

## 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](mailto:mohsen.khakzad777@gmail.com)

**Leila Mirbod** Instructor, Department of Law, Rasht Branch, Islamic Azad University, Rasht, Iran. E-mail: [Leila\\_mirbod@yahoo.com](mailto: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



© Author(s)

**Publisher:** Iranian Association of International Studies

**DOI:** 10.22034/irr.2024.463239.2557



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی

## 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](mailto:mohsen.khakzad777@gmail.com)

لیلا میربد مدرس گروه حقوق، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران.

ایرانیه: [Leila\\_mirbod@yahoo.com](mailto:Leila_mirbod@yahoo.com)

چکیده	درباره مقاله
<p>صلح و امنیت در بعد ملی و بین المللی در دوره های متوالی، تعبیر 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 دگرین حقوق بین الملل و حقوق بین الملل عرفی به مثابه برهم زنده 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 - 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 مخمل 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 کار خود قرار دهند.</p>	<p>نوع مقاله: مقاله پژوهشی</p> <p>کلیدواژه‌ها: امنیت سایبری، صلح بین المللی، امنیت انسانی، تروریسم سایبری، هوش مصنوعی</p> <p>تاریخچه مقاله تاریخ دریافت: ۱۴۰۳/۶/۸ تاریخ پذیرش: ۱۴۰۳/۹/۲۵</p>

استاد به این مقاله: خاکزاد شاهاندشتی، محسن و 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

© نویسنده (گان)

ناشر: انجمن ایرانی روابط بین الملل





برقراری صلح و امنیت امروزه غایت تلاش‌های بین‌المللی دولت‌ها و ملت‌هاست. از نگاه نظام و ستفالیایی، 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 مسالمت‌آمیز اختلافات تلقی می‌شده است. از این زاویه، حاکمیت و استقلال دولت‌ها مهم‌ترین رکن امنیت بین‌المللی 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 بین‌الملل، 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 تجزیه‌ناپذیر 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 بین‌الملل، 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 می‌زند و باعث طرح دعوا علیه دولت‌ها نیز می‌شود. رای اخیر دیوان اروپایی حقوق بشر در دعوی زنان شهروند سوئیس و انجمن ورین کلیماسنیورین<sup>۱</sup> 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 بیماری‌های دوره سالخوردگی در معرض خطر مرگ قرار داده است. گرمایش ناشی از تغییرات آب و هوایی به کیفیت زندگی افراد لطمه می‌زند و آنان را حتی در معرض خطر مرگ قرار می‌دهد و این نقض امنیت روانی نه تنها یک ملت بلکه امنیت بین‌المللی می‌شود. در صورتی که پنجاه سال پیش، چنین امری متصور نبود و جزو دغدغه‌های امنیتی دولت‌ها نیز به شمار نمی‌رفت. این بدان

<sup>1</sup> Verein KlimaSeniorinnen



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



برای مجریان قانون و دولت‌ها ایجاد می‌کند که نیازمند رویکردی چندوجهی است. تروریسم سایبری می‌تواند اثرات مخربی بر طیف وسیعی از افراد و سازمان‌ها 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، زیرساخت‌های حیاتی مانند شبکه‌های برق، بیمارستان‌ها و سیستم‌های حمل و نقل می‌توانند مختل شود و امنیت ملی به مخاطره افتد. بررسی حوادث سایبری تروریسمی که در ده سال گذشته رخ داده است، تأثیرات آن‌ها بر اقتصاد کشور، بی‌ثباتی سیاسی و نیز اقدامات اتخاذ شده برای مقابله با آن حایز اهمیت است و می‌تواند به توسعه استراتژی‌ها و سیاست‌های بهتر برای مقابله با تروریسم سایبری کمک کند.»

سرنا بیانچی و همکاران در مقاله‌ای با عنوان هوش مصنوعی و مبارزه با تروریسم سایبری (۲۰۲۳) در حوزه اهمیت استفاده از هوش مصنوعی در تسهیل ارتکاب تروریسم سایبری آورده‌اند: «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 رضا زاده 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 می‌گردد. افزایش سریع کاربران اینترنت و اتکاء به آن به طرز نگران‌کننده‌ای ریسک‌های امنیتی را افزایش داده است علیرغم اینکه تدابیر امنیتی مناسبی برای کمک به پیشگیری از ریسک‌های امنیتی وجود داشته ولی کافی نبوده است. این تهدیدات می‌تواند به طور بالقوه، امنیت ملی ایران و زیرساخت‌های حیاتی آن را مورد آسیب قرار دهد. ترکیبی از راهکارهای پیشگیرانه اجتماعی و موقعیت‌مدار می‌تواند مناسب باشد که شامل بهره‌گیری از خبرگان، جرم‌انگاری براساس پیشرفت‌های تکنولوژی، آگاه‌سازی و اطلاع‌رسانی همگانی، اقدامات آموزش محور، افزایش و ارتقای درجه رفاه همگانی و مهیا سازی زمینه و بستر عدالت اجتماعی است.»



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



می‌کند. تمام این مکاتب جایگاه خود را در نقطه مابین دو قطب افراطی آرمان‌گرایی و واقع‌گرایی حفظ کرده‌اند. اندیشه ایجاد صلح از طریق روابط بازرگانی و تفکر 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 مواجه کند. (نای، ۱۳۸۷: ۱۲۴). گذشته از مفهوم امنیت در زمینه داخلی و بین‌المللی، صلح نیز از جمله مفاهیم مورد مناقشه در حقوق و روابط بین‌الملل است. صلح را باید چیزی فراتر از فقدان جنگ دانست.<sup>۱</sup> 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 معمولاً 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 بین‌الملل، قدرت و منافع ملی به مقوله امنیت می‌پردازند. واقع‌گرایان امنیت ملی را همان امنیت بین‌المللی شناسایی

<sup>۱</sup> 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.





پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



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 مجموعه ای از حملات با انگیزه های سیاسی، مذهبی و یا ایدئولوژیک و که با هدف القا ترس و تخریب صورت می گیرد تعریف کنیم، بسیاری از حوادثی که در سال های اخیر اتفاق افتاده اند می توانند نمونه هایی از تروریسم سایبری باشند. بنابراین می توان به تحلیل گفتمان تروریسم سایبری از یک زاویه مطالعات امنیتی پردازیم. 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 می کند، این امر با ورود هوش مصنوعی نیز پیچیدگی های خاص خود را به دنبال دارد. امروزه سازمان های ارائه دهنده خدمات، سیستم های مالی و بانکداری، شبکه های ارتباطات اجتماعی، روزنامه نگاری و حتی پلیس، سازمان ها و تشکیلات امنیتی با طبقه بندی های حفاظتی به فضاهای مجازی ورود پیدا کرده و از این عرصه برای تسهیل ارتباطات و کارکردها بهره می گیرند. 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 سازمان ها و دستگاه های اداری را تشکیل داده است.

به امنیت فناوری اطلاعات، وابسته به سیاست دولت ها، امنیت سایبری گفته می شود. امنیت سایبری یا امنیت اینترنتی به جوانب امنیت شبکه و اصول سیاست گذاری شبکه ها 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 مقوله ای استراتژیک قلمداد می شود و به همین دلیل است که در ارزیابی از تهدیدات امنیت ملی و بین المللی، مفهوم امنیتی فضای سایبری، وارد اسناد پایه ای امنیتی شده است. (موسوی، حیدری و قنبری، ۱۳۹۲: ۸-۹) توانایی استفاده از فضای سایبری، یکی از مهم ترین منابع قدرت در قرن ۲۱ به حساب می آید. بازیگران دولتی و غیردولتی از این قدرت استفاده می کنند تا به اهداف اجتماعی، ایدئولوژیک، سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی دست یابند. از منظر امنیت ملی می توان گفت که در شرایط حاضر، دولت ها و ملت ها با زنجیره ای از تهدیدات نامشخص در محیط های مجازی مواجهند که امنیت آن ها را به چالش



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



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 بین‌المللی 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 آسیب‌پذیری‌های 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



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



### ۲-۳. 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 بین‌المللی 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 بی‌رویه، بیماری‌های مسری، سلاح‌های کشتار جمعی و تروریسم سایبری را شامل می‌گردد.<sup>۱</sup> فناوری ارتباطات، اهمیت و فراوانی داده‌های حیاتی و تعدد کنش‌گران بین‌المللی، فضای سایبر را نیز به حوزه‌های امنیت داخلی و بین‌المللی وارد نموده است.

امنیت بین‌الملل تدریجاً مفهوم وستفالیایی خود را از دست می‌دهد و بازیگران فراملی 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 بین‌المللی 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، گروگان‌گیری 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 خطرناک‌تر از حملات تروریستی سنتی و کلاسیک است. تروریسم سایبری ممکن است برای تعداد کثیری از مردم بسیار ویران‌کننده‌تر 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 سرمایه‌گذاری کلان، امکان حمله و آسیب به

<sup>۱</sup> 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 فیما بین دولت‌ها، مخاصمات داخلی از قبیل جنگ‌های داخلی و نسل‌کشی، تولید و گسترش سلاح‌های شیمیایی، بیولوژیکی و هسته‌ای، تروریسم و جرایم سازمان یافته. (اشرافی، ۱۳۹۳: ۹۱)



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



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 روش های نرم افزار محور واکنش مؤثرتری از خود نشان می دهند. در سال های اخیر، هوش مصنوعی به عنوان فناوری مورد نیاز برای تقویت تیم های امنیت اطلاعات نیز ظاهر شده است. از آن جایی که انسان ها نمی توانند به اندازه کافی از امنیت سایبری به شیوه های قبلی محافظت کنند، هوش مصنوعی تجزیه، تحلیل و شناسایی تهدید مورد نیاز را ارائه می کند که می تواند توسط متخصصان امنیت سایبری برای کاهش خطر نقض و بهبود وضعیت امنیتی به کار گرفته شود. در زمینه امنیت، هوش مصنوعی می تواند خطر را شناسایی و اولویت بندی 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 تیم های امنیت سایبری اجازه می دهد تا مشارکت های انسانی و ماشینی قدرتمندی را ایجاد کنند که مرزهای دانش ما را جابجا می کند، زندگی ما را غنی می کند و امنیت سایبری را به گونه ای هدایت می کند که بیشتر از مجموع اجزای آن به نظر می رسد باید دانست هوش مصنوعی یک شمشیر دولبه است که می تواند 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 بین الملل از اهمیت بالایی 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.





پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



و افرادی که به نظر می‌رسد 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 زیرساخت‌ها و اجرای کنترل‌های امنیتی، به حمایت فیزیکی آن‌ها کمک می‌کند و همچنین می‌تواند راهی برای شناسایی اهداف احتمالی تروریست‌ها باشد. جنبه دوم شامل جلوگیری از شروع حملات است که با دستگیری تروریست‌ها قبل از انجام برنامه‌های خود، مبارزه با استخدام تروریست‌ها و افراط‌گرایی در آینده، تحمیل محدودیت در حرکت و آزادی افراد مظنون انجام می‌شود. پیش‌بینی ضد تروریسم به نوعی هوش مصنوعی نیاز دارد که دانش و پیش‌بینی‌ها را از داده‌های دیجیتال متنوع و وسیع استخراج کند. در بسیاری از موارد، تجزیه و تحلیل داده‌ها بدون چنین رویکردی غیرممکن خواهد بود. با این حال، مشکل این است که پیش‌بینی عملیات تروریستی نیاز به گسترش فضای نظارت برای افراد دارد که این مسئله محدودیت‌هایی را بر حقوق بشر از جمله حق بر حریم خصوصی تحمیل می‌کند. بنابراین، در آینده نزدیک، پیش‌بینی‌های موثری مبتنی بر تکنیک‌های هوش مصنوعی در مورد اینکه چه کسی با چه نوع نظارتی را باید تحت نظر گرفته شود، می‌تواند 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، به دلیل نقض برخی از اصول بنیادین حقوق بشری انجامیده است. نگرانی‌هایی از این دست و نبود مقررات جامع و لازم‌الاجرا در زمینه نظارت و کنترل آثار ناشی از کاربرد هوش مصنوعی، اتحادیه 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 می‌کند که احتمالاً پیامدهای جهانی را به همراه دارد. تروریسم سایبری را می‌توان به عنوان استفاده از رایانه و فناوری اطلاعات با انگیزه سیاسی برای ایجاد اختلال و ترس در بین غیرنظامیان



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



این چالش‌ها عبارتند از چالش‌های فنی: از قبیل تشخیص نادرست، وجود سوگیری در داده‌ها، ابهام و عدم شفافیت در نحوه تصمیم‌گیری، نقش بخش خصوصی در فرایندهای مرتبط با طراحی و توسعه هوش مصنوعی و نیز چالش‌های 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 بین‌الملل می‌توان تحقیقات رو به رشدی را یافت که ارتباط بین هوش مصنوعی و امنیت بین‌المللی را تحلیل می‌کند. 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 انقلاب‌های آتی در امور سیاسی و نظامی می‌دهد و نحوه ورود دولت‌ها به تعاملات استراتژیک در عرصه هوش مصنوعی چگونه باید مدیریت شود. (Kopanja, 2023)

مسائل چالش‌برانگیزی که در نقطه تلاقی کاربردهای هوش مصنوعی و امنیت مطرح می‌شود دلالت بر این دغدغه‌های به‌غایت مهم دارد: هوش مصنوعی این امکان را خواهد داشت تا دوران جدیدی از صلح بین‌المللی را به ارمغان می‌آورد؟ آیا این امر منجر به تغییر توازن قدرت در صحنه جهانی می‌شود؟ هوش مصنوعی می‌تواند منجر به جابجایی گسترده و افزایش ناآرامی‌های سیاسی، ملی‌گرایی و حمایت‌گرایی شود؟ و... ناگفته پیداست که برخی از کاربردهای مستقیم هوش مصنوعی مربوط به اهداف امنیت ملی است. نمونه‌های 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 به‌عنوان نمونه‌های گویای کاربرد هوش مصنوعی در حوزه امنیت ملی در نظر گرفته می‌شود.

به‌عنوان مثال در بحث امنیت سایبری، دامنه سایبری، یک عرصه بالقوه برجسته برای هوش مصنوعی است. در اکتبر ۲۰۱۶، مایکل راجرز، مدیر آژانس امنیت ملی<sup>۱</sup> اظهار داشت که این آژانس هوش مصنوعی را «پایه‌ای برای آینده امنیت سایبری» می‌داند. نقش هوش مصنوعی در تغییر چشم‌انداز تهدیدات علیه امنیت داده‌ها نیز حائز اهمیت است. این تکنولوژی نوین پیامدهای جدی برای امنیت اطلاعات دارد که

<sup>۱</sup> NSA



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



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 منسجم 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 پیرامون هوش مصنوعی و کاربردهای آن در نظر گرفته و آن ها را ملزم به پیشینی 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



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



فرصت‌های قابل توجه حاصل از پیشرفت علم و فناوری در کنار توان قابل ملاحظه 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 می‌انجامد.

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 می‌نماید. ماده ۵ به عنوان یکی از مهم‌ترین 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





پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



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 جانبه‌گرایی خود تبدیل کرده‌اند. (قربانی و سیمبر، ۱۳۸۸: ۱۵۴-۱۴۶) امنیت، صلح و حقوق بشر غایت تلاش‌های بین‌المللی است. با پیشرفت تکنولوژی‌های نوظهور همواره این مفاهیم در معرض بازتعریف قرار داشته‌اند. چه زمانی که سلاح‌های غیر متعارف توسط دولت‌ها 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 بین‌المللی و صلح جهانی است، این در حالی است که هیچ سند بین‌المللی لازم‌الاجرائی این جنایت علیه صلح و امنیت بین‌المللی را تعریف نکرده و کنوانسیون‌های موجود در بیان برخی مصادق آن توفیق یافته‌اند. این امر نشان‌گر مطلوبیت جرم‌انگاری 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 نمی‌شود. هدف جامعه جهانی باید «ائتلاف علیه تروریسم برای صلح عادلانه» باشد، ائتلافی که در آن همکاری بین‌المللی به سمت هماهنگی بین‌المللی پیش رود. تا آن زمان اقدامات دولت‌ها باید در راستای تعیین 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 داده‌های دیجیتال، دولت الکترونیکی، بانکداری الکترونیکی، امنیت هوایی و بسیاری از حوزه‌های زیرساختی حیاتی دولت‌ها امروزه متکی به امنیت سایبری است. تهدیدات و تروریسم سایبری نه تنها امنیت ملی و بین‌المللی تأثیر را به خطر انداخته، امنیت اقتصادی و انسانی را نیز مورد تهدید و نقض قرار داده در حالی که تنها سازمان‌های امنیت محوری چون ناتو در مرکز عالی دفاع سایبری، در مبارزه با آن با جمیع راهکارهای فنی و حقوقی، توانسته‌اند به توفیق دست یابند. چالش‌های نوین حاصل از هوش مصنوعی نیاز به رویکردهای نوین امنیتی در حوزه روابط بین‌الملل را بیش از پیش متجلی نموده است. تهدیدی با ماهیت جهانی، اراده و شیوه‌های بین‌المللی برای مبارزه را طلب می‌کند و حاکمیت‌ها اگرچه همچنان تمایل به جرم‌انگاری و مبارزه با تروریسم سایبری در حوزه صلاحیت ملی خود دارند، با توجه به ماهیت



پرو، شہسکاه علوم انسانی و مطالعات فرہنگی  
پرتال جامع علوم انسانی



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>