Supreme National Defense University Quarterly Journal of Defense Logistics and Technology

https://amfad.sndu.ac.ir E-ISSN: 2980-8073

Vol. 8, Special Issue, Issue. 28, Winter 2025 **Received:** 2025/04/16 **Accepted:** 2025/08/18

Research paper

Cyberterrorism: The Transformation of Terrorism in the Age of Information Technology

Mohammad Bagher Mokaramipour
PhD Student, Department of Political Science/Islamic Revolution Political Studies, Faculty of Literature and Humanities, Shahed University, Tehran, Iran (Corresponding Author)
Email: mbmokaramipour@gmail.com
Sobhan Mohammadi
PhD in International Relations, Faculty of Law and Political Science, Islamic Azad University, Science and Research Branch, Tehran, Iran
Email: sobhan.mohammadi@srbiau.ac.ir
Mohammad Ali Kiani
PhD student, Department of Political Geography, Faculty of Geography, University of Tehran, Tehran, Iran
Email: keyani@ut.ac.ir

Abstract

Objective: Recent global developments, including the pervasiveness of communications, the increasing development of new technologies referred to as the "information revolution" and the "media revolution," along with assumptions such as uncertainties in the field of international security, have fundamentally changed the concept of "threat." This study seeks to examine the nature and forms of terrorism, and to explain the evolution in its concept, and to analyze this issue by highlighting and focusing on cyberterrorism as a known threat in terms of pervasiveness in the information age.
Method: In a descriptive-analytical approach, the reasons for the how and why of the problem and its dimensions are described and explained. Next, using the theoretical framework of "cybernetics," the cause of the connection between systemic communications and information with social effects and consequences is studied. Findings: Issues such as a significant gap between strategies and actions, updating laws and protective considerations in the field of cybersecurity with a non-political approach, the substantive difference between individuals and governmental and non-governmental organizations - real and legal - in terms of the exploitation of cyberspace, the foreign origin of most cyber attacks, the development of third-generation artificial intelligence with problem-solving capabilities, the targeting of most cyber attacks to the infrastructure-service, economic-financial, and security-psychological areas, and the "substitutability" capability of artificial intelligence have been identified.
Conclusion: Cyber threats are potentially increasing, the vulnerability of critical infrastructures compared to other sources in cyberterrorism attacks, and the increasing attractiveness of cyberspace for terrorism compared to more traditional methods are among the most important inferences.

Keywords: Terrorism, Cyberterrorism, Technology, Artificial Intelligence, Security

سال هشتم ویژه‌نامه (پیاپی ۲۸)، زمستان ۱۴۰۴، صص. ۵۵-۹۸
تاریخ دریافت: ۱۴۰۴/۰۱/۲۷ ـ تاریخ پذیرش: ۱۴۰۴/۰۵/۲۷

مقاله پژوهشی

تروریسم سایبری: دگردیسی تروریسم در عصر فناوری اطلاعات

محمدباقر مکرمی‌پور
دانشجوی دکتری، گروه علوم سیاسی، گرایش مطالعات سیاسی انقلاب اسلامی، دانشکده ادبیات و علوم انسانی، دانشگاه شاهد، تهران، ایران (نویسنده مسئول).
Email: mbmokaramipour@gmail.com

سبحان محمدی
دانش‌آموخته مقطع دکتری روابط بین‌الملل، دانشکده حقوق و علوم سیاسی واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران
Email: sobhan.mohammadi@srbiau.ac.ir

محمدعلی کیانی
دانشجوی دکتری گروه جغرافیای سیاسی، دانشکده جغرافیا، دانشگاه تهران، تهران، ایران
Email: Email: keyani@ut.ac.ir

چکیده

پژوهش حاضر به دنبال بررسی ماهیت و اشکال تروریسم و تبیین تحول در مفهوم آن بوده و با برجسته‌سازی و تمرکز بر تروریسم سایبری به‌عنوان یک تهدید شناخته‌شده از حیث فراگیری در عصر اطلاعات، اقدام به واکاوی این مسئله می‌کند. در روش تحقیق این پژوهش با رویکرد توصیفی-تحلیلی، به تشریح و تبیین دلایل چگونگی و چرایی مسئله و ابعاد آن پرداخته می‌شود. در ادامه، با استفاده از قالب نظری «سایبرنتیک»؛ علت پیوند ارتباطات سیستمی و اطلاعات با تأثیرات و تبعات اجتماعی مورد مطالعه قرار می‌گیرد. یافته‌های پژوهش شامل مواردی ازجمله شکاف قابل‌توجه میان استراتژی‌ها و اقدامات، روزآمدسازی قوانین و ملاحظات حفاظتی در حوزهٔ امنیت سایبری با رویکردی غیرسیاسی، تفاوت ماهوی مابین افراد و سازمان‌های دولتی با غیردولتی، حقیقی و حقوقی، در نگاه به بهره‌برداری از فضای سایبر، منشأ خارجی بیشتر حملات سایبری، توسعه نسل سوم هوش مصنوعی با قابلیت حل مسئله، هدف بیشتر حملات سایبری به حوزه‌های زیرساختی - خدماتی، اقتصادی - مالی و امنیتی- روانی و قابلیت «بدیل‌سازی» هوش مصنوعی، شناسایی شده است. نتیجه‌گیری پژوهش عبارت است از اینکه تهدیدات حوزه سایبری به‌طور بالقوه در حال افزایش است و آسیب‌پذیری زیرساخت‌های حیاتی به نسبت سایر منابع در حملات تروریسم سایبری و جذابیت روزافزون فضای سایبر برای جریان تروریسم به نسبت روش‌های سنتی‌تر از مهم‌ترین موارد استنتاجی است.

کلیدواژه‌ها: تروریسم، سایبر تروریسم، فناوری، هوش مصنوعی، امنیت

20.1001.1.28212606.1404.8.5.2.5 https://amfad.sndu.ac.ir/ E-ISSN: 2980-8073

مقدمه

ویژگی‌های بی‌همتای فناوری‌های اطلاعات و ارتباطات، تحولات بنیادینی را در قلمرو حیات بشری پدید آورده است. نخستین ویژگی بی‌همتای فناوری‌های اطلاعات و ارتباطات، جهانگیری گسترش این فناوری‌ها است. این ویژگی باعث گردیده است فناوری‌های اطلاعات و ارتباطات نفوذ جهان‌گستری به دست آورند و در یک گسترهٔ جغرافیایی خاص و محدود نگنجند (برهانی و حاج محمدی، ۱۳۹۸: ۱۰۴).

در عهد فناوری اطلاعات و بسط تکنولوژی با گونه نوینی از تروریسم مواجه هستیم و حضور بی‌سابقه این نوع از تروریست‌ها گویای این است که این پدیده روزبه‌روز در حال گسترش و تغییر چهره است که از آن‌ها به‌عنوان تروریسم یاد می‌شود. سایبرتروریسم، یکی از اشکال نوین تروریسم بین‌المللی است و همان‌گونه که اشاره شد، دولت‌ها در تعاریف تروریسم، غالباً به جرم انگاری از طریق بیان مصادیق آن پرداخته‌اند. با این وصف، به‌خوبی می‌توان دریافت که سایبرتروریسم نیز به تبعیت از تروریسم، مفهومی کلی دارد (قاسمی و باقرزاده،۱۳۹۴: ۲۳۲).

تروریسم سایبری شامل استفاده از روش‌های متداول هک کردن مانند دسترسی غیرمجاز به رایانه‌ها، ویروس‌ها، بمب‌های ایمیلی و ... با هدف آسیب رساندن است. با وابستگی بیشتر جامعه به سامانه‌های رایانه‌ای، تروریست‌های سایبری از آسیب‌پذیری این سامانه‌ها استفاده می‌کنند. سامانه‌های کنترل ترافیک، تسهیلات پزشکی، نظامی، امنیت عمومی و سامانه‌های ارتباطات، ازجمله حوزه‌های آسیب‌پذیر است. همچنین حملاتی که به مرگ یا صدمه جسمی منتهی می‌شود، انفجار، سقوط هواپیما، آلوده کردن آب یا خسارت اقتصادی شدید ازجمله موارد است (عاملی،۱۳۹۰: ۲۳۹). این پدیده نوین، قادر است با استفاده از ابزارهای موجود در فضای سایبر، به خشونت هسته‌ای، بیولوژیکی، شیمیایی یا هر چیز دیگری که قابلیت تبدیل‌شدن به سلاح کشتارجمعی را داشته باشد، به‌منظور دستیابی به اهداف خود در همه سطوح دست بزند. این امر، تهدید جدی برای کلیه کشورها چه در سطوح محلی، ملی و بین‌المللی است، به‌طوری‌که دامنه این تهدید، حتی به کشورهایی که ظاهراً از کانون این

مسئله دور هستند کشیده شده است. برای یک تروریست، سایبرتروریسم بر روش‌های فیزیکی، برتری‌هایی دارد، ازجمله می‌تواند از راه دور انجام گیرد و احتمال دستگیری توسط طرف مقابل، بسیار پایین است؛ هزینه آن کم است و نیازی به حمل مواد منفجره و آلات و ادوات مورد استفاده در حملات تروریستی در مأموریت انتحاری یا غیر آن ندارد. تروریست‌های سایبری در اقدام هماهنگ و گسترده در بازه زمانی مشخص می‌توانند آسیب‌های جدی به سامانه‌های زیرساختی و حیاتی کشور مورد هدف وارد با توجه به مصادیق یادشده، به نظر فرِد کهن، اقدامات تروریستی سایبری، به چهار شیوه انجام می‌شود: ۱. یورش به اطلاعات که همان دگرگونی یا از میان بردن محتوای فایل‌های الکترونیکی، سامانه‌های رایانه‌ای یا محتویات گوناگون موجود در آن‌ها است؛ ۲. یورش به زیرساخت که بر پایهٔ آن، سخت‌افزارها، پایگاه‌های عملیاتی یا برنامه‌های محیط رایانه مختل می‌شود؛ ۳. معاونت فنی در ارتکاب که عبارت است از به‌کارگیری ارتباطات الکترونیکی برای فرستادن نقشه‌ها و طرح‌ها به‌منظور انجام یورش‌های تروریستی یا تحریک به انجام آن‌ها یا توسل به سایر تسهیلات؛ ۴. افزایش یا ارتقای منابع مالی که به‌موجب آن، تروریست‌ها با بهره‌گیری از اینترنت برای خشونت سیاسی یا دیگر رفتارها، به گرفتن کمک‌های مالی افراد یا سازمان‌ها می‌کوشند (عالی پور،۱۳۸۹: ۱۱۸).

پژوهش پیش‌رِو با موضوع تروریسم سایبری در گام اول به سراغ تحلیل ادبیات پیشینی و تحلیل‌های موجود به‌منظور دستیابی به یک کلیت مفهومی حرکت کرده است. در ادامه و گام بعدی، با بهره‌گیری از چهارچوب نظری تعیین‌شده، تحولات مفهومی و کارکردی تروریسم را تبیین خواهد کرد تا گذار عملیاتی تروریسم به فضای سایبر اثبات شود. در کنار آن، توجه به یک فهم آینده‌پژوهانه از موضوع، به ادراک بیشتر، آگاهی کامل‌تر و تحلیلی واقعی‌تر از مسئله کمک می‌کند و دانسته‌های ما نیز تکمیل می‌گردد. چراکه ظهور ابزارها و برنامه‌های جدید با قابلیت دسترسی عمومی مانند «دیپ فیک» و توسعه سریع «هوش مصنوعی» این حوزه را با دگرگونی‌ها و پیچیدگی‌هایی جدیدی مواجه کرده که تلاش شده در این پژوهش به آن‌ها نیز پرداخته شود. در ادامه، این پژوهش می‌تواند به توسعه ابزارهای

مورد نیاز، استراتژی‌ها و سیاست‌های بهتر و مؤثرتر برای مقابله با تروریسم سایبری بینجامد. همچنین درخصوص اهمیت و ضرورت پژوهش، موارد زیر قابل بررسی است:

- ❖ پرداختن به این موضوع برخی از خلأهای موجود در ادبیات راهبردی و حکمرانی را حل‌وفصل می‌نماید؛
- ❖ انجام این پژوهش می‌تواند در شناخت تروریسم سایبری در عصر فناوری اطلاعات مؤثر باشد؛
- ❖ انجام این پژوهش می‌تواند پژوهشگران و مسئولان را با نقش تروریسم سایبری، در عصر فناوری اطلاعات آشنا نماید؛
- ❖ نپرداختن به این موضوع موجب تداوم خلأ موجود در ادبیات راهبردی و حکمرانی کشور خواهد بود؛
- ❖ انجام نشدن این تحقیق منجر به عدم شناخت تروریسم سایبری در عصر فناوری اطلاعات می‌شود.

۱. پیشینهٔ پژوهش

موضوع پژوهش پیش‌رِو، از جدیدترین و چالشی‌ترین تهدیدات امنیتی در حوزه سیاسی، فناوری و بین‌الملل محسوب می‌شود و طیف قابل‌توجهی از پژوهش‌های منتشرشده اخیر داخلی و خارجی را به خود اختصاص داده است.

پاکزاد (۱۳۹۳) در پژوهشی با عنوان ماهیت تروریسم سایبری به این مسئله می‌پردازد که حضور تروریست‌ها در جهان مجازی یا سایبر گویای این است که پدیده تروریسم سایبری روزبه‌روز در حال گسترش و تغییر چهره است. بهره‌گیری از فناوری‌های نوین در اقدامات تروریستی و یا هدف قرار دادن این فناوری‌ها توسط تروریست‌ها، سبب شده تا تروریسم سایبری هم در مجموعه جرائم تروریستی سایبری نه همچون یک نوع یا شیوه از اقدام‌های خشونت‌آمیز تروریستی است که بتوان به‌طور دقیق در زیر تروریسم جایش داد و نه ویژگی‌هایش محدود به ویژگی‌های جرائم سایبری است که آن را در این دسته نهاد. همین

ابهام در جایگاه تروریسم سایبری سبب شده تا این پدیده به یک چالش و مسئله جدی هم برای تحقیق و هم برای سیاست‌گذاری در مقابله با آن تبدیل گردد. این تحقیق درصدد است هم برای تحقیق و هم برای سیاست‌گذاری در مقابله با آن تبدیل گردد. این تحقیق درصدد شناخت ماهیت متفاوت این پدیده جدید است. لازمه شناخت ماهیت آن آگاهی از مفهوم ویژگی‌ها و گونه‌های آن است. اگرچه در یک رویکرد حقوقی محض تروریسم سایبری فقط شامل اقدامات سایبری ضد سیستم‌ها و داده‌ها و اطلاعات با انگیزه‌های سیاسی است یعنی تروریسم سایبری، به تروریسم سایبری مفهومی موسع داده و آن را شامل همه اشکال استفاده از اینترنت و فضای سایبر توسط تروریست‌ها نموده است، اعم از اینکه فضای سایبر افراز یا هدف اقدامات تروریستی باشد.

یزدانی و همکاران (۱۳۹۳)، در پژوهشی با عنوان سایبر تروریسم شکل نوینی از ترور علیه منافع ملی به این مسئله می‌پردازند که سایبر تروریسم با هدف از کار انداختن عملیات زیرساخت‌های بحرانی یک کشور انجام می‌شوند که با توجه به رشد روزافزون تکنولوژی و ویژگی‌های منحصربه‌فرد فضای سایبر، تمامی دولت‌ها را با چالش‌های جدیدی روبه‌رو کرده است. سؤال اصلی نوشتار این است که با توجه به در دسترس و منحصربه‌فرد بودن فضای سایبر، چگونه می‌توان بر تهدیدات سایبر تروریسم علیه منافع دولت‌ها فائق آمد؟ فرضیه نوشتار در پاسخ به سؤال این است که در عصر جدید با پیشرفت تکنولوژی و فناوری با تهدیدات جدیدی روبه‌رو شده‌ایم که دیگر نمی‌توان مانند گذشته امنیت ملی را تنها در محدوده مرزهای داخلی یک کشور نگاه کرد. امروزه مهاجمان تنها با در دست داشتن یک دستگاه رایانه، تهدیدی برای منافع یک کشور محسوب می‌شوند. چنین خطر نافذی، تمامی برداشت‌های رایج و سنتی از مفهوم امنیت ملی را زیر سؤال برده است. مقاله به روش توصیفی- تحلیلی و با ابزار کتابخانه به رشته تحریر درآمده است.

برودِرز و همکاران (۲۰۲۳) در مقاله «خطری در همین نزدیکی: تروریسم سایبری و امنیت اطلاعات در سیاست‌های ملی و دیپلماسی بین‌المللی» تهدیدات نوین سایبری را در سطوح ملی و بین‌المللی و با تمرکز بر تأثیرات متقابل، بازتعریف مفاهیم، ضرورت ارتقای امنیت

فناوری و همچنین؛ اقدامات سازمان‌های درگیر با این موضوع را بررسی کرده‌اند (Broeders & Others, 2023: 1).

پلاتنِک و اِسلی (۲۰۲۰) در پژوهش خود با عنوان «تروریسم سایبری: یک تعریف و طبقه‌بندی همگن»، ضمن تمرکز بیشتر بر مفاهیم و هستی‌شناسی تروریسم سایبری، این تهدید را به‌عنوان بخشی از تهدیدات نوین شناسایی می‌کنند و در تلاش هستند که با کالبدشکافی این شکل از تروریسم (مانند عامل، هدف، انگیزه و ...) راهکارهایی برای تعریف استانداردهای مشترک و مقابله، ارائه کنند (Plotnek & Slay, 2020: 2).

امیرلی و ثقفی (۱۴۰۲) در مقاله «ارائه مدل مفهومی مدیریت تهدیدات ناشی از تروریسم سایبری» همان‌طور که از عنوانش پیداست، پیشینه و تعاریف مفاهیم از موضوع در کانون توجه نویسندگان قرارگرفته و با توجه به اهمیت آن در اسناد بالادستی، ارائه یک مدل مفهومی برای مدیریت تهدیدات ناشی از تروریسم سایبری به‌عنوان نتیجه این تحقیق مشخص‌شده است (امیرلی و ثقفی، ۱۴۰۰: ۲).

همچنین «رویکرد ویژه سازمان‌های تروریستی به رسانه‌های اجتماعی و مجازی» از دیگر عناوین پژوهشی است که به تبارشناسی و ساختار شناسی این شکل از تهدید پرداخته است (فریدپور و قربانی زواره، ۱۴۰۰: ۱).

از نظر جنبه نوآوری باید اذعان نمود که در پژوهش حاضر کوشش شده است برخی کاستی‌های موجود در تحلیل‌های پیشین برطرف گردد. زیرا برخی کارها صرفاً تحول محور بودند ضمن آن‌که بسیاری نیز تک‌بُعدی به موضوع نگریسته‌اند؛ اما پژوهش حاضر به جهت رویکرد نوینی که مدنظر دارد، درصدد است تا به درک وسیع‌تر و جامع‌تری از تروریسم سایبری: دگردیسی تروریسم در عصر فناوری اطلاعات بپردازد.

۲. مبانی نظری پژوهش

۲-۱. «سایبرنتیک»[1]

سایبرنتیک مطالعه روش‌های کنترل، تنظیم یا نظارت در یک سیستم مشخص از طریق فناوری است. دستیابی به بازخوردها یا اطلاعاتی که در یک سیستم از طریق محیط آن دریافت یا انتشار می‌یابد، به‌عنوان سایبرنتیک شناخته می‌شود. نظریه‌های سیستمی، فلسفه، نظریه بازی‌ها، کنترل ادراکی، معماری، هوش مصنوعی و بسیاری از زمینه‌های مطالعاتی دیگر، تحت تأثیر سایبرنتیک قرار گرفته‌اند؛ بااین‌حال، هدف اصلی یکسان است: بررسی پایش‌های سیستم برای همه مکانیسم‌های اساسی (Swapna, 2022). جامعه را می‌توان از طریق مطالعه پیام‌ها و امکانات ارتباطی متعلق به آن درک نمود (August, 2021: 4-5). نوربرت وینر در دهه ۱۹۵۰ کتاب خود، کاربری بشری در هستی انسانی: سایبرنتیک و جامعه، را منتشر کرد وینر با تکیه بر کتاب اول خود؛ سایبرنتیک، کنترل و ارتباطات در حیوانات و ماشین – که در سال ۱۹۴۸ منتشر شد (با ویرایش دوم در ۱۹۶۱) و اکنون منبع اصلی سایبرنتیک مدرن محسوب می‌شود – در مورد کاربردهای بالقوه ایده‌ها در قالب سایبرنتیک برای طراحی و تولید فناوری‌های مهاجم هشدار داد؛ به‌ویژه رباتیک و هوش مصنوعی که قابلیت‌های خودکار را دارا هستند (Richards, 2019: 1). از زاویه‌ای دیگر تعریف وینر از سایبرنتیک، مطالعه علمی کنترل و ارتباط در مسائل مرتبط با ماشین و سایر موجودات است. در تعریف ابتدایی دیگری در کنفرانس‌های «سایبرنتیک میسی»[2] از سایبرنتیک به‌عنوان مطالعه مکانیسم‌های علّی و بازخورد محوری در سیستم‌های بیولوژیکی و اجتماعی یاد شده است. «ای. ان. کُلموگوروف»، سایبرنتیک را روش مطالعه سیستم‌هایی با ماهیت گوناگون می‌داند که قادر به ذخیره و پردازش اطلاعاتی هستند که به‌منظور کنترل از آن‌ها استفاده می‌گردد و دابلیو رز اَشلی هم معتقد است که سایبرنتیک، هنر هدایت‌گری است؛ هنری که با تمام اشکال رفتار تا جایی که منظم یا تعیین‌کننده یا قابل تکرار هستند سروکار دارد (University of São Paulo, 2021: 3).

1. Cybernetics
2. Macy

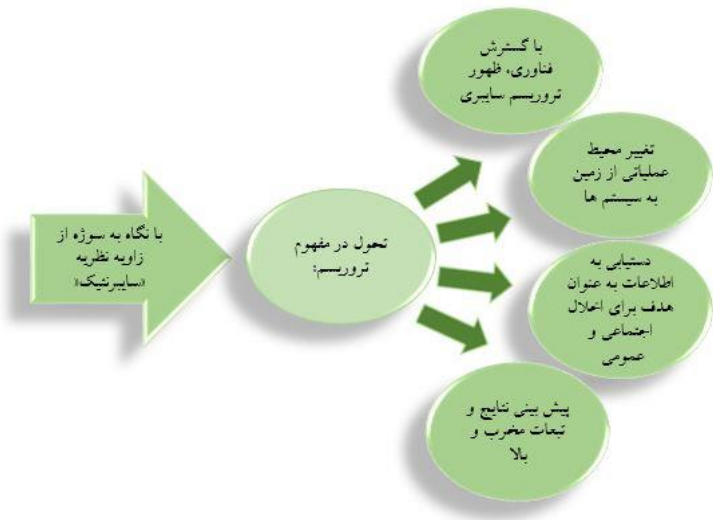
سایبرنتیک درباره اهداف جریان‌های اطلاعاتی هدفمند و فرایندهای کنترل تصمیم‌گیری و بازخورد آن در تمام سطوح سیستم‌های زنده است (Corning, 1996: 2). سایبرنتیک نظریه‌ای است که مقوله کنترل و ارتباطات را مورد بحث قرار می‌دهد؛ به‌بیان‌دیگر، فلسفه و زبانی است که سیستم‌های هدف‌گرا را توصیف می‌نماید. از سایبرنتیک و تئوری کنترل به‌طور گسترده در رشته‌های مختلف ازجمله یادگیری و مدیریت اجتماعی محیطی استفاده می‌شود. ظهور این فضای ناوبری یکپارچه، نوع جدیدی از تولید دانش مشترک توسط تعداد بسیاری از انسان‌ها و ماشین‌ها را امکان‌پذیر می‌کند. اساساً هر چیزی که هدفی را دنبال می‌نماید در سایبرنتیک یکسان در نظر گرفته می‌شود؛ گرچه اجزا متفاوت هستند؛ اما مکانیسم‌ها ثابت می‌مانند (Birawal, 2022: 1). رسانه‌های عملیاتی که تأثیرگذاری اجتماعی را دنبال می‌کنند اغلب به‌صورت یک الگوریتم و با انجام یک کار در یک مدار سایبرنتیکی سازمان‌دِهی می‌شوند.

در مجموع، از تعاریف علمی سایبرنتیک در منابع مختلف می‌توان نکات کلیدی ذیل را استخراج کرد:

- ❖ سایبرنتیک دانش مطالعه پیوند ارتباطات سیستمی و اطلاعات با تأثیرات و تبعات اجتماعی است؛
- ❖ برای کاربرد سایبرنتیک در تحلیل موضوع، تعریف و شناخت ساختاری از سوژه، تعریف کارکردها و نتایج و اطلاعات خروجی آن ضروری است؛
- ❖ فناوری و کنترل موضوع مطالعه در سایبرنتیک است. با توسعه و پیشرفت فناوری، روش‌های کنترل، نظارت و مطالعه یک سیستم (به‌طور خاص مثلاً شبکه‌های مجازی یا هوش مصنوعی) نیز توسعه می‌یابند. سایبرنتیک مطالعه موارد فوق را سازمان‌دهی می‌کند؛
- ❖ در مسئله اجتماعی، با مطالعه سیستم‌ها و ابزارهای ارتباطی و همچنین کم و کیف محتوا و مخاطبان، می‌توان به اطلاعات حیاتی و تعیین‌کننده رسید؛

❖ جریان اطلاعات در عصر حاضر و در سیستم‌های ارتباطی عمومی اجتماعی، یک مقوله چندوجهی و چند سویه در نظر گرفته می‌شود (به‌عبارت‌دیگر، افراد و یا گروه‌ها می‌توانند هم عامل اطلاعات باشند و هم تابع آن) و بستر انتقال این اطلاعات، برنامه‌های کاربردی و عمومی اجتماعی است.

حال با این تفاسیر و گزاره‌های فوق، سایبرنتیک چه کمکی به پیشبرد موضوع و هدف پژوهش پیش‌رِو می‌کند؟ در پاسخ باید گفت که ابتدا، ساختار و تشکیلات سوژه (تروریسم) مورد بررسی قرار می‌گیرد. دوم، نقش فناوری در تحولات و تغییرات – چه ماهوی و چه شکلی – سوژه مورد مطالعه قرار می‌گیرد. سوم، پیوند سوژه ساختارمند دگرگون‌شده با مسئله اجتماعی و ربط آن‌ها به یکدیگر مشخص می‌شود و چهارم، تبعات و تأثیرات آن در حال و آینده را می‌توان به‌صورت احتمال و پیش‌بینی در نظر گرفت.



شکل ۱: با نگاه به سوژه از زاویه نظریه «سایبرنتیک»

۲-۲. ترور – تروریسم

ریشه لغوی تروریسم به زبان یونانی Tras به معنی ترس‌ولرز بازمی‌گردد. فعل Tres یا Ters در زبان لاتینی به همین معنا آمده است. در زبان انگلیسی، اصل کلمه Terreur به فعل لاتینی Ters

برمی‌گردد که آن‌هم به معنی «ترساندن» یا ترس و وحشت» است که بیشتر مشقات آن حول همین معانی مشخص می‌چرخند. در فرهنگ پیشرفته آکسفورد آمده است: «تروریسم نیز به روشی اطلاق می‌شود که هدفش استفاده از خشونت یا تهدید به استفاده از خشونت برای دستیابی به اهداف سیاسی است» (Oxford Advanced Learners Dictionery 1993).

داریوش آشوری در کتاب «دانشنامه سیاسی در توضیح واژه «ترور» می‌نویسد: ترور در لغت فرانسه به معنای هراس و هراس‌افکنی است و در سیاست به کارهای خشونت‌آمیز و غیرقانونی حکومت‌ها برای که برای سرکوبی مخالفان خود و ترساندن آن‌ها به کار می‌برند ترور میگویند و نیز کردار گروه‌های مبارزی که برای رسیدن به هدف‌های سیاسی خود دست به کارهای خشونت‌آمیز و هراس‌انگیز می‌زنند «ترور» نامیده می‌شود بنابراین، تعریف ترور و تروریسم روشی است که هم حکومت‌ها و هم گروه‌های سیاسی مخالف حکومت برای هراس‌افکنی و ترساندن طرف مقابل به کار می‌گیرند ترور به معنای کشتار سیاسی به کار می‌رود و کسانی را که به کشتار سیاسی دست بزنند تروریگر (تروریست) می‌خوانند» (آشوری،۱۳۸۲: ۹۹).

۲-۲-۱. جامع‌ترین تعریف تروریسم

یکی از جامع‌ترین تعاریف آکادمیک از تروریسم که مکرراً نقل شده، تعریف «آلکس پ اشمیت» است او در کتاب مشهورش تروریسم سیاسی، یک راهنمای تحقیقی که در سال ۱۹۸۴ (۱۳۶۳) منتشر شد، فقط ۱۰۹ تعریف مختلف و متفاوت را بین سال‌های ۱۹۳۶ تا ۱۹۸۱ (۱۳۱۴ تا ۱۳۶۰) مورد شناسایی قرار داده است و در نهایت نتیجه می‌گیرد که تروریسم شیوه اقدامات تکراری به‌منظور ایجاد دلهره و رعب و وحشت است که به دلایل سلیقه‌ورزی، جنایی و یا سیاسی توسط گروه‌های مختلف به کار گرفته می‌شود؛ البته تعریف اشمیت به همین‌جا ختم نمی‌شود و در ادامه بین نوع اهداف موردنظر تفکیک قائل می‌شود بنابراین چندان عجیب نیست که حتی اشمیت بعداً قبول می‌کند که حتی تعریف دقیق و طولانی وی را احتمال ندارد که دولت‌ها به کار برند.

تعریف اشمیت حاصل ترکیب ۱۰۹ تعریف است که در آن ۱۶ عنصر قابل تعریف از ۲۲ عنصر اصلی موردنظر اندیشمندان مختلف آمده و مثالی کلاسیک از یک تعریف آکادمیک به شمار می‌رود بدین لحاظ از این تعریف به دلیل پیچیدگی و تاحدی تناقض‌آمیز بودن و نیز فایده ناچیز آن انتقاد گردیده است.

اما به نظر می‌رسد که «پال پیلار» جامع‌ترین تعریف را از تروریسم ارائه داده است. او معتقد است که تروریسم خشونت از پیش طراحی‌شده با جهت‌گیری سیاسی بر ضد اهداف غیرنظامی از سوی گروه‌های خرده ملی و عوامل مخفی که معمولاً برای تأثیرگذاری بر مخاطبان به کار گرفته می‌شود.

این تعریف دارای چهار عنصر اساسی است:

۱. تروریسم عملی است از پیش طراحی‌شده و ناشی از فکر و تصمیم عده‌ای که می‌خواهند آن را انجام دهند؛

۲. این کنش دارای جهت‌گیری سیاسی است و با دیگر خشونت‌های برآمده از انگیزه‌هایی همچون انگیزه‌های مالی یا انتقام شخصی و ... فرق دارد؛ مرتکبین این اعمال انگیزه‌های کلان دارند و می‌خواهند وضع موجود را تغییر دهند؛

۳. عنصر سوم این تعریف مربوط به قربانیان تروریست‌هاست که شامل افرادی است که توانایی دفاع از خود ندارند مانند کشته شدن تمامی سرنشینان هواپیماهایی که در حادثه ۱۱ سپتامبر علیه برج‌های دوقلوی نیویورک و پنتاگون (وزارت دفاع آمریکا) به کار گرفته شد و همچنان تمامی ساکنان که در برج‌های دوقلوی محله منهتن نیویورک و ساختمان پنتاگون کشته شدند توانایی هیچ‌گونه دفاعی را از خود نداشتند؛

۴. چهارمین عنصر در ارتباط با مرتکبین اعمال تروریستی است که از گروه‌های فروملی تا عوامل سرّی هستند که کارشان از عملیات نظامی دولت‌ها و کاربرد آشکار نیروهای نظامی بر ضد اهداف نظامی متمایز است. با این تعریف روشن می‌شود که روش تروریست‌ها هراس‌افکنی و خشونت غیرقانونی است و استراتژی آن‌ها

دستیابی به اهداف سیاسی و اجتماعی است کـه بـا اهداف جنایتکاران عادی مانند دزدان و تبهکاران فرق می‌کند. آنان از وضع موجود جامعه سیاسی ناراضی و تلاش می‌کنند وضع موجود را به هم بزنند و از این جهت با انقلابیون برای رسیدن به اهداف سیاسی از روش‌های خشونت برای کشتار افراد استفاده نمی‌کنند و قربانیان آن‌ها حداکثر می‌توانند نیروهای اطلاعاتی و امنیتی رژیم حاکم باشند نه افرادی عادی و بی‌گناه (ماهنامه اطلاعات سیاسی و اقتصادی، ۱۳۸۰).

بنابراین پدیده تروریسم را می‌توان از زوایای مختلفی تعریف کرد. هرچند این مسئله متأخر است و در تعاریف آن، اختلافات و ابهامات زیادی به چشم می‌خورد. از زاویه سیاسی تروریسم عبارت است از «استفاده سازمان‌یافته از خشونت برای حمله به افراد غیرنظامی یا دارایی‌هایشان، برای اهداف سیاسی» یا در تعریف دیگری، «تروریسم در کاربرد متداول خود، دلالت بر شرارت دارد و با خشونت بی‌قاعده و بی‌رحمی عجین شده است» (Kamal, 2008). در ایران و بر پایهٔ شرع مقدس، در برابر اقدامات تروریستی قوانینی در نظر گرفته شده است. مطابق با سیستم قضایی و کیفری جمهوری اسلامی ایران، اعمال تروریستی مصداق عنوان «محاربه» در نظر گرفته‌شده است؛ برابر با قانون مجازات اسلامی محاربه تعریف و مجازات آن پیش‌بینی شده است. در بند ۱۸۳ آن ذکر شده که هرکس به قصد رعب و وحشت سلاح اختیار کند و آزادی و امنیت مردم را سلب و مختل کند، دشمن خداست و فساد را گسترش داده است.

این مفهوم را با مثال ایران تکمیل می‌کنیم. ایران با اشکال مختلفی از تروریسم مواجهه است که در ظاهر متفاوت‌اند، اما در حقیقت با یکدیگر دارای اشتراکاتی هستند و به اصطلاح همپوشانی دارند. ۱. تروریسم سازمان‌یافته (یک سازمان سیاسی، اجتماعی یا نظامی، دولتی یا غیردولتی است که بنا به دلایل گوناگون سعی در حذف فیزیکی مخالفان خود دارد. سازمان مجاهدین خلق (منافقین) از مهم‌ترین سازمان‌های تروریستی سازمان‌یافته علیه ایران محسوب می‌شوند؛ ۲. تروریسم مرتبط با قاچاق مواد مخدر؛ ۳. تروریسم ملی‌گرا (شکلی از خشونت که در آن افراد مرتبط با آن گروه در جهت تشکیل یک دولت مستقل با گرایش‌های قومی و

مذهبی اقدام می‌کنند؛ ۴. تروریسم بنیادگرا (گروه‌های تکفیری و سلفی)؛ ۵. تروریسم مدرن که بسیاری این شاخه از تروریسم را به‌منظور تخریب هرچه بیشتر فرهنگ انسانی- مادی و ... می‌دانند) (Qasemi, 2016).

ابزارهای استفاده‌شده از سوی تروریست‌ها (در شکل کلاسیک آن) عبارتند از: هواپیماربایی، گروگان‌گیری، خراب‌کاری، بمب‌گذاری، آدم‌ربایی سیاسی و قتل. سازمان‌های تروریستی سعی می‌کنند با اقداماتی که انجام می‌دهند توجه رسانه‌ها و مردم را به خود جلب کنند. شکلی از اقدامات خشونت‌بار دولتی و یا غیردولتی که با هدف دستیابی به یک هدف سیاسی صورت می‌گیرد، هرچند که تروریسم با انواع دیگر خشونت شباهتی ندارد ولی تروریسم سعی دارد تا نگاه کشورهای دیگر را به یک بی‌عدالتی (خواه واقعی، خواه غیرواقعی) جلب کند (جفری و رجینالد،۱۳۷۴: ۲۶).

۲-۳. تروریسم سایبری

این واژه نخستین بار از سوی کالین باری در دهه ۱۹۸۰ مطرح شد و بیشتر به معنای حمله یا تهدید به حمله علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آن‌هاست (قاسمی،۱۳۹۴: ۲۳۰). به گفته کانوی، تروریسم سایبری عبارت است از: حمله عمدی و آگاهانه با انگیزه‌های سیاسی به‌وسیله گروه‌های فروملی یا عوامل پنهانی علیه اطلاعات، سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌ها که منتهی به خشونت علیه افراد غیرنظامی شود (Sedon,2004: 20).

تروریسم سایبری در واقع به طیفی از عملیات اطلاعاتی علیه موجودیت یک کشور گفته می‌شود که برای رسیدن به اهداف سیاسی انجام می‌گیرد (Theohary,2005:20). امروز دنیای رایانه که در ارتباط با زندگی مردم است، دنیایی است که هرلحظه مورد تهدید تروریست‌ها است و این نگرانی از احتمال وقوع، هرچه بیشتر مردم جوامع را دچار ترس و وحشت می‌کند (طیب،۱۳۸۲: ۸۹). اقدام تروریست‌ها شامل افزایش منابع برای حمایت از عملیات خود، برنامه‌ریزی عملیات، استفاده از ابزارهای در دسترس همانند Google Earth، فرماندهی

و کنترل عملیات، انجام عملیات نفوذی و آموزش و استقرار وسایل انفجاری می‌شود (Starr2009). از سوی دیگر در تروریست سایبری زیرساخت‌های الکترونیکی، مقیاس بازی وضعیت هویتی شهروندان و نوع تصویرسازی از گفتمان رسانه‌ای نیز می‌تواند مهم انگاشته شود (Jarvis,2017: 64). امروزه تروریسم سایبری افکار شهروندان را نیز تحت تأثیر قرار داده است؛ مانند اندیشه و بیان یک حمله تروریستی در فرودگاه یا تیراندازی در مرکز خرید و ... هدف امروزی تروریسم سایبری، نابودی روان شهروندان است (Gross,2016: 288).

این مفهوم از همگرایی فضای سایبر با تروریسم شکل‌گرفته است. «درتی دنینگ»[1] می‌گوید که حمله یا تهدید به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره‌شده در آن‌ها که به شکل غیرقانونی با هدف تهدید یک دولت یا مردم برای دست یافتن به اهداف سیاسی و اجتماعی انجام می‌شود (هالپین، ۱۳۸۹). تروریسم سایبری به استفاده از رسانه‌های اینترنتی و بسترهای ارتباطی برای انجام حملات تروریستی یا ترویج آن اشاره دارد. این حملات می‌تواند اشکال مختلفی مانند انتشار تبلیغات، سرقت یا دستکاری داده‌ها یا ایجاد اختلال در زیرساخت‌های حیاتی داشته باشد. همچنین می‌توان از آن به‌عنوان یک حمله غیرمجاز و یا ایجاد تهدید علیه شبکه‌های رایانه‌ای و داده‌هایی که در آن نگهداری و منتشر می‌شود، یاد کرد. همچنین برای دستیابی به یک هدف سیاسی یا اجتماعی، این کار از طریق ارعاب یا تهدید یک دولت یا شهروندان آن صورت می‌گیرد (Iftikhar, 2024: 2). بنابراین سایبرتروریسم به تروریسمی اطلاق می‌شود که در دنیای مجازی کامپیوتری صورت می‌گیرد. اهداف سایبر تروریست‌ها متمرکز بر روی منابع موجود روی فضای مجازی است به‌عنوان مثال می‌توان حمله به یک سیستم کامپیوتری در یک بیمارستان در یک هواپیما در مرکز خطوط حمل‌ونقل هوایی و زمینی، حمله به کامپیوترهای پنتاگون و کاخ سفید برای مختل کردن سیستم‌های پیام‌رسانی و یا دزدیدن اطلاعات و یا حتی رخنه در یک کامپیوتر شخصی برای انتقام شخصی را ذکر کرد. همه این موارد به نحوی اتفاق می‌افتد که هرگز قربانی نمی‌تواند عامل یا عاملین آن‌ها را شناسایی کند.

1. Dorothy Dning

ابزار مورد نیاز یک حمله اینترنتی در همهٔ دنیا مشترک بوده و شامل یک دستگاه کامپیوتر شخصی و یک خط اینترنتی که بتواند کامپیوتر شخصی را به شبکه جهانی متصل کند، می‌شود. امروزه وابستگی در کلیه زمینه‌های اقتصادی، فرهنگی، سیاسی و اجتماعی به کامپیوتر بر کسی پوشیده نیست؛ همه سازمان‌ها و وزارتخانه‌ها و شرکت‌های بزرگ و چندملیتی تا شرکت‌های کوچک و محلی وابسته به کامپیوتر شده‌اند؛ درحالی‌که بسیاری از آن‌ها نسبت به آسیب‌پذیری کامپیوترها و فاش شدن اطلاعاتشان توسط هکرها ناآگاه هستند.

نظر به اهمیت جنگ‌های سایبری دولت آمریکا در سال ۱۹۹۶ کمیسیونی را تحت عنوان «کمیسیون حفاظت از زیرساخت‌های حیاتی» (Critical Infrastructure Protection) تشکیل داد کمیسیون مذکور به این نتیجه رسید که باید فعالیت‌های خود را بر روی صنایعی چون صنایع الکترونیکی، مخابرات و ارتباطات و کامپیوتر، متمرکز کند زیرا بیشترین حملات جنگ‌های مجازی متوجه آن‌ها خواهد بود.

به‌طور کلی استفاده از ابزارهای دیجیتال و سامانه‌های کامپیوتری برای ایجاد خشونت و تهدید یا هر نوع عملیات خرابکارانه را سایبرتروریسم می‌نامند. به اعتقاد کالین، تروریسم مجازی به حمله یا حملاتی اطلاق می‌شود که با برنامه‌ریزی قبلی و با اغراض سیاسی، توسط گروه‌های ضد دولتی خارجی یا مأموران مخفی خارجی، یا اشخاص حقیقی علیه سامانه‌های اطلاعاتی و ارتباطی، سامانه‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌ها انجام می‌شود (برجعلی‌زاده، ۱۴۰۰). در بین سازمان‌های تروریستی، داعش موسوم به (دولت اسلامی شام و عراق) از رسانه‌های نوین برای هدایت افکار عمومی به‌خوبی بهره گرفته و جدیدترین فیلم‌ها، اعلامیه‌ها و نشریات را در فضای مجازی، تالارهای گفت‌وگو و انجمن‌ها قرار داده و در شبکه‌های اجتماعی نظیر توییتر، فیس‌بوک و گوگل پال بازنشر می‌کنند (جعفری و برجعلی زاده، ۱۳۹۹).

۲-۴. فناوری

فناوری درعینِ‌حال که یکی از کلیدواژه‌های مهم دنیای ما محسوب می‌شود، اما از سردرگم‌کننده‌ترین کلمات کلیدی نیز هست. به‌عنوان یک مقوله تحلیلی، برای درک ما از کل تاریخ بشریت و در واقع فراتر از آن ضروری به نظر می‌رسد. تکنولوژی تنها در نیمه دوم قرن بیستم به یک کلمه رایج تبدیل شد. تا آن زمان سردرگمی مفهومی به این معنا بود که این اصطلاح را می‌توان به معنای وسیع یا محدود به‌کار برد و گاه مؤلفه‌های فرهنگی یا اجتماعی را در برمی‌گرفت و گاه به ابزار صرف یا ابزاری برای رسیدن به اهداف عقلانیت تقلیل می‌یافت (Agar, 2019: 5). هایکمن ادعا می‌کند که فناوری یکی از ویژگی‌های اصلی (ارتباط) انسان– طبیعت و انسان– انسان و مجموعه‌ای از تکنیک‌ها است. فناوری را می‌توان تولید هوشمندانه ابزارهای جدید شامل ابزارهای مفهومی و ایدئال برای رویارویی با موقعیت‌های مشکل‌ساز دانست (Coccia, 2019: 2).

۳. روش تحقیق

روش تحقیق در این پژوهش از نوع کیفی، با رویکرد توصیفی–تحلیلی و شیوه گردآوری داده‌ها کتابخانه‌ای است. از این‌رو، داده‌ها به‌شیوه اسنادی و سنجش مقررات بر پایه اسناد و منابع مکتوب و نیز مطالعه و واکاوی دیدگاه‌های صاحب‌نظران با ابزار فیش‌برداری جمع‌آوری و مورد تجزیه‌وتحلیل قرار گرفته است. پرسش اصلی تحقیق تحلیل و دگردیسی تروریسم سایبری در عصر فناوری اطلاعات به چه نحو است. در پژوهش پیش‌رِو به یافته‌های ادبیات پژوهشی پیشین، مقالات علمی و نظرسنجی‌های معتبر استناد شده است. بر این اساس، تلاش شده است علاوه بر تحلیل تروریسم و سایبر تروریسم در عصر فناوری اطلاعات، به تشریح و تبیین چگونگی با استفاده از قالب نظری «سایبرنتیک»؛ علت پیوند ارتباطات سیستمی و اطلاعات با تأثیرات و تبعات اجتماعی مورد مطالعه قرار گیرد. هدف بیشتر حملات سایبری به حوزه‌های زیرساختی– خدماتی، اقتصادی– مالی و امنیتی– روانی و قابلیت «بدیل‌سازی» هوش مصنوعی، شناسایی‌شده است.

۴. تجزیه‌وتحلیل یافته‌ها

همان‌طور که پیش‌تر اشاره شد، این مقاله از حیث روش‌شناسی یک مطالعه کیفی است و یافته‌های مقاله به‌صورت گزاره‌های کلی مورد اشاره قرار خواهد گرفت. ازآنجایی‌که هدف اصلی این پژوهش، مطالعه تحولاتی است که پیرامون توسعه سریع ابزارها و برنامه‌های کاربردی ناشی از فناوری‌های نوین ارتباطی هوشمند که در دسترس همگانی نیز قرار دارند شکل‌گرفته است؛ پس سوژه امنیت و حفاظت نیز به‌خودی‌خود مطرح و اهمیت بالایی پیدا می‌کند. چراکه این مبحث از یک‌سو، حریم و داده‌های حفاظت‌شده افراد و سازمان‌ها را می‌تواند تحت تأثیر قرار دهد و از سوی دیگر، نگرانی‌هایی را برای نظام حکمرانی از منظر تبعات سوءاستفاده و دست‌کاری عامدانه به جهت مهندسی افکار عمومی، تغییرات سیاسی و اجتماعی، امنیتی‌سازی یا بالعکس امنیت‌زدایی، مختل‌سازی زیرساخت‌ها و در کل، اثرگذاری بر رضایت همگانی و کارآمدی ساختاری برای نیات خاصی به وجود آورد. پژوهش پیش‌رو با بررسی ادبیات موجود تحقیقی، تحلیل گزاره‌های تجربی و عینی و نیم‌نگاهی به سناریوهای محتمل در قالب آینده‌پژوهی، به موارد ذیل دست‌یافته است:

شکاف قابل توجهی میان استراتژی‌ها و اقدامات در این حوزه احساس می‌شود؛ به‌عبارت‌دیگر، توازن مؤثر پیشگیرانه و پیش‌دستانه در برابر تحولات سریع حوزه سایبری هنوز برقرار نشده است؛ روزآمدسازی قوانین و ملاحظات حفاظتی در حوزه امنیت سایبری، یک حوزه غیرسیاسی و فنی است و در چهارچوب امنیت ملی در نظر گرفته می‌شود؛ مجموعه‌ها و افراد حقیقی و بخش خصوصی با انگیزه رقابتی، همگان‌سازی بین‌المللی و نگاه کارکردی به فناوری و ابزارهای مرتبط می‌نگرند؛ در نتیجه فارغ از هر ملاحظه دیگری در استفاده از این بستر تعجیل دارند. این نگاه با رویکرد دولتی که امنیت و حراست از حاکمیت ملی در اولویت است تفاوت ماهوی دارد. پس سیاست‌گذاری‌های کلان در بحث امنیت سایبری باید متناسب با بخش‌های مختلف اعم از دولتی و غیردولتی باشد؛ ازآنجایی‌که منشأ بسیاری از حملات و نفوذ سایبری خارج از مرزهای ملی است، ایجاد کانال‌های رسمی تبادل اطلاعات دو یا چندگانه به جهت بهره‌برداری از تجارب و راهبردها در اتخاذ یک رویکرد

پیش‌بینانه ضرورت دارد؛ نسل سوم هوش مصنوعی درحالِ‌توسعه است و قابلیت حل مسئله آن مشابه توانایی‌های انسانی، امنیت سایبری را در آینده به میزان قابل توجهی پیچیده می‌کند.

حملات تروریسم سایبری بیشتر متوجه حوزه‌های زیرساختی- خدماتی، اقتصادی- مالی و امنیتی- روانی است. آشفتگی اجتماعی- سیاسی به‌منظور اخلال در توانایی مدیریت بحران در سطوح ملی، در منتهی‌الیه هدف تروریسم سایبری قرار دارد. در مراتب پایین‌تر، جنگ‌های ترکیبی (ایجاد زمینه اغتشاشات، جنگ‌های نامتعارف و نامتوازن نقطه‌ای و منطقه‌ای و یا جنگ رسانه‌ای- روانی) نارضایتی معیشتی و اقتصادی با انحراف سرمایه‌گذاری‌های عمومی به‌طرف منابع کاذب و ایجاد توقعات فزاینده مالی و قطبی‌سازی‌های هویتی و ادراکی از طریق ابزارهای رسانه‌ای و ارتباطی می‌توانند جزء اهداف ثانویه تروریسم سایبری تعریف شوند.

هوش مصنوعی همانند شبکه‌های مجازی آنلاین قابلیت «بدیل‌سازی» دارند. یعنی به همان میزان و یا شاید بیشتر، می‌تواند ابزاری تقابلی و دفاعی تلقی و تعریف شوند. دستیابی به این هدف در گرو اولویت دادن به نگاه پژوهش و توسعه و در مرحله بعد، قوانین منعطف در بحث تکنولوژی‌های نوظهور است.

شکل ۲: یافته‌های پژوهش

۴-۱. سنخ شناسی تروریسم

در این بخش با بررسی تاریخی، سوگیری‌های سیاسی، انگیزه و ابزار کاربردی به سنخ‌شناسی تروریسم می‌پردازیم.

۴-۱-۱. سنخ‌شناسی براساس عینیت تاریخی

از حیث تاریخی تروریسم را می‌توان به سنخ‌های مختلفی تقسیم کرد:

۱. تروریسم سنتی: تروریسم سنتی به دنبال نابود کردن موجودیت فیزیکی اشخاصی که از قدرت برخوردار هستند؛ اما از نظر آن‌ها، قدرت آن شخص نامشروع است (فیرحی و ظهیری، ۱۳۸۷: ۱۵۱)؛

۲. تروریسم مدرن: تروریسم مدرن در اواخر قرن هجدهم و پس از انقلاب فرانسه آغاز و برای توصیف اقدامات دولت جمهوری جدید فرانسه برای سرکوب ضدانقلابیون استفاده شد. در اینجا از خشونت با انگیزه‌های سیاسی توسط بازیگران غیردولتی پرداخته می‌شود که در عصر دولت‌محوری اقدام می‌کردند (Walls B. A, 2017: 17). در واقع تروریسم مدرن با ظهور مفهوم دولت- ملت و تعریف یک جامعه خاص در مرزهای ملی مشخص و به‌عنوان قدرت سیاسی شناخته شدن آن هم‌دوره است (فیرحی، ۱۳۸۷: ۱۵۲)؛

۳. تروریسم فرامدرن: در این قِسم، ضمن اینکه تروریسم فرامدرن از دوگونه پیشین خود – سنتی و مدرن – الهام می‌گیرد؛ اما فراتر از آن عمل می‌کند. ضدیت با مدرنیته و جهانی‌سازی و مظاهر آن و به چالش کشیدن نظم مدرن به هر شکل و هر قیمتی و با هر ابزاری، از تروریسم فرامدرن مفهومی مجزا و پیچیده ساخته است (آل غفور و صادقیان، ۱۳۹۷: ۱۳).

۴-۱-۲. سنخ‌شناسی براساس سوگیری‌های سیاسی

از لحاظ سیاسی تروریسم به موارد زیر دسته‌بندی می‌شود:

۱. تروریسم جنبشی: خط اساسی در تروریسم جنبشی این بود که خشونت برای برانگیختن شورش در میان طبقه گسترده کارگر و متحدانش علیه سرمایه‌داری ضروری است. مکانیسم‌های مختلفی که از طریق آن خشونت تروریستی ممکن است با بسیج افراد مرتبط شود، با توجه ویژه به دکترین آنارشیستی «تبلیغ با عمل» که در پایان قرن نوزدهم توسعه یافت، تحلیل می‌شود (Cuenca I. 2019: 1)؛

۲. تروریسم شبه جنبشی: این نوع تروریسم در پیِ از بین بردن نظام سیاسی موجود نیست و هدف آن اعمال تغییر در ساختار سیاسی و اجتماعی است (Vössing K, 2017)؛

۳. تروریسم سرکوب‌شده: براساس ابزارهای سرکوبی که توسط دولت یا یک جنبش انقلابی یا آزادی‌بخش ملی در رابطه با جامعه به‌منظور اعمال رفتار خاص مدنظر خود تعریف می‌شود (Chojnowski, 2020: 14).

۴-۱-۳. سنخ‌شناسی براساس انگیزه

انگیزه تروریست‌ها از ترور هم می‌تواند مبنایی برای تقسیم‌بندی انواع تروریسم باشد که عبارتند از:

۱. تروریسم جدایی‌طلب: اهداف جنبش‌های رادیکال ملی یا جدایی‌طلبانه ریشه در نارضایتی‌هایی مانند تبعیض، بی‌عدالتی و به حاشیه رفتن اقلیت اجتماعی یا سیاسی دارد. ایدئولوژی‌های سیاسی جدایی‌طلبی ریشه در آرمان‌هایی دارد که مورد حمایت بخشی از یک جامعه برای تعیین سرنوشت هستند و از سوابق تاریخی پشتیبانی می‌شوند (Forest, 2018: 1)؛

۲. تروریسم مذهبی: گروه‌های تروریستی که با عنوان مذهب فعال هستند بر این اعتقادند که فعالیت آن‌ها امری مقدس است؛ اما در واقع انگیزه این گروه‌ها، سیاسی بوده و مذهب صرفاً ابزاری برای مشروعیت ساختن اقدامات آن‌ها است (مطلبی و همکاران، ۱۳۹۵: ۵).

۳. تروریسم سیاسی: این شکل از تروریسم در پیِ تحول در یک جامعه و دستیابی به اهداف سیاسی، اجتماعی و یا گروهی خود است؛
۴. تروریسم بنیادگرا: جف هینس، بازتاب و تأثیرات مدرنیته را عامل اصلی شکل‌گیری جنبش‌های بنیادگرا در برخی کشورهای اسلامی می‌داند. چراکه برخی از حکومت‌های سکولار اقدام به تحمیل ارزش‌های غربی به‌جای ارزش‌های دینی کردند. آنتونی گیدنز معتقد است که بنیادگرایی مرتبط با دوران معاصر است. درواقع بنیادگرایی واکنشی انفعالی نسبت به فرایند جهانی‌سازی است. اندرو هیوود هم معتقد است که اگرچه بنیادگرایان با دنیای مدرن در ستیزند؛ اما درعینِ‌حال محصول همین جهان مدرن هستند. هیوود در ادامه علت ایجاد جنبش‌های بنیادگرا را، گسترش سکولاریسم در جهان اسلام، روند عصر پسااستعماری، شکست سوسیالیسم انقلابی و جهانی‌سازی می‌داند (امیری و دیگران، ۱۴۰۰: ۱۱).

۴-۱-۴. سنخ‌شناسی براساس ابزار و کارکرد

گروه‌های تروریستی به لحاظ ابزار و کارکرد به اقسام زیر تقسیم‌بندی می‌شوند:

۱. تروریسم سیستمی: دیدید کلاریج معتقد است که یکی از ویژگی‌های کلیدی تروریسم، ماهیت سیستماتیک آن است که آن را از سایر اقدامات تروریستی پراکنده یا آنی متمایز می‌سازد. وی تصریح می‌کند که به این دلیل بر ویژگی سیستماتیک تروریسم دولتی به‌جای ویژگی عامدانه بودن آن تأکید می‌کند که اثبات قصد دولت در ارتکاب تروریسم بسیار دشوار است و سیستماتیک بودن اقدامات دولت بر قصد آن هم دلالت دارد (محمدی ده چشمه، ۱۳۹۷: ۱۴)؛
۲. تروریسم سایبری: تروریسم سایبری می‌تواند از طریق فضای سایبر و مجازی حملاتی را انجام دهد که جهان فیزیکی و فضای مجازی را در هم ادغام و درگیر کند. جرائم سایبری تروریسم و جنگ سایبری همگی از موضوعات رایج در حوزه امنیت سایبری هستند. تروریسم فیزیکی و تروریسم سایبری عناصر مشترک و هدف مشترکی به نام

ارعاب و تخریب دارند. درمجموع، حملات سایبری یکی از مهم‌ترین تهدیدات امنیت ملی در سراسر جهان محسوب می‌شوند (Milov & Others, 2021: 1)؛

۳. تروریسم اتمی: حمله تروریستی با استفاده از مواد اتمی یا رادیواکتیو یک رویداد با احتمال کم، اما با پیامد بالا است؛ اما در صورت اجرا منجر به اختلالات و آسیب‌های روانی، اقتصادی و اجتماعی بی‌سابقه‌ای خواهد شد (Pomper And Tarini, 2017: 1)؛

۴. «نارکو تروریسم»[1]: مفهوم نارکو تروریسم یا «پیوند تروریسم با مواد مخدر» به عبارت ساده به «فعالیت تروریستی که مرتبط با تجارت مواد مخدر است» اشاره دارد و در سال ۱۹۸۳ توسط رئیس‌جمهور پرو – بلاند تری– برای تحلیل حملاتی که علیه پلیس مبارزه با مواد مخدر کشورش صورت گرفته بود معرفی شد. همچنین، باندهای مواد مخدر با تلاش برای کسب نفوذ سیاسی، سعی در تأثیرگذاری بر سیاست یک کشور با ایجاد ارعاب و مانع‌تراشی در پیگیری قضایی داشتند (Hartelius, 2008: 7).

۴-۲. علت اقبال به تروریسم سایبری

امروزه تروریسم در فضای مجازی و در نظام‌های حقوقی جرم انگاری کیفری شده و با وجود نوظهور بودن، نسبت به سایر تروریست‌ها خطرناک‌تر است، به این دلیل که ساختار اقتصادی و خدمات‌رسانی بسیاری از کشورها مبتنی بر فناوری‌های اطلاعاتی و ارتباطی بناشده و تهدیدات آن به حوزه امنیت ملی دولت‌ها کشیده شده است. جرم‌انگاری سایبری رشته‌هایی مانند روان‌شناسی، جرم‌شناسی، جامعه‌شناسی، علوم کامپیوتر و امنیت سایبری را ترکیب می‌کند تا درک عمیقی از جرائم سایبری به دست آید. جرائم و امنیت سایبری در ارتباط با پلتفرم‌ها، بازیگران و مکان‌های مختلف به هم مرتبط هستند. مسائل در ارتباط با جرائم سایبری به‌طور مداوم و به‌سرعت با توجه به ظهور فناوری‌های جدید، در حال تغییر و توسعه‌اند (shick Choi And Seungeun Lee, 2018: 1). تروریست‌ها اهداف خود را از طریق فضای مجازی گسترش می‌دهند و اقدام به جذب نیرو در فضای مجازی و دریافت کمک‌های

1. Narco Terrorism

مالی و غیرمالی می‌کنند، روش بعدی آن‌ها این است که آموزش و راه‌های ترور در فضای فیزیکی به کاربر آموزش داده شود؛ مانند ساخت بمب‌های دستی و یا نحوه تهیه سلاح. القاعده و داعش، جهت انجام اقدامات تروریستی خود از این راه بهره زیادی برده و موفق به اغفال بسیاری از جوانان از کشورهای مختلف شده است. در تروریسم کلاسیک مواد منفجره و سلاح‌های گرم اصلی‌ترین ابزار تروریسم هستند ولی مهم‌ترین ابزار تروریست‌های سایبری، رایانه است.

به‌طور خلاصه از دلایل گسترش تروریسم سایبری نسبت به تروریسم سنتی می‌توان به موارد زیر اشاره کرد:

۱. تعدد بازیگران در فضای مجازی: کم بودن هزینه فناوری، اتصال به اینترنت و سهولت تولید نرم‌افزار مخرب بدین معنا است که هر شخصی می‌تواند وارد این نوع نرم‌افزارها شود و این اشخاص شامل گروه‌های تروریستی و شرکت‌های خصوصی هستند؛
۲. هزینه کم و سرعت‌بالا برای اقدام: هر شخص یا دولتی برای حمله سایبری فقط نیازمند یک رایانه و دانش فنی در زمینه سایبری دارد. در نتیجه می‌توان گفت که فضای سایبری وضعیتی را فراهم می‌سازد تا با هزینه کم عملیات خطرناکی را در زمان و سرعت بالا انجام داد؛
۳. سخت بودن ردیابی و شناسایی و دستگیری مرتکبین تروریسم سایبری: اینترنت به‌عنوان یک سیستم نامتمرکز طراحی شده است تا کاربران ناشناخته باقی بمانند و این باعث می‌شود تا هیچ اثری از حملات سایبری باقی نماند؛
۴. تأثیرگذاری بالا: وقوع حمله‌های سایبری و بروز اختلال در شبکه‌ها می‌تواند موجب خسارت مالی و اطلاعات حساس و همچنین جان افراد شود و تأثیر و پیامدهای بیشتری بر جای می‌گذارد؛
۵. ساختار فضای اینترنت: بهره‌برداری از این فضا توسط شهروندان به‌گونه‌ای که جداسازی آن‌ها از یکدیگر کار سختی است؛

۶. پایین بودن احتمال بازخواست عملیات مجرمانه در فضای مجازی: در این صورت بازخواست اقدامات مجرمانه کمتر است و افراد در این فضا در مقایسه با سایر گزینه‌های غیرسایبری دارای خطر کمتری هستند (عظیمی و خشنودی، ۱۳۹۵: ۱۶۳).

۴-۳. روش‌های رایج عملیات تروریسم سایبری

برخی از روش‌های رایجی که از طریق آن تروریسم سایبری انجام می‌شود عبارتند از:

۱. بدافزار: نرم‌افزارهای مخرب مانند ویروس‌ها، کرم‌ها، تروجان‌ها و باج‌افزارها می‌توانند برای به خطر انداختن سیستم‌های کامپیوتری و سرقت اطلاعات حساس، مختل کردن زیرساخت‌های حیاتی یا ایجاد هرج‌ومرج مورد استفاده قرار گیرند. تروریست‌های سایبری ممکن است بدافزار را برای دستیابی به اهداف خود توسعه دهند یا مستقر کنند؛

۲. «فیشینگ»[1](کلاه‌برداری اینترنتی): حملات فیشینگ شامل استفاده از ایمیل‌ها وب‌سایت‌ها یا پیام‌های فریبنده برای فریب دادن افراد به افشای اطلاعات حساس مانند اعتبار ورود، جزئیات مالی یا داده‌های شخصی است. از این تاکتیک‌ها می‌توان برای جمع‌آوری اطلاعات یا دسترسی به سیستم‌های حیاتی استفاده کرد؛

۳. محروم‌سازی از اطلاعات و گسترش آن[2]: شامل تحت‌فشار قرار دادن سیستم‌های کامپیوتری یا شبکه هدف با ترافیک بیش‌ازحد است که باعث می‌شود آن‌ها در دسترس نباشند. تروریست‌های سایبری ممکن است از این حملات برای ایجاد اختلال در عملکرد زیرساخت‌ها یا خدمات حیاتی استفاده کنند؛

۴. مهندسی اجتماعی: تکنیک‌های مهندسی اجتماعی شامل دستکاری (روانی) افراد برای افشای اطلاعات محرمانه یا انجام اقداماتی است که ممکن است امنیت را به خطر بیندازند. تروریست‌های سایبری ممکن است برای دسترسی به داده‌ها یا سیستم‌های حساس، هویت افراد یا نهادهای مورد اعتماد را جعل کنند.

1. Phishing
2. Denial of Service (DoS) and Distributed Denial of Service (DDoS)

۵. حمله به ارتباط دوجانبه[1]: این حملات، ارتباطات بین دو طرف را اغلب بدون اطلاع آن‌ها رهگیری و تغییر می‌دهد. تروریست‌های سایبری می‌توانند از شکل از حمله، برای استراق سمع اطلاعات حساس، دستکاری پیام‌ها یا به خطر انداختن امنیت کانال‌های ارتباطی استفاده کنند؛

۶. باج‌افزار: باج‌افزار نوعی بدافزار است که داده‌های قربانی را رمزگذاری می‌کند و تا زمان پرداخت باج غیرقابل دسترسی است. تروریست‌های سایبری ممکن است باج‌افزاری را برای مختل کردن سیستم‌های حیاتی یا اخاذی از سازمان‌های هدف مستقر کنند؛

۷. تهدیدهای داخلی: تهدیدهای داخلی شامل افرادی در یک سازمان می‌شود که عمداً یا ناخواسته به تروریست‌های سایبری در فعالیت‌های خود کمک می‌کنند. این افراد ممکن است به اطلاعات یا سیستم‌های حیاتی دسترسی داشته باشند؛

۸. حملات مشابه استاکس نت: استاکس نت نمونه معروفی از حملات سایبری هدفمند است که به‌طور خاص با هدف ایجاد اختلال در سیستم‌های کنترل صنعتی، مانند مواردی که در تأسیسات اتمی استفاده می‌شود، انجام شد. تروریست‌های سایبری ممکن است سیستم‌های زیرساختی حیاتی را هدف قرار دهند تا آسیب فیزیکی یا تخریب ایجاد کنند؛

۹. بهره‌برداری‌های برای روز صفر[2]: تروریست‌های سایبری ممکن است از آسیب‌پذیری‌های ناشناخته در سیستم‌های نرم‌افزاری یا سخت‌افزاری معروف برای بهره‌برداری‌های روز صفر استفاده کنند تا دسترسی یا کنترل غیرمجاز بر سیستم‌ها را به دست آورند. این آسیب‌پذیری‌ها معمولاً برای سازندگان، فروشندگان نرم‌افزار و یا عموم فاش نمی‌شوند.

1. Man-in-the-Middle (MITM)
2. Zero Day

تروریست‌های سایبری اغلب از ترکیبی از این روش‌ها برای دستیابی به اهداف خود استفاده می‌کنند و انگیزه‌های آن‌ها می‌تواند بسیار متفاوت باشد، ازجمله سیاسی، ایدئولوژیک، مالی یا صرفاً ایجاد هرج‌ومرج و اختلال (Iftikhar, 2024: 5).

تأثیرات منفی تروریسم سایبری:

- ❖ اختلال در زیرساخت‌های حیاتی؛
- ❖ خسارات اقتصادی؛
- ❖ تضعیف اعتماد عموم؛
- ❖ تهدید امنیت ملی؛
- ❖ آسیب به حریم خصوصی؛
- ❖ ترویج خشونت و افراط‌گرایی؛
- ❖ افزایش ترس و عدم اطمینان؛
- ❖ تأثیرات مثبت تروریسم سایبری؛
- ❖ تقویت همکاری‌های بین‌المللی؛
- ❖ تدوین قوانین و مقررات مناسب؛
- ❖ افزایش آگاهی عمومی؛
- ❖ توسعه فناوری‌های امنیتی؛
- ❖ مقابله با انتشار افراط‌گرایی؛
- ❖ حقوق تروریسم سایبری.

عبارت «حقوق تروریسم سایبری» از دو حوزهٔ مجزا، اما مرتبط تشکیل‌شده است: حقوق (به‌ویژه حقوق بین‌الملل) و تروریسم سایبری (Cyber Terrorism) در اینجا توضیح داده‌ایم که این مفهوم دقیقاً به چه معناست و چه مباحثی را در برمی‌گیرد و چه چهارچوب‌های حقوقی بر آن حاکم‌اند.

چهارچوب‌های حقوقی مرتبط با تروریسم سایبری

الف. حقوق بین‌الملل عمومی

منع استفاده از زور: حملات سایبری می‌توانند به‌مثابه «استفاده از زور» علیه دولت دیگر تلقی شوند (ماده ۲، منشور ملل متحد)؛

اصل عدم‌مداخله: نفوذ در سامانه‌های دولتی کشور دیگر، بدون رضایت، می‌تواند نقض اصل حاکمیت باشد.

ب. حقوق بین‌الملل بشردوستانه (IHL)

اگر حمله سایبری در شرایط جنگ مسلحانه رخ دهد، باید اصول IHL مثل تناسب، تمایز میان غیرنظامیان و نظامیان و ضرورت نظامی رعایت شود.

ج. حقوق بشر بین‌الملل

مقابله با تروریسم سایبری نباید ناقض حقوق بشر باشد، مانند حق حفظ حریم خصوصی، آزادی بیان و دسترسی به اطلاعات.

۴-۴. هوش مصنوعی؛ چالشی‌ترین و جدیدترین سوژه در حوزه امنیت سایبری

کار و مطالعه بر روی هوش مصنوعی مدتی پس از پایان جنگ جهانی دوم آغاز شد و در ۱۹۵۶، بود که این عنوان به آن تعلق گرفت؛ تکامل و اهمیت کاربرد آن نیز تا به امروز ادامه داشته است. کاربرد این حوزه، امروزه از بازی‌های رایانه‌ای تا تشخیص بیماری‌ها و از آموزش یا حل مسائل ریاضی تا رانندگی خودکار را شامل می‌شود و این گستردگی به یک میدان جهانی بدل شده است (Russell & Norvig, 2010: 20). کمیسیون اروپا در سال ۲۰۱۸، هوش مصنوعی را این‌گونه تعریف نموده است: «به سیستم‌هایی اطلاق می‌شود که با تجزیه‌وتحلیل محیط خود و انجام اقداماتی با درجاتی از استقلال برای دستیابی به اهداف خاص، رفتار هوشمندانه‌ای را نشان می‌دهند». موج اول تکنیک‌های هوش مصنوعی، هوش مصنوعی «نمادین» نام داشت که الگوریتم‌هایی که کامپیوتر می‌توانست براساس آن‌ها به یک پاسخ هوشمند برسد توسط مهندسان تعریف می‌شد. در دو دهه گذشته و در موج دوم، «داده‌محوری» توسعه یافت که بر مبنای آن، فرایند یادگیری الگوریتم‌ها خودکار انجام می‌شود و نقش متخصصان انسانی حذف می‌شود. این روش از شبکه‌های عصبی مغز انسان الگو

گرفته شده است. موج سوم هم، آینده این حوزه است که در حال حاضر پیش‌بینی‌ها را شامل می‌شود (Boucher, 2020: 5).

پوول و مک وُرث هوش مصنوعی را به‌عنوان زمینه‌ای که سنتز و تجزیه‌وتحلیل عوامل محاسباتی را که هوشمندانه عمل می‌کنند مطالعه می‌کند، تعریف می‌کنند. عامل چیزی است که عمل می‌کند. یک عامل وقتی هوشمند تلقی می‌شود که:

۱. اقدامات آن متناسب با شرایط و اهداف آن است؛
۲. در برابر تغییر محیط و تغییر اهداف انعطاف‌پذیر است؛
۳. از تجربیات یاد می‌گیرد؛
۴. با توجه به محدودیت‌های ادراکی و محاسباتی خود، انتخاب‌های مناسبی انجام می‌دهد.

همچنین این پژوهشگران چهار مکتب پیرامون هوش مصنوعی را مورد شناسایی قرار دادند؛ برخی بر روی ایجاد ماشین‌هایی تمرکز می‌کنند که مانند انسان فکر می‌کنند. برخی دیگر به دنبال ماشین‌هایی هستند که همانند انسان عمل کنند. جریان سوم، به دنبال توسعه ماشین‌هایی هستند که منطقی (که در ارتباط با بهینگی است) عمل کنند. در نهایت طیف چهارم، بر توسعه ماشین‌هایی متمرکز است که عقلانی فکر کنند (Bartneck & Lütge, 2021).

با گسترش هوش مصنوعی، کارشناسان تغییرات منفی و مثبتی را در زندگی دیجیتال تا سال ۲۰۳۵، پیش‌بینی می‌کنند. در این باره، آن‌ها نگرانی‌های عمیقی (از گسترش هوش مصنوعی) در مورد رفاه کلی مردم و جامعه دارند. همچنین، انتظار مزایا و تحولات مثبتی را هم در مراقبت‌های بهداشتی، پیشرفت‌های علمی و آموزش با توسعه هوش مصنوعی دارند. بااین‌حال، یکی از نگرانی‌های عمده پژوهشگران و کارشناسان این حوزه، آسیب‌های رشد این فناوری در بحث ارتباطات انسانی، نهادی و دولتی است. هوش مصنوعی به لطف پیشرفت‌های تکنولوژیکی و با دسترسی به حجم زیادی از داده‌ها، روش یادگیری ماشینی و افزایش قدرت محاسباتی، به ابزاری قدرتمند تبدیل شده است. انتشار «چت جی.پی.تی»[1] در

۱. چت‌جی‌پی‌تی ChatGPT، یک بات مکالمه است که توسط شرکت Open AI توسعه یافته است. چت جی.پی.تی به‌عنوان یک نمونه اولیه در نوامبر ۲۰۲۲، معرفی شد و به‌سرعت به دلیل پاسخ‌های دقیق و واضح خود در بسیاری از حوزه‌ها، توجه‌ها را به خود جلب کرد.

پایان سال ۲۰۲۲، یک پیشرفت جدید در هوش مصنوعی بود. این گستره وسیع از امکانات مربوط به انطباق هوش مصنوعی همه‌منظوره با مجموعه وسیعی از وظایف و ایجاد هوش مصنوعی مولد برای تولید محتوای مصنوعی براساس درخواست‌های ورودی توسط کاربر را نشان می‌دهد. پیش‌بینی می‌شود که تا سال ۲۰۲۶، ۹۰ درصد از محتوای آنلاین ممکن است به‌صورت مصنوعی تولید شود؛ اما نگرانی‌ها در مورد استفاده از هوش مصنوعی، از اواخر دهه دوم قرن بیست‌ویکم به وجود آمده است؛ نگرانی‌هایی که ابتدا به فرایند انتخابات مربوط می‌شد و این نگرانی با تکامل اخیر هوش مصنوعی افزایش‌یافته است. زیرا ابزاری قدرتمند برای اطلاع‌رسانی و تزریق اطلاعات نادرست است که هر دو می‌توانند باعث ایجاد تنش و درگیری‌های مرتبط با انتخابات و حتی خشونت شوند. برای مثال، هوش مصنوعی می‌تواند اطلاعات نادرست تولید کند یا سوگیری یا نظراتی را منتشر کند که بیانگر احساسات عمومی نیست. درمجموع، علی‌رغم مزایایی که هوش مصنوعی به‌همراه دارد، این پتانسیل را نیز دارد که بر روندهای اجتماعی– سیاسی مانند انتخابات به روشی منفی تأثیر بگذارد (Adam And Hocquard, 2023: 1).

کارشناسانی که به این مسائل پرداخته‌اند، نگرانند که هنجارها، استانداردها و مقررات پیرامون فناوری به اندازه کافی برای بهبود تعاملات اجتماعی و سیاسی افراد و سازمان‌ها تکامل نخواهند یافت. دو نگرانی اساسی در این بین وجود دارد؛ گرایش به سلاح‌های خودران و جنگ سایبری و چشم‌انداز سیستم‌های دیجیتال مجزا. آن‌ها همچنین معتقدند که ممکن است با شتاب گرفتن سرعت تغییرات فناوری، اوضاع بدتر شود. ممکن است بی‌اعتمادی مردم به یکدیگر افزایش یابد و اطمینان آن‌ها به نهادها و سازمان‌ها کاهش یابد. این به‌نوبه خود می‌تواند سطح نامطلوبی از قطبی شدن، ناهماهنگی شناختی را ایجاد و کناره‌گیری عمومی از گفتمان‌های اصلی را عمیق‌تر کند. همچنین سیستم‌های دیجیتال بسیار تأثیرگذار خواهند شد؛ چیزی که نمی‌توان از آن اجتناب کرد و همه کاربران را متأثر خواهد کرد (Anderson & Rainie, 2023: 7). در طول تاریخ، سیاست از طریق کنش آگاهانه و تعاملات

جمعی مرتبط در درون شبکه‌ها و سازمان‌ها هدایت شده صورت گرفته است؛ اما در حال حاضر، می‌توان پیش‌بینی کرد که پیشرفت هوش مصنوعی، چشم‌انداز ما را از سیاست و در تمامی سطوح مورد تغییر اساسی قرار خواهد داد. به‌عبارت‌دیگر، ایده یک نهاد غیرانسانی دارای عاملیت خاص می‌تواند تغییرات اساسی در درک ما از سیاست در گسترده‌ترین سطوح ایجاد نماید (Chatham House, 2018). در بین رفتارهای مرتبط با انسان، سیاست ممکن است یکی از دشوارترین آن‌ها برای ماشینی کردن و غیرارادی‌سازی به نظر بیاید. همان‌طور که معمولاً درک می‌شود، سیاست یک کار ذاتاً پیچیده است که پیچیدگی رفتار انسان را در مقیاس فردی و جمعی منعکس می‌کند. این پیچیدگی در سطح روابط بین‌الملل دوچندان می‌گردد. در دسترس بودن داده‌ها و قدرت محاسبه، دو ویژگی هستند که اخیراً از طریق هوش مصنوعی فراگیر شده است. این امر منجر به استفاده روزافزون از هوش مصنوعی در طیف گسترده‌ای از امور مانند کمپین‌های سیاسی و بازارهای کار گرفته تا بهداشت، آموزش و ... شده است. فرصت‌های جدید و برخی رسوایی‌های مرتبط با فناوری مانند قضیه پرونده کمبریج آنالیتیکا (در سال ۲۰۱۰، اطلاعات شخصی میلیون‌ها کاربر فیس‌بوک بدون رضایت آن‌ها توسط شرکت مشاوره بریتانیایی «کمبریج آنالیتیکا» جمع‌آوری شد که عمدتاً برای تبلیغات سیاسی استفاده شد)، بحث‌هایی را در میان سیاست‌گذاران، سیاست‌مداران، کارشناسان و ذی‌نفعان در مورد نکات مثبت و اثرات منفی هوش مصنوعی بر سیاست، اقتصاد، بازار کار، عدالت، حریم خصوصی و سایر مسائل کلیدی اجتماعی برانگیخته است. خط‌مشی عمومی و حکمرانی می‌تواند نقش مهمی در حصول اطمینان از پیشرفت‌های مفید و آگاهی از آسیب‌های هوش مصنوعی ایفا کند. درحالی‌که اخیراً توسعه هوش مصنوعی عمدتاً توسط شرکت‌های خصوصی بزرگ جهانی و انگیزه‌های سودآوری آن‌ها انجام شده است، تحولات سیاسی نوظهور نشان می‌دهد که دولت‌ها و سازمان‌های بین‌المللی با همکاری طیف گسترده‌ای از سهام‌داران، در حال آماده‌سازی چهارچوب‌های حاکمیتی برای هوش مصنوعی هستند (Ulnicane And Others, 2022: 3).

در کنار موارد فوق از تحولات صورت گرفته در حوزه‌های سیاسی و اجتماعی پیرامون توسعه و فراگیری هوش مصنوعی، در مباحثات امنیتی نیز، موارد مشابهی در جریان است. هوش مصنوعی به سازمان‌های تروریستی، گروه‌های افراطی و افراد مرتبط با آن‌ها فرصت‌های جدیدی برای انجام حملات سایبری پیچیده‌تر و مخرب‌تر می‌دهد. هوش مصنوعی می‌تواند پیچیدگی و اثربخشی حملات سایبری تروریستی را افزایش دهد و درعینِ‌حال شناسایی آن‌ها را کاهش دهد؛ همچنین، سازمان‌های تروریستی از هوش مصنوعی برای توسعه ابزارها و نرم‌افزارهای پیشرفته برای راه‌اندازی حملات سایبری بهره می‌برند (Monther Abed, 2024: 10). از طرف دیگر، برای مقابله تروریسم سایبری می‌توان از هوش مصنوعی بهره برد که البته نیازمند رویکردی چند رشته‌ای است که زمینه‌های حقوقی، فناوری و امنیتی را ترکیب می‌کند. علاوه بر این، با برای توسعه تکنیک‌های تشخیص الگو و تجزیه‌وتحلیل کلان داده‌ها برای شناسایی و مبارزه با فعالیت‌های تروریستی بالقوه، هوش مصنوعی می‌تواند نقش مهمی در بهبود توانایی‌ها برای شناسایی سریع و دقیق الگوهای مشکوک داشته باشد، بنابراین ما را قادر می‌سازد به‌طور مؤثرتری با تهدیدات تروریستی سایبری مقابله کنیم. موارد جانبی شناسایی‌شده پیرامون هوش مصنوعی تاکنون بر پایه این فرض استوار بوده که هوش مصنوعی به‌خودیِ‌خود مشکل‌ساز نیست و نشان می‌دهد که آنچه به‌طور بالقوه مشکل‌ساز است آن است که هوش مصنوعی چگونه، در چه زمینه‌هایی و چه کسانی را هدف قرار می‌دهد و چه کسانی ذی‌نفعان واقعی آن هستند. بااین‌حال، پیش‌بینی‌های متفاوتی درباره آینده هوش مصنوعی وجود دارد. در اروپا، برخی صاحب‌نظران امیدوارند که به کمک هوش مصنوعی، فرایندهای سیاسی و تقویت ارتباط میان جامعه و سیاست‌مداران بهبود بخشد. هرچند به‌طور کلی نگرانی‌ها پیرامون تأثیر هوش در مسائلی مانند امنیت عمومی، رفاه عمومی و نبود قوانین جامع و اثرگذار به قوت خود باقی است. دسترسی قابل‌توجه به اطلاعات و قدرت محاسبه بالا، کاربری عمومی و قابلیت دسترسی آسان در کنار استقلال هوش مصنوعی از عامل انسانی، فراگیرترین سطح نگرانی از توسعه

هوش مصنوعی است. بنابراین موضوع تغذیه تروریسم سایبری از طریق هوش مصنوعی می‌تواند چالشی مهم در عصر مدرن در نظر گرفته می‌شود.

۴-۵. ابعاد اجتماعی و فرهنگی سایبر تروریسم و راهکارهای آن

ظهور و بسط گروه‌های تروریستی مجازی و سایبری به‌عنوان بازیگرانی جدید در عرصه داخلی و بین‌المللی تأثیر جدی بر نفوذ و گسترش قدرت تروریسم گذاشته است.

هزینه محدود ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از گروه‌های سازمان‌یافته و تروریستی و افراد با ورود به این فضا، زمینهٔ تهدیدات سایبری در برخی جوامع را فراهم آورند.

عمده‌ترین راهکاری مقابله با تروریسم سایبری در بُعد اجتماعی و فرهنگی عبارتند از:

- ❖ گسترش حوزه نفوذ رسانه‌های داخلی؛
- ❖ ایجاد و بسط شبکه‌های اجتماعی داخلی؛
- ❖ گسترش قدرت مانور دولت‌ها در فضای سایبری؛
- ❖ ایجاد ارتش‌های سایبری پنهان برای مقابله با تهدیدات سایبری.

۴-۶. چشم‌انداز پیش‌رِو در حوزه تروریسم سایبری

تحقیقات آتی در مورد تروریسم سایبری باید حوزه‌های مختلف حیاتی را در برگیرد تا درک جامعی از این چشم‌انداز تهدید در حال تحول به دست آید. بررسی ادراکات و آگاهی در میان ذی‌نفعان مختلف، مانند افراد، سازمان‌ها و سازمان‌های دولتی، سطح آمادگی و شناخت خطرات تروریسم سایبری را روشن می‌کند. در گام بعدی، تجزیه‌وتحلیل تأثیر حملات سایبری بر بخش‌های مختلف ازجمله مالی، مراقبت‌های بهداشتی و زیرساخت‌های حیاتی، بینش ارزشمندی را در مورد پیامدهای بالقوه و آسیب‌پذیری‌هایی که باید مورد توجه قرار گیرند، ارائه می‌کند. علاوه بر این، ارزیابی اثربخشی اقدامات متقابل و استراتژی‌های موجود،

همراه با شناسایی روندهای فناوری نوظهور، می‌تواند به درک سیاست‌گذاران و کارشناسان امنیتی در مورد بهترین شیوه‌ها برای کاهش مؤثر تهدیدات سایبری کمک کند. یکی دیگر از جنبه‌های مهم تحقیق مبتنی بر مطالعه این موضوع، بررسی تجارب بین‌المللی و امکان‌سنجی همکاری در مبارزه با تروریسم سایبری است. ازآنجایی‌که ممکن است حملات سایبری از مرزهای ملی فراتر رود، میزان اشتراک اطلاعات و تلاش‌های مشترک می‌تواند زمینه‌هایی را که همکاری فراملی را تقویت می‌کند برجسته کند. علاوه بر این، بررسی چهارچوب‌های حقوقی و سیاسی کشورهای مختلف در واکنش به تروریسم سایبری برای شناسایی شکاف‌ها و ناهماهنگی‌ها ضروری است و امکان تدوین قوانین سایبری هماهنگ و مؤثر را فراهم می‌کند. چنین تحقیقاتی می‌تواند به درک عمومی و نفوذ رسانه‌ها نیز بپردازد، زیرا درک عمومی چگونگی عملیات تروریسم سایبری می‌تواند بر استراتژی‌ها و سیاست‌های عمومی تأثیر بگذارد (Iftikhar, 2024: 9).

در چشم‌انداز همیشه در حال تحول امنیت سایبری، نکات مهمی در مورد چالش‌های چندوجهی پیش‌رِوی تصمیم‌گیرندگان در سراسر جهان قرار می‌گیرد. بی‌ثباتی ژئوپلیتیکی، فناوری‌های به‌سرعت در حال پیشرفت و شکاف فزاینده در قابلیت‌های سایبری سازمانی نیاز به ایجاد انعطاف‌پذیری و توانمندسازی را تقویت می‌کند. در سال ۲۰۲۳، جهان با نظم ژئوپلیتیکی قطبی‌شده، درگیری‌های مسلحانه متعدد، بدبینی و اشتیاق در مورد پیامدهای فناوری‌های آینده و عدم اطمینان اقتصادی جهانی مواجه شد. شکاف شدیدی بین سازمان‌های مقاوم در برابر تهدیدات سایبری و سازمان‌هایی که در حال مبارزه هستند، پدید آمده است. این شکاف در برابری امنیت سایبری با خطوط چشم‌انداز تهدیدات، روندهای اقتصاد کلان، مقررات صنعت و پذیرش زودهنگام فناوری‌های تغییردهنده پارادایم، توسط برخی سازمان‌ها تشدید می‌شود. سایر موانع، ازجمله افزایش هزینه دسترسی به خدمات سایبری نوآورانه، ابزارها، مهارت‌ها و تخصص، همچنان بر توانایی اکوسیستم جهانی برای ایجاد فضای سایبری ایمن‌تر در مواجهه با تغییرات بی‌شمار آن تأثیر می‌گذارد. نابرابری فزاینده‌ای از حیث امنیتی بین سازمان‌هایی که انعطاف‌پذیری سایبری دارند و آن‌هایی که این‌گونه نیست وجود دارد.

فناوری در حال ظهور چالش‌های مرتبط با تاب‌آوری سایبری را تشدید خواهند کرد. ازآنجایی‌که سازمان‌ها برای پذیرش فناوری‌های جدید مانند هوش مصنوعی مولد (AI) رقابت می‌کنند، به درک اساسی از پیامدهای فوری، میان‌مدت و بلندمدت این فناوری‌ها برای وضعیت انعطاف‌پذیری سایبری آن‌ها نیاز است. تقریباً نیمی از مدیران می‌گویند که پیشرفت در قابلیت‌های متخاصم سایبری (فیشینگ، بدافزار، جعل پیشرفته یا دیپ فیک[1]) نگران‌کننده‌ترین تأثیر هوش مصنوعی مولد بر امنیت سایبری است (Jurgens & Dal Cin, 2024).

نتیجه‌گیری و پیشنهاد

تهدیدات بالقوه ناشی از تروریسم سایبری هشدارهای قابل‌توجهی را برانگیخته است. بسیاری از کارشناسان امنیتی، سیاستمداران و دیگران خطر هک کردن سیستم‌های کامپیوتری دولتی و خصوصی توسط تروریست‌های سایبری و فلج کردن بخش‌های مالی، خدماتی و امنیتی در اقتصادهای توسعه‌یافته را اعلام کرده‌اند. برای مثال، ساختار در جوامع غربی از طریق رایانه‌ها شبکه‌بندی شده است، پیش از این و حتی تا به امروز نیز، تهدید هک و هکرها وجود داشته است. اگرچه انگیزه هکرها همان اهدافی نیست که الهام‌بخش تروریست‌ها است؛ اما نشان داده‌شده که افراد می‌توانند به اطلاعات حساس و عملیات خدمات حیاتی دسترسی پیدا کنند. تروریست‌ها حداقل در تئوری، می‌توانند از راه هکرها پیروی کنند و سپس با نفوذ به سیستم‌های کامپیوتری دولتی و خصوصی، بخش‌های نظامی، مالی و شهری را فلج کرده یا حداقل از کار بیندازند. اقتصادهای امروزی و وابستگی فزاینده جوامع ما به فناوری اطلاعات، شکل جدیدی از آسیب‌پذیری را ایجاد کرده است و به تروریست‌ها این فرصت را می‌دهد که به اهدافی نزدیک شوند که تا پیش‌ازاین کاملاً غیرقابل حمله بودند، مانند سیستم‌های دفاع ملی و سیستم‌های کنترل ترافیک هوایی. با توجه به این نکته، هرچه کشوری از نظر فناوری توسعه‌یافته‌تر باشد، در برابر حملات سایبری علیه زیرساخت‌های خود آسیب‌پذیرتر می‌شود؛ پس باید در کنار توسعه فناوری، بحث دفاع سایبری را نیز به‌پیش ببرد.

1. Deepfake

در کنار این مسئله، انگیزه‌های روانی، سیاسی و اقتصادی برای ترویج ترس از تروریسم سایبری ترکیب شده‌اند. از منظر روان‌شناختی، دو مورد از بزرگ‌ترین ترس‌های دوران مدرن در اصطلاح «تروریسم سایبری» ترکیب شده است: ترس از قربانی شدن تصادفی به شکل اجباری با نوعی بی‌اعتمادی و ترس آشکار از برخی از فناوری‌های مرتبط با رایانه، البته در این بین، عده‌ای از کارشناسان هم اعتقاد دارند که در مورد تأثیرات و تهدیدات تروریسم سایبری اغراق شده است؛ چراکه در کل حملات سایبری به اجزای حیاتی زیرساخت‌های ملی غیرمعمول نیست و موارد متعددی از آن وجود دارد؛ اما تاکنون توسط تروریست‌ها انجام‌نشده است و آسیبی که به‌عنوان یک عملیات وسیع توسط تروریسم سایبری از آن یاد کنیم (به شکل بالفعل) تاکنون ثبت نشده است (به‌عبارت‌دیگر، تروریسم سایبری از حیث تهدید وجود دارد؛ اما در طی یک عملیات واقعی و مؤثر هنوز صورت نگرفته است).

بااین‌حال، تروریسم سایبری به چند دلیل گزینه جذابی برای تروریست‌های مدرن است: کم‌هزینه‌تر از روش‌های سنتی تروریسم است؛ بیش از روش‌های سنتی تروریستی ناشناس باقی خواهد ماند؛ تنوع و تعداد اهداف بسیار زیاد است (چندین مطالعه نشان داده است که زیرساخت‌های حیاتی، مانند شبکه‌های برق و خدمات اضطراری، در برابر حملات تروریستی سایبری آسیب‌پذیر هستند)؛ تروریسم سایبری می‌تواند از راه دور انجام شود؛ تروریسم سایبری این پتانسیل را دارد که بر تعداد بیشتری از مردم نسبت به روش‌های سنتی تأثیر بگذارد و در نتیجه پوشش رسانه‌ای بیشتری ایجاد خواهد شد که در نهایت این چیزی است که تروریست‌ها می‌خواهند. تعداد زیاد و پیچیدگی اهداف بالقوه تضمین می‌کند که تروریست‌ها می‌توانند نقاط ضعف و آسیب‌پذیری برای سوءاستفاده پیدا کنند.

شکل ۳: تفکیک مفاهیم، سازوکار و اهداف تروریسم سایبری

پیشنهادهای پژوهش

با توجه به مطالب فوق پیرامون واکاوی ماهیت، سازوکار و اهداف «تروریسم سایبری»، اکنون می‌توان مهم‌ترین موارد جهت اتخاذ یک رویکرد دفاعی و پیشگیرانه در برابر این تهدید نوظهور را به‌اختصار بیان کرد:

حوزهٔ جرم انگاری تروریسم سایبری و یا روزآمدسازی قوانین آن، به علت زوایای متعدد تحلیلی و تبعات پیچیده این تهدید، یک حوزه میان‌رشته‌ای محسوب می‌شود و نیازمند مشارکت طیف وسیعی از کارشناسان و تصمیم‌گیرندگان است؛

روش و مسیر عملیاتی تروریسم سایبری نسبت به اشکال سنتی‌تر تروریسم، به دلیل گسترش و در دسترس بودن فضای آنلاین و ابزارهای کاربری مربوطه، تنوع اهداف، قابلیت اختفا پیش و پس از عملیات، همچنین کم‌هزینه‌تر بودن آن به نسبت روش‌های پیشین هموارتر است؛

اساساً اینترنت یک بستر نامتمرکز است. به همین علت، ردیابی تروریسم سایبری پس از عملیات، بسیار سخت‌تر از روش‌هایی است که در گذشته مورد بهره‌برداری قرار گرفته‌اند؛ روزآمدسازی بی‌وقفه شبکه دفاعی مجازی، مشخص کردن سناریوهای تهاجمی ممکن و پیش‌بینی راه‌های نفوذ احتمالی؛ باید در اولویت تصمیم‌گیرندگان قرار بگیرد؛

پذیرش زودهنگام فناوری‌های تغییردهنده قواعد و پارادایم‌های موجود مانند هوش مصنوعی، مقوله امنیت را در پیچیده‌ترین مقطع تاریخ خود قرار داده است. هوش مصنوعی به‌صورت عمومی دارای سه ویژگی برجسته است؛ ۱. سرعت محاسبه و منابع اطلاعاتی بسیار بالا؛ ۲. استقلال از عامل انسانی و ۳. در دسترس بودن و سادگی کاربردی. چنین فناوری حساس و پیشرفته‌ای امروزه می‌تواند سریع‌تر و هوشمندانه‌تر از هر سازمان و مجموعه‌ای، به کاربران مشاوره و پیشنهاد دهد.

در مسئله امنیت سایبری میان بخش عمومی و حاکمیتی یا به‌عبارت‌دیگر بخش کاربران مستقل و سازمانی، نابرابری امنیتی و شکاف حفاظتی مشهودی وجود دارد. این شکاف محل نفوذ و عملیات احتمالی تروریسم سایبری است. ضرورت توسعه مبحث آموزش (مخصوصا به پرسنل حفاظتی و فنی)، الزام کاربری ایمن و اطلاع‌رسانی همگانی در برابر تهدیدات نوظهور مجازی بیش‌ازپیش احساس می‌شود.

قابلیت‌های متخاصم سایبری از قبیل فیشینگ (کلاهبرداری سایبری)، بدافزار، جعل پیشرفته یا (Deep Fake)، اخلال در حمل‌ونقل و بخش خدمات عمومی، تخریب زیرساخت‌های شهری، نفوذ، انتقال و یا آسیب به مراکز ثبت و پردازش اطلاعات و انتشار اخبار و اطلاعات فریب‌دهنده از طریق رسانه‌ها (Disinformation) بیش از سایر تهدیدات مطرح شده‌اند.

گسترش همکاری بین کشورها برای به اشتراک‌گذاری اطلاعات و توسعه استراتژی‌های مشترک برای مبارزه با تغذیه تروریسم سایبری با استفاده از هوش مصنوعی.

فهرست منابع

- ام الیوت، جفری؛ رابرت رجینالد (۱۳۷۴). ***فرهنگ اصطلاحات سیاسی استراتژیک***، ترجمه میرحسن رئیس زاده لنگرودی. تهران: معین: ۲۶.
- امیرلی، حسین؛ کامیار، ثقفی (۱۴۰۰). ***ارائه مدل مفهومی مدیریت تهدیدات ناشی از تروریسم سایبری***. فصلنامه مطالعات راهبردی فضای سایبر ۱(۲): ۲
- امیری، سروش؛ مرادی، عبدالله؛ عباسعلی، جباری ثاتی (۱۴۰۰). ***تأثیر مدرنیته در پیدایش بنیادگرایان مذهبی تروریستی در عراق؛ با تأکید بر بحران نوسازی سیاسی، اقتصادی، اجتماعی، فرهنگی***، فصلنامه علمی امنیت ملی ۱۱(۴۰): ۱۱-۱۳.
- آشوری، داریوش (۱۳۸۲). ***دانشنامه سیاسی***، تهران: انتشارات مروارید.
- آل غفور، سید محسن؛ رضا، صادقیان (۱۳۹۷). ***مدرنیته، جهانی‌شدن و پدیده تروریسم مدرن و پسا مدرن***. فصلنامه سیاست ۴۸(۳): ۱۳.
- برجعلی زاده، محمد؛ جعفری، علی؛ کردی، ناهید (۱۴۰۰). ***نقش فناوری‌های نوین ارتباطی در گسترش دیپلماسی در عرصه بین‌الملل (مورد مطالعه: استادان دانشگاه، کارشناسان و پژوهشگران رسانه)***، فصلنامه پژوهش‌های ارتباطی، شماره ۱(پیاپی ۱۰۵)، ص.۴۱-۶
- برهانی، محسن؛ حاج محمدی، عاطفه (۱۳۹۸). ***بررسی تطبیقی تروریسم سایبری در قوانین جزایی کشورهای ایران و آمریکا***، فصلنامه مطالعات حقوق، شماره سام، بهار.
- پاکزاد، بتول (۱۳۹۰). ***ماهیت تروریسم سایبری ویژه‌نامه شماره ۴ مجله تحقیقات حقوقی دانشگاه شهید بهشتی***، دوره ۱۴، شماره ۴.
- پلینو، جک سی؛ روی آلتون (۱۳۷۵). ***فرهنگ روابط بین‌الملل***. ترجمه و تحقیق حسن پستا. تهران: فرهنگ معاصر: ۲۴۳.
- جعفری، علی؛ برجعلی زاده محمد (۱۳۹۹). ***فضای سایبر و جهانی‌شدن گسترده تهدیدات امنیتی***، فصلنامه علمی امنیت ملی، سال دوازدهم، شماره چهل و چهارم، تابستان.
- طیب، علیرضا (۱۳۸۴). ***تروریسم در فراز و فرود تاریخ***، تهران: نشرنی.
- عالی پور، حسن (۱۴۰۰). ***حقوق کیفری فناوری اطلاعات***، تهران: خرسندی.
- عاملی، سید سعیدرضا (۱۳۹۰). ***رویکرد دو فضایی به آسیب‌ها، جرائم، قوانین و سیاست‌های فضای مجازی***، تهران: امیرکبیر.

- عظیمی، فاطمه؛ خشنودی، هادی (۱۳۹۵). ***نقش تروریسم سایبری در تهدید علیه امنیت ایران و راه‌های پیشگیری از آن***، فصلنامه مطالعات سیاسی، سال نهم، شماره ۲۴.
- فریدپور، داود؛ محمدحسین، قربانی زواره (۱۴۰۰). ***رویکرد ویژه سازمان‌های تروریستی به رسانه‌های اجتماعی و فضای مجازی***. فصلنامه علوم خبری ۱۰ (۳۹): ۱.
- فضلی، حسن؛ دهشیری، محمدرضا (۱۳۹۵). ***بررسی و تحلیل تروریسم سایبری با رویکرد پیشگیری وضعی***، فصلنامه علمی تخصصی دانش انتظامی لرستان، سال چهارم، شماره دوم.
- فیرحی، داوود؛ ظهیری، صمد (۱۳۸۷). ***تعریف، تاریخچه و رهیافت‌های موجود در تحلیل پدیده تروریسم***. فصلنامه سیاست. ۷(۳۸): ۱۵۲-۱۵۷.
- قاسمی، غلامعلی؛ باقرزاده، سجاد (۱۳۹۴). ***جایگاه مبارزه با سایبر تروریسم***، مجله حقوقی بین‌المللی، شماره ۵۲، بهار و تابستان، صص:۲۵۴-۲۲۷.
- ماهنامه اطلاعات سیاسی اقتصادی (۱۳۸۰)، شماره ۱۷۱-۱۷۲
- محمدی ده چشمه، نواب (۱۳۹۷). ***تروریسم دولتی: پندار یا واقعیت***. مجله پژوهش‌های حقوقی ۳۶: ۱۴.
- مطلبی، مسعود؛ آرایش، حسن؛ سید رضا، رحیمی عماد (۱۳۹۵). ***تروریسم از منظر بنیادگرایان اسلامی رادیکال و فقه سیاسی شیعه؛ با نگاهی به عملیات استشهادی***. فصلنامه پژوهش‌های سیاسی جهان اسلام ۶(۴): ۵.
- هالپین، ادوارد و همکاران (۱۳۸۹). ***جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی***، ترجمه روح‌الله آرانی، دفتر مطالعات سیاسی مرکز پژوهش‌های مجلس.
- یزدانی و همکاران (۱۳۹۳). ***سایبر تروریسم شکل نوینی از ترور علیه منافع ملی***، فصلنامه پژوهش‌های بین‌الملل، دوره ۴، شماره ۱۳.

References

- Adam, Michael And Clotilde, Hocquard. (2023). Artificial intelligence, democracy and elections. EPRS | European Parliamentary Research Service. PE 751.478: 1.
- Agar, Jon. (2019). What is technology?. Annals of Science: 5.
- Al-Ghafour, Seyyed Mohsen and Reza, Sadeghian. (2018). Modernity, Globalization and the Phenomenon of Modern and Postmodern Terrorism. Journal of Politics 48(3): 13 .[In Persian]
- Amiri, Soroush, Moradi, Abdullah and Abbasali, Jabbari Sati. (1400). The impact of modernity on the emergence of terrorist religious fundamentalists in Iraq (with emphasis on the crisis of political, economic, social and cultural modernization). Quarterly Journal of National Security 11(40): 11-13. [In Persian]
- Amirli, Hossein and Kamyar, Saghafi. (2021). Presenting a conceptual model for managing threats arising from cyber terrorism. Quarterly Journal of Strategic Cyberspace Studies 1(2): 2 [In Persian]
- Anderson, Janna And Lee, Rainie. (2023). As AI Spreads, Experts Predict the Best and Worst Changes in Digital Life by 2035. Pew Research Center: 7.
- August. Vincent. (2021). Network concepts in social theory: Foucault and cybernetics. SAGE | European Journal of Social Theory: 1–21.
- Azimi, Fatemeh and Khosnoudi, Hadi (2016), The role of cyber terrorism in the threat to Iran's security and ways to prevent it, Quarterly Journal of Political Studies 9, No. 24, pages 159-172. [In Persian]
- Bartneck, Christoph. And Christoph Lütge. (2021). What Is AI?. An Introduction to Ethics in Robotics and AI. Berlin: Springer Nature.
- Birawal. Imam. (2022). Implication of Artificial Intelligence in Cybernetics. Int J Swarm Evol Comput. 11(12): 1.
- Boucher, Philip. (2020). Artificial intelligence: How does it work, why does it matter, and what can we do about it?. STOA | Panel for the Future of Science and Technology. PE 641.547: 5-6.
- Broeders, Dennis, Fabio, Icon & Daan, Weggemans. (2023). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy. Studies in Conflict & Terrorism 46(12): 1.
- Chatham House. (2018). Artificial Intelligence and International Affairs Disruption Anticipated. The Royal Institute of International Affairs. No. 208223: 5.
- Chojnowski, Lech. (2020). On Terrorism And Its Typologies. Security Dimensions 33: 14.
- Coccia, Mario. (2019). What is technology and technology change? A new conception with systemic-purposeful perspective for technology analysis. Journal of Social and Administrative Sciences 6(3): 2.
- Corning, Peter A. (1996). Synergy, Cybernetics and the Evolution of Politics. International Political Science Review. 17(1): 2.
- Cuenca I. Sánchez. (2019). Revolutionary Terrorism and Its Ideological Roots, In: The Historical Roots of Political Violence: Revolutionary Terrorism in Affluent Countries. Cambridge University Press: 1.

- Fairhi, Davoud; Zahiri, Samad (2008). Definition, history and existing approaches in analyzing the phenomenon of terrorism. Quarterly Journal of Politics. 7(38): 152-157. [In Persian]
- Faridpour, Davud and Mohammad Hossein, Ghorbani Zavareh. (2021). The special approach of terrorist organizations to social media and cyberspace. Quarterly Journal of News Sciences 10 (39): 1. [In Persian]
- Forest, James J.F. (2018). Nationalist and separatist terrorism. London: Routledge.
- Gross, Michael L, Canetti, Daphna, Dana R. Vashdi (2016), "The psychological effects of cyber terrorism", Journal Bulletin of the Atomic Scientists, Vol. 72, 2016-Issue 5.
- Halpin, Edward et al. (2010), Cyber War, Internet Warfare, and Revolution in Military Affairs, translated by Ruhollah Arani, Political Studies Office, Majlis Research Center. [In Persian]
- Hartelius, Jonas. (2008). Narcoterrorism. EastWest Institute and the Swedish Carnegie Institute: 7.
- Iftikhar, Saman. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Comput Sci: 5-9.
- Jarvis, Lee, Macdonald, Stuart, Whiting, Andrew (2017), "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat", Access, Vol. 2, Issue 1, February 2017, pp. 64-87.
- Jurgens, Jeremy And Paolo,Dal Cin. (2024). Global Cybersecurity Outlook 2024. World Economic Forum: 4.
- Kamal, M. (2008). The meaning of terrorism: a philosophical inquiry. NCEIS Res Pap, 1, 1-1.
- M. Elliott, Geoffrey, and Robert Reginald (1995). Dictionary of Strategic Political Terms, translated by Mir Hassan Raeiszadeh Langrudi. Tehran: Moein: 26. [In Persian]
- Milov, Oleksandr; Melenti, Yevgen; Milevskyi, Stanislav; Pohasii, Serhii And Serhii
- Milov, Oleksandr; Melenti, Yevgen; Milevskyi, Stanislav; Pohasii, Serhii; and Serhii Yevseiev. (2021). Cyber Terrorism as an Object of Modeling. International Scientific And Practical Conference "Information Security And Information Technologies: 1.
- Mohammadi Deh Cheshmeh, Navab. (2018). State Terrorism: Imagination or Reality. Journal of Legal Research 36: 14. [In Persian]
- Monther Abed-Alrazzaq Musleh Al-Amaireh.Artificial Intelligence and Nurturing Electronic Terrorism (2024). International Journal of Religion 5(11): 10.
- Motlabi, Masoud, Arayesh, Hassan and Seyed Reza, Rahimi Emad. (2016). Terrorism from the perspective of radical Islamic fundamentalists and Shiite political jurisprudence; with a look at martyrdom operations. Quarterly Journal of Political Research in the Islamic World 6(4): 5. [In Persian]
- Oxford Advanced Learners Dictionery 1993
- Plinio, Jack C., and Roy Alton. (1996). The Culture of International Relations. Translated and researched by Hassan Pesta. Tehran: Contemporary Culture: 243. [In Persian]

- Plotnek, Jordan J. And Jill, Slay. (2020). Cyber Terrorism: A Homogenized Taxonomy and Definition. Computers & Security: 2.
- Pomper, Miles A. And Gabrielle Tarini. (2017). Nuclear Terrorism – Threat or Not?. Nuclear Weapons and Related Security Issues: 1.
- Qasemi, H. R. (2016). Iran and its policy against terrorism Eradicating Terrorism from the Middle East. Berlin: Springer.
- Richards, Laurence D. (2019). Cybernetics and Society Redux: The Necessity of Design. Indiana University East: 2.
- Russell., Stuart J. and Peter Norvig. (2010). Artificial Intelligence A Modern Approach Third Edition. USA, New Jersey: Upper Saddle River.
- shick Choi, Kyung And Claire, Seungeun Lee. (2018). The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity. International Journal of Cybersecurity Intelligence and Cybercrime 1(1): 1.
- Starr, Stuart H. (2009), "Towards an Evolving Theory of Cyber power", National Defense University, Center for Technology and National Security Policy.
- Swapna, Sanika. (2022). Cybernetics and Cybersecurity. Journal of Computer Science & Systems Biology 16(1): 1.
- Theohary, Catherine A.; Rollins, John W. (2015), "Cyberwarfare and Cyberterrorism", In: Brief, Congressional Research Service
- Ulnicane, Inga, And William Knight, Tonii Leach, Bernd Carsten Stahl, and Winter-Gladys Wanjiku. (2022). Governance of Artificial Intelligence Emerging International Trends and Policy Frames: The Global Politics of Artificial Intelligence. Florida: CRC Press.
- University of São Paulo. (2021). Cybernetics. Public university in São Paulo, Brazil: 3.
- Vössing K. (2017). Outcomes: Dominant Models of Class Politics and Institutionalization Success. In: How Leaders Mobilize Workers: Social Democracy, Revolution, and Moderate Syndicalism. Cambridge University Press.
- Walls B. A, Erin. (2017). Waves Of Modern Terrorism: Examining The Past and Predicting The Future. Georgetown University: 17.