Supreme National Defense University Quarterly Journal of National Security
https://ns.sndu.ac.ir E-ISSN: 2980-8251
Vol. 15, No. 4, Issue. 58, Winter 2026 **Received:** 2024/01/16 **Accepted:** 2025/02/17
Research paper

Cyberspace; Social Artificial Automatic Control System

Ehsan Khoshhalpour
Master of Information Technology Engineering - Information Security, Malek Ashtar University of Technology, Tehran
Email: khoshhalpour@chmail.ir

Abstract

The cyberspace has created a new form of interactions among humans through machines and computer technologies, thus shaping an extensive human-machine system. Despite the profound impact of cyberspace developments on various aspects of human life, effectively managing this phenomenon is considered a challenging issue. One of the essential prerequisites for effectively managing these developments is a correct and shared understanding of cyberspace among all actors that influence or are influenced by it. Although various understandings of cyberspace have been presented, it seems that these understandings are incomplete due to a lack of attention to the scientific roots of this technological phenomenon, and therefore cannot encompass all its aspects. In order to address this gap, the present article aims to answer the question: What is the concept of cyber, and what understanding of cyberspace can be derived from this concept? This article constitutes a fundamental qualitative study conducted through conceptual analysis and utilizes library study as method for data collection. To this end, information was gathered from reputable scientific databases using a snowball sampling method. After extracting relevant data from the sources, a categorization of the information was performed to conduct a conceptual analysis. The results of the research indicate that cyber technology represents an artificial and machine-based realization of cybernetics, and the social application of this technology shapes cyberspace. Consequently, cyberspace should be recognized as social artificial automatic control system.

Keywords: Cyberspace, Cyber, Cybernetics, Human-Machine System, Social Automatic Control

فصلنامه امنیت ملی

سال پانزدهم، شماره چهارم (پیاپی ۵۸)، زمستان ۱۴۰۴، صص. ۱۸۱-۲۱۶
تاریخ دریافت: ۱۴۰۲/۱۰/۲۶ ـ تاریخ پذیرش: ۱۴۰۳/۱۱/۲۹

مقاله پژوهشی

فضای سایبری؛ سیستم کنترل خودکار مصنوعی اجتماعی

احسان خوشحال‌پور
کارشناس ارشد مهندسی فناوری اطلاعات-امنیت اطلاعات، دانشگاه صنعتی مالک اشتر، تهران، ایران
Email: khoshhalpour@chmail.ir

چکیده

فضای سایبری با ایجاد گونه‌ای جدید از تعاملات انسان‌ها از طریق ماشین‌ها و فناوری‌های رایانه‌ای، یک سیستم انسان-ماشین گسترده را شکل داده است. علی‌رغم تأثیر شگرف تحولات سایبری بر جوانب مختلف زندگی بشر، مواجهه با این پدیده و مدیریت مؤثر آن به‌عنوان امری چالش‌برانگیز مطرح است. از مهم‌ترین پیش‌نیازهای مواجهه و مدیریت مؤثر تحولات مذکور، وجود شناخت صحیح و مشترک از فضای سایبری در میان همه بازیگرانی است که بر فضای سایبری تأثیر گذاشته و یا از آن تأثیر می‌پذیرند. با وجود شناخت‌های مختلف ارائه‌شده برای فضای سایبری؛ اما این شناخت‌ها به دلیل عدم توجه به ریشه‌های علمی پیدایش این پدیده فناورانه، درکی ناقص از پدیده ارائه داده و نمی‌توانند همه جوانب آن را بشناسانند. در راستای این ریشه‌یابی، مقاله حاضر به دنبال پاسخ به این سؤال است که مفهوم سایبر چیست و با درک این مفهوم چه شناختی از فضای سایبری حاصل می‌گردد؟ این مقاله یک پژوهش بنیادی از نوع کیفی بوده که به روش تحلیل مفهومی انجام شده است و از روش مشاهده اسنادی برای گردآوری اطلاعات استفاده می‌کند. بدین منظور اطلاعات از پایگاه‌های معتبر علمی و با استفاده از روش نمونه‌گیری گلوله‌برفی گردآوری شده است و پس از فیش‌برداری از منابع، با مقوله‌بندی اطلاعات به تحلیل مفهومی آن‌ها پرداخته شده است. نتایج پژوهش حاکی از آن است که فناوری سایبر، تحقق مصنوعی و ماشینی علم سایبرنتیک بوده و کاربرد اجتماعی این فناوری، فضای سایبری را شکل می‌دهد و در نتیجه باید فضای سایبری را به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی شناخت.

کلیدواژه‌ها: فضای سایبری، سایبر، سایبرنتیک، سیستم انسان-ماشین، کنترل خودکار اجتماعی

https://ns.sndu.ac.ir/ E-ISSN: 2980-8251

مقدمه

«فضای سایبری»[1] به‌عنوان پدیده‌ای فناورانه، تحولات گسترده و شگرفی را در زندگی بشر در پی داشته است، به‌گونه‌ای که پسوند «سایبری»[2] با الحاق به مفاهیم مختلف، مفاهیمی نظیر «جامعه سایبری»، «زندگی سایبری»، «جنگ سایبری» و «هرچیز سایبری» را موجب شده و سبب تغییر معنای این مفاهیم نسبت به معنای اولیه آن‌ها شده است (اوتیس و لورنتس[3]، ۲۰۱۰: ۲۶۷؛ استریت[4]، ۱۹۹۹: ۳۸۲)؛ این در حالی است که هنوز درک صحیح و مورد تفاهمی تفاهمی از مفهوم فضای سایبری وجود ندارد و همین امر سبب عدم درک صحیح و واحد از مفاهیم مشتق شده از ادغام این مفهوم با سایر مفاهیم می‌گردد؛ این امر می‌تواند موجب گردد که مفاهیم مشتق شده غیر از معنای واقعی خود و یا با معنایی ناقص فهمیده شوند (اوتیس و لورنتس، ۲۰۱۰: ۲۶۷) و در نتیجه مواجهه با آن‌ها نیز براساس همین درک ناقص صورت پذیرد. از مهم‌ترین پیش‌نیازهای مواجهه مؤثر با تحولات فضای سایبری، وجود یک درک مشترک و صحیح از این تحولات در میان همه بازیگران تأثیرگذار و یا تأثیرپذیر از این فضا است؛ چراکه مواجهه مؤثر نیازمند همکاری و هماهنگی همه بازیگران بوده و همکاری مؤثر نیز نیازمند درک مشترک و صحیح است. علی‌رغم این ضرورت، شناخت‌های فعلی ارائه شده برای فضای سایبری عمدتاً درکی ناقص و یا سطحی نسبت به این فضا ایجاد می‌کنند؛ درنتیجه از یک‌سو هیچ‌کدام از آن شناخت‌ها نمی‌تواند زمینه اجماع و اتفاق‌نظر بازیگران مختلف را فراهم آورد و از سوی دیگر هرگونه برنامه‌ریزی مواجهه و مدیریت تحولات فضای سایبری با توجه به نقص در شناخت، محکوم به ناکارآمدی یا شکست خواهد بود. دیوید هریس (هریس[5]، ۲۰۱۷: ۲۴) در این زمینه بیان می‌کند که درک صحیح فضای سایبری برای انجام دو کار مفید خواهد بود: ۱. مدیریت و بهره‌برداری موفقیت‌آمیز از آن در زمان حال و ۲. کسب آمادگی به‌موقع و انعطاف‌پذیر برای آینده‌ای که نامشخص است.

1. Cyberspace
2. Cyber
3. Ottis and Lorents
4. Strate
5. Harries

در زمینه اهمیت اتفاق‌نظر بر یک شناخت واحد از فضای سایبری و عدم وجود چنین شناختی در حال حاضر، کریمی قهرودی اشاره می‌کند (کریمی قهرودی و همکاران، ۱۴۰۲: ۱۰): «سازمان‌ها، مراکز و نهادهای علمی و پژوهشی کشورهای مختلف تاکنون تعاریف و توصیف‌های گوناگونی برای فضای سایبری و عناصر اصلی آن ارائه داده‌اند؛ وجود برداشت‌ها، توصیف‌ها و تعاریف نسبتاً متنوع در کشور، سبب ایجاد ابهام، ضعف زبان مشترک، بروز مشکلات، ناهماهنگی و تعارض‌هایی در سیاست‌گذاری‌ها، تقنین، تقسیم‌کار ملی، برنامه‌ریزی‌ها و توسعه فضای سایبری و امنیت فضای سایبری و ... در کشور شده است. سازمان‌دهی نامناسب، موازی‌کاری‌ها و پراکنده‌کاری‌ها، ضعف در قاعده‌گذاری‌ها و بروز اختلافات و چالش‌ها در تقسیم‌کار ملی ازجمله شواهد این مسئله است.»

عدم درک صحیح و مورد اجماع از فضای سایبری سبب ابهام در پژوهش‌های دانشگاهی و همچنین در حوزه‌های سیاست‌گذاری و تصمیم‌گیری‌های کلان می‌گردد. همان‌طور که فوتر اشاره می‌کند (فوتر[1]، ۲۰۱۸: ۲۰۳): «این واقعیت که معنای واژه سایبر برای افراد مختلف بسیار متفاوت فهم می‌شود، دلیلی کلیدی برای شکست محققان و سیاست‌گذاران در تعامل جدی با چالش‌های بی‌شماری است که این واژه را در برمی‌گیرد.» برای مثال همان‌طور که دین مارکو (مارکو[2]، ۲۰۲۳: ۱) اشاره می‌کند، امنیت سایبری که ازجمله مفاهیم فرعی فضای سایبری است، به مفهومی فراگیر در سیاست‌های عمومی، شرکت‌ها و سرمایه‌گذاری‌های خصوصی و نیز تعاریف حوزه نظامی یا نهادی بدل شده است و درعین‌حال عدم درک صحیح از مفهوم فضای سایبری و هم‌پوشانی معنایی آن با مفاهیمی نظیر اینترنت، دیجیتال و متاورس، باعث ایجاد ابهام و تضاد در درک امنیت سایبری شده و در نتیجه عدم عملکرد سایبری مقتضی از سوی بازیگران مختلف را در پی داشته است.

این مقاله برای دستیابی به درک صحیح از فضای سایبری، به دنبال پاسخ به این سؤال است که مفهوم سایبر چیست و در نتیجه درک این مفهوم، چه شناختی از فضای سایبری حاصل می‌شود؟ فرضیه پژوهش آن است که ترکیب «فضا»ی «سایبر»ی یک ترکیب معتبر

1. Futter
2. MarcCo

برای نام‌گذاری این پدیده است و این پدیده ایجادکننده فضایی از جنس سایبر است و با تمرکز بر واژه سایبر و شناخت آن، می‌توان به شناختی صحیح از فضای سایبری دست‌یافت.

مهم‌ترین نوآوری‌های مقاله حاضر عبارت است از:

- ارائه رویکردی جدید برای شناخت فضای سایبری با تمرکز بر شناخت «سایبر»؛
- ارائه یک شناخت جدید از فناوری فضای سایبری مبتنی بر علم سایبرنتیک.

۱. مبانی نظری

۱-۱. سایبر

«کالرا»[1] (۲۰۱۷) سایبر را پیشوندی در زبان انگلیسی می‌داند که در تعداد فزاینده‌ای از اصطلاحات برای توصیف چیزهای جدیدی استفاده می‌شود که با گسترش رایانه‌ها ممکن می‌شوند. طبق نظر «جوزف و ری»[2] (۲۰۲۰) کلمه سایبر در معنای عامیانه به معنای هر چیزی است که به رایانه، فناوری اطلاعات، اینترنت و واقعیت مجازی مربوط می‌شود. «کاولتی»[3] (۲۰۰۸) معتقد است که پیشوند سایبر از کلمه سایبرنتیک گرفته‌شده است و معنای تحت‌اللفظی آن «از طریق استفاده از رایانه» است. الکسی (۲۰۲۲) نیز معتقد است که سایبر از سایبرنتیک گرفته‌شده که به‌عنوان تعامل بین انسان و ماشین توصیف می‌شود، در نتیجه می‌تواند یک محیط جایگزین برای این تعامل ایجاد نماید و تعریف اصطلاح سایبر باید شامل عامل انسانی و تعامل آن با سیستم‌ها و فناوری‌ها باشد. از نظر آزادی (آزادی، ۱۳۹۷: ۱۶۵) سایبر ابزار و ادواتی از سنخ فناوری اطلاعات است که متکفل مناسبات انسان و ماشین بوده و اساساً مفهوم پردازش در ذات آن نهفته است. به گفته گیگن و پیترز (گیگن و پیترز[4]، ۲۰۱۶: ۱) پیشوند سایبر اکنون در توصیف پدیده‌های الکترونیکی و دیجیتالی گسترده شده است. بورگمن (بورگمن[5]، ۲۰۰۷: ۱۹) نشان می‌دهد که چگونه اغلب پیشوند سایبر به‌عنوان معادلی

1. Kalra
2. Joseph & Ray
3. Cavelty
4. Geoghegan & Peters
5. Borgman

برای پیشوند «e-» که مخفف الکترونیک است، استفاده می‌شود و بیان می‌کند که «e-» بیشتر در اروپا و آسیا استفاده می‌شود، درحالی‌که ایالات متحده آمریکا پیشوند سایبر را ترجیح می‌دهد.

۱-۲. فضای سایبری

با مرور منابع علمی در زمینه شناخت «فضای سایبری» این نتیجه حاصل می‌شود که دو دیدگاه عمده در زمینه شناخت این فضا وجود دارد (انگلمان[1]، ۲۰۰۰؛ برایانت[2]، ۲۰۰۱؛ لیوباچوسکایا[3]، ۲۰۱۳): شناخت فضای سایبری به‌عنوان یک جهان «رایانه»[4] ساخته و شناخت فضای سایبری به‌عنوان یک زیرساخت سخت‌افزاری ارتباطی.

افراد متعددی فضای سایبری را از منظر «جهانی مجازی»[5] و رایانه‌ای که می‌توان در آن حضور یافته و به حرکت و تعامل پرداخت، نگریسته‌اند. برخی محققین فضای سایبری را یک جهان مجازی می‌دانند که توسط شبکه‌ها، مسیریاب‌ها، کارگزارها و دستگاه‌های دیجیتالی مجهز به اینترنت ایجاد می‌شود (باراز و مونتاساری[6]، ۲۰۲۳: ۶۰). برخی دیگر معتقدند که فضای سایبری که به‌عنوان یک فضا یا جهان نیز شناخته می‌شود، محیطی مجازی است که توسط شبکه‌های رایانه‌ای ایجاد می‌شود و شامل اینترنت و زیرساخت‌های پشتیبانی‌کننده از آن و دستگاه‌های مختلف متصل‌شونده به آن و نیز اطلاعات و داده‌های ذخیره‌شده و ارسال‌شده در این شبکه‌ها است (کساوامورتی و کارتیکیان[7]، ۲۰۲۴: ۱). محقق دیگری فضای سایبری را به‌عنوان بستری برای امکان ارتباطات مجازی در جهانی الکترونیکی که از طریق رایانه قابل‌دسترسی است، معرفی می‌کند (ونکاتسوبرامانیان[8]، ۲۰۲۳: ۱).

برخی دیگر از محققین، فضای سایبری را به‌عنوان سخت‌افزارها و زیرساخت‌های ارتباطی

1. Angleman
2. Bryant
3. Lioubachevskaia
4. Computer
5. Virtual world
6. Baraz & Montasari
7. Kesavamoorthy & Karthikeyan
8. Venkatsubramanian

مبتنی بر رایانه که برای مبادله و مدیریت اطلاعات به کار گرفته می‌شوند، معرفی کرده‌اند. لیپرت (لیپرت و کلوتیر[1]، ۲۰۲۱: ۱) معتقد است که فضای سایبری مجموعه‌ای از سیستم‌هایی است که به‌طور منطقی با یکدیگر شبکه شده و روی زیرساخت فیزیکی مستقرشده‌اند و در آن از طیف الکترومغناطیسی برای ذخیره‌سازی، تغییر و تبادل داده‌ها استفاده می‌شود. تربینسکی (تربینسکی[2]، ۲۰۲۳: ۵) نیز فضای سایبری را دامنه جمع‌آوری، ذخیره‌سازی و پردازش اطلاعات به‌صورت دیجیتالی می‌داند که براساس انتقال سیگنال‌های دیجیتال و تشعشعات الکترومغناطیسی عمل می‌کند. از نظر شیامسودین (شیامسودین و علی[3]، ۲۰۲۴: ۱۱۷) فضای سایبری یک رسانه الکترونیکی در شبکه‌های رایانه‌ای است که به‌طور گسترده برای ارتباطات «برخط»[4] یک‌طرفه یا دوطرفه استفاده می‌شود. آزادی (آزادی، ۱۳۹۷: ۱۶۵) نیز فضای سایبری را پیوند ماشین‌های برآمده از فناوری اطلاعات توسط فناوری اطلاعات، یعنی توسط شبکه، معرفی می‌کند.

گفته می‌شود که عبارت «فضای سایبری» توسط گیبسون در دهه ۱۹۸۰ میلادی ابداع‌شده است (کریمی قهرودی و همکاران، ۱۴۰۲: ۱۱) و او آن را یک توهم توافقی معرفی می‌کند که روزانه توسط میلیاردها کاربر در کشورهای مختلف تجربه می‌شود و آن را یک بازنمایی گرافیکی از داده‌های به‌دست‌آمده از رایانه‌های موجود در سیستم انسانی می‌داند (گیبسون[5]، ۱۹۸۴: ۵۱)؛ اما کیکرپیل (کیکرپیل[6]، ۲۰۲۱: ۷) تصریح می‌کند که اصطلاح فضای سایبری قبل از توصیف آن به‌عنوان «توهم دیجیتال» از سوی گیبسون، توسط زوج معمار دانمارکی سوزانه اوسینگ و کارستن هاف در سال ۱۹۶۸ میلادی استفاده‌شده بود. نینگ (نینگ[7]، ۲۰۲۲: ۱؛ نینگ و همکاران، ۲۰۱۸: ۱۸۴۳) معتقد است که به‌کارگیری این اصطلاح توسط این معماران دانمارکی نمایانگر نگاه سایبرنتیکی آن‌ها به معماری ساختمان و ایده ایجاد «فضاهای

1. Lippert & Cloutier
2. Terebiński
3. Syamsudin & Ali
4. Online
5. Gibson
6. Kikerpill
7. Ning

حسی»[1] بوده است، یعنی یک فضای فیزیکی که می‌تواند رفتارها یا تغییرات مختلف انسان و و سایر موارد موجود در فضا را حس کند و با آن سازگار شود؛ البته باید توجه داشت که در به‌کارگیری این اصطلاح از سوی معماران دانمارکی، تأکیدی بر استفاده از هرگونه فناوری ازجمله رایانه‌های دیجیتال نشده بود (کیکرپیل، ۲۰۲۱: ۷) و با به‌کارگیری گیبسون از این اصطلاح بود که مفهوم فضای سایبری برای اولین بار به‌عنوان مترادف یک جهان دیجیتال ایجادشده توسط رایانه‌ها شناخته شد و مورد توجه زیادی قرار گرفت (نینگ، ۲۰۲۲: ۱).

۱-۳. سایبرنتیک

سایبرنتیک عمدتاً به‌عنوان علم ارتباطات و کنترل معرفی می‌شود و می‌توان آن را به‌طور گسترده‌تر به‌عنوان علم مطالعه روابط متقابل بین اجزای یک سیستم یا مجموعه‌ای از سیستم‌های تعاملی بدون توجه به ساختار درونی آن‌ها معرفی کرد (یولس[2]، ۲۰۲۱: ۴). سیستم سایبرنتیک بر روی کنترل مبتنی بر «بازخورد»[3] متمرکز است، فرآیندی که در آن یک سیستم از خروجی (عمل) خود به‌عنوان ورودی (اطلاعات) برای اصلاح رفتار خود به سمت هدف مورد نظر استفاده می‌کند (جفرسو[4]، ۲۰۲۴: ۳). سایبرنتیک بر شناخت و کنترل عوامل مختلفی که پتانسیل ایجاد اختلال در خود سیستم و یا محیط آن را دارند، تمرکز دارد تا با تطبیق‌پذیر نمودن سیستم در پاسخ به رویدادهای پیش‌بینی‌نشده ناشی از آن عوامل، امکان رسیدن سیستم به هدفش را فراهم آورد (سیبو و همکاران[5]، ۲۰۲۳: ۱). هر موجود زنده یا سیستم خودکار برای حفظ بقا و دستیابی به هدف در محیط پرتلاطم بیرونی، باید بتواند وضعیت‌های محیط و دنیای بیرون خود را حس کند، حالت‌های درک شده را با شرایط مطلوب آن حالت‌ها مقایسه کند و برای دستیابی و حفظ شرایط مطلوب بر آن‌ها تأثیر بگذارد (وونگ[6]، ۲۰۲۴:

1. Sensory spaces
2. Yolles
3. Feedback
4. Jefferso
5. Cibu et al.
6. Wong

۲۳۹) و یا با آن «سازگار»[1] شود (تابیلوآلوارز و رامیرزکورا[2]، ۲۰۲۳: ۴). سایبرنتیک اغلب از مفاهیمی مانند اطلاعات، بازخورد، تنوع، زنده بودن، هموستاز و آنتروپی استفاده می‌کند و رویکرد آن کلی‌نگر است (یولس، ۲۰۲۱: ۴).

۲. پیشینهٔ پژوهش

دی‌نوبرگا (دی‌نوبرگا و همکاران[3]، ۲۰۲۴: ۴) معتقد است که محققان و متخصصان معمولاً از واژه مخفف «سایبر» در مطالعات و اظهارنظرهای خود استفاده می‌کنند که از نظر معنایی کوتاه‌شده «فضای سایبر (نتیک)» است؛ بااین‌حال با این مختصرسازی، اغلب جزئیاتی به ظاهر بی‌اهمیت نادیده گرفته می‌شود، درحالی‌که این جزئیات برای بررسی رویکردهای نظری برای متخصصان لازم و ضروری است. علی‌رغم ضرورتی که دی‌نوبرگا به آن اشاره می‌کند، تعداد کمی از محققین به ارائه شناخت فضای سایبری با تمرکز بر شناخت واژه سایبر پرداخته‌اند؛ به‌ویژه آنکه در سال‌های اخیر توجه چندانی از سوی محققین به این مسئله مهم نشده است. در ادامه به برخی تحقیقات در این زمینه اشاره می‌گردد.

برخی محققین در توصیف رابطه سایبر و فضای سایبری، این فضا را برخوردار از خودکنترلی و سازگارشوندگی سایبرنتیکی معرفی می‌کنند. طبق نظر دیوید هریس (هریس، ۲۰۱۷: ۲۴) فضای سایبری یک موجودیت ناملموس خودسازمان‌ده است که هرگونه کنترل فعال علیه خود را به چالش می‌کشد. جیسون ویتکر (ویتکر[4]، ۲۰۰۳: ۹) با تأکید بر سهم مهم سایبرنتیک در مفاهیم فضای سایبری، این فضا را یک سیستم پیچیده می‌داند که درست مثل یک موجود زنده یا یک سیستم اجتماعی پرتنوع، سازگار می‌شود، تغییر می‌کند و به‌منظور ادامه عملکرد تغییر مسیر می‌دهد. دیوید پیم (پیم[5]، ۲۰۲۱: ۲۲،۱۰) نیز فضای سایبری را فضای سایبرنتیکی دانسته است و در نگاهی فنی برای ارائه درک سایبرنتیکی خود از فضای

1. Adapt
2. Tabilo Alvarez & Ram´ırez-Correa
3. De Nobrega et al.
4. Whittaker
5. Pym

سایبری، به مبحث سیستم‌های توزیع‌شده متوسل می‌شود و اشاره می‌کند که سیستم‌های توزیع‌شده مدلی از محاسبات را ارائه می‌دهند که در آن دستگاه‌های پردازش اطلاعات در شبکه‌ها قرار دارند و با یکدیگر و با محیط ارتباط برقرار می‌کنند و اقدامات خود را با ارسال پیام‌هایی بین یکدیگر و محیط هماهنگ می‌کنند. تعامل اجزای این سیستم‌ها باهم و با محیط آن‌ها، خدمات سیستم را به مشتریان خود ارائه می‌دهد.

از سوی دیگر در برخی تحقیقات قدیمی‌تر برخی محققین ضمن نگاه به فضای سایبری از منظر سایبرنتیک، این فضا را نه برخوردار از خودکنترلی و سازگارشوندگی بلکه به‌عنوان ابزار تأمین‌کننده ارتباط دوطرفه و ایجادکننده حلقه بازخورد و در نتیجه ابزاری برای اعمال کنترل سایبرنتیکی معرفی کرده‌اند.

لانس استریت (استریت، ۱۹۹۹: ۴۰۲) بیان می‌کند که فضای سایبری اساساً «فضای سایبرنتیکی» است و در واقع حسی از فضا است که از طریق بازخورد ایجاد می‌شود. به گفته وی به‌کارگیری عبارت فضای سایبری توسط ویلیام گیبسون نیز مستقیماً با سایبرنتیک مرتبط بوده و بر بازخورد تأکید دارد و این نگاه الهام گرفته از بازی‌های ویدیویی است که در آن یک حلقه بازخورد تقریباً یکپارچه میان بازیکنان و ماشین‌های بازی به‌واسطه ارتباطی که بین صفحه ویدیوی ماشین و چشم‌ها و سیستم عصبی انسان ایجاد می‌شود، تشکیل می‌شود. راندال والسر (والسر[1]، ۱۹۹۱) نیز توجه ما را به ارتباط سایبرنتیکی که از طریق فضای سایبری بین فرد و آواتار وی – به‌عنوان بدن مجازی او – ایجاد می‌شود، جلب می‌کند و می‌گوید: «فضای سایبری نوعی از شبیه‌سازی تعاملی به نام شبیه‌سازی سایبرنتیک است که این نوع شبیه‌سازی تعاملی، انسان را به‌عنوان جزئی ضروری در برمی‌گیرد. شبیه‌سازی سایبرنتیک یک مدل پویا از جهانی است که پر از اشیایی است که هرکدام درجات مختلفی از هوشمندی را از خود نشان می‌دهند. در این جهان شبیه‌سازی شده، اشیاء خاصی که به تعبیر او عروسک‌های خیمه‌شب‌بازی هستند، توسط اعمال انسان‌هایی، او آن‌ها را حامیان می‌نامد، که حرکاتشان توسط مجموعه‌ای از حسگرها رصد می‌شود، کنترل می‌شوند. کار اساسی فناوری فضای

1. Walser

سایبری، علاوه بر شبیه‌سازی یک جهان، ارائه یک حلقه بازخورد محکم بین انسان و آن عروسک است، تا به حامی این توهم را بدهد که او به معنای واقعی کلمه توسط عروسک تجسم‌یافته است. عروسک به حامی یک بدن مجازی می‌دهد و حامی به عروسک شخصیت می‌بخشد.» در کنار این کنترل سایبرنتیکی یک فرد بر بدن مجازی که والسر به آن اشاره کرده است، لانس استریت همچنین اعمال کنترل سایبرنتیکی یک فرد بر افراد دیگر را نیز مورد توجه قرار می‌دهد.

استریت می‌گوید: «گفتگوی ایدئال دوطرفه ممکن است به نفع رابطه نسبتاً یک‌طرفه بین کنشگر و مخاطب وی مهار شود. به‌عنوان مثال، یکی از اعضای یک لیست گفتگوی برخط ممکن است پیام‌هایی را با هدف تحت تأثیر قرار دادن دیگران ارسال کند – مثلاً بخواهد آن‌ها را شوکه کند یا تحسین آن‌ها را برانگیزد – به جای اینکه بخواهد آن‌ها را در یک گفتگوی واقعی درگیر کند.» (استریت، ۱۹۹۹: ۴۰۵).

همان‌طور که مشاهده می‌شود، پژوهش‌های اندکی به شناخت فضای سایبری با تمرکز بر مفهوم سایبر پرداخته‌اند. آن دسته از پژوهش‌های موجود نیز که توجهی به واژه سایبر داشته‌اند، سایبر را واژه‌ای مخفف و معادل سایبرنتیک دانسته‌اند و تمایز واضحی میان مفاهیم سایبر و سایبرنتیک قائل نشده‌اند. براساس بررسی صورت گرفته در پژوهش‌های موجود، هیچ پژوهشی که به مفهوم‌شناسی و ماهیت‌یابی دقیق اصطلاح سایبر متمایز از مفهوم سایبرنتیک و شناخت مفهوم فضای سایبری براساس آن پرداخته باشد، یافت نشد و پژوهش حاضر این شکاف پژوهشی را مرتفع می‌سازد. این مقاله در رویکردی متفاوت و با ریشه‌یابی و مراجعه به مبدأ پیدایش مفهوم سایبر و سیر تحول آن، به شناخت این مفهوم می‌پردازد و بر پایه آن درکی جدید از فضای سایبری به‌عنوان ترکیبی معتبر – و نه تعبیری ذوقی و سلیقه‌ای– و «فضا»یی از جنس «سایبر» ارائه می‌دهد.

۳. روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف، پژوهشی بنیادی است که رویکردی کیفی داشته و به روش تحلیل مفهومی انجام می‌شود و از روش مشاهده اسنادی و کتابخانه‌ای برای جمع‌آوری اطلاعات استفاده می‌کند. برای دستیابی به منابع کتابخانه‌ای شامل کتب، مقالات، پایان‌نامه‌ها و پایگاه‌های اینترنتی دربردارنده محتوای معتبر علمی، از روش نمونه‌گیری گلوله‌برفی استفاده‌شده است. در این روش پس از شناسایی اولین واحد نمونه‌گیری در منابع موجود، از آن‌ها برای شناسایی و انتخاب دومین واحد نمونه‌گیری استفاده می‌شود و به همین ترتیب دیگر واحدهای نمونه‌گیری شناسایی و انتخاب می‌شوند. اولین واحد نمونه‌گیری با جستجوی عبارت term cyber meaning در پایگاه Google Scholar در محدوده زمانی سال ۲۰۱۸ تا ۲۰۲۴ با مرتب‌سازی نتایج براساس میزان ارتباط و تمرکز بر مواردی از میان ۲۰ نتیجه نخست جستجو که عنوان آن‌ها صرفاً عبارت سایبر و نه عبارات ترکیب‌شده با سایبر را شامل می‌شوند، به‌دست‌آمده است. انتخاب جمعیت نمونه به‌صورت زنجیره‌وار تا جایی ادامه یافته است که اطمینان از اعتبار منابع و احساس اشباع نظری و تکرار مطالب برای محقق حاصل‌شده است.

جمع‌آوری اطلاعات از منابع با استفاده از روش فیش‌برداری صورت گرفته است و مطالب کلیدی هر منبع به روش نقل مستقیم به همراه نام منبع، تاریخ انتشار و آدرس دسترسی به آن منبع در قالب فیش‌هایی در نرم‌افزار Microsoft Word ثبت‌شده است؛ سپس محقق به شیوه تحلیل مفهومی و با مقوله‌بندی اطلاعات براساس ارتباط مفهومی آن‌ها، به تجزیه‌وتحلیل، ارزیابی و تکمیل اطلاعات و استنباط دیدگاه‌های جدید بر مبنای آن‌ها پرداخته است. اساساً در یک پژوهش تحلیلی، محقق باید از حقایق یا اطلاعات موجود استفاده کرده و با تجزیه‌وتحلیل و ارزیابی موشکافانه مطالب، به نتیجه‌گیری از آن‌ها بپردازد (کوتاری[1]، ۲۰۰۴: ۳).

اعتبار و روایی پژوهش حاضر از نوع سازه‌ای است؛ ازآنجاکه با جمع‌آوری داده تا رسیدن

1. Kothari

اشباع نظری، از مراجعه به تمامی منابع موجود اطمینان حاصل می‌شود و نیز مفهوم‌شناسی واژگان و مفاهیم مورد بررسی، با جمع‌آوری داده‌ها از منابع متعدد معتبر و مرجع در حوزه نظری مربوطه صورت می‌گیرد، در نتیجه می‌توان از اعتبار پژوهش اطمینان حاصل نمود.

۴. یافته‌های پژوهش

آنچه از مطالعه منابع پژوهش برمی‌آید آن است که مفهوم واژه سایبر را باید در واژه سایبرنتیک جستجو نمود که در چندین مورد از منابع به این ارتباط مفهومی اشاره شده است. در تبارشناسی زبانی واژه «سایبر»، ریشه «سایبر» در فعل یونان باستان κυβερεω (Kybereo) معرفی شده است که به معنی «هدایت کردن»[1]، «راهنمایی کردن»[2]، «کنترل کردن»[3] است (لهتو[4]، ۲۰۱۳: ۱؛ ماتئوس، پیترز و واندربرگ[5]، ۲۰۱۶: ۳). شکل فاعلی این واژه در یونان باستان به‌صورت κυβερνήτης (Kybernetikes) بوده است که در معانی «سکاندار»[6]، «خلبان»[7]، «فرماندار»[8] و یا راهنما استفاده می‌شده است (لیدل و اسکات[9]، ۱۹۴۰: ۱۰۰۴) و بعدها در زبان انگلیسی به Cybernetics برگردان شده است.

۴-۱. سایبرنتیک

سایبرنتیک مفهومی است که در طول زمان معنای آن دستخوش تغییر شده است و معنای کنونی آن متفاوت از معنای ابتدایی و بلکه بسط یافته آن است و در برخی منابع به این تحول معنایی اشاره شده است. اولین مورد استفاده از این واژه را می‌توان در گفت‌وگوی بین افلاطون و آلکیبیادس در کتاب آلکیبیادس اول یافت که افلاطون از این کلمه برای برجسته کردن

1. To steer
2. To guide
3. To control
4. Lehto
5. Maathuis, Pieters, and Van Den Berg
6. Steersman
7. Pilot
8. Governor
9. Liddell and Scott

اهمیت مهارت «ناوبری»[1] و هدایت کشتی استفاده کرده است (ازمی و کائوتسارینا[2]، ۲۰۱۹: ۲۴). پس‌ازآن، آندره ماری آمپر در سال ۱۸۴۳ میلادی در جلد دوم کتابی که در آن به طبقه‌بندی تمام دانش بشری تا آن زمان پرداخته است، عبارت Cybernétique را در زبان فرانسه ابداع و آن را به‌عنوان بخشی از علم سیاست طبقه‌بندی کرد. در نظر وی هرچند معنای اولیه سایبرنتیک هنر هدایت کشتی بوده است؛ اما بعدها حتی در میان یونانیان هم در یک معنای کلی‌تر به معنای هنر حکومت‌داری گسترش یافته است (آمپر[3]، ۱۸۴۳: ۱۴۰–۱۴۱). هم‌زمان با آمپر، ترنتوفسکی در سال ۱۸۴۳ میلادی، سایبرنتیک را با عبارت Cybernetyki در زبان لهستانی به کار برد و آن را «هنر نحوه حکومت بر یک ملت» عنوان کرد (نویکو[4]، ۲۰۱۶: ۱). ترنتوفسکی ضمن به کار بردن عبارت Cyberneta برای اشاره به فرد حاکم، بیان می‌کند که این حاکم است که در هر زمان کشتی یک کشور را هدایت می‌کند و شهرت یا بدنامی تاریخی متوجه اعمال او خواهد بود (ترنتوفسکی[5]، ۱۸۴۳: ۱۸۸،۱۹۲)؛ اما نقطه عزیمت به سمت معنای کنونی سایبرنتیک، کار بنیادینی است که توسط نوربرت وینر در سال ۱۹۴۸ انجام شد و از عبارت Cybernetics در زبان انگلیسی استفاده کرد (کیکرپیل، ۲۰۲۱: ۳) و به این واژه معنایی جدید و متفاوت از معانی قبلی آن داد و آن را مترادف با یک علم کاملاً جدید مطرح نمود (وونگ، ۲۰۲۴: ۲۲۵). وینر سایبرنتیک را به‌عنوان علم مطالعه کنترل و ارتباطات در حیوان و ماشین تعریف می‌کند. نظریه او بر مکانیسم‌های «خودتنظیم»[6] در سیستم‌های سایبرنتیک تمرکز دارد. وی به مفهوم مکانیسم بازخورد به‌عنوان منشأ رفتارهای هوشمند رسمیت می‌بخشد (دی‌نوبرگا و همکاران، ۲۰۲۴: ۴).

به‌بیان‌دیگر هرچند اولین بار افلاطون این واژه را در زبان یونانی جعل نمود و معنای هنر هدایت کشتی را برای آن مراد نمود، بعدها آمپر و ترنتوفسکی به ترتیب آن را در زبان فرانسوی و لهستانی و به معنای علم یا هنر حکومت‌داری به کار بردند؛ اما در نهایت این

1. Navigation
2. Azmi and Kautsarina
3. Ampère
4. Novikov
5. Trentowski
6. Self-regulating

نوربرت وینر آمریکایی بود که با آوردن این واژه به زبان انگلیسی، آن را به معنای علم ارتباطات و کنترل در حیوان و ماشین به کار گرفت که معنای کنونی این واژه نیز همین معنای مورد نظر وینر است. بر این اساس سایبرنتیک را می‌توان علم تشریح چگونگی شکل‌گیری کنترل مبتنی بر انتخاب هدف‌گرا و به تعبیر دیگر چگونگی شکل‌گیری رفتار هوشمند دانست. افلاطون انتخاب هدف‌گرا را در کشتی‌رانی مطرح کرد، آمپر و ترنتوفسکی موضوع انتخاب هدف‌گرا را به حوزه حکومت‌داری تعمیم دادند و وینر در یک تعمیم‌دهی گسترده‌تر، آن را به انتخاب هدف‌گرا در عملکردهای کنترلی درونی حیوان و ماشین و به تعبیر خودش در تمام زمینه‌هایی که مفهوم کنترل در آن‌ها کاربرد دارد، بسط داد.

سایبرنتیک به‌عنوان علم کنترل و ارتباطات در سیستم‌های حیوانی و ماشینی تعریف می‌شود (پاسونن[1]، ۲۰۱۱: ۳۳۶). در بیانی دقیق‌تر علم سایبرنتیک، علم سیستم کنترل خودکار هم در موجودات زنده و هم در ماشین‌هایی است که نیازمند «ارتباط» و «بازخورد» هستند (ازمی و کائوتسارینا، ۲۰۱۹: ۲۴). وینر مفهوم بازخورد را این‌گونه توضیح می‌دهد که بازخورد روشی برای کنترل یک سیستم با وارد نمودن مجدد نتیجه عملکرد گذشته سیستم به درون خود آن سیستم است (وینر[2]، ۱۹۵۴: ۶۱).

در این بیان از سایبرنتیک، توجه به چند نکته اساسی ضروری است: نکته اول اینکه وینر مبحث سیستم‌های کنترل خودکار را مورد توجه قرار می‌دهد؛ نکته دوم آنکه وینر مفهوم کنترل – یعنی اقداماتی که به امید رسیدن به هدف انجام می‌شوند– را به مفهوم ارتباطات، یعنی اتصال و جریان اطلاعات بین کنشگر و محیط، متصل می‌کند. در واقع وینر اشاره می‌کند که اقدام مؤثر مستلزم ارتباط است؛ همچنین نکته سوم اینکه وینر بیان می‌کند که هم حیوانات (سیستم‌های بیولوژیکی) و هم ماشین‌ها (سیستم‌های غیربیولوژیکی یا مصنوعی) می‌توانند براساس اصول سایبرنتیک کار کنند (پانگارو[3]، ۲۰۱۳). به عبارت دیگر سایبرنتیک مفهوم‌سازی انسان‌ها، حیوانات و ماشین‌ها به‌عنوان سیستم‌های سایبرنتیک – یعنی سیستم‌های

1. Paasonen
2. Wiener
3. Pangaro

با عملکرد مبتنی بر مکانیسم بازخورد – که در کارکردهای خود و نه الزاماً در ساختارهایشان مشابه یکدیگر هستند را ممکن ساخته است (پاسونن، ۲۰۱۱: ۳۳۶). بر این اساس سایبرنتیک را در بیانی ساده باید به‌عنوان علم «سیستم‌های کنترل خودکار در موجودات زنده و ماشین‌ها» معنا نمود.

۴-۲. سایبر

با توجه به ارتباط زبان‌شناسانه میان سایبر و سایبرنتیک، آیا می‌توان سایبر را مخفف سایبرنتیک و این دو واژه را معادل یکدیگر دانست؟ برای پاسخ به این سؤال باید توجه داشت که سایبرنتیک در دو شکل طبیعی و مصنوعی مطرح است. اساساً وینر معتقد بود که ماشین‌های خودکار از معادلی مصنوعی از سیستم عصبی انسانی یا حیوانی بهره‌مند هستند. در نتیجه از نظر وینر سازوکار سیستم کنترل خودکار برای رسیدن به هدف چه در انسان، چه در حیوان و چه در ماشین مشابه هم هستند؛ به تعبیر دیگر همان سیستم کنترل خودکار یعنی سیستم عصبی که در انسان و حیوان وجود دارد، در ماشین قابل معادل‌سازی است. درستی چنین ادعایی را باید در تجارب عملی نوربرت وینر در خلال سال‌های جنگ جهانی دوم جستجو نمود، جایی که تلاش کرد سایبرنتیک طبیعی انسانی را به‌صورت مصنوعی برای توپخانه ضدهوایی معادل‌سازی کند و بدین طریق به توپخانه ضدهوایی خودکار دست یابد. وینر سیستم کنترل خودکار مصنوعی را برای تحقق توپخانه ضدهوایی خودکار به‌منظور پیش‌بینی و تعقیب موقعیت آتی بمب‌افکن‌های برخوردار از مانور پروازی و مورد اصابت قرار دادن آن‌ها ایجاد و استفاده نمود. در واقع ایده وینر بر این اصل استوار بود که به‌دلیل تشابه سیستم کنترل خودکار در انسان و ماشین، می‌توان همان مکانیسم کنترل خودکار که در انسان وجود دارد را در ماشین مشابه‌سازی کرد و وینر از همین ایده برای ایجاد دستگاهی به نام «پیش‌بینی‌کننده AA»[1] برای مشابه‌سازی و پیش‌بینی رفتار خلبان بمب‌افکن دشمن استفاده کرد.

1. Anti-Aircraft (AA) Predictor

وینر می‌گوید (وینر، ۱۹۶۱: ۱۱۳): «هنگامی‌که ما به تیراندازی اردک می‌رویم، خطایی که سعی می‌کنیم آن را به حداقل برسانیم، خطای بین موقعیت تفنگ و موقعیت واقعی هدف نیست، بلکه بین موقعیت تفنگ و موقعیت پیش‌بینی‌شده هدف است.» وینر ایده خود برای پیش‌بینی رفتار خلبان را به کمک فناوری اطلاعات و در قالب شبکه‌های الکتریکی پیاده‌سازی کرد تا مشابه آنچه در تیراندازی اردک مطرح کرده بود، قادر به محاسبه موقعیت آتی هواپیمای مهاجم و حداقل‌سازی خطا در شلیک به آن گردد.

پیش‌بینی‌کننده وینر حرکت بعدی خلبان را حدود ۱۰ ثانیه زودتر – یعنی قبل از آنکه خود خلبان تصمیم به آن حرکت گرفته باشد – پیش‌بینی می‌کرد؛ این کار مستلزم آن بود که مکانیسم کنترل رفتار خلبان به شکلی در ماشین مشابه‌سازی شده باشد تا ماشین قادر به این پیش‌بینی باشد؛ اصابت به هدف نیز به معنای موفقیت‌آمیز بودن این مشابه‌سازی و پیش‌بینی حاصل از آن بود. به‌عبارت‌دیگر وینر اعتقاد داشت که خلبان بمب‌افکن تحت شرایط استرس پرواز، به‌عنوان یک مکانیسم خودکار یا «سرومکانیسم»[1] عمل کرده و رفتار او قابل پیش‌بینی و تکرارشونده است و نشان داد که پیش‌بینی‌کننده AA که او ساخته است، می‌تواند تا سطح قابل قبولی این رفتار را پیش‌بینی کند. موفقیت نسبی این پیش‌بینی‌کننده، عملاً اثباتی بر این ادعای وینر بود که انسان‌ها و ماشین‌ها براساس اصول سایبرنتیکی واحد کار می‌کنند و در کارکردهای خود مشابه هم هستند.

ایجاد معادلی مصنوعی از سیستم عصبی طبیعی انسانی برای ماشین‌ها، بروز رفتارهای هدفمند از سوی ماشین‌ها را موجب می‌شود. همان‌طور که تابیلوآلوارز (تابیلوآلوارز و رامیرزکورا، ۲۰۲۳: ۵) اشاره می‌کند، سایبرنتیک بر نحوه استفاده سیستم از اطلاعات و اتخاذ اقدامات کنترلی برای جهت‌دهی خود و حفظ حرکت به سمت اهداف در عین مقابله با اختلالات مختلف تمرکز دارد و این کار را با شناخت و کنترل عوامل مختلفی که پتانسیل ایجاد اختلال در خود سیستم و یا محیط آن را دارند، انجام می‌دهد (سیبو و همکاران، ۲۰۲۳: ۱).

1. Servomechanism

در واقع در ایده‌ای معکوس نسبت به زیست‌شناسان و فیزیولوژیست‌هایی نظیر «یاکوب فون اوکسکول»[1] که معتقد بودند باید به موجودات زنده با نگاه ماشینی نگاه کرد، وینر معتقد بود که ماشین‌ها می‌توانند مشابه انسان عمل کنند. با این نگاه ماشین‌ها می‌توانند رفتارهای انسانی از خود نشان دهند و چنین رفتارهایی برای انسان و ماشین، در قالب یک تحلیل رفتارگرایانه واحد قابل‌فهم است؛ در نتیجه با نگاه به انسان و ماشین به‌عنوان «جعبه سیاه»[2] و صرفاً توجه به اثرات ورودی بر خروجی و مستقل از ساختار داخلی آن‌ها، می‌توان جایگزین‌های ماشینی برای تولید رفتارهای انسانی ایجاد نمود.

از مطالب فوق‌الذکر می‌توان نتیجه گرفت که انسان‌ها و ماشین‌ها به‌عنوان سیستم‌های سایبرنتیک در کارکردهای خود مشابه هم بوده و براساس اصول سایبرنتیک کار می‌کنند؛ همچنین سیستم‌های کنترل خودکار در انسان و ماشین که رفتار هدفمند را در آن‌ها موجب می‌شود از منظر رفتارگرایانه مشابه هم هستند و این تشابه به حذف مرز بین انسان و ماشین و امکان ایجاد سیستم‌های سایبرنتیکی یکپارچه انسان–ماشین می‌انجامد. در واقع وینر معتقد بود که اطلاعات زبان مشترک موجودات زنده و ماشین است، زبان مشترکی که از مرزهای آن‌ها عبور می‌کند و با حذف مرزها میان موجود زنده و ماشین، ایجاد سیستم‌های یکپارچه زنده–ماشین را ممکن می‌سازد.

هرچند در سیستم یکپارچه انسان–ماشین، هر دو سیستم کنترل خودکار انسانی و ماشینی ذیل عنوان کلی سایبرنتیک و اصول این علم قرار می‌گیرند و یک سیستم سایبرنتیکی واحد را تشکیل می‌دهند؛ اما اصطلاح سایبر نه اصطلاحی معادل و مخفف علم سایبرنتیک، بلکه اصطلاحی فناورانه و مربوط به مصنوعات و دست‌ساخته‌های بشر است؛ به‌بیان‌دیگر هرچند سایبرنتیک یک علم و تشریح‌گر سازوکار ارتباطات و کنترل در کل سیستم یکپارچه انسان–ماشین است؛ اما سایبر یک فناوری است و فقط به بخش ماشینی این سیستم سایبرنتیکی یکپارچه اشاره دارد.

بااین‌حال استفاده گسترده از واژه سایبر، سبب عامیانه شدن معنای آن و تمایز و فاصله

1. Jakob von Uexküll
2. Black box

گرفتن آن از مفهوم ابتدایی و اصیل این واژه شده است، به‌طوری‌که عمدتاً این واژه به معنای هر چیز مرتبط با رایانه یا شبکه‌های رایانه‌ای به کار گرفته می‌شود. همان‌طور که وینستون راج سردبیر مجله جهان رایانه هنگ‌کنگ در مطلبی می‌نویسد (لی[1]، ۲۰۱۱: ۵۸): «من از استفاده از پیشوند سایبر در مفاهیم یا پدیده‌هایی که به‌طور مستقیم یا غیرمستقیم ارتباطی با رایانه را نشان می‌دهند، ناراحت هستم. معضل من به منشأ این پیشوند یا معنای اصلی و ریشه‌های یونانی آن مربوط می‌شود. سایبر به اعتقاد من واقعاً به چیزی اشاره دارد که با کنترل و تا حدی ارتباط مرتبط است. نوربرت وینر ریاضیدان آمریکایی و بنیان‌گذار سایبرنتیک، یعنی نظریه کنترل و فرآیندهای ارتباطی، کلمه انگلیسی سایبرنتیک را در دهه ۱۹۴۰ معرفی کرد. از آنجا بود که سایبر به‌عنوان پیشوند گرفته‌شده از سایبرنتیک، به کلمه‌ای جذاب و پرمحتوا برای هر چیزی که با رایانه مربوط می‌شود تبدیل شد و در نهایت کاربران منشأ آن را فراموش کردند.»

بنابراین این تصور نادرست است که سایبر را به معنای هر چیز مرتبط با رایانه و یا صرفاً به‌عنوان مخفف شده سایبرنتیک و عبارتی پیشوندی در زبان انگلیسی معادل علم سایبرنتیک بدانیم، بلکه سایبر واژه‌ای فناورانه منشعب شده از علم سایبرنتیک است. هرچند سایبرنتیک علم تشریح‌گر هر دو سیستم کنترل خودکار انسانی و ماشینی یا به تعبیر دیگر هر دو سیستم کنترل خودکار طبیعی و مصنوعی است و تمام گستره سیستم کنترل خودکار یکپارچه انسان-ماشین را در برمی‌گیرد؛ اما مفهوم سایبر فقط دربردارنده بخش‌های ماشینی و فناورانه آن یعنی سیستم‌های کنترل خودکار مصنوعی است و بخش‌های انسانی یعنی سیستم‌های کنترل خودکار طبیعی را شامل نمی‌شود. بر این اساس باید گفت که سایبر، نه معادل علم سایبرنتیک، بلکه فناوری محقق کننده علم سایبرنتیک است. در واقع سایبر، پیاده‌سازی فناورانه، رایانه‌ای و ماشینی سایبرنتیک است و نه همه آن. سایبر، «سایبرنتیک مصنوعی» یا همان «سیستم کنترل خودکار مصنوعی» است.

وینر در نتیجه کار بر روی پیش‌بینی‌کننده AA خود، ضمن معرفی علم سایبرنتیک به این

1. Lee

نتیجه رسید که می‌توان به کمک فناوری اطلاعات، سایبرنتیک مصنوعی و ماشینی ایجاد نمود و از این طریق نسبت به ایجاد سیستم یکپارچه انسان–ماشین اقدام نموده و از آن برای پیش‌بینی رفتار خلبان و تعقیب خودکار و ساقط نمودن هواپیمای بمب‌افکن دشمن استفاده کرد. این سایبرنتیک مصنوعی یا ماشینی، همان چیزی است که سایبر نامیده می‌شود.

۴-۳. فضای سایبری

روشن گردید که سایبر به معنای سایبرنتیک مصنوعی یا همان ماشین برخوردار از سیستم کنترل خودکار است، در این صورت فضای سایبری به چه معناست؟ برای پاسخ به این سؤال لازم است اشاره گردد که هرچند سایبرنتیک در ابتدا بیشتر بر ماشین‌ها و انسان‌ها تمرکز داشت؛ اما این ایده همواره کلی‌تر بوده و بعدها به ارگانیسم‌ها و موقعیت‌های اجتماعی نیز تعمیم پیدا کرد (تابیلوآلوارز و رامیرزکورا، ۲۰۲۳: ۵). اساساً وینر در عین پرداختن به کاربرد اولیه فناوری سایبر در ضدهوایی خودکار، دو کاربرد دیگر این فناوری را نیز مورد توجه قرار داد، یک کاربرد به پروتزها و اندام‌های مصنوعی مربوط بوده و کاربرد دیگر به ایجاد اتحاد و هماهنگی اجتماعی در جوامع انسانی و جانوری و شکل‌گیری جوامع گسترده از طریق آن مربوط می‌شود (وینر، ۱۹۶۱: ۱۵۵، ۱۳۳). در واقع با توجه به اینکه نوربرت وینر به سیستم‌های کنترل از نقطه‌نظر اطلاعات نگاه کرد و جوهره کنترل را ارتباطات دانست، با این نگاه امکان مطالعه پدیده‌های مختلف ماشینی، طبیعی و همچنین اجتماعی را از دیدگاهی کاملاً جدید و یکپارچه فراهم کرد (وونگ، ۲۰۲۴: ۲۲۹). بنابراین علم سایبرنتیک علاوه بر تشریح سیستم کنترل خودکار انسانی و ماشینی، سیستم‌های کنترل خودکار بیولوژیکی و اجتماعی را نیز تشریح می‌کند؛ در نتیجه فناوری سایبر علاوه بر معادل‌سازی مصنوعی سیستم کنترل خودکار عصبی انسانی، برای معادل‌سازی مصنوعی سیستم کنترل خودکار بیولوژیکی و اجتماعی نیز قابل‌استفاده است و می‌توان با اتصال آن به سیستم‌های بیولوژیکی یا اجتماعی، سیستم‌های یکپارچه زنده–ماشین ایجاد نمود.

وینر در زمینه به‌کارگیری فناوری سایبر در سیستم کنترل خودکار بیولوژیکی، از جایگزینی

اندام‌های طبیعی با اندام‌های مصنوعی صحبت به میان می‌آورد. در این ایده وینر، سیستم کنترل خودکار مصنوعی با سیستم کنترل خودکار طبیعی بیولوژیکی انسانی یکپارچه‌شده و به‌عنوان مثال به بازگرداندن بینایی از دست رفته فرد می‌انجامد. وینر همچنین کندوی زنبورعسل را به‌عنوان سیستم کنترل خودکار طبیعی اجتماعی مثال می‌زند. او در کتاب سایبرنتیک خود این پرسش را مطرح می‌کند که چگونه یک کندوی زنبورعسل با هماهنگی متغیر، منظم و منطبق‌شونده عمل می‌کند؟ وی در پاسخ اشاره می‌کند که راز چنین اتحاد و هماهنگی در عملکرد را باید در ارتباطات داخلی میان اعضای آن کندو جستجو نمود. او همچنین با اشاره به اینکه رشد یک جامعه به میزان اندازه توسعه انتقال مؤثر اطلاعات میان اعضای آن جامعه است، از جایگزینی ارتباطات طبیعی با فناوری‌های ارتباطی میان اعضای یک جامعه در مواردی که ارتباط مستقیم اعضا با یکدیگر ممکن نیست، سخن می‌گوید (وینر، ۱۹۶۱: ۱۵۶–۱۵۸). در این بیان وینر، فناوری سایبر با سیستم اجتماعی یکپارچه‌شده و جایگزینی مصنوعی برای ارتباطات طبیعی میان اعضای جامعه فراهم می‌آورد. وونگ در این زمینه معتقد است که سایبرنتیک در کاربرد اجتماعی، از تنظیم مبادله اطلاعات در ارتباطات میان اعضای جامعه برای دستیابی به هدف کنترل استفاده می‌کند (وونگ، ۲۰۲۴: ۲۳۴).

بنابراین فناوری سایبر در سیستم اجتماعی قابل‌استفاده است و ماشین کنترل خودکار علاوه بر کاربرد مستقلانه‌اش در مواردی نظیر ضدهوایی خودکار، می‌تواند به‌عنوان واسطه در ارتباطات انسانی نیز ایفای نقش کند؛ اما آیا می‌توان تعبیر فضای سایبری را به این کاربرد از فناوری سایبر اطلاق نمود؟ آیا استفاده از فناوری سایبر در سیستم اجتماعی به ایجاد یک فضا می‌انجامد؟ باید توجه داشت که ماشین سایبری، ماشین دودویی و ماشین مبتنی بر صفر و یک است، چراکه وینر برای معادل‌سازی مصنوعی سیستم کنترل خودکار طبیعی انسانی یا حیوانی در ماشین، از محاسبات دودویی و ماشین محاسباتی دیجیتالی استفاده نمود؛ در نتیجه امکان تعامل مستقیم انسان با این ماشین به‌خودی‌خود وجود ندارد و چنین تعاملی نیازمند یک ترجمه میان زبان ماشین و زبان قابل‌فهم برای انسان است.

سایبر به‌عنوان یک ماشین کنترل خودکار، برای اینکه در یک سیستم اجتماعی انسانی قرار

بگیرد، نیازمند تأمین رابط‌های کاربری انسانی است تا امکان درک و تعامل با این ماشین برای انسان فراهم آید؛ اینجاست که اطلاعات درونی ماشین دودویی باید به‌گونه‌ای ادراک‌پذیر برای انسان تبدیل شود که در نتیجه این تبدیل، احساس وجود یک فضای جدید برای فرد تداعی می‌شود؛ فضایی که ماشین دودویی برای انسان ایجاد نموده و نمایشی انسان‌فهم از مقادیر درونی خود را در بردارد و محتوای ماشین محاسباتی را برای انسان ادراک‌پذیر و تعامل‌پذیر می‌نماید. روشن است که این فضای جدید که حاصل از به‌کارگیری فناوری سایبر در سیستم اجتماعی است، یک فضای مصنوعی است، یعنی فضایی فناورانه، دست‌ساخته و مصنوع انسان است؛ فضایی که زیربنای جدیدی برای درک فرد از جهان اطراف بوده و امکان حضور و تعامل با دیگر انسان‌ها را برای فرد فراهم می‌آورد. فضایی که به گفته برایانت (برایانت، ۲۰۰۱: ۱۴۲) چهار زیرمفهوم «محل»[1]، «اندازه»[2]، «فاصله»[3] و «مسیر»[4] که از مفاهیم فرعی کلان‌مفهوم «فضای فیزیکی»[5] هستند، در مورد این فضای جدید نیز صدق می‌کنند.

بر این اساس وقتی فناوری سایبر در سیستم اجتماعی به‌کارگیری می‌شود، در نتیجه تعامل انسان با این ماشین کنترل خودکار، یک فضا ایجاد می‌گردد؛ در واقع فضای سایبری حاصل تعامل انسان با فناوری سایبر یعنی همان ماشین محاسباتی کنترل خودکار و یا تعامل با دیگر موجودیت‌های محیطی از طریق این ماشین است که در نتیجه آن، یک فضای ارتباطی جدید شکل می‌گیرد؛ ازآنجاکه این فضای جدید از جنس سایبر و ایجادشده مبتنی بر فناوری سایبر است، به آن فضای سایبری گفته می‌شود؛ یعنی فضایی که ماهیت آن همان سایبر یا سیستم کنترل خودکار مصنوعی است که امکان تعامل با آن یا تعامل با دیگر انسان‌ها از طریق آن برای اعضای جامعه انسانی فراهم آمده است؛ بر این اساس فضای سایبری حاصل استقرار سیستم کنترل خودکار مصنوعی در میان اجزای سیستم اجتماعی است؛ در نتیجه فضای سایبری را باید «سیستم کنترل خودکار مصنوعی اجتماعی» دانست.

1. Place
2. Size
3. Distance
4. Route
5. Physcical space

در کنار اینکه فضای سایبری به‌عنوان یک فضای جدید، امکان ارتباط فرد با افراد دیگر را فراهم می‌آورد، امکان ارتباط فرد با دارایی‌های فیزیکی و ارگانیسم‌ها نیز از طریق این فضا وجود دارد. برای این کار لازم است امکان اتصال دارایی‌های فیزیکی و ارگانیسم‌ها به فضای سایبری فراهم آید. سایبورگ که خلاصه‌شده عبارت «ارگانیسم سایبرنتیکی»[1] است را می‌توان ارگانیسمی معرفی کرد که امکان اتصال به جریان داده شبکه‌های رایانه‌ای را یافته است (سور[2]، ۲۰۱۳: ۸۷). از سوی دیگر «رابط‌های فیزیکی–سایبری»[3] نیز وجود دارند که شکاف بین ماشین‌های محاسباتی و دارایی‌های فیزیکی را پر می‌کنند (راجهانز و همکاران[4]، ۲۰۰۹: ۴)؛ در نتیجه امکان اتصال موجودیت‌های فضای فیزیکی به فضای سایبری را فراهم می‌آورند.

همان ماشین محاسباتی پیش‌بینی‌کننده وینر که امکان کنترل خودکار را در سیستم مکانیکی ضدهوایی خودکار فراهم آورد، حال با ایجاد یک فضا یا حسی از فضا، امکان به‌کارگیری در سیستم اجتماعی را می‌یابد و کاربرد اجتماعی آن، همان چیزی است که فضای سایبری نام‌گرفته است.؛ در نتیجه همان‌گونه که پیش‌بینی‌کننده ضدهوایی وینر امکان غلبه بر خلبان بمب‌افکن و مورد اصابت قرار دادن هواپیمای او را فراهم می‌آورد، سیستم کنترل خودکار مصنوعی اجتماعی نیز قابلیت غلبه، تأثیرگذاری و کنترل بر موجودیت‌های متصل به فضا، شامل فرد و جامعه انسانی و جانوری و نیز موجودیت‌های فیزیکی و ارگانیسم‌های متصل به فضا و تحقق هدف تعیین‌شده را فراهم می‌آورد؛ بنابراین با استقرار فناوری سایبر در سیستم اجتماعی و پیدایش فضای سایبری، امکان کنترل خودکار یا کنترل از طریق فضای سایبری روی فرد، جامعه، ارگانیسم‌ها و یا دارایی‌های فیزیکی متصل به فضا فراهم می‌آید. گفتنی است که هرچه سطح هوشمندی درونی در این سیستم کنترل خودکار مصنوعی بالاتر باشد و هرچه سطح اتصالات بالاتری با موجودیت‌های متصل داشته باشد، سطح کنترل خودکار مصنوعی بالاتری را فراهم خواهد آورد.

1. Cybernetic organism
2. Sever
3. Cyber-physical interface
4. Rajhans et al.

۴-۴. جمع‌بندی

یافته‌های پژوهش حاکی از آن است که فضای سایبری را باید به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی شناخت. هرچند پژوهش حاضر با رویکردی نظری انجام پذیرفته است؛ اما شواهد عملی موجود در تحقیقات برخی محققین نیز مؤید یافته‌های این پژوهش است. در ادامه به برخی از این تحقیقات و شواهد عملی ارائه‌شده در آن‌ها اشاره می‌گردد.

لینگز و همکاران (لینگز و همکاران[1]، ۲۰۱۹: ۱) اشاره می‌کنند که مدیریت استفاده از دستگاه‌های دیجیتال به امری دشوار برای بسیاری از مردم تبدیل‌شده است و به‌عنوان راه‌حل پیشنهاد می‌کنند که از ابزارهای خودکنترلی که در درون دستگاه‌های دیجیتال در قالب برنامه کاربردی یا افزونه مرورگر قابل طراحی است، استفاده شود تا به‌مرور عادت استفاده درست در کاربر شکل گیرد. آن‌ها (لینگز و همکاران، ۲۰۱۹: ۳) به چند برنامه کاربردی برای نمونه اشاره می‌کنند، ازجمله یک برنامه کاربردی که استفاده از تلفن همراه را در تاریکی تشخیص می‌دهد و به کاربر اطلاع می‌دهد که باید آن را کنار بگذارد. همچنین برنامه کاربردی دیگری معرفی می‌کنند که به کاربران اجازه می‌دهد مفهومی به نام «اتاق مجازی» ایجاد کنند تا هنگامی‌که به مکان یا زمان خاصی وارد می‌شوند، اعلان‌ها و برنامه‌ها به‌طور خودکار مسدود شوند. یک برنامه کاربردی دیگر نیز معرفی می‌نمایند که امکان ردیابی استفاده از برنامه‌های مختلف تلفن هوشمند و تعیین محدودیت‌های زمانی برای استفاده از هر برنامه و وادار نمودن کاربران برای بستن برنامه در صورت رسیدن به محدودیت تعیین‌شده را فراهم می‌کند.

دامبرا و همکاران (دامبرا و همکاران[2]، ۲۰۱۹) راهکاری مبتنی بر فناوری فضای سایبری را برای مدل کردن، شبیه‌سازی و پیش‌بینی رفتار یک جمعیت انسانی در یک گردهمایی جمعی که افراد آن می‌توانند بازدیدکننده، تماشاگر، معترض یا به هر نام دیگری نامیده شوند و اطلاع‌رسانی مخاطرات محتمل به اپراتور انسانی برای تصمیم‌گیری آگاهانه به‌منظور پیشگیری از خطراتی نظیر اعمال مجرمانه و حملات تروریستی قبل از وقوع پیشنهاد داده‌اند.

از دیگر شواهد قابل اشاره، می‌توان به تنظیم مبادله اطلاعات در ارتباطات میان افراد در

1. Lyngs et al.
2. Dambra et al.

«رسانه‌های اجتماعی»[1] اشاره کرد. بسیاری از رسانه‌های اجتماعی کنونی از الگوریتم‌های مبتنی بر هوش مصنوعی برای سفارشی‌سازی انتقال محتوا میان کاربران به‌منظور بهبود تجربه کاربری و در اختیار قرار دادن مرتبط‌ترین یا مطلوب‌ترین محتوا برای هر کاربر استفاده می‌کنند. از این تنظیم محتوا توسط این رسانه‌ها می‌توان به‌عنوان رفتار هدفمند و خودکنترل آن‌ها برای افزایش تعداد کاربران، افزایش رضایت کاربران، افزایش مدت‌زمان استفاده کاربران از آن‌ها و نیز تأثیرگذاری بر رفتار کاربران تعبیر نمود.

«گس» در یک مطالعه عملی نشان می‌دهد که الگوریتم‌های رسانه‌های اجتماعی که برای بهینه‌سازی ترتیب ارائه محتوا به کاربران طراحی شده‌اند، چگونه بر نگرش‌ها و رفتارهای سیاسی افراد ازجمله در انتخابات تأثیر می‌گذارند. این تحقیق که سیستم‌های رتبه‌بندی خوراک شخصی‌سازی‌شده را در الگوریتم‌های رسانه‌های اجتماعی موردتوجه قرار می‌دهد، نشان می‌دهد که این سیستم‌ها به قرار گرفتن مکرر فرد در معرض محتوای هم‌فکر و تقویت‌کننده منجر می‌شوند و اثرات مختلفی ازجمله دوقطبی‌سازی سیاسی جامعه و نیز تأثیرگذاری بر میزان مشارکت سیاسی را در پی دارند (گس و همکاران[2]، ۲۰۲۳: ۱).

برخی تحقیقات در حوزه امنیت سایبری نیز مؤید ماهیت کنترل خودکار فضای سایبری است؛ قاسمی و پارسا (قاسمی و پارسا، ۱۳۹۷: ۱۲۴) اشاره می‌کنند که برخی «بدافزارها»[3] از روش‌های «ضدتحلیل»[4] برای دور زدن روش‌های تحلیلی مبتنی بر رفتار زمان اجرا بهره می‌برند. این نوع بدافزارها که به آن‌ها «بدافزارهای محیط-آگاه»[5] گفته می‌شود، پیش از اجرای کد مخرب خود، به بررسی محیط اجرا می‌پردازند و در صورت شناسایی حضور در یک محیط تحلیل مانند «ماشین مجازی»[6]، «جعبه شنی»[7] و یا «اشکال‌زدا»[8]، رفتار مخرب خود را پنهان می‌کنند؛ به‌طوری‌که یا بلافاصله به اجرای خود پایان می‌دهند و یا رفتاری مشابه

1. Social netwrok
2. Guess et al.
3. Malware
4. Anti-analysis
5. Environment-aware malware
6. Virtual machine
7. Sandbox
8. Debugger

نرم‌افزارهای بی‌خطر از خود نشان می‌دهند؛ اما چنانچه اجرای بدافزار در محیطی فاقد ابزارهای تحلیلی صورت پذیرد و یا بدافزار موفق به شناسایی ابزارهای تحلیلی موجود نشود، رفتار مخرب را از خود بروز می‌دهد.

تحقیقات فوق‌الذکر به‌خوبی برخی نمونه‌هایی عملی از برخی سیستم‌های کنترل خودکار و قابلیت‌های محیط‌آگاهی، پیش‌بینی و کنترل خودکار که فضای سایبری از آن برخوردار است را برجسته و روشن می‌سازند و یافته‌های آن‌ها تأییدکننده یافته‌های پژوهش حاضر یعنی ماهیت کنترل خودکار فضای سایبری است.

نتیجه‌گیری و پیشنهاد

در این مقاله با تأیید نگاه سایبرنتیکی برای شناخت فضای سایبری، ضمن نشان دادن معتبر بودن تعبیر «فضای سایبری» برای نام‌گذاری این پدیده، شناخت جدید از این فضا به‌عنوان فضایی از جنس سایبر با رویکرد تبیین مفهوم سایبر ارائه گردید. مشخص گردید که سایبرنتیک تشریح‌کننده انواع سیستم‌های کنترل خودکار طبیعی و مصنوعی است و سایبر به‌عنوان فناوری محقق کننده سایبرنتیک، به بخش ماشینی، فناورانه و مصنوعی سایبرنتیک اشاره دارد. همچنین اشاره شد که سایبر به‌عنوان سیستم کنترل خودکار مصنوعی، برای خودکارسازی مصنوعی سیستم‌های مختلف فیزیکی، بیولوژیکی و اجتماعی قابل به‌کارگیری است و کاربرد آن در سیستم اجتماعی همان چیزی است که فضای سایبری نام‌گرفته است.

بیان شد که به‌کارگیری فناوری سایبر در سیستم اجتماعی، ایجادکننده یک فضای جدید ارتباطی و عملاً به معنای استقرار یک سیستم کنترل خودکار مصنوعی در سیستم اجتماعی است و بر این اساس فضای سایبری به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی معرفی گردید.

نگاه به فضای سایبری از منظر موجودیتی برخوردار از خودکنترلی سایبرنتیکی و شناخت آن به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی، به‌خوبی منعکس‌کننده قابلیت‌های کنترلی این فضا شامل کنترل فرد، اجتماع، ارگانیسم‌ها، دارایی‌های فیزیکی و خودکنترلی

درونی فضا بوده که همگی به‌دلیل ماهیت کنترل خودکار مصنوعی این فضا ناشی از سایبری بودن آن است. آنچه در شناخت‌های موجود از آن غفلت شده است، توجه به سایبر یعنی سیستم کنترل خودکار مصنوعی است که همین امر سبب گشته تا برخی قابلیت‌های این فضا و برخی آثار ناشی از به‌کارگیری آن صرفاً با اتکا به آن شناخت‌ها قابل توجیه و توضیح نباشد.

شناخت فضای سایبری به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی، نه‌تنها انکارکننده دو دیدگاه عمده موجود در زمینه شناخت این فضا نیست، بلکه در بردارنده و اعم از آن‌ها است. آنچه به‌عنوان جهان مجازی ادراک می‌شود، در واقع رویه و پوسته‌ای مجازی برای این سیستم کنترل خودکار مصنوعی اجتماعی است تا به زبان مشترک میان انسان و ماشین بدل شده و امکان ارتباط متقابل انسان و ماشین و ارتباط انسان‌ها با یکدیگر از طریق ماشین را فراهم آورد. آنچه به‌عنوان زیرساخت سخت‌افزاری ارتباطی ادراک می‌شود نیز بخش پشتی و فیزیکی این سیستم کنترل خودکار است که امکان انتقال، ذخیره‌سازی، پردازش و نمایش اطلاعات را فراهم می‌آورد. نگاه به فضای سایبری به‌عنوان ابزار کنترل سایبرنتیکی نیز کاربردی خاص از این سیستم کنترل خودکار مصنوعی و به‌کارگیری قابلیت‌های کنترلی این سیستم از سوی یک فرد برای اعمال کنترل روی دیگر افراد یا موجودیت‌ها است.

یافته‌های پژوهش، فرضیه پژوهش را تأیید می‌کند و نشان می‌دهد که از مسیر مفهوم‌شناسی واژه سایبر، می‌توان به شناختی صحیح از فضای سایبری به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی دست‌یافت، شناختی که نسبت به سایر شناخت‌های موجود، درک دقیق‌تر و گسترده‌تری از این فضا ارائه می‌دهد و تحقیقات عملی انجام‌شده نیز مؤید آن است.

از شناخت فضای سایبری به‌عنوان کاربرد اجتماعی فناوری سایبر و ایجادکننده سیستم کنترل خودکار مصنوعی اجتماعی این نتیجه حاصل می‌شود که این فضا عملاً یک سیستم هدفمند و خودکنترل بوده و قادر است تمام عوامل اجتماعی را که پتانسیل ایجاد اختلالات در مسیر تحقق اهداف تعیین‌شده در آن را دارند، شناسایی نموده و با کنترل آن‌ها و سازگار شدن با وضعیت‌های پیش‌بینی‌نشده ناشی از فعالیت‌های آن عوامل، اهداف خود را محقق

کند. دستیابی به این درک از فضای سایبری به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی، به‌خوبی می‌تواند راهگشای سیاست‌گذاران، تصمیم‌گیران، محققین و فعالان حوزه فضای سایبری برای درک زوایای پنهان این فناوری و مدیریت کارآمدتر و برنامه‌ریزی مواجهه مؤثرتر با آن باشد. همچنین در صورتی که این شناخت از فضای سایبری با توجه به دقت و جامعیتش در مقایسه با سایر شناخت‌های موجود، بتواند مورد اجماع بازیگران مختلف تأثیرگذار و تأثیرپذیر از فضای سایبری در کشور قرار گیرد، می‌تواند مبنایی برای هماهنگی‌ها و رفع تعارضات میان آن‌ها در حوزه تصمیم‌گیری‌های کلان کشور فراهم آورد.

دغدغه‌های متعددی در زمینه مسائل و آسیب‌های اجتماعی ناشی از فضای سایبری در پژوهش‌های جامعه‌شناسی و حوزه‌های مختلف علوم اجتماعی به چشم می‌خورد، در پژوهش‌های حوزه سیاست‌گذاری و حکمرانی فضای سایبری نیز وضعیت مشابهی مشاهده می‌شود؛ اما تحلیل‌های انجام‌شده در این‌گونه پژوهش‌ها عمدتاً مبتنی بر شناختی سطحی از فضای سایبری به انجام می‌رسند و از عدم درک درست این فضا رنج می‌برند؛ بر این اساس پیشنهاد می‌گردد که شناخت منتج شده از پژوهش حاضر و توجه به ماهیت کنترل خودکار فضای سایبری، مبنای تحلیل‌های پژوهش‌های مذکور قرار گیرد تا در رفع این مشکل و انطباق بیشتر آن‌ها با واقعیات فضای سایبری راهگشا باشد و به اتقان بالاتر نتایج آن پژوهش‌ها و کاربردپذیری بیشتر نتایج آن‌ها بینجامد. همچنین بر مبنای این درک از فضای سایبری، می‌توان نسبت به مفهوم‌شناسی و ارائه تعریف برای اصطلاحات مختلفی که از ادغام با پسوند سایبری به دست می‌آیند، اقدام نمود.

یکی از چالش‌های مهم مطرح برای سیاست‌گذاران، درک چگونگی عملکرد و تأثیرگذاری فناوری‌های سایبری ازجمله رسانه‌های اجتماعی بر کاربران است. ساده‌انگاری و درک نادرست از عملکرد رسانه‌های اجتماعی می‌تواند به سیاست‌گذاری‌های غلط و ناکارآمد بینجامد. سیاست‌گذاران حوزه فضای سایبری باید متوجه ماهیت کنترل خودکار این فضا باشند و بر این اساس بتوانند درک بهتری از عملکرد رسانه‌های اجتماعی و چرایی و چگونگی تأثیرات مختلف فردی و اجتماعی این رسانه‌ها به دست آورند. شناخت فضای سایبری

به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی به‌خوبی توجیه‌کننده چرایی آثار اجتماعی رسانه‌های اجتماعی ازجمله تأثیرگذاری بر نتایج انتخابات، تأثیرات فرهنگی-اجتماعی این رسانه‌ها و همچنین اعتیادآور بودن استفاده از آن‌ها برای کاربران است و در نتیجه می‌تواند به درک بهتر سیاست‌گذاران از تحولات مربوطه و سیاست‌گذاری‌های مؤثرتر در این زمینه بینجامد.

جستجویی مختصر در محتوای برخط فارسی پیرامون دانش سایبرنتیک و فناوری فضای سایبری، نشانگر فهم ناقص از این مفاهیم از سوی برخی دانشگاهیان و فعالان این حوزه است که به نشر این درک ناقص در میان مسئولان، سیاست‌گذاران و افکار عمومی انجامیده است. پیشنهاد می‌گردد یافته‌های این پژوهش در خصوص بازخوانی مفهوم سایبرنتیک و فضای سایبری، مورد توجه دانشگاهیان و محققان فعال در این حوزه قرار گیرد تا ضمن اصلاح درک فعلی آن‌ها از این مفاهیم، تبیین بهتر این مفاهیم از سوی آن‌ها و در نتیجه ترویج فهم عمومی دقیق‌تر در میان مسئولان، سیاست‌گذاران و افکار عمومی صورت پذیرد.

حفظ فرهنگ و هویت ملی در کنار توسعه حداکثری فناوری‌های سایبری، از دیگر دغدغه‌ها و چالش‌های مطرح در خصوص تحولات فضای سایبری است. هوشمندسازی خدمات مختلف دولتی و اجتماعی، عملاً به معنای کاهش عوامل انسانی در زنجیره خدمات و سپردن امور به ماشین‌های کنترل خودکار است. این امر در کنار محاسنی نظیر سرعت، دقت و سهولت، می‌تواند تأثیرات نامطلوب عدیده‌ای بر فرهنگ و هویت ملی و دینی در پی داشته باشد که لازم است ذیل مبحث تعامل مطلوب انسان-ماشین، مورد توجه سیاست‌گذاران فرهنگی کشور قرار گیرد.

توسعه‌دهندگان فناوری‌های سایبری باید ماهیت کنترل خودکار فضای سایبری را مورد توجه قرار دهند و خدمات سایبری خود را به‌گونه‌ای طراحی و پیاده‌سازی کنند که از قابلیت‌های کنترل خودکار این فضا حداکثر استفاده را به‌منظور ارائه خدمات بهتر به مشتریان خود بنمایند؛ تنها در این صورت است که توسعه‌دهندگان فناوری‌های سایبری قادر به ارائه محصولاتی رقابت‌پذیر در سطح جهانی خواهند بود تا ضمن جلب رضایت مشتریان خود،

به حفظ استقلال کشور در فضای سایبری کمک نمایند.

نگاه به فضای سایبری به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی روشن می‌سازد که امنیت سایبری صرفاً یک موضوع فنی نیست و نمی‌توان آن را با امنیت اطلاعات یکی دانست و با تأمین سه‌گانه محرمانگی، یکپارچگی و دسترس‌پذیری که در ادبیات امنیت اطلاعات مطرح است، به دنبال تأمین امنیت سایبری بود؛ بلکه با شناخت فضای سایبری به‌عنوان سیستم کنترل خودکار اجتماعی، جنبه‌های اجتماعی و همچنین جنبه‌های کنترل الگوریتمی این فضا به‌خوبی برجسته شده و ماهیت چندوجهی تأمین امنیت فضای سایبری تبیین می‌گردد. همچنین با توجه به روشن شدن امکان اتصال موجودیت‌های فیزیکی و بیولوژیکی به فضای سایبری، توجه به جنبه‌های بیولوژیکی و فیزیکی تأمین امنیت سایبری نیز ضروری به نظر می‌رسد. بر این اساس پیشنهاد می‌گردد که با مبنا قرار دادن شناخت ارائه‌شده در این مقاله در پژوهش‌ها و طرح‌های امنیت سایبری، از مغفول ماندن جنبه‌های مختلف تأمین امنیت سایبری جلوگیری به عمل آید.

پژوهش حاضر از جنبه نظری و مبتنی بر مطالعات کتابخانه‌ای به معرفی فضای سایبری به‌عنوان سیستم کنترل خودکار مصنوعی اجتماعی پرداخته است؛ لذا پیشنهاد می‌گردد در پژوهش‌های آتی شناخت حاصل‌شده از این پژوهش با انجام تجزیه‌وتحلیل‌های عملی و تجربی و مطالعات موردی تکمیل گردد. همچنین کاوش در پایگاه‌های اطلاعاتی دیگر مانند Web of Science و Scopus برای غنی‌سازی وسعت و عمق نتایج پژوهش حاضر، می‌تواند در پژوهش‌های آتی مورد توجه قرار گیرد.

فهرست منابع

- آزادی، جواد (۱۳۹۷). ***امنیت سایبری یا امنیت فضای مجازی؟***. تأملات رشد، سال ۱، شماره ۱، ۱۶۴–۱۶۸.
- قاسمی، سیروس؛ پارسا، سعید (۱۳۹۷). ***ارائه یک راه‌کار مؤثر برای تشخیص بدافزارهای آگاه به محیط مبتنی بر مقایسه تفاوت‌های رفتاری***. فصلنامه پدافند الکترونیکی و سایبری، ۶(۴)، ۱۲۳–۱۳۳.
- کریمی قهرودی، محمدرضا؛ معین آزاد، شیما؛ کریمی قهرودی، ابراهیم (۱۴۰۲). ***گونه‌شناسی مفهوم و عناصر اصلی فضای سایبری در اسناد راهبردی امنیت سایبری ملی کشورهای منتخب***. فصلنامه امنیت ملی، سال ۱۳، شماره ۴۷، ۹–۳۶.

References

- Alexei, A., & Alexei, A. (2022). The Difference Between Cyber Security Vs Information Security. Journal of Engineering Science, 29(4), 72–83.
- Ampère, A. M. (1843). Essai Sur la Philosophie de Sciences ou Exposition Analytique d'une Classification Naturelle de Toutes les Connaissances Humaines (Vol. 2). Bachelier, Paris.
- Angleman, S. (2000). What does it mean to dwell in cyberspace and why do we go there? A look at theories and definitions. Unpublished manuscript, Arkansas State University, Jonesboro. http://www.jrily.com/LiteraryIllusions/TheoryResearchPaperIndex.html.
- Azmi, R., and Kautsarina, K. (2019). Revisiting Cyber Definition. 18th European Conference on Cyber Warfare and Security, 22–30.
- Baraz, A., & Montasari, R. (2023). Law Enforcement and the Policing of Cyberspace. In R. Montasari, V. Carpenter, & A. J. Masys, Digital Transformation in Policing: The Promise, Perils and Solutions. Advanced Sciences and Technologies for Security Applications (pp. 59–83). Springer.
- Borgman, C. L. (2007). Scholarship in the Digital Age: Information, Infrastructure, and the Internet. The MIT Press.
- Bryant, R. (2001). What Kind of Space is Cyberspace? Minerva - An Internet Journal of Philosophy, 5, 138–155.
- Cavelty, M. D. (2008). Cyber-Security and Threat Politics US Efforts to Secure the Information Age. Routledge.
- Cibu, B., Delcea, C., Domenteanu, A., & Dumitrescu, G. (2023). Mapping the Evolution of Cybernetics: A Bibliometric Perspective. Computers, 12(11).
- Dambra, C., Gralewski, A., & Arias, J. (2019). LETSCROWD: Dynamic Risk Assessment for Mass Gatherings. Proceedings of the 16th ISCRAM Conference.
- De Nobrega, K. M., Rutkowski, A.-F., & Saunders, C. (2024). The whole of cyber defense: Syncing practice and theory. The Journal of Strategic Information Systems, 33(4).
- Futter, A. (2018). 'Cyber' semantics: Why we should retire the latest buzzword in security studies. Journal of Cyber Policy, 3(2), 201–216.
- Geoghegan, B., & Peters, B. (2016). Cybernetics. The International Encyclopedia of Communication Theory and Philosophy, 1–4.
- Gibson, W. (1984). Neuromancer. Grafton.
- Guess, A. M., Malhotra, N., Pan, J., & Barberá, P. (2023). How do social media feed algorithms affect attitudes and behavior in an election campaign? Science, 381(6656), 398–404.
- Harries, D. (2017). Narrative Mapping of Cyberspace. Context and Consequences. Cyberspace: Risks and Benefits for Society, Security and Development, 23–40.
- Jefferso, B. J. (2024). Cybernetic States: Communication, Control, and State-Space in the Advanced Research Projects Agenc. Political Geography, 113.
- Joseph, V., & Ray, D. (2020). India: Cyber Crimes Under The IPC And IT Act—An Uneasy Co-Existence. Argus Partners.

- Kalra, K. (2017). Emergence of Cyber Crimes: A Challenge for the New Millennium. Bharati Law Review, 86–103.
- Kesavamoorthy, R., & Karthikeyan, P. (2024). Cyberspace and Outer Space Security and Mitigation Strategies. In Cyber Space and Outer Space Security (1st Edition). River Publishers.
- Kikerpill, K. (2021). Asking the 'Cyber' question: Whose use of what information and communication technology creates which changes for whom? (Available at SSRN 3852365, pp. 1–15). Institute of Social Studies, University of Tartu, Estonia.
- Kothari, C. R. (2004). Research Methodology (2nd Edition). New Age International Pvt Ltd Publishers.
- Lee, W. (2011). Research Commentary: "CyberEthics"? International Journal of Cyber Ethics in Education (IJCEE), 1(1), 58–59.
- Lehto, M. (2013). The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies. International Journal of Cyber Warfare and Terrorism (IJCWT), 3(3), 1–18.
- Liddell, H. G., and Scott, R. (1940). A Greek-English Lexicon (Ninth Edition). Clarendon Press. Oxford.
- Lioubachevskaia, E. (2013). Place Matters. Carleton University.
- Lippert, K. J., & Cloutier, R. (2021). Cyberspace: A Digital Ecosystem. Systems, 9(3).
- Lyngs, U., Lukoff, K., Slovak, P., Binns, R., Slack, A., Inzlicht, M., Van Kleek, M., & Shadbolt, N. (2019). Self-Control in Cyberspace: Applying Dual Systems Theory to a Review of Digital Self-Control Tools. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1–18.
- Maathuis, C., Pieters, W., and Van Den Berg, J. (2016). Cyber Weapons: A Profiling Framework. IEEE 1st International Conference on Cyber Conflict U.S., 1–8.
- MarcCo, D. (2023). Cyber & Cyberspace Is A Domain Not Just A Security Function. Birkbeck, University Of London.
- Ning, H. (2022). A Brief History of Cyberspace. CRC Press (Auerbach Publications).
- Ning, H., Ye, X., Bouras, M. A., Wei, D., and Daneshmand, M. (2018). General Cyberspace: Cyberspace and Cyber-Enabled Spaces. IEEE Internet of Things Journal, 5(3), 1843–1856.
- Novikov, D. A. (2016). Cybernetics: From Past to Future. In Studies in Systems, Decision and Control (Vol. 47). Springer.
- Ottis, R., and Lorents, P. (2010). Cyberspace: Definition and Implications. Proceedings of the 5th International Conference on Information Warfare and Security, 267–270.
- Paasonen, S. (2011). Revisiting cyberfeminism. Communications, 36(3), 335–352.
- Pangaro, P. (2013). Cybernetics—A definition. https://www.pangaro.com/definition-cybernetics.html.
- Pym, D. J. (2021). The Origins of Cyberspace. In P. Cornish, The Oxford Handbook of Cybersecurity. Oxford University Press.

- Rajhans, A., Cheng, S.-W., Schmerl, B., Garlan, D., Krogh, B. H., Agbi, C., and Bhave, A. (2009). An Architectural Approach to the Design and Analysis of Cyber-Physical Systems. Electronic Communications of the EASST, 21.
- Sever, S. (2013). Prostheses, Cyborgs and Cyberspace—The Cyberpunk Trinity. ELOPE English Language Overseas Perspectives and Enquiries, 10(2), 83–93.
- Strate, L. (1999). The Varieties of Cyberspace: Problems in Definition and Delimitation. Western Journal of Communication (Includes Communication Reports), 63(3), 382–412.
- Syamsudin, S., & Ali, H. (2024). The Influence of Cyberspace, Computerization, and Technology on Information Systems. Siber International Journal of Education Technology (SIJET), 1(3), 116–120.
- Tabilo Alvarez, J., & Ram´ırez-Correa, P. (2023). A Brief Review of Systems, Cybernetics, and Complexity. Complexity, 2023(1), 1–22.
- Terebiński, B. A. (2023). The Technical Borders of Cyberspace. Wiedza Obronna, 285(4).
- Trentowski, B. F. (1843). Stosunek Filozofii do Cybernetyki Czyli Sztuki Rządzenia Narodem. J. K. Żupańskiego, Poznań.
- Venkatsubramanian, S. (2023). Critical Analysis of the Issue with Copyrights of Cyberspace. Indian Journal of Law and Legal Research, 5(1).
- Walser, R. (1991). The Emerging Technology of Cyberspace. In S. K. Helsel and J. P. Roth, Virtual reality: Theory, practice, and promise. Information Today Inc.
- Whittaker, J. (2003). The Cyberspace Handbook. Routledge.
- Wiener, N. (1954). The Human Use of Human Beings: Cybernetics and Society. Doubleday & Company, New York.
- Wiener, N. (1961). Cybernetics or Control and Communication in the Animal and the Machine (2nd Edition). The MIT Press, Cambridge, Massachusetts.
- Wong, K. K. L. (2024). Revisiting Cybernetics and Relation to Cybernetical Intelligence. In Cybernetical Intelligence: Engineering Cybernetics with Machine Intelligence (pp. 225–247). IEEE.
- Yolles, M. (2021). Metacybernetics: Towards a General Theory of Higher Order Cybernetics. Systems, 9(2).