وسیله نیروهای نظامی تعریف کرد. خطر فضای سایبر و اینترنت تمام برداشت‌های رایج و سنتی از مفهوم امنیت ملی را زیر سؤال برده است. مسئله این است که تهدیدات سایبری چگونه بر امنیت ملی تأثیر می‌گذارند؟

تهدید سایبری پدیده انتشار قدرت را به وجود می‌آورد که نه تنها باعث شده دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت در این فضا بهره مند شوند بلکه ورود بازیگران جدیدی همچون شرکت‌ها، گروه‌های سازمان یافته و افراد به معادلات جهانی را سبب شده است. (خلیلی پور رکن آبادی و نورعلی وند، ۱۳۹۱: ۱۶۷) بنابراین در حوزه سایبری با تحول مفهوم امنیت در دو بعد ملی و بین المللی روبرو هستیم. چالش دیگری که وجود دارد چند بعدی بودن مفهوم امنیت و عدم امکان ارائه تعریف جامع از آن است، که به دلیل: تغییر مفهوم امنیت با گذر زمان، ذهنی بودن و متأثر از نظریه بودن آن و نیز تعیین طبقه و مقوله‌ای که امنیت ذیل آن قرار می‌گیرد، وجود دارد.

ریچارد اولمن یکی از جامع‌ترین تعاریف را در این حوزه ارائه نموده است: «تهدید امنیت ملی اقدام یا سلسله رویدادهایی است که نخست به شکل مؤثر، در دوره زمانی کوتاه خطر افت کیفیت زندگی را برای ساکنان کشور پیش می‌آورد و دوم با خطر جدی کاهش طیف خط مشی‌هایی که حکومت یا واحدهای غیر حکومتی خصوصی موجود در کشور می‌توانند از میان آن‌ها دست به انتخاب زنند، همراه باشد. مسلماً با این تعریف تصور ما از عوامل تهدید زا دامنه بیشتری می‌یابد.» (تریف، ۱۳۸۳: ۴۹). تهدید سایبری از بدترین تهدیدات علیه منافع و امنیت ملی است. تا جایی که برخی کشورها مانند امریکا اعلام کرده‌اند آن را به مثابه حمله نظامی تلقی می‌کنند و به آن واکنش فیزیکی و نظامی نشان خواهند داد. پیامد دستکاری داده‌ها حتی ممکن است خسارات و تلفاتی بیش از یک حمله نظامی از خود به جای بگذارد.

۳-۲. تروریسم سایبری تهدید و نقض امنیت بین المللی

نگاه وستفالیایی به امنیت بین‌المللی، نگاهی محدود است که از محدوده مرزهای دولت‌ها چندان فراتر نمی‌رود. استقلال و حاکمیت ملی دولت‌ها، در این زمان مهم‌ترین رکن امنیت بین المللی بود و دول هم منشاء تأمین امنیت بودند و هم منشاء اصلی تهدید تلقی می‌شدند. اما امروزه شاخص‌های تهدید بسیار متنوع شده و طیف وسیعی از مهاجرت بی رویه، بیماری‌های مسری، سلاح‌های کشتار جمعی و تروریسم سایبری را شامل می‌گردد.[۱] فناوری ارتباطات، اهمیت و فراوانی داده‌های حیاتی و تعدد کنش گران بین المللی، فضای سایبر را نیز به حوزه‌های امنیت داخلی و بین المللی وارد نموده است.

امنیت بین‌الملل تدریجاً مفهوم وستفالیایی خود را از دست می‌دهد و بازیگران فروملی و فراملی نیز منشأ تهدیدات می‌باشند؛ در مقصد تهدیدات نه صرفاً دولت‌ها بلکه بازیگران غیر دولتی نیز مورد توجه قرار می‌گیرند؛ امنیت بازیگران چنان به همدیگر گره می‌خورد که برخی، از اصطلاحاتی چون امنیت جهانی یا امنیت بشری به جای امنیت بین‌الملل استفاده می‌کنند. ماهیت تهدیدات نه تنها نظامی بلکه، سیاسی، اقتصادی، اجتماعی و حتی زیست محیطی است. واکنش‌ها نیز فقط نظامی نیستند؛ مسئولان متعددی برای تأمین امنیت بازیگران و به طور کلی امنیت بین‌المللی در مفهوم جدید در نظر گرفته می‌شود. در عرصه جهانی شدن ارزش‌هایی چون حقوق و نیازهای اساسی بشر و حفاظت از محیط زیست نیز اهمیت پیدا می‌کنند. (اشرافی، ۱۳۹۳: ۸۶-۸۷) والتر لاکور، متخصص تروریسم در مرکز مطالعات استراتژیک و بین المللی ادعا کرده است که می‌تواند با مبلغ یک میلیارد دلار و تعداد ۲۰ هکر حرفه‌ای، ایالت متحده آمریکا را فلج کند. اگرچه هدف تروریست‌ها معمولاً ترور سران و رهبران سیاسی، گروگان گیری و یا حمله ناگهانی به تأسیسات دولتی، نظامی، پلیسی و یا عمومی است، اما تهدیداتی که ممکن است به وسیله حمله‌های سایبری به شبکه‌های رایانه‌ای وارد گردد، بسیار خطرناک تراز حملات تروریستی سنتی و کلاسیک است. تروریسم سایبری ممکن است برای تعداد کثیری از مردم بسیار ویران کننده تر از جنگ‌های بیولوژیک و یا شیمیایی باشد. (آنجلیز، ۱۳۸۳: ۱۶) زیرا فضای سایبر با توجه به ویژگی‌هایی از جمله، مخفی ماندن هویت مجرم، عدم نیاز به سرمایه گذاری کلان، امکان حمله و آسیب به

[۱] آقای کوفی عنان دبیرکل سابق ملل متحد، هیئت عالی رتبه‌ای را برای تهیه گزارشی راجع به مطالعه و بررسی تهدیدات بر صلح تعیین کرد. این هیئت تهدیدات را بر شش دسته تقسیم کرد که با یکدیگر نیز مرتبط‌اند. از نظر هیئت، این تهدیدات عبارتند از: تهدیدات اجتماعی، اقتصادی، بیماری‌های واگیردار و آلودگی‌های زیست محیطی، مخاصمات فیمابین دولت‌ها، مخاصمات داخلی از قبیل جنگ‌های داخلی و نسل کشی، تولید و گسترش سلاح‌های شیمیایی، بیولوژیکی و هسته‌ای، تروریسم وجرایم سازمان یافته. (اشرافی، ۱۳۹۳: ۹۱)

زیرساخت‌ها و تلفات بسیار، امکان هدایت از راه دور و عدم نیاز به سلاح خاص و ... برای تروریست‌ها محیط جذابی به شمار می‌آید. همین شکل از تروریسم سبب تضعیف دولت‌ها، اقدامات صلح آمیز سازمان‌های بین المللی چون ملل متحد، مانع رشد اقتصادی و ایجاد جنگ سایبری در سطوح بالاتر حمله می‌گردد. امنیت مفهومی به هم پیوسته است امروزه آنچه امنیت ملی را تهدید می‌کند حتی اگر از مرزهای یک کشور فراتر نرود تهدید علیه امنیت بین المللی به حساب می‌آید.

باید توجه داشت که تروریسم سایبری هم از بابت ارتباط با سایر جرائم سایبری چون پول شویی، قاچاق و سابوتاژ، و هم از بابت احتمال تبدیل به جنگ سایبری امنیت بین المللی را به مخاطره می‌اندازد. از سوی دیگر مباحثی چون امنیت انسانی و اطلاعات امروزه در حوزه امنیت بین المللی قرار می‌گیرند، لذا در این حوزه نیز تروریسم سایبری تهدید جدی علیه امنیت بین المللی است. بر این مبنا عدم ثبات و پایداری در زمینه‌های اجتماعی، اقتصادی، سیاسی و نقض حقوق بشر تهدید علیه صلح و امنیت بین المللی به حساب می‌آیند نمونه‌های بسیاری از حملات سایبری وجود دارد که می‌تواند نقض امنیت حتی در نوع بین المللی آن باشد. باج افزاری[1] سیستم‌های ویندوز ارگان‌ها و نهادهای دولتی را در سراسر جهان هدف قرار داد که از طریق دریافت ایمیل مشکوک، فعال شده و دسترسی کاربران به اطلاعات حیاتی و ارزشمندی چون داده‌های مالی یا پزشکی را منوط به پرداخت باج به هکرها نمود. دستکاری سیستم‌ها، سرقت اطلاعات طبقه بندی شده، حذف اطلاعات، تخریب وب سایت‌ها از انواع اقدامات دیگری هستند که تروریست‌های سایبری برای اجرای برنامه‌هایشان جهت ارتقاء منابع مالی، توزیع تبلیغات و ارتباطات امنیتی مورد استفاده قرار می‌دهند.[2] تروریسم در آینده بدون گلوله و صرفاً از طریق تخریب زیرساخت‌هایی که متکی به فناوری ارتباطات هستند اتفاق می افتد. اهداف بالقوه سیستم‌هایی هستند که دفاع ملی و زیرساخت‌های حیاتی را کنترل می‌کنند. امکانات گسترده‌ای که محیط سایبری در اختیار تروریست‌ها قرار می‌دهد، باعث می‌شود در بعد میزان آسیب و هدف قراردادن شبکه‌های دولتی، مالی و نیروگاه‌ها اقدامات تروریست‌ها به سهولت ارتکاب یابد.

۳. هوش مصنوعی، تروریسم سایبری و امنیت

هوش مصنوعی به عنوان یک رشته از علوم کامپیوتر، به تئوری و تولید سیستم‌های رایانه‌ای اختصاص دارد که وظیفه آن ها ادراک بصری، تشخیص گفتار، ترجمه و حل مسئله است. (Nikolic, 2024) هوش

[1] wannacrypt

[2] رمزی یوسف برنامه ریز اصلی حمله به مرکز تجارت جهانی با رمز گذاری فایل‌ها و پست الکترونیک از جزئیات نقشه‌ها برای تخریب استفاده می‌کرد.

مصنوعی برای حل بسیاری از چالش های زمانه ما بسیار مناسب است و امنیت سایبری مطمئناً در این دسته قرار می گیرد، در زمانی که حمله وسیعی رخ می دهد و در شرایطی که کمبود متخصصان امنیتی ماهر نیز وجود دارد، هوش مصنوعی تهدید را به صورت خودکار تشخیص می دهد و نسبت به روش‌های نرم‌افزار محور واکنش مؤثرتری از خود نشان می‌دهند. در سال‌های اخیر، هوش مصنوعی به عنوان فناوری مورد نیاز برای تقویت تیم‌های امنیت اطلاعات نیز ظاهر شده است. از آن جایی که انسان‌ها نمی‌توانند به اندازه کافی از امنیت سایبری به شیوه های قبلی محافظت کنند، هوش مصنوعی تجزیه، تحلیل و شناسایی تهدید مورد نیاز را ارائه می‌کند که می‌تواند توسط متخصصان امنیت سایبری برای کاهش خطر نقض و بهبود وضعیت امنیتی به کار گرفته شود. در زمینه امنیت، هوش مصنوعی می‌تواند خطر را شناسایی و اولویت‌بندی کند، هر بدافزاری را در شبکه شناسایی کند، برای واکنش به حمله راهنمایی کند و نفوذها را قبل از شروع شناسایی نماید. هوش مصنوعی به تیم‌های امنیت سایبری اجازه می‌دهد تا مشارکت‌های انسانی و ماشینی قدرتمندی را ایجاد کنند که مرزهای دانش ما را جابجا می‌کند، زندگی ما را غنی می‌کند و امنیت سایبری را به گونه‌ای هدایت می‌کند که بیشتر از مجموع اجزای آن به نظر می‌رسد باید دانست هوش مصنوعی یک شمشیر دولبه است که می‌تواند در هم در ارتکاب جرایم سایبری به تروریست ها کمک کند و هم در پیشگیری، کشف و سرکوب آن ها نیز نقش دارد. از سوی دیگر اهمیت یافتن هوش مصنوعی در حوزه امنیت سایبری، ملی و بین المللی نیز اهمیت می یابد در ادامه این موضوعات، مورد بررسی قرار خواهد گرفت.

الف- هوش مصنوعی و مبارزه با تروریسم سایبری

توسعه فناوری در شیوه منفی آن در خطراتی که امنیت کشورها و افراد را تهدید می کند، به ویژه پدیده تروریسم که خطر آن با پیشرفت فناوری به طور پیوسته افزایش یافته است، اهمیت دارد. بنابراین، روش مدیریت تروریسم پیچیده تر شده است، زیرا گروه های تروریستی از فضای سایبری برای انجام حملات با استفاده از اینترنت و برنامه های پیچیده استفاده می کنند، بنابراین تروریسم از شیوه سنتی مبتنی بر سلاح به تروریسم سایبری مبتنی بر قدرت نرم تبدیل شده است. تأثیر مثبت توسعه فناوری هوش مصنوعی خود را در پیشگیری و کنترل جرایم، از جمله جرایم تروریسم سایبری نشان می دهد. فضای مجازی در امنیت بین‌الملل از اهمیت بالا یی است، زیرا از طریق ظهور نوع جدیدی از قدرت، که قدرت مجازی است، به پایان دادن به انحصار قدرت سنتی کمک می کند. با این حال این قدرت، نه تنها به صورت مسالمت آمیز، بلکه توسط گروه های تروریستی برای انجام حملات خود استفاده می شود.

علاوه بر این، توسط افراد و بازیگران غیردولتی برای نفوذ به شبکه های اطلاعاتی یا جاسوسی و سایر اهداف نیز استفاده می گردد. تهدیدات گروه های تروریستی و همچنین آشنایی گسترده آنان با فضای مجازی، فعالان حوزه هوش مصنوعی را بر آن داشت تا با توسل به هوش مصنوعی به منظور مبارزه علیه تروریسم، تلاش کنند. موضوع مهمی که دبیر کل سازمان ملل متحد، آنتونی گوترش نیز در چارچوب استراتژی دبیر کل برای فناورهای جدید به آن اشاره کرد: «اگر هوش مصنوعی به درستی کنترل شود و ارزش ها و تعهدات تعیین شده در منشور ملل متحد و اعالمیه جهانی حقوق بشر را ارج نهد، می تواند نقش مؤثری در تحقق توسعه پایدار، از طریق پایان دادن به فقر، حفاظت از زمین و تضمین صلح و رفاه برای همگان، داشته باشد.» به همین نحو، هوش مصنوعی می تواند ابزاری قدرتمند در مبارزه با تروریسم سایبری باشد. (رزمخواه، ۱۴۰۳: ۷)

بنابراین اولین کاربرد هوش مصنوعی در حوزه مورد بحث این پژوهش، استفاده به عنوان ابزاری برای جلوگیری و مبارزه با تروریسم سایبری است و از آن جایی که ویژگی های بسیاری دارد، به عنوان یک سرمایه گذاری مؤثر در بسیاری از زمینه ها، از جمله در برنامه ریزی و تجزیه و تحلیل اطلاعات در نظر گرفته می شود. نقش هوش مصنوعی در جلوگیری از حملات سایبری را می توان در این حوزه ها خلاصه نمود: شناسایی الگوهای مشکوک، تحلیل داده‌های بزرگ و کنترل خودکار محتوا، شبیه‌سازی و پیش‌بینی حملات و اقدامات تروریستی، تقویت سیستم‌های احراز هویت، شناسایی افراد و زیرساخت های آسیب پذیر.

باید افزود تکنیک های هوش مصنوعی نقش مهمی در پیش بینی عملیات تروریستی از طریق تجزیه و تحلیل داده ها دارند، اما در عین حال با چالش های مربوط به حقوق بشر نیز روبرو هستند که باعث می شود مسائلی در مورد محدودیت کاربردهای پیش بینی کننده آن ها در مبارزه با تروریسم و پیامدهای آن در نظر گرفته شود. (KATHLEEN, 2019) از تکنیک های استفاده از هوش مصنوعی در مبارزه با تروریسم سایبری می توان به استفاده از شبکه های دوربین نظارتی و امنیتی برای نظارت بر صدها هزار چهره به صورت روزانه در جستجوی مظنون عملیات تروریستی برای کاهش ریسک ارتکاب جنایات تروریستی استفاده نمود. استفاده از ویژگی های حملات قبلی، آموزش در شناسایی تروریست ها در مناطق شلوغ، استفاده از سیستم های اطلاعاتی برای تجزیه و تحلیل فیلم های نظارتی در تحقیقات جنایی، شناسایی افراد مشکوک، تعیین مدل های اصلی خودرو و تجزیه و تحلیل معاملات مالی مشکوک

و افرادی که به نظر می رسد رفتارهای غیرمعمول مانند بازدید مکرر از یک سایت خاص دارند، از جمله منافع استفاده از هوش مصنوعی در مبارزه با تروریسم سایبری است.

دو راه برای جلوگیری از حملات تروریستی وجود دارد. اولین مورد بازدارندگی است، هوش مصنوعی با محافظت از زیرساخت ها و اجرای کنترل های امنیتی، به حمایت فیزیکی آن ها کمک می کند و همچنین می تواند راهی برای شناسایی اهداف احتمالی تروریست ها باشد. جنبه دوم شامل جلوگیری از شروع حملات است که با دستگیری تروریست ها قبل از انجام برنامه های خود، مبارزه با استخدام تروریست ها و افراط گرایی در آینده، تحمیل محدودیت در حرکت و آزادی افراد مظنون انجام می شود. پیش بینی ضد تروریسم به نوعی هوش مصنوعی نیاز دارد که دانش و پیش بینی ها را از داده های دیجیتالی متنوع و وسیع استخراج کند. در بسیاری از موارد، تجزیه و تحلیل داده ها بدون چنین رویکردی غیرممکن خواهد بود. با این حال، مشکل این است که پیش بینی عملیات تروریستی نیاز به گسترش فضای نظارت برای افراد دارد که این مسئله محدودیت هایی را بر حقوق بشر از جمله حق بر حریم خصوصی تحمیل می کند. بنابراین، در آینده نزدیک، پیش بینی های موثری مبتنی بر تکنیک های هوش مصنوعی در مورد اینکه چه کسی با چه نوع نظارتی را باید تحت نظر گرفته شود، می تواند در کاهش میزان سوء استفاده از فضای سایبری نقش داشته باشد.(Madaou, 2023: 12-13)

ب- هوش مصنوعی و تسهیل ارتکاب تروریسم سایبری

مقابله با اقدامات تروریستی در فضای مجازی از جمله مواردی است که تحت عنوان مزایای ناشی از به‌کارگیری هوش مصنوعی مطرح شده است. اما توسل به این فناوری با وجود مزایای مختلف، به تسهیل ارتکاب تروریسم سایبری و نیز طرح نگرانی‌های جدی از سوی حامیان حقوق بشر، به‌دلیل نقض برخی از اصول بنیادین حقوق بشری انجامیده است. نگرانی‌هایی از این دست و نبود مقررات جامع و لازم‌الاجرا در زمینهٔ نظارت و کنترل آثار ناشی از کاربرد هوش مصنوعی، اتحادیهٔ اروپا را بر آن داشت تا با هدف قانونمندسازی فعالیت‌های مرتبط با هوش مصنوعی در بخش‌های مختلف، از جمله مقابله با اقدامات تروریستی، پیش‌نویس همسان‌سازی قوانین حاکم بر هوش مصنوعی را ارائه دهد.(رزمخواه، ۱۴۰۳: ۱)

هوش مصنوعی ممکن است به تروریست‌ها و سایر گروه‌ها در توسعه حملات سایبری پیچیده‌تر و خطرناک‌تر کمک می کند که احتمالاً پیامدهای جهانی را به همراه دارد. تروریسم سایبری را می توان به عنوان استفاده از رایانه و فناوری اطلاعات با انگیزه سیاسی برای ایجاد اختلال و ترس در بین غیرنظامیان

و هدف قرار دادن افراد، سازمان ها و دولت ها تعریف کرد. تروریست ها ممکن است از هوش مصنوعی برای اهداف تروریستی سایبری برای خودکارسازی حملات خود استفاده کنند و از تکنولوژی یادگیری اتوماتیک برای بهره برداری از ضعف های امنیت سایبری هدف خود استفاده نمایند. با استفاده از یادگیری ماشینی، هکرها می توانند الگوریتم هایی را توسعه دهند که پیچیده تر و دقیق تر هستند. هر بار که یک هکر سعی کند وارد یک سیستم شود و از طریق اتوماسیون شکست بخورد، حمله سایبری بعدی مرگبارتر خواهد بود. این به تروریست های سایبری پتانسیل باورنکردنی در میزان آسیبی که می توانند وارد کنند را ارائه می دهد. به عنوان مثال با توانایی هوش مصنوعی برای افزایش حملات در سطح جهانی، حمله باج‌افزار WannaCry در سال ۲۰۱۷ سازمان‌هایی را در بیش از ۱۵۰ کشور در سراسر جهان مورد حمله قرار داد و با استفاده از ویژگی‌های هوش مصنوعی باعث اختلال گسترده شد. این باج افزار صدها هزار رایانه را تحت تأثیر قرار داد و با بهره‌برداری از آسیب‌پذیری‌های رایانه‌های ویندوزی در سراسر شبکه‌ها گسترش یافت. در عرض چند ثانیه دیسک‌های سخت را فلج کرد و آغاز کننده حملات کپی‌برداری شد. یکی از بزرگ ترین مؤسساتی که تحت تأثیر قرار گرفته، «خدمات بهداشت ملی»[1]، در بریتانیا بود. حدود ۷۰۰۰۰ دستگاه، نه تنها از جمله رایانه‌ها، بلکه اسکنرهای MRI، یخچال‌های ذخیره‌سازی خون و سایر تجهیزات تحت تأثیر قرار گرفتند. در برخی موارد، آمبولانس‌ها و بیماران به دلیل عدم امکان ارائه خدمات به دلیل باج‌افزار، مجبور به تغییر مسیر شدند. این نشان می دهد که حملات سایبری عواقب تهدید کننده حیاتی دارند بنابراین امنیت سایبری به یکی از مهم ترین جنبه های امنیت ملی و بین المللی تبدیل شده است. این باج افزار نشان می دهد که چگونه تروریست ها می توانند از ویژگی های هوش مصنوعی برای تخریب گسترده استفاده کنند. گسترش مستقل باج افزار به دلیل استقلال و سرعت انتشار آن به عنوان یکی از ویژگی های هوش مصنوعی در نظر گرفته می شود. می توان تصور کرد که حملات سایبری که توسط هوش مصنوعی پشتیبانی می شوند چقدر مرگبارتر از حملات سایبری ارتکابی در گذشته خواهند شد و نیاز فوری به اقدامات امنیتی موثر و همیشه در حال تکامل، بیش از پیش هویدا گردیده است.(Nikolic, 2024)

اگرچه استفاده از هوش مصنوعی در مبارزه با تروریسم سیابری، مزایای گسترده ای دارد اما نباید از نظر دور داشت که هوش مصنوعی چالش هایی نیز در فرایند مقابله با تروریسم سایبری در پیش رو دارد،

[1] NHS

این چالش ها عبارتند از چالش های فنی: از قبیل تشخیص نادرست، وجود سوگیری در داده ها، ابهام و عدم شفافیت در نحوه تصمیم گیری، نقش بخش خصوصی در فرایندهای مرتبط با طراحی و توسعه هوش مصنوعی و نیز چالش های حقوقی مهمی چون نقض حق بر حریم خصوصی و نیز نقض قاعده منع تبعیض (رزمخواه، ۱۴۰۳: ۹-۱۴)

ج- هوش مصنوعی و تحول مفهوم امنیت

در ادبیات پژوهشی نوین در حوزه علوم سیاسی و حقوق بین الملل می توان تحقیقات رو به رشدی را یافت که ارتباط بین هوش مصنوعی و امنیت بین المللی را تحلیل می کند. این پرداخت وسیع به مقوله هوش مصنوعی و امنیت با در نظر گرفتن این نکته قابل درک است که روند توسعه هوش مصنوعی و پیاده‌سازی آن در حوزه امنیت، منجر به دگرگونی اساسی در نحوه انجام امور سیاسی و نظامی می‌شود. ارتباط بین هوش مصنوعی و امنیت بین‌المللی در این نهفته است که چگونه توسعه و پیاده‌سازی هوش مصنوعی خبر از انقلاب های آتی در امور سیاسی و نظامی می‌دهد و نحوه ورود دولت ها به تعاملات استراتژیک در عرصه هوش مصنوعی چگونه باید مدیریت شود.(Kopanja, 2023)

مسائل چالش برانگیزی که در نقطه تلاقی کاربردهای هوش مصنوعی و امنیت مطرح می شود دلالت بر این دغدغه های به غایت مهم دارد: هوش مصنوعی این امکان را خواهد داشت تا دوران جدیدی از صلح بین المللی را به ارمغان می آورد؟ آیا این امر منجر به تغییر توازن قدرت در صحنه جهانی می شود؟ هوش مصنوعی می تواند منجر به جابجایی گسترده و افزایش ناآرامی های سیاسی، ملی گرایی و حمایت گرایی شود؟ و... نا گفته پیداست که برخی از کاربردهای مستقیم هوش مصنوعی مربوط به اهداف امنیت ملی است. نمونه های بسیاری از این کاربردها در حوزه امنیت سایبری، امنیت اطلاعات، ابزارهای اقتصادی و مالی دولت‌سازی، دفاع، امنیت داخلی، دیپلماسی و توسعه وجود دارد که این موارد به عنوان نمونه های گویای کابرد هوش مصنوعی در حوزه امنیت ملی در نظر گرفته می شود.

به عنوان مثال در بحث امنیت سایبری، دامنه سایبری، یک عرصه بالقوه برجسته برای هوش مصنوعی است. در اکتبر ۲۰۱۶، مایکل راجرز، مدیر آژانس امنیت ملی[1] اظهار داشت که این آژانس هوش مصنوعی را «پایه ای برای آینده امنیت سایبری» می داند. نقش هوش مصنوعی در تغییر چشم‌انداز تهدیدات علیه امنیت داده ها نیز حائز اهمیت است. این تکنولوژی نوین پیامدهای جدی برای امنیت اطلاعات دارد که

[1] NSA

نشان‌دهنده تأثیر گسترده‌تر هوش مصنوعی از طریق ربات‌ها و سیستم‌های مرتبط در عصر اطلاعات است. استفاده از هوش مصنوعی می تواند اثرات اطلاعات نادرست را در یک سیستم اطلاعاتی در حال تکامل، تشدید نموده و یا کاهش دهد. به طور مثال هوش مصنوعی در حملات سایبری، مکانیسم‌هایی را برای تطبیق تبلیغات با مخاطبان هدف و همچنین افزایش انتشار داده های نادرست یا بدافزارها در مقیاس بالا فراهم می‌کند. در حوزه جرایم بین المللی و نقض امنیت بین المللی باید افزود، هوش مصنوعی می تواند وجوه غیرقانونی را از طریق سیستم های مالی بین المللی انتقال دهد و از تروریسم، پولشویی و گسترش سلاح های کشتار جمعی حمایت مالی کند. در حوزه نظامی، از آن جایی که امروزه نیروهای نظامی در سرتاسر جهان در حال حاضر تکنولوژی مبتنی بر رباتیک و سیستم‌های خودکار بیشتری را با نیروهای فیزیکی خود ترکیب می‌کنند، هوش مصنوعی به این سیستم‌ها اجازه می‌دهد تا وظایف چالش برانگیزتری را در طیف وسیع‌تری از فعالیت های نظامی انجام دهند. به دلیل ماهیت فراگیر فناوری هوش مصنوعی، گروه ها و افراد غیر دولتی نیز می توانند از این فناوری استفاده کنند که این خود چالشی نوین در دسترسی تروریست ها به چنین فناوری هایی است. (Horowitz and others, 2018: 4-10) هوش مصنوعی در دیپلماسی عمومی و دیپلماسی داده ها، سیاست امنیتی، نظریه های مدرن ارتباطات استراتژیک ورود جدی نموده است، تا جایی که در نشست اولین کمیته (خلع سلاح و امنیت بین‌الملل) در سال۲۰۲۳ در مورد هوش مصنوعی و امنیت بین المللی، اعلام شد بدون محافظت کافی، هوش مصنوعی امنیت جهانی را از الگوریتم ها تا تسلیحات تهدید می کند، مسائل سایبری به موضوعات مورد توجه سیاست خارجی تبدیل شده است این که چگونه استفاده از علم و فناوری می تواند امنیت را تضعیف کند. مقیاس چالش ها مستلزم یک پاسخ چند جانبه چند جانبه و کل نگر است. مسائل سایبری به موضوعات استراتژیک سیاست خارجی تبدیل شده است که نگرانی فوری برای همه کشورها دارد، در بدایت امر به نظر می رسد راه حل رفتار مسئولانه دولت مطابق با چارچوب سازمان ملل متحد در فضای سایبری و همچنین به اشتراک گذاری عمومی نحوه اجرا، تفسیر و رعایت این چارچوب است تا در این رهگذار شفافیت، مسئولیت پذیری، پیش بینی پذیری و ثبات ایجاد شود. (press.un.org) نهایتاً باید گفت فرصت های تکنولوژیکی که هوش مصنوعی ایجاد می کند آینده را شکل می دهد، اما آن را تعیین نمی کند. ملت ها، گروه ها و افراد در مورد نحوه به کارگیری و واکنش به کاربردهای مختلف هوش مصنوعی، انتخاب هایی دارند. پاسخ‌های آن ها می‌تواند استفاده‌های خاصی از هوش مصنوعی را راهنمایی، محدود یا تشویق کند. به منظور مدیریت چالش های پیش رو، دولت ها

باید یک استراتژی ملی برای نحوه استفاده از مزایای هوش مصنوعی و در عین حال کاهش اثرات مخرب آن اتخاذ کند.(Horowitz and others, 2018: 22) در بحث حاکمیت و امنیت ملی باید گفت، هوش مصنوعی می تواند حکمرانی دولت ها را با چالش جدی مواجه کند؛ به وسیله این فناوری دولت های اقتدارگرا، از سطح اقتدار بیشتری بهره خواهند برد، کشورهای ضعیف همچنان از توسعه عقب خواهند ماند و کشورهای مردم سالار با چالش های حکمرانی بیشتر مواجه خواهند شد، لذا تمامی دولت ها در هر سطح بهره مندی از هوش مصنوعی باید خط مشی و سیاست های خود را در پرتو هوش مصنوعی مورد بازنگری جدی قرار دهند. **امنیت** نظامی، اقتصادی، سیاسی و اجتماعی در آینده به شکل وسیعی از هوش مصنوعی تاثیر خواهد پذیرفت، لذا با این پیش فرض که طراحی، توسعه و استفاده از هوش مصنوعی برای امنیت ملی طیف گسترده ای از چالش های قانونی و اخلاقی را به همراه دارد، استراتژی ها و خط مشی های امنیتی موجود باید باز تعریف شوند و البته یکی از مهم ترین این حوزه ها امنیت سایبری است.

۴. ظرفیت های هوش مصنوعی و امنیت ملی جمهوری اسلامی ایران

امنیت ملی گستره ای مطول از عوامل سخت، از قبیل پهنه جغرافیایی، قدرت نظامی و نرم مثل فرهنگ و انسجام ملی، هویت منسنجم و واحد، سطح آموزش شهروندی، سطح رشد اقتصادی، محیط زیست و ... را شامل می گردد. گرچه هوش مصنوعی روزبه روز در تمامی ساحات زندگی بشر و امور حکمرانی رو به رشد می باشند، لیکن این فناوری تهدیدها و فرصت هایی را برای امنیت دولت ها به دنبال دارد و از این رو، دولت ها را به این تفکر وامی دارد که در استراتژی های امنیت ملی خود حوزه جدیدی پیرامدن هوش مصنوعی و کاربردهای آن در نظر گرفته و آن ها را ملزم به پیشبینی بودجه های لازم برای تحقیق و توسعه در این راستا می نمایند. دولت ها و دیگر بازیگران نظام بین الملل برای کاهش خطرات ناشی از این فناوری می باید از ظرفیت های بین المللی نظیر کنوانسیون ها، سازمان های بین المللی، رویه ها و قواعد بین المللی برای تدوین رژیم های حقوقی بین المللی و نظارت بر عملکرد صاحبان هوش مصنوعی استفاده نمایند. (احمدی، زرگر و آدمی، ۱۴۰۲: ۲۳)

قابلیت های هوش مصنوعی پتانسیل قابل توجهی برای امنیت ملی دارد. هوش مصنوعی با ایجاد تغییرات در سه زمینه بر امنیت ملی تأثیر می گذارد: الف) برتری نظامی، پیشرفت در هوش مصنوعی هم قابلیت های جدید را فراهم می کند و هم قابلیت های موجود را برای طیف وسیع تری از بازیگران مقرون به

صرفه می کند. در حوزه سایبری، فعالیت هایی که در حال حاضر به نیروی کار با مهارت زیاد نیاز دارند، مانند عملیات علیه تهدیدات پیشرفته، ممکن است در آینده تا حد زیادی خودکار و به راحتی در دسترس باشند. ب) برتری اطلاعاتی، هوش مصنوعی قابلیت های جمع آوری و تجزیه و تحلیل داده ها و همچنین ایجاد داده های جدید را به طرز چشمگیری افزایش می دهد اما به همان میزان جعل رسانه ها، با هوش مصنوعی به سرعت در حال بهبود کیفیت و کاهش هزینه است و ج) حوزه برتری اقتصادی، این نظریه بسیار مطرح است که پیشرفت‌های هوش مصنوعی می‌تواند منجر به یک انقلاب صنعتی جدید شود. (belfercenter.org) در حوزه تلاقی هوش مصنوعی، حملات سایبری و امنیت ملی نیز در سرتاسر جهان، سازمان‌های اطلاعاتی از قدرت هوش مصنوعی برای افزایش قابلیت‌های خود به روش‌های مختلف استفاده می‌کنند. به عنوان مثال، الگوریتم های هوش مصنوعی در حال بررسی مجموعه داده های گسترده ای از ترافیک ارتباطات جهانی، تصاویر ماهواره ای و پست های رسانه های اجتماعی هستند تا تهدیدات بالقوه امنیت سایبری، فعالیت های تروریستی و تحولات ژئوپلیتیکی را شناسایی کنند. این تحلیل‌های پیش‌بینی‌کننده، می‌تواند به آژانس‌های امنیتی کمک کند تا حملات تروریسم سایبری را خنثی کنند و به بحران‌های ژئوپلیتیکی نوظهور واکنش مؤثرتری نشان دهند. در امنیت سایبری، سیستم‌های مبتنی بر هوش مصنوعی به طور مداوم شبکه‌ها را رصد می‌کنند و به سرعت حملات سایبری را شناسایی کرده و به آن ها پاسخ می‌دهند. هوش مصنوعی در سیستم های خودران نیز نقش مهمی ایفا می کند. پهپادهای مبتنی بر هوش مصنوعی می توانند مأموریت های نظارتی، شناسایی و حتی جنگی را با کمترین مداخله انسانی انجام دهند. این پیشرفت ها اگرچه کارایی را افزایش می دهد، در عین حال خطرات را نیز برای پرسنل انسانی کاهش می دهد. در حوزه فناوری تشخیص چهره، با استفاده از هوش مصنوعی می‌توان به سرعت چهره‌ها را با فهرست‌های نظارتی مقایسه کرد و این به شناسایی و دستگیری سریع مظنونان کمک می کند. (onlinewilder.vcu)

استفاده از پهپاد ها در جاسوسی از مراکز هسته ای، استفاده از هوش مصنوعی در ترور شخصیت ها و حملات سایبری به زیرساخت های حیاتی ایران از جمله در قضیه بدافزار استاکس نت، نیاز به تدوین سیاست های کلان دولت در بهره مندی از ظرفیت های هوش مصنوعی از حمله در پیش بینی حملات و نیز شناخت میزان آسیب پذیری در این حوزه را، بیش از پیش مهم می نماید. جمهوری اسلامی ایران این تعیین سیاست و چارچوب را در سند ملی هوش مصنوعی جمهوری اسلامی ایران که در جلسه ۹۰۱ تاریخ ۲۹ خردادماه ۱۴۰۳ شورای عالی انقلاب فرهنگی به تصویب رسیده، به انجام رسانیده است.

فرصت‌های قابل توجه حاصل از پیشرفت علم و فناوری در کنار توان قابل‌ملاحظه آن برای درک مسائل و همچنین قدرت پیشگیرانه آن در مهار بحران‌ها و مشکلات پیش روی جوامع، موجب شده است تا در سطح بین‌المللی در اسناد ملی و برنامه‌های کلان، سرفصل مهمی به این موضوع اختصاص یابد. کشورهای پیشرو با استفاده از تکنولوژی هوش مصنوعی برای شناسایی و پیشگیری از تهدیدات سایبری، سیستم‌های دفاعی هوشمندی ایجاد کرده‌اند. ایران نیز باید با تدوین قوانین و قواعد لازم از هوش مصنوعی برای پیشگیری و شناسایی تهدیدات سایبری بهره‌برداری کند. اجرای موثر این قوانین در پرتو سند ملی به توسعه سیستم‌های هوشمند امنیت سایبری و استفاده از الگوریتم‌های هوش مصنوعی برای شناسایی تهدیدات سایبری می انجامد.

تدوین سند ملی هوش مصنوعی جمهوری اسلامی ایران گام مهمی برای وصول به مؤلفه‌های تمدن نوین اسلامی، ارتقای کیفیت حکمرانی و تقویت بنیان‌های علمی و پژوهشی در راستای پیشرفت کشور در همه عرصه‌های مرتبط با حکمرانی منطقه‌ای و ملی و ارتباطات جهانی است. همچنین هوش مصنوعی در همه قلمروهای اولویت‌دار از قبیل آموزش و پژوهش، بهداشت و درمان، حکمرانی دولتی و خدمات عمومی، دفاعی، امنیتی و انتظامی، صنایع، انرژی، محیط زیست و کشاورزی، فرهنگ ایرانی و تمدن اسلامی، رسانه و فضای مجازی و امور مرتبط با فناوری‌های مهم و راهبردی اعم از هوافضا، فناوری زیستی، فناوری نانو، علوم شناختی و سایر عرصه‌های علم و فناوری، منشأ تغییر و تحولات بزرگ است. (سند ملی هوش مصنوعی جمهوری اسلامی ایران، ۱۴۰۳)

این سند در برخی مواد، در حوزه مورد بحث مقاله حاضر نیز مندرجات قابل ملاحظه ای دارد: در ماده ۲ در بیان اصول و مبانی ارزشی، حفظ استقلال، امنیت، منافع و اقتدار ملی در مواجهه با توسعه فناوری هوش مصنوعی، حفاظت از امنیت داده‌ها و اطلاعات در زیست‌بوم هوش مصنوعی؛ مواجهه هوشمندانه با قدرت‌های بزرگ با رویکرد انحصارزدایی و ... مورد تاکید قرار گرفته است. ماده ۳ به چشم‌انداز، اهداف کلان و شاخص‌های ارزیابی پرداخته و اهداف سند را در راستای تحقق چشم‌انداز و بهره‌گیری از هوش مصنوعی به عنوان زیست‌بوم اثرگذار بر همه عرصه‌های اقتصادی، سیاسی – امنیتی و فرهنگی با رویکرد تأمین پیشرفت اسلامی – ایرانی کشور معرفی می نماید. ماده ۵ به عنوان یکی از مهم ترین مواد این سند، راهبردها و اقدامات ملی را در زیرساخت‌های حکمرانی چنین توصیف نموده است: ایجاد و ارتقای زیرساخت‌های فنی، قانونی، تنظیم‌گری و استانداردها برای جهت‌دهی، شتاب‌دهی و گسترش هوش مصنوعی با تدوین نظام حکمرانی داده با حفظ ملاحظات امنیت ملی، رعایت حریم خصوصی و

اخلاق عمومی و تدوین استانداردهای مربوط به مالکیت، تولید، نگهداری، تبادل و به‌اشتراک‌گذاری داده و همچنین ایمنی و امنیت سیستم‌ها و خدمات هوش مصنوعی. ماده ۶ سند نیز، به اولویت های ملی به‌کارگیری هوش مصنوعی اشاره دارد و عرصه‌های اقتصادی، سیاسی- امنیتی را جزو این حوزه ها معرفی نموده است.

لذا از بررسی مندرجات سند ملی هوش مصنوعی و پرداختن به مسائلی چون امنیت سایبری، امنیت داده ها، رعایت مبانی حقوق بشری چون حفظ حریم خصوصی و منع تبعیض در کنار توجه به حوزه های سنتی امنیت از جمله، امنیت سیاسی و اقتصادی، این گونه برمی آید که، در بحث کنونی امنیت ملی، دیگر نمی‌توان تنها به شیوه‌ها و تاکتیک‌های امنیتی سنتی مانند تجزیه و تحلیل اطلاعاتی یا بهره مندی از تکنولوژی سایبری صرف تکیه کرد. در عوض، باید مهارت های تکنولوژیکی خاصی را داشت تا قادر بود تا به طور موثر از ابزارهای هوش مصنوعی استفاده نمود. این مهارت ها ممکن است شامل درک جامعی از الگوریتم های هوش مصنوعی، تجزیه و تحلیل داده ها و تکنیک های امنیت سایبری باشد و البته همکاری بین المللی با سازمان ها و دولت هایی که تجارب خوبی در این زمینه دارند نباید دور از نظر باشد.

نتیجه گیری

با به روز شدن حملات سایبری در سطح تروریسم یا حتی جنگ سایبری، سیستم‌های امنیت سایبری مبتنی بر هوش مصنوعی می‌توانند دانش به‌روز خور را در مورد تهدیدهای خاص جهانی را به کاربرده تا به تصمیم‌گیری‌های مهم در اولویت‌بندی واکنش به آن حمله منجر شوند. هوش مصنوعی می‌توانند پیش‌بینی کنند که چگونه و در کجا احتمال نفوذ وجود دارد، بنابراین به درک نقاط قوت و ضعف سیستم های امنیتی کمک شایانی می کند. از سوی دیگر از آن جایی که هوش مصنوعی با سرعتی باورنکردنی به توسعه خود ادامه می دهد، زیربنای امنیتی نیز باید همزمان با آن تغییر کرده و توسعه پیدا کنند. تاثیر هوش مصنوعی بر امنیت فیزیکی و سایبری بسیار قابل توجه است زیرا تروریست ها و سایر جنایتکاران از آن به نفع خود استفاده می کنند، هوش مصنوعی پتانسیل بالایی برای حملات ارائه می دهد و به آن ها برتری نامتقارنی نسبت به نهادهای دولتی می دهد. با توجه به ماهیت فراملی هوش مصنوعی و تأثیر آن، باید واکنش قوی و نهادینه نسبت به آن در سطح جهانی وجود داشته باشد. در نهایت، پتانسیل هوش مصنوعی برای ایجاد بی‌ثباتی و تخریب بسیار زیاد است و نیاز به واکنش به آن در سطح ملی و بین‌المللی

وجود دارد. از سوی دیگر باید گفت صلح و امنیت در طول تاریخ به دلیل فاصله گرفتن انسان از اخلاق و ارزش‌های الهی، به کرات تهدید و نقض شده و امروزه، این وضعیت به سطحی ناگوار و وخیم منتهی شده است: شکاف عمیق میان جوامع، موجب شکل‌گیری طبقات غنی و فقیر در روابط بین‌المللی شده و برخی دولت‌ها با تمرکز و انحصار قدرت‌های مادی، جهان را به صحنه‌ی هژمونی و یک جانبه‌گرائی خود تبدیل کرده‌اند. (قربانی و سیمبر، ۱۳۸۸: ۱۵۴– ۱۴۶) امنیت، صلح و حقوق بشر غایت تلاش های بین المللی است. با پیشرفت تکنولوژی های نوظهور همواره این مفاهیم در معرض بازتعریف قرار داشته اند. چه زمانی که سلاح های غیر متعارف توسط دولت ها به کار گرفته شد و چه زمانی که فضای سایبر، جنگ سایبری را وارد گفتمان امنیت نمود.

تروریسم سایبری به عنوان یکی از تهدیدات القوه فراروی امنیت بین المللی و صلح جهانی است، این در حالی است که هیچ سند بین المللی لازم الاجرایی این جنایت علیه صلح و امنیت بین المللی را تعریف نکرده و کنوانسیون های موجود در بیان برخی مصادق آن توفیق یافته اند. این امر نشان گر مطلوبیت جرم انگاری و مبارزه با تروریسم در تمامی انواع آن در قوانین ملی است. این اقدامات در بسیاری از موارد خود نقض صلح و حقوق بشر را در پی داشته است. تا زمانی که صلح و امنیت با موازین حقوق بشر و حقوق بشر دوستانه همراه نباشد، صلح عادلانه محقق نمی شود. هدف جامعه جهانی باید «ائتلاف علیه تروریسم برای صلح عادلانه» باشد، ائتلافی که در آن همکاری بین المللی به سمت هماهنگی بین المللی پیش رود. تا آن زمان اقدامات دولت ها باید در راستای تعین محورهای مبارزه با تروریسم سایبری با توجه به معیارهای حقوق بشر و بشر دوستانه باشد. با توجه به ابعاد گسترده تروریسم سایبری باید گفت نه تنها امنیت نظامی در راستای این مفهوم تحول یافته بلکه دادهای دیجیتال، دولت الکترونیک، بانکداری الکترونیک، امنیت هوایی و بسیاری از حوزه های زیرساختی حیاتی دولت ها امروزه متکی به امنیت سایبری است. تهدیدات و تروریسم سایبری نه تنها امنیت ملی و بین المللی تأثیر را به خطر انداخته، امنیت اقتصادی و انسانی را نیز مورد تهدید و نقض قرار داده در حالی که تنها سازمان های امنیت محوری چون ناتو در مرکز عالی دفاع سایبری، در مبارزه با آن با جمیع راهکارهای فنی و حقوقی، توانسته اند به توفیق دست یابند. چالش های نوین حاصل از هوش مصنوعی نیاز به رویکردهای نوین امنیتی در حوزه روابط بین الملل را بیش از پیش متجلی نموده است. تهدیدی با ماهیت جهانی، اراده و شیوه های بین المللی برای مبارزه را طلب می کند و حاکمیت ها اگرچه همچنان تمایل به جرم انگاری و مبارزه با تروریسم سایبری در حوزه صلاحیت ملی خود دارند، با توجه به ماهیت

فراسرزمینی این پدیده توفیقی در سرکوب آن به شیوه منفرد نخواهند یافت. همکاری های موثر در کاهش چنین تهدیداتی می تواند می تواند چندین مزیت داشته باشد، از جمله به اشتراک گذاری دانش علمی، آژانس های ملی مختلف می توانند سطوح مختلفی از تخصص و بینش در مورد فناوری های هوش مصنوعی داشته باشند. همکاری به آن ها اجازه می دهد تا دانش خود را با هم ترکیب کنند، بهترین شیوه ها را به اشتراک بگذارند و از تجربیات یکدیگر بیاموزند. دیگری بهینه سازی منابع است. تلاش های مشترک اغلب منجر به تخصیص کارآمدتر منابع می شود. دولت ها می‌توانند به طور جمعی در برنامه‌های آموزشی هوش مصنوعی سرمایه‌گذاری کنند و اطمینان حاصل کنند که مؤثرترین روش‌های آموزشی به کار گرفته می‌شوند. مزیت دیگر امنیت اطلاعات است. به اشتراک گذاری اطلاعات و استراتژی ها بین دولت ها می تواند تاثیر اقدامات امنیتی را افزایش دهد. به عنوان مثال، آموزش مشترک امنیت سایبری می تواند به متخصصان کمک کند تا در برابر تهدیدات مبتنی بر هوش مصنوعی بتوانند واکنش به موقع و موثر داشته باشند.

منابع

احمدی، علی، زرگر، افشین، آدمی، علی. (۱۴۰۲).«فناوری هوش مصنوعی و تغییر در امنیت ملی دولت‌ها»، ***سیاست دفاعی***، ۹۲، ۱۲۳

اشرافی، داریوش (۱۳۹۳). «تفسیر جدید از صلح و امنیت بین المللی و تأثیر آن بر مفهوم حاکمیت ملی»، فصلنامه پژوهش حقوق عمومی، سال پانزدهم، شماره ۴۲.

آنجلیز، جینا دی (۱۳۸۳). **جرایم سایبر**، ترجمه سعید حافظی و عبدالصمد خرم آبادی، نشر دبیرخانه شورای عالی اطلاع رسانی.

بندک، ولفگانگ و مانگوپولوس، آلیس (۱۳۸۹). **تروریسم و حقوق بشر**، ترجمه: محمد جعفر ساعد و دیگران: دادگستر.

تریف، تری و دیگران (۱۳۸۳). **مطالعات امنیتی نوین**، مترجمین علی رضا طیب، وحید بزرگی، تهران: پژوهشکده مطالعات راهبردی.

حسن بیگی، ابراهیم (۱۳۸۴). **حقوق و امنیت در فضای سایبر**، تهران: موسسه فرهنگی مطالعات وتحقیقات بین المللی ابرار خلیلی پور رکن آبادی، علی و نورعلی وند، یاسر (۱۳۹۱). «تهدیدات سایبری و تاثیر آن بر امینت ملی»، فصلنامه مطالعات راهبردی، سال پانزدهم، شماره دوم.

رزمخواه، نجمه (۱۴۰۳). «نقدی بر پیش‌نویس قانون اتحادیهٔ اروپا در همسان‌سازی قوانین حاکم بر هوش مصنوعی، از منظر مقابله با تروریسم سایبری»، ***فصلنامه مطالعات حقوق عمومی دانشگاه تهران***.

سند ملی هوش مصنوعی جمهوری اسلامی ایران، ۱۴۰۳

سید محمد رضا موسوی، خدیجه حیدری، و علی قنبری (۱۳۹۲). «تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن»، مطالعات بین المللی پلیس، شماره ۱۴.

سیمبر، رضا، قربانی، ارسلان (۱۳۸۸). «دیپلماسی نوین در روابط خارجی؛ رویکردها و ابزارهای متغیر»، فصلنامه بین المللی روابط خارجی، شماره ۴.

شفیعی، نوروز (۱۳۸۹). «تحول در مفهوم صلح»، Available at: http://drshafie.blogfa.com/post-93.aspx

عبدالله خانی، علی (۱۳۸۲). **نظریه های امنیت: مقدمه ای بر طرح ریزی دکترین امنیت ملی**، جلد اول، تهران: موسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران.

قبادی، مرضیه (۱۳۹۴). «تحول مفهوم امنیت در پرتو دستاوردهای حقوق بشر معاصر و آثار حقوقی آن»، رساله دکتری حقوق بین الملل، دانشکده حقوق دانشگاه علوم و تحقیقات تهران.

نای، جوزف (۱۳۸۷). «قدرت در عصر اطلاعات: از واقعیت تا جهانی شدن»، ترجمه سعید میرترابی، تهران: پژوهشکده مطالعات راهبردی.

همپستون، فن اوسلر(۱۳۹۰). **امنیت انسانی، در درامدی بر بررسی های امنیت**، ویراسته پل ویلیامز، ترجمه علی رضا طیب، تهران: موسسه انتشارات امیرکبیر.

وکیل، امیر ساعد و عسکری، پوریا (۱۳۸۴). **نسل سوم حقوق بشر**، چاپ اول، انتشارات مجد.

یزدان فام، محمود (۱۳۸۶). **دگرگونی در نظریه ها و مفهوم امنیت بین المللی**، فصلنامه مطالعات کاربردی شماره ۳۸.

Artificial Intelligence (AI) Challenges and Advantages in National Security, December 6, 2023, available at: *https://onlinewilder.vcu.edu/blog/ai-challenges-and-opportunities-national-security/*

Convention on cyber crime, Budapest, 23, XI, 2001

KATHLEEN, M. (2019). Artificial Intelligence Prediction and Counterterrorism. Britain: Chattam House.

Kopanja, Mihajlo. (2023). Artificial intelligence and international security: The upcoming revolution in military affairs. Socioloski pregled. 57. 102-123.

Michael Horowitz, Paul Scharre, Gregory C. Allen, Kara Frederick, Anthony Cho and Edoardo Saravalle (2018), "Artificial Intelligence and International Security", Center for a New American Security available at: https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security

Nadjia, Madaoui, (2023). The role of artificial intelligence in combating cyber terrorism, Lounici Ali, University of Blida2, Algeria.

Nikolic, Mateja, (2024), Artificial Intelligence: Terrorism and International Relations, *Center for International Relations and Sustainable Development, available at:* https://www.cirsd.org/en/young-contributors/artificial-intelligence-terrorism-and-international-relations