

مقاله پژوهشی: بررسی تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر در

جمهوری اسلامی ایران

حسن محمدی منفرد^۱، محمدمهدی نژادنوری^۲ و محسن آقایی^۳

تاریخ پذیرش: ۱۳۹۹/۰۱/۲۴

تاریخ دریافت: ۱۳۹۸/۰۶/۰۸

چکیده

نظام سلطه در ادامه تقابل دائمی خود با نظام مقدس جمهوری اسلامی ایران از ظرفیت فضای سایبر برای تضعیف پشتوانه مردمی و تقلیل قدرت ملی آن به طور فزاینده‌ای بهره‌برداری می‌نماید. در این میان، به منظور ایجاد سازوکار مناسب برای تضمین منافع ملی در فضای سایبر، ارائه تصویر جامع و روشن از ابعاد مختلف این مسئله در سطح جامعه، به دغدغه بسیاری از صاحب نظران این حوزه تبدیل شده است. این تحقیق که از حیث هدف، پژوهشی کاربردی محسوب می‌گردد با هدف دستیابی به «تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر در جمهوری اسلامی ایران» انجام شده است. محقق در این تحقیق، نخست با گردآوری اطلاعات به روش کتابخانه‌ای و مطالعات اسنادی نسبت به شناخت فضای سایبر و مؤلفه‌های آن اقدام نموده است و در ادامه به منظور احصاء تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر در جمهوری اسلامی ایران و تعیین وضعیت آن‌ها از روش زمینه‌ای - موردی و با روش پیمایشی، در قالب پرسش‌نامه توزیع شده اقدام به تحلیل و جمع‌بندی نتایج نموده است. در نتیجه بر اساس بررسی و تحلیل اظهار نظر خبرگان و کارشناسان مربوطه مشخص گردید، کاربردهای اجتماعی فضای سایبر در جمهوری اسلامی ایران برای امنیت ملی، مخاطره آمیز می‌باشد و از این بین تهدیدات حوزه انسانی و شناختی با ۳۸ درصد، حوزه اطلاعاتی با ۳۴/۵ درصد و حوزه فیزیکی و زیرساختی با ۲۷/۵ درصد به ترتیب در اولویت یک تا سه قرار دارند. همچنین در رکن انسانی / شناختی، مؤلفه‌های جهانی‌سازی فرهنگی و تسخیر فضای اجتماعی کشورها و نیز ذائقه‌سازی و تغییر سبک زندگی به خصوص در جوامع شرقی به ترتیب در اولویت اول می‌باشند.

کلیدواژه‌ها: فناوری‌های اجتماعی، فضای سایبر، کاربرد اجتماعی فضای سایبر، تهدیدات اجتماعی فضای سایبر

۱. دانشجوی دکتری مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی (نویسنده مسئول) h. mohammadi@sndu. ac. ir
۲. دانشیار دانشگاه صنعتی مالک اشتر
۳. دانش‌آموخته دکترای مدیریت سیستم از دانشگاه تهران و پژوهشگر ارشد گروه مدیریت راهبردی فضای سایبر دانشگاه عالی دفاع ملی

مقدمه

امام علی (علیه السلام) می فرمایند: «إِنَّ أَخَا الْحَرْبِ الْأَرْقَ وَ مَنْ نَامَ لَمْ يَنْمِ عَنَّهُ؛ آن کس که همواره با جنگ همراه است، هرگز به خواب نمی رود و کسی که بخوابد، دشمن در مقابل او بیدار است» (نهج البلاغه، نامه ۶۲). امام خامنه ای (مدظله العالی) در مورد ضرورت توجه به فضای سایبر می فرمایند: «اهمیت فضای سایبر به اندازه خود انقلاب اهمیت دارد». همچنین ایشان در اجتماع بسیجیان در ورزشگاه آزادی دو مطالبه اساسی را از مسئولین این فضا از قبیل «شناخت فضای سایبر» و «جدیت در کار» مطرح فرمودند (بیانات رهبر انقلاب، ۱۳۹۷/۰۷/۱۲). در بیان چیستی و شناخت فضای سایبر، منابع مختلف با رویکردهای گوناگون انواع تعاریف را از فضای سایبر ارائه نمودند، ولیکن به طور حتم، در تبیین پدیده فضای سایبر می توان «فناوری» را کاربردی ترین رکن آن معرفی نمود. چراکه این رکن مورد توجه تمامی تحلیلگران بوده است تا آنجا که برخی بر این اعتقادند که فضای سایبر محصول تکوین، رشد و کاربست فناوری های نوین است (تسای^۱، ۱۹۹۷: ۴۶). همچنین بسیاری دیگر از پژوهشگران بر این باورند که ما اکنون، در آستانه ورود به عصر پسا صنعتی هستیم. در این عصر، مرز بین فناوری های فیزیکی، دیجیتالی و اجتماعی کمرنگ می شود. این یعنی، فناوری های فیزیکی که عصر صنعتی را ایجاد کردند، دیگر فقط فیزیکی نیستند، بلکه ترکیبی از فیزیکی - دیجیتالی هستند. به گونه ای که: امروزه ما شاهد ظهور طیف گسترده ای از فناوری های اجتماعی هستیم که عبارت اند از: شیوه بهره گیری ما انسان ها از این فناوری های دیجیتالی - فیزیکی که ترکیبی جدید برای رفع نیازها و امیال ما می باشند (مکینزی، ۲۰۱۲). برای مثال، شبکه های اجتماعی (فیس بوک، لینکداین،^۲ واتساپ،^۳ اینستاگرام،^۴ اسنپ چت^۵) و غیره و بسیاری برنامه های جدید وب محور، نشان دهنده تغییری اساسی در شیوه تعامل اجتماعی و حرفه ای بسیاری از ما انسان ها می باشد.

-
1. See Tsai
 2. LinkedIn
 3. Whatsapp
 4. Instagram
 5. Snapchat

پیشرفت‌های حوزه فناوری اطلاعات و ارتباطات به‌عنوان پیشران‌های اصلی فناوری‌های اجتماعی از یک طرف و شیوه استفاده‌ی ما از این فناوری‌ها به‌عنوان اعضای جامعه، در حال ایجاد دگرگونی‌های اساسی است. فرایندی که برخی از صاحب‌نظران این حوزه از آن به انقلاب «سکویی»^۱ یاد می‌کنند (پارکر، ۲۰۱۶) و از فناوری برای پیوند دادن افراد، سازمان‌ها و منابع در زیست‌بومی تعاملی استفاده می‌کنند که در این فضا به تولید قدرت و تبادل آن مبادرت می‌شود. این مقاله در راستای تبیین تهدیدات متأثر از کاربردهای اجتماعی فضای سایبر در جمهوری اسلامی ایران، نخست به طرح موضوع پرداخته است و سپس مفاهیم فناوری‌های اجتماعی و فضای سایبر را توصیف و در ادامه با مراجعه به بیانات مقام معظم رهبری، اسناد بالادستی، خبرگان موضوع و ادبیات مرتبط در سطح داخلی و خارج ضمن تبیین کاربردهای اجتماعی فضای سایبر، تهدیدات آن را تعیین و تشریح می‌نماید.

بیان مسئله

نظام جمهوری اسلامی ایران به علت ماهیت عدالت‌خواهی و ظلم‌ستیزی‌اش همواره از سوی مستکبران عالم در معرض انواع تهدیدات نرم و سخت قرار داشته و دارد. از سوی دیگر گسترش فناوری‌ها به مرور زمان عمق این تهدیدات را افزایش داده است (درویشی، ۱۳۸۷: ۱۶۸). ابزارها و خدمات فناوری ارتباطات و اطلاعات به‌طور فزاینده‌ای در زندگی روزمره انسان‌ها نفوذ کرده‌اند، به طوری که در سال ۲۰۱۶ میلادی، تقریباً نصف جهان (۳,۵ میلیارد کاربر) از اینترنت استفاده می‌کردند. گروه تجارت فدرال آمریکا^۲ برآورد کرده است که تعداد وسایل مرتبط به اینترنت در حال حاضر ۲۵ میلیارد است و به ۵۰ میلیارد در سال ۲۰۲۰ میلادی خواهد رسید (اف تی سی، ۲۰۱۵). همچنین در کنار رشد وسایل مرتبط به اینترنت، میزان داده‌های ایجادشده در این فضا به‌صورت نمایی در حال افزایش می‌باشد و بر اساس گزارش آی بی ام ۲/۵ کوئینتیلیون بیت روزانه در این فضا ساخته می‌شود و ۹۰ درصد

-
1. Platform
 2. Federal Trade Commission (FTC)

داده‌های جهان به‌تنهایی در دو سال گذشته ایجاد شده‌اند (آی بی ام، ۲۰۱۵). با این حال، درست مثل جهان واقعی، جهان سایبر نیز در معرض تهدیدات متنوع با آثار و صدمات گسترده قرار دارد.

امروزه جهان در حال تجربه نوینی از به‌کارگیری فناوری‌های اجتماعی است که در آن تلاش می‌شود از قابلیت برقراری ارتباط متقابل در فضای سایبر، برای هدایت منابع انسانی جوامع و به‌منظور تأثیرگذاری بر بینش و کنش‌های رفتاری آنان در راستای منافع مالکان خود استفاده بهینه شود. این راهبرد در صورت موفقیت می‌تواند از ظرفیت‌ها و قابلیت‌های این مخاطبین، در جهت ساماندهی، سازمان‌دهی و هدایت جوامع استفاده کند. در واقع با تکیه بر همین راهبرد اساسی، در چند سال گذشته با استفاده از سرمایه‌های انسانی و اجتماعی، از اقبال مختلف جامعه انسانی برای ایجاد تغییرات هدفمند در کشورها به خوبی استفاده می‌شود. نتایج تحقیقات مختلف بیانگر آن است که می‌توان از ظرفیت فناوری‌های اجتماعی در بسیاری از سطوح فردی و اجتماعی به‌منظور شناسایی مسائل و نیازهای اجتماعی، برقراری روابط اجتماعی و رهنمون‌سازی افراد در مسیر دستیابی به اهداف استفاده نمود و این مهم سبب شده است که فناوری‌های اجتماعی به‌طور چشمگیر و روزافزونی توجه آحاد جامعه، محققین صنعت و دانشگاه و نیز دست‌اندرکاران امور، سیاسی، امنیتی و دفاعی را به خود جلب نماید. همچنین جمهوری اسلامی ایران کاملاً آگاه است که نظام سلطه راهبرد تضعیف پشتوانه مردمی نظام را از طریق فضای سایبر و با به‌کارگیری فناوری‌های اجتماعی برای خود ترسیم نموده است. به‌گونه‌ای که تشدید حملات فنی و شناختی سایبری علیه ایران در سال‌های اخیر گواه این مدعا می‌باشد.

ضرورت و اهمیت تحقیق

انجام این تحقیق از آن جهت حائز اهمیت است که با بررسی تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر، مزیت‌های زیر حاصل می‌گردد.

۱. باعث توسعه مرزهای دانشی شناخت فضای سایبر در حوزه کاربردها و مخاطرات و تهدیدات آن می‌شود.

۲. روند شناسایی تهدیدات مربوط به کاربردهای اجتماعی فضای سایبر را تسریع می‌نماید.

۳. اذهان تصمیم‌سازان و تصمیم‌گیران را نسبت به تهدیدات این فضا روشن‌تر می‌کند.

۴. معیار و شاخص مناسب برای ارزیابی اقدامات عملیاتی تعیین می‌گردد.

نبود تصویر روشن از تهدیدات در سنوات پیشین، سبب بروز آسیب پذیری در حوزه های مختلف شده است. لذا بدیهی است عدم توجه به موضوع تحقیق، موجب خواهد شد تا ضمن لاینحل ماندن مسئله تحقیق، کاستی‌ها و ضعف‌های ناشی از عدم برخورداری از مزیت‌های یادشده به وجود آید. علاوه بر این:

۱. عدم آگاهی از تهدیدات و مخاطرات کاربردهای اجتماعی فضای سایبر و اتخاذ مواضع انفعالی در مواجهه با آنها.

۲. افول قدرت تصمیم‌سازی و تصمیم‌گیری برای مدیران، در حوزه مواجهه فعال با مخاطرات و تهدیدات این فضا.

۳. بهره‌مندی از فرصت‌ها در فضای سایبر را با مشکل مواجه می‌سازد.

در راستای نیل به موارد یادشده هدف و سؤال‌های زیر طرح گردیده است.

اهداف تحقیق

هدف اصلی

بررسی تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر در جمهوری اسلامی ایران

اهداف فرعی

۱. شناسایی کاربردهای اجتماعی فضای سایبر

۲. شناسایی تهدیدات کاربردهای اجتماعی فضای سایبر

۳. شناخت و ارائه مؤلفه‌های مهم تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر

سؤالات تحقیق

سؤال اصلی

تهدیدات عمده ناشی از کاربردهای اجتماعی فضای سایبر کدامند؟

سؤالات فرعی

۱. مؤلفه‌های فضای سایبری کدامند؟

۲. ویژگی‌های فضای سایبری کدامند؟

۳. کاربردهای اجتماعی فضای سایبری در کشور ما کدامند؟

پیشینه پژوهش

ادبیات و نوشته‌های مربوط به فضای سایبر، در چند سال اخیر رشد بسیار خوبی داشته است. به گونه‌ای که فضای سایبر برای ما دیگر فضای گنگ و مبهمی نیست. با توجه به گستردگی ادبیات این حوزه، تنها به بررسی آن دسته از نوشته‌هایی خواهیم پرداخت که به متغیر مستقل ما، یعنی کاربردهای اجتماعی فضای سایبر مربوط می‌شود. ضمن آنکه با توجه به بررسی‌های انجام‌شده، کمتر پژوهشی به بررسی دو موضوع کاربردهای اجتماعی فضای سایبر و تهدیدات متأثر از آن به صورت توأمان پرداخته است که از این حیث این تحقیق دارای نوآوری می‌باشد.

۱- به عنوان اولین نمونه می‌توان به کتاب «جوزف نای» با عنوان «آینده قدرت در قرن ۲۱» اشاره کرد. این اثر بی‌شک مهم‌ترین بستری است که سایر محققین و پژوهشگران می‌توانند از آن بهره‌برداری کنند. ایشان قدرت سایبر را احراز نتایج ترجیحی از طریق استفاده از منابع اطلاعاتی به هم پیوسته الکترونیکی در حوزه سایبر تعریف می‌کند. «نای» در این کتاب دو بعد از قدرت سایبری را برمی‌شمرد: وجه فیزیکی قدرت سایبر و وجه مجازی قدرت سایبر. بر همین اساس اهداف و مرجع نهایی قدرت سایبر را نیز در دو حوزه دسته بندی می‌کند. دسته اول در درون فضای سایبر اتفاق می‌افتد که وجه

سخت و نرم دارد؛ مانند «حملات سایبری» که در وجه سخت جای می‌گیرد و تأثیرگذاری بر ارزش‌ها و معیارهای زندگی دیگران که در وجه نرم صورت‌بندی می‌شود. اما دسته دوم خارج از فضای سایبر روی می‌دهد که آن هم به وجه سخت و نرم تقسیم می‌شود. نای از کنترل بر سیستم‌های تبادل اطلاعات و جریان آزاد اطلاعات به‌عنوان وجه سخت و استفاده از فضای سایبر برای دیپلماسی عمومی در عرصه روابط خارجی و بین‌المللی کشور به‌عنوان وجه نرم یاد می‌کند (نای، ۲۰۱۱).

۲- مانوئل کاستلز با نگارش اثر سه‌جلدی خود با عنوان «عصر اطلاعات: اقتصاد، جامعه و فرهنگ» سهم بسزایی در مطالعات مربوط به فضای مجازی و معرفی علمی این پدیده دارد. این کتاب یکی از منابع ارزشمندی است که در خصوص جامعه اطلاعاتی و تبعات اقتصادی و فرهنگی و اجتماعی آن نوشته شده است.

به‌گونه‌ای که می‌توان سایر متون را به‌نوعی وام‌دار آن دانست. در این اثر که به دایره‌المعارفی کامل و تحلیلی در موضوع فضای مجازی شهرت یافته است، نویسنده سه محور اساسی را به بحث گذارده است که عبارت‌اند از: جامعه شبکه‌ای، قدرت هویت، پایان هزاره. در «جامعه شبکه‌ای» مؤلف نشان داده که وقوع انقلاب در حوزه فناوری اطلاعات تمامی روندهای سیاسی، اجتماعی، اقتصادی و نظامی را در جوامع معاصر تحت تأثیر قرار داده و با تأسیس شرایطی تازه و گفتمانی نوین، زمینه تغییر جوامع مدرن را به جوامع شبکه‌ای فراهم ساخته است. جامعه شبکه‌ای را با نظریه‌ها و الگوهای متعارف نمی‌توان فهم نمود، چراکه در آن با فضای جریان‌های اطلاعاتی و مجازهای واقعی روبه‌رو هستیم؛ مؤلفه‌هایی که الگوی نوین از حیات را تداعی و بیان می‌نمایند (کاستلز، ۲۰۰۱).

۳- کلی شیرکی^۲ در کتاب «همه می‌آیند: قدرت سازمان‌دهی بدون سازمان» نشان می‌دهد که فناوری اطلاعات مدرن توانایی جامعه در ایجاد ارتباط، بسیج و تأثیردهی تغییر را به شکلی چشم‌گیر اصلاح کرده است. او بیان می‌کند که فناوری‌های نوین به همه اجازه

1. Nye
2. Clay Shirky

می دهد که عملکرد اجتماعی بزرگتر از گذشته را داشته باشند، «آن ها را قادر به ساختن انواع جدید گروه می کند» و به این گروه ها اجازه می دهد تا قدرت و نفوذ فراوان در حوزه هایی داشته باشند که عموماً به روی آن ها بسته است (شیرکی، ۲۰۰۸: ۲۱).

۴- مرکز پژوهش پيو^۱ در سال ۲۰۱۴ میلادی یک مطالعه پیمایشی با موضوع «زندگی دیجیتال در سال ۲۰۲۵ میلادی و اینکه چگونه فضای مجازی جامعه را در آینده تغییر خواهد داد» را با استفاده از نظر خبرگان موضوع با جامعه آماری ۲۵۵۸ نفری، انجام داد. یافته ها و نتایج آن، بیانگر شکل گیری «فضای مجازی، عظیم و ناپیدا است». در این جامعه، بهبود واقعیت از طریق فناوری های پوشیدنی و کاشتنی در بدن، اختلال در الگوهای کاری موجود و جاری و «برچسب گذاری، قرار دادن در پایگاه داده و نقشه کشی تحلیلی هوشمند در حوزه های فیزیکی و اجتماعی» اتفاق خواهد افتاد (اندرسون^۲، ۲۰۱۴).

۵- مؤسسه رند در سال ۲۰۱۳ میلادی پژوهشی با موضوع افراط گرایی انجام داد. نتایج این تحقیق بیانگر این موضوع می باشد که «اینترنت و فضای مجازی فرصت افراطی گرایی را به کمک افزایش ارتباط با افراد هم فکر از سراسر جهان در کل شبانه روز» افزایش می دهد. این مطالعه نشان می دهد فضای مجازی، نه تنها همچون انعکاس دهنده ای عمل می کند که تأییدی بر باورهای موجود است، بلکه این فرصت را برای ارتباط با افراد نادرست به وجود می آورد که در دنیای حقیقی ممکن نیست (رند، ۲۰۱۳). بنا بر برخی تخمین ها بیش از ۱۵۰۰۰ جنگجو برای پیوستن به داعش که در سوریه می جنگد به آنجا گسیل شدند و انگیزه این امر حداقل تا حدودی تلاش های آنلاین برای عضوگیری بوده است.

۶- یوسفی در مقاله ای با عنوان «استفاده های اطلاعاتی - امنیتی جریان تکفیری از شبکه های اجتماعی مجازی (فیس بوک و یوتیوب)» با روش تحلیل محتوا از صفحات وابسته به این جریان و نمونه گیری تصادفی به این نتیجه رسیده است که جریان های

تکفیری، از کارکردهای شبکه‌ها در راستای آموزش و گسترش عقاید خود بهره‌برداری نموده‌اند. همچنین جریان تکفیری از این شبکه‌ها برای جمع‌آوری اطلاعات جاسوسی و انجام عملیات روانی به منظور تأثیرگذاری بر مخاطبان خود استفاده نموده است (یوسفی و روشنی، ۱۳۹۳).

مبانی نظری تحقیق

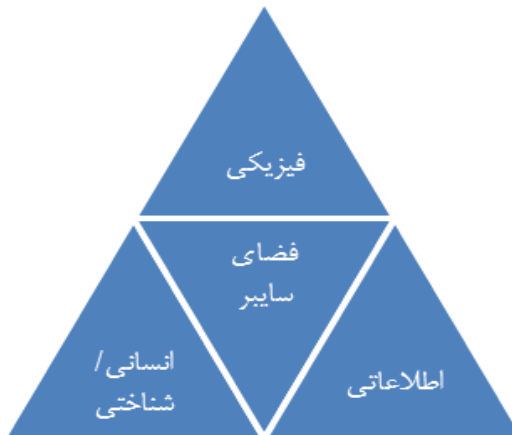
۱. چیستی فضای سایبر

فضای مجازی (سایبری)، مفهوم خیلی جدیدی نیست. این اصطلاح، نخستین بار توسط ویلیام اف. گیبسون^۱ در رمان علمی - تخیلی «برنینگ کروم»^۲ در سال ۱۹۸۲ به کار برده شد و سپس در رمان بعدی گیبسون به نام «نرومانسر»^۳ شناخته شد و به رغم معرفی، اصطلاحی مبهم باقی ماند (گیبسون، ۲۰۰۳: ۲۲۴). نزدیک به ۲۰ سال بعد، در سال ۲۰۰۳ میلادی بوش رئیس جمهور آمریکا، سیاست فضای مجازی امن را در راهبرد ملی فضای مجازی مطرح کرد. سپس در سال ۲۰۰۴ میلادی، در راهبرد ملی نظامی آمریکا این حوزه به عنوان پیش‌نیاز فضای نبرد عملیاتی مطرح شد (ریچارد، ۲۰۰۴: ۷۶). این سند، نشان می‌دهد که ایالات متحده آمریکا، از فناوری اطلاعات به عنوان ابزاری برای جنگ در حوزه فضای سایبری استفاده می‌کند.

تا آن زمان، هنوز فضای سایبری، به عنوان اصطلاحی قابل درک مطرح نبود و منابع مختلف با رویکردهای گوناگون انواع تعاریف را از این فضا ارائه نمودند. بر اساس تعریف وزارت دفاع آمریکا از فضای سایبر، فضای سایبری یک قلمرو جهانی در محیط اطلاعاتی است که از شبکه وابسته به هم از زیرساخت‌های فناوری اطلاعات شامل اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای و پردازشگرها و کنترلرهای جاسازی شده^۴ تشکیل

-
1. William F. Gibson
 2. Burning Chrome
 3. Neuromancer
 4. embedded

شده است (دی او دی^۱، ۲۰۱۰). از طرفی، محیط اطلاعاتی عبارت است از: «مجموعه‌ای از افراد، سازمان‌ها و سیستم‌هایی که اطلاعات خود و دیگران را جمع‌آوری، پردازش یا منتشر می‌کنند یا بر اساس اطلاعات، اقدام می‌کنند». محیط اطلاعاتی یک مجموعه به هم مرتبط از اطلاعات، زیرساخت‌های اطلاعاتی و فرایندهای مبتنی بر اطلاعات است. یک سیستم اطلاعاتی تلفیقی از شبکه‌ها، پردازشگرها، مراکز فرماندهی و اپراتورها است (استاف^۲، ۲۰۱۲). لذا بر اساس تعریف فوق و مستندات منتشرشده آمریکایی‌ها، فضای سایبر دارای ابعاد زیر است:



شکل (۱): مؤلفه‌های فضای سایبر

بعد فیزیکی: فضای سایبر یک شبکه ارتباطی گسترده جهانی متشکل از زیرساخت‌های ارتباطی و فناوری اطلاعات است.

بعد اطلاعاتی: فضای سایبر یک منبع اطلاعاتی توزیع شده حاوی انواع و سطوح مختلف داده، اطلاعات و دانش است.

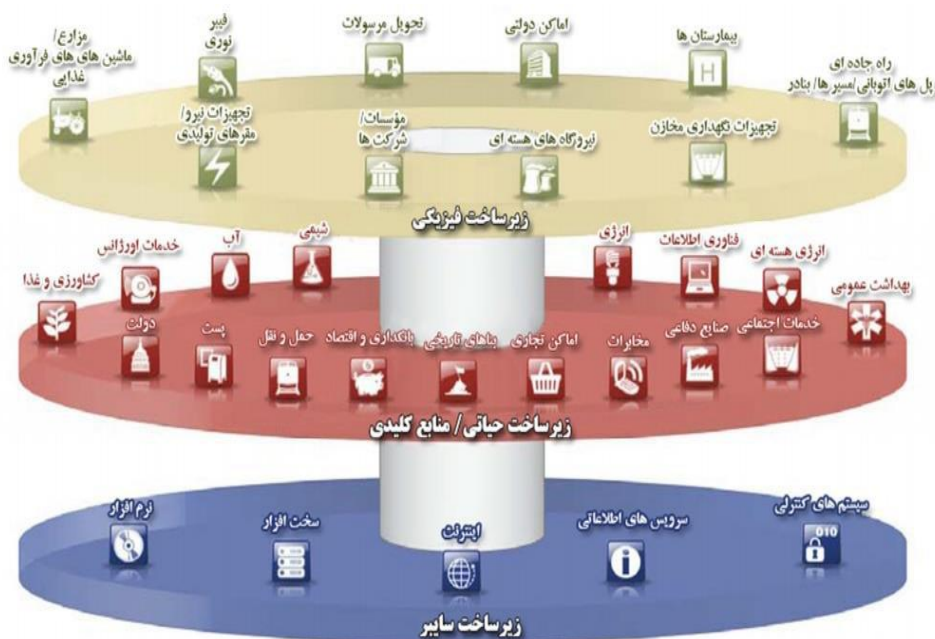
بعد انسانی / شناختی: فضای سایبر یک جامعه مجازی است که اعضای آن، قابلیت انجام فعالیت‌های اجتماعی، اقتصادی، سیاسی و فرهنگی را دارند.

1. Department of Defense Dictionary
2. Staff

۲. ویژگی‌های فضای سایبر

فضای سایبر، دارای ماهیت چندوجهی و کاربردهای متعددی می‌باشد که به‌طور چشم‌گیر و روزافزونی مورد استفاده بخش‌های مختلف و عموم جامعه قرار می‌گیرد. لذا با توجه به ادبیات موضوع و کسب نظر خبرگان، می‌توان ویژگی‌های فضای سایبر را به شرح زیر برشماری نمود:

۲-۱. زیرساخت تمامی زیرساخت‌ها



شکل (۲) - مدل زیرساختی فضای سایبر

(سند اقدامات و ظرفیت‌های عملیات سایبری ایالات متحده، ۲۰۱۷)

با توجه به وابستگی بالای زیرساخت‌ها به فضای سایبر در کشورهای مختلف، به‌خصوص کشورهای صنعتی و مبتنی بر داده و ارائه خدمات متنوع اجتماعی به واسطه این زیرساخت‌ها، لذا موضوع امنیت فضای سایبر برای آن‌ها امری حیاتی است و تدابیر فراوانی را در حفاظت از زیرساخت‌های خود بر بستر فضای سایبر اتخاذ می‌کنند.

۲-۲. جذابیت و تنوع

فضای سایبر مشتری محور محض است. لذا کلیه برنامه‌های نرم‌افزاری با هدف جلب مشتری طراحی و اجرا می‌شود و در همین راستا از قابلیت‌های طیف‌های متنوعی از مشتریان برای تولید و توزیع محصولات جدید نیز بهره‌گیری می‌شود. ظهور خبرنگار اجتماعی از جمله نمونه آن است.

۲-۳. تغییرات سریع

پیتر رالف معتقد است که یکی از مهم‌ترین ویژگی‌های فضای مجازی و رسانه‌های ارتباطی، توانمندی در ایجاد تغییر است. این توانمندی که معمولاً نادیده گرفته می‌شود در جنگ مجازی به‌خوبی قابل مشاهده است (ماه‌پیشانیان، ۱۳۸۹: ۴۰۷).

۲-۴. کنترل و هدایت متمرکز

فضای سایبر که به واسطه گسترش فناوری‌های اجتماعی به وجود آمده است از حیث معماری به‌گونه‌ای طراحی شده است که سازندگان و تهیه‌کنندگان تجهیزات و برنامه‌های سخت‌افزاری و نرم‌افزاری امکان کنترل و هدایت متمرکز این فضا را در اختیار دارند.

۲-۵. آسیب‌پذیری‌های متعدد و متنوع

اگرچه فناوری‌های اجتماعی در رشد اقتصادی، کیفیت آموزش و اطلاع‌رسانی، بهبود خدمات و ظرفیت، افزایش بهره‌وری، پیشرفت نوآوری و پایداری حکمرانی هر کشور تأثیر می‌گذارد. با این حال، در دسترس بودن، صحت و یکپارچگی و محرمانگی این زیرساخت اصلی، همواره در معرض آسیب‌های متعدد از ناحیه افراد، گروه‌ها و جوامع با مقاصد گوناگون می‌باشد.

۳. تهدید

فرهنگ آکسفورد تهدید را این‌گونه تعریف می‌کند «امکان به وحشت انداختن، ترساندن یا ایجاد فاجعه برای یک فرد یا جامعه و آسیب زدن به کسی یا چیزی و نتایج ناخوشایند

به بار آوردن» (جعفرزاده، ۱۳۹۴: ۶۷). در یک تعریف عمومی، تهدید عبارت است از «فقدان امنیت؛ ایجاد اختلال در توانایی‌های کشور در کسب اهداف ملی؛ اقداماتی که کمیت و کیفیت زندگی مردم یک کشور یا دامنه اختیارات حکومت را به‌طور جدی کاهش دهد» (بوزان، ۱۳۷۸: ۳۰).

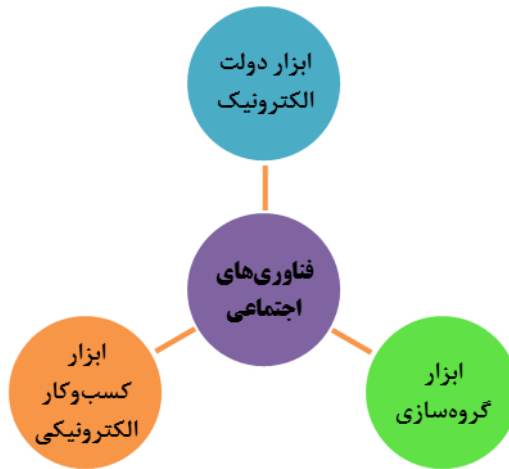
۴. فناوری‌های اجتماعی

فناوری‌های اجتماعی، برنامه‌های رایانه‌ای و خدماتی برای فعال نمودن تعامل اجتماعی هستند. این موارد محصول ۴۰ سال پیشرفت فناوری و تحقق چشم انداز بلندمدت در حوزه قابلیت‌های رایانه‌ها و حوزه دیجیتال هستند (کو^۱ و همکاران، ۲۰۱۲).

رشد سریع وب و قابلیت آن، به عنوان وسیله‌ای برای تعامل، مرحله‌ای را برای رشد انفجاری فناوری‌های اجتماعی ایجاد می‌کند. «فناوری‌های اجتماعی از نیروهای خلاق در میان کاربران استفاده می‌کنند و روابط جدید و پویای گروه را فعال می‌کنند. همان‌طور که ایمیل و پیام‌های فوری جایگزین تماس تلفنی شده است، فناوری‌های اجتماعی می‌توانند در تغییر پویایی ارتباطات تأثیر مشابه داشته باشند» (جنارو^۲، ۲۰۱۰). «مردم از محدودیت‌های دنیای فیزیکی آزاد می‌شوند و می‌توانند از فناوری‌های اجتماعی برای اتصال بین کاربران دیگر بدون شرایط مکانی و زمانی استفاده کنند و ضریب نفوذ خود را بر تعداد بیشتری از افراد بالا ببرند» (بیگین^۳ و همکاران، ۲۰۱۱). کو و همکاران تأکید کردند: با وجودی که اصطلاح «فناوری‌های اجتماعی» بیشتر برای اشاره به رسانه‌های جدید اجتماعی؛ مانند توییتر و فیس بوک استفاده می‌شود، ولیکن امروزه مفهوم فناوری اجتماعی دارای چندین جنبه می‌باشد که تصویر غالب فناوری را بی‌ثبات می‌کند. تمرکز این فناوری‌ها بر علوم اجتماعی، علوم انسانی و بازیگران انسانی به عنوان شکل دهنده اساس جامعه، می‌باشد (کو و همکاران ۲۰۱۱). این فناوری به عنوان یکی از دوازده فناوری نوظهور (شالوده شکن) و تغییردهنده زندگی،

-
1. Chui
 2. De Gennaro
 3. Bughin

کسب و کار و اقتصاد جهانی می‌باشد (منیکا^۱ ۲۰۱۳). فناوری‌های اجتماعی شامل طیف گسترده‌ای از ابزارهای مختلف فناوری است که می‌تواند توسط افراد، سازمان‌های خصوصی یا بخش دولتی یا به‌عنوان یک ابزار تعامل بین آن‌ها استفاده شود. آن‌ها شامل بسیاری از فناوری‌هایی هستند که به‌عنوان «رسانه‌های اجتماعی»، «وب ۳٫۰» و «ابزارهای همکاری» طبقه‌بندی می‌شوند. بر اساس شکل زیر، فناوری‌های اجتماعی به سه دسته: ابزار کسب و کار الکترونیکی، ابزارهای دولت الکترونیکی و ابزارهای گروه‌سازی تفکیک شده است (اسکارزوسکین^۲، ۲۰۱۳) که در تعامل با یکدیگر و همکاری با اهداف که توسط کاربران آن‌ها تعیین می‌شود، تعامل دارند.



شکل (۳): دسته‌بندی فناوری‌های اجتماعی

به‌طور کلی خاستگاه اصلی فضای سایبر در حوزه اجتماعی ارتباطات و رسانه می‌باشد و منظور از فناوری اجتماعی محدوده وسیعی از تجهیزات ارتباطی و محاسباتی نامتجانس است که تمامی این تجهیزات در بستر شبکه جهانی اینترنت به‌طور مستقیم یا غیرمستقیم به یکدیگر مرتبط شده تا فضای سایبر را شکل دهد. این شبکه‌بندی جهانی از تجهیزات،

1. Manyika
2. Skaržauskiene

موجب نزدیک تر شدن ارتباطات و تعاملات انسانی از طریق کم رنگ شدن مرزهای مکانی و زمانی شده است.

۵. ضرورت توجه به بعد اجتماعی فضای سایبر

«خود جهان فیزیکی در حال تبدیل به شبکه اطلاعات است»، اینترنت و فضای سایبر در نهایت همه وسایل مرتبط به خود از رایانه ها و تلفن ها تا وسایل «هوشمند» و پوشیدنی ها را در بر خواهد گرفت، بلکه همچنین میزان بی سابقه ای از داده های جمع آوری شده از دنیای اطراف را در بر خواهد گرفت (چو و همکاران ۲۰۱۰). لذا رشد ضریب نفوذ فضای سایبر و تولید کلان داده ها، پیامدهای چشمگیری برای جامعه به صورت کلی دارد. چراکه در این فضا داده ها مدیریت شده و از آن به عنوان بستر و پشتیبانی در تحلیل های فردی و اجتماعی استفاده می شود.

تقریباً تمامی بخش های جامعه از بهداشت تا تولید و حمل و نقل و غیره تحت تأثیر قرار خواهند گرفت به طوری که دو نتیجه عمده مدیریت فضای سایبر و کلان داده های موجود در آن را به شرح زیر می توان دسته بندی نمود:

۱- توانایی ردگیری (مردم، چیزها، رفتارها و غیره)

۲- توانایی پیش بینی

به عنوان مثال داده های به دست آمده از مچ بندهای سلامت و ساعت های هوشمند می تواند به بیمه گران در خصوص امید به زندگی افراد اطلاعات بی شماری را ارائه دهد یا اینکه اطلاعات به دست آمده از وسایل موجود در «خانه های هوشمند»^۱ به همراه داده های جی پی اس^۲ می تواند در مورد تخلیه بودن خانه اطلاع بدهد.

دغدغه مهم دیگر در خصوص محیط کلان داده ها مفهوم حباب های فیلتری و تمایز^۳ است. الگوریتم هایی که از داده های پیشین استفاده می کنند به کاربران دیجیتالی این تجربه

-
1. smart home
 2. GPS
 3. Discrimination

آنلاین ویژه را می دهند که اثر «حباب پالایه‌ای»^۱ را ایجاد کنند، اثری که به واسطه آن محتوا، تبلیغات و حتی اخبار برای هر فردی پالایه می شود. اگرچه منافع بسیاری در این عمل وجود دارد ولی ممکن است مضراتی همچون تفاوت‌های وخیم سیاسی و فرهنگی در جوامع و یا حتی تبعیض قیمتی ناخواسته برای برخی گروه‌های مشتری پیش آید. شرکت‌ها در حال حاضر از داده‌های به دست آمده از خریدهای مشتریان و رفتار اینترنتی آن‌ها برای طراحی و بازاریابی محصولات و خدمات به افراد استفاده می کنند. جناح‌های سیاسی نیز می توانند از چنین داده‌هایی برای پیشبرد «هدف‌گذاری جزئی» بر روی رأی‌دهندگان استفاده کنند. مسئله هشداردهنده‌تر توانایی پیش‌بینی است (سادیلک^۲ و کروم^۳، ۲۰۱۲)؛ و در آینده این توان پیش‌گویانه داده‌ها با پیشرفت در پردازش رایانه و هوش مصنوعی قطعاً افزایش خواهد یافت.

۶. کاربردهای اجتماعی فضای سایبر

با توجه به مطالب و موضوعات بیان‌شده و نیز کسب نظر از خبرگان در قالب پرسش‌نامه، کاربردهایی به شرح زیر در حوزه اجتماعی قابل برشماری است.

الف. بعد فیزیکی و زیرساخت

- اتصال تمام اشیای زندگی به فضای سایبر در قالب اینترنت همه اشیاء^۴
- توسعه ذخیره‌سازی و رایانش ابری فراگیر در جامعه
- استفاده از منابع مشترک (اطلاعات، نرم‌افزار و سخت‌افزار)
- شبکه‌سازی و هوشمندی زیرساخت‌های مجموعه‌های خدمات‌رسان اجتماعی از قبیل (بانک‌ها، پالایشگاه‌ها، نیروگاه‌ها، سدها، شبکه‌های حمل‌ونقل و ترافیک، شبکه‌های توزیع برق، آب، گاز و...).

1. Filter bubble
 2. Sadilek
 3. Krumm.
 4. Internet of everything

- امکان بارگذاری و بازانتشار اطلاعات برای بازیگران و کنشگران اجتماعی به صورت فنی
- امکان ارتباطات فراگیر تعاملی، افقی، منعطف و ارزان برای کنشگران اجتماعی
- توسعه دسترسی همگانی
- کاهش هزینه‌ها و تسهیل فرآیندهای کاری مدیریت اجتماعی
- بهبود و ارتقاء سطح عملکرد خدمات اجتماعی
- اشراف بر وضعیت موجود و سرعت در عیب‌یابی و نگهداری آن‌ها

ب. بعد اطلاعاتی

- توسعه جامعه دانایی محور با (دسترسی آزاد و به‌هنگام به بانک های اطلاعاتی دانشی، علمی، آموزشی و ...)
- توسعه عدالت اجتماعی اطلاعات محور
- ساخت اجتماعی با هنجارسازی و شکل‌گیری در جامعه
- اطلاع‌رسانی و خبررسانی
- تبلیغات و ایجاد کمپین تبلیغاتی
- مهندسی اجتماعی
- تصویرسازی در جامعه
- ایجاد وابستگی
- مدیریت یکپارچه اطلاعات
- پایش و کنترل اجتماعی به صورت متمرکز

ج. بعد انسانی و شناختی

- دسترسی سهل و آسان به اطلاعات
- تولید، عرضه و مصرف اطلاعات
- شبکه‌سازی و گروه‌سازی

- تعامل با عناصر مختلف جامعه اطلاعاتی
- جلب توجه
- هویت‌سازی و شکل‌گیری هویت‌های مجازی
- اعلام موجودیت
- کسب مشروعیت
- کسب قدرت اجتماعی
- وابستگی و سرگرمی
- توسعه مشارکت‌های مفید اجتماعی و ایجاد انسجام اجتماعی

۷. تهدیدات متأثر از کارکردهای اجتماعی فضای سایبر

تهدیدات دارای ابعاد مختلفی می‌باشد که بر سر ماهیت یا سرشت آن اختلاف نظر گسترده‌ای حاکم است. تری تریف و دیگران معتقدند که: عاملی که زندگی آرام و اطمینان بخش افراد در جامعه را دچار آسیب نماید، به‌مثابه یک تهدید اجتماعی مطرح است و در راستای ایجاد یک جامعه امن می‌بایست آن را مدیریت نمود (تری تریف و دیگران، ۱۳۸۳: ۴۷). از طرفی مصادیق تهدید اجتماعی بسیار زیاد و متنوع می‌باشد و به تعبیر نویسندگانی همچون سوبارائو^۱، با نرجی^۲ و برایث ویت^۳ متناسب با تحول جوامع انسانی، تغییر یافته و زیاد می‌شوند (افتخاری، ۱۳۸۵: ۱۹۵). در خصوص تهدیدات فضای سایبر می‌توان دو رویکرد اصلی را از یکدیگر تمیز داد. رویکرد اول، تک‌بعدی می‌باشد و به واسطه آن، نوع خاصی از تهدیدات فضای سایبر مشخص می‌شود. به طوری که تهدیدات رسانه‌ای، تهدیدات فناورانه و یا پدیده‌هایی از این قبیل به‌عنوان موضوع محوری تهدیدات فضای سایبر شناخته می‌شوند (عبدالله‌خانی، ۱۳۸۶). رویکرد دوم، یک رویکرد چندبعدی می‌باشد که وجوه مختلف فعالیت تهدیدات فضای سایبر را شناسایی

1. Sobarao
2. Bonnerjee
3. Braith wait

و به تصویر می‌کشاند (افتخاری، ۱۳۹۴). لذا نگارنده در این تحقیق با عنایت به ارکان تشکیل دهنده فضای سایبر و رویکرد چندبعدی و نیز کسب نظر از خبرگان در قالب پرسش نامه، تهدیداتی به شرح زیر را در حوزه اجتماعی برشماری نموده است که می‌بایست به آزمون گذاشته شود.

الف. بعد فیزیکی و زیرساخت

- نقض حریم خصوصی با فراگیر شدن اینترنت همه اشیاء
- اختلال در زیرساخت‌های مجموعه‌های خدمت‌رسان اجتماعی از قبیل (بانک‌ها، پالایشگاه‌ها، نیروگاه‌ها، سدها، شبکه‌های حمل و نقل و ترافیک، شبکه‌های توزیع برق، آب، گاز و...)
- انهدام و یا آسیب‌رسانی به تأسیسات صنعتی کشور (پالایشگاه‌ها، نیروگاه‌ها و ...)
- با نفوذ در سیستم‌های رایانه‌ای و کنترلی آن‌ها
- تسری یافتن تهدیدات با توجه به بستر شبکه‌ای
- ممانعت از استفاده از برخی سرویس‌های فضای سایبر به بهانه تحریم‌ها
- کمک ابزاری به نیروهای معارض در سطح جامعه
- بروز ضعف ساختاری فنی برای مدیریت یکپارچه
- قطع ارتباط با مراکز نگهداری داده در مواقع حساس و ضروری

ب. بعد اطلاعاتی

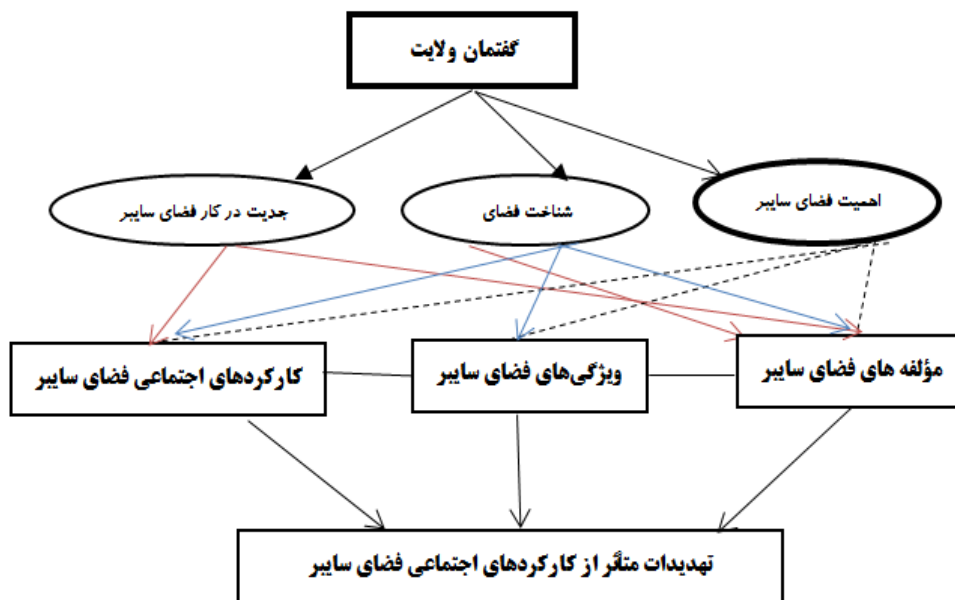
- وابستگی افراطی و مصرف‌گرایی اطلاعات
- جمع‌آوری اطلاعات اجتماعی و فرهنگی جامعه
- انگاره‌سازی و هنجارسازی معارض در جامعه
- شبیه‌سازی الگوهای رفتاری جامعه
- حمله به بانک‌های اطلاعاتی دستگاه‌ها و نهادهای خدمات‌رسان اجتماعی در سطح کشور

- دست‌کاری و مخدوش نمودن اطلاعات موجود در فضای سایبر
- ایجاد محدودیت در دسترسی به اطلاعات
- افکارسنجی جامعه
- فضاسازی کاذب و پخش شایعات
- تصویرسازی امنیتی از جامعه
- پایش و کنترل اجتماعی به صورت متمرکز

ج. بعد انسانی و شناختی

- جعل هویت و کلاه‌برداری
- امکان توانایی ره‌گیری افراد در فضای سایبر
- امکان پیش‌بینی رفتار افراد
- انجام عملیات‌های روانی و ادراکی
- ورود غیر قانونی به حریم خصوصی افراد
- شبکه‌سازی و گروه‌سازی معارضین در سطح جامعه
- بستری مناسب و تسهیل‌کننده برای فعالیت‌های تروریسم سایبری
- تضعیف سرمایه‌های اجتماعی
- جعل هویت در فضای سایبر و شیوع زندگی آواتاری
- ذائقه‌سازی و تغییر سبک زندگی به خصوص در جوامع شرقی
- جهانی‌سازی فرهنگی و تسخیر فضای اجتماعی کشورها

۸. چهارچوب نظری تحقیق



شکل (۴): چهارچوب نظری تحقیق

روش تحقیق

تحقیق حاضر به لحاظ هدف از نوع کاربردی و از نظر روش، توصیفی و تحلیلی می‌باشد. روش گردآوری داده‌ها کتابخانه‌ای و میدانی می‌باشد. همچنین شیوه تجزیه و تحلیل داده‌ها استفاده از رویکردهای کمی و کیفی به صورت توأمان می‌باشد. محقق در این تحقیق، نخست با گردآوری اطلاعات به روش کتابخانه‌ای و مطالعات اسنادی نسبت به شناخت فضای سایبر و مؤلفه‌های آن اقدام نموده است که پذیرش مدل سه‌لایه‌ای برای فضای سایبر محصول آن می‌باشد. در ادامه به منظور احصاء تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر در جمهوری اسلامی ایران و تعیین وضعیت آن‌ها از روش زمینه‌ای - موردی و با روش پیمایشی، در قالب پرسش‌نامه توزیع شده استفاده نموده است.

روش نمونه‌گیری مورد استفاده در این تحقیق روش نمونه‌گیری هدفمند است. حجم نمونه تا حد اشباع نظری می‌باشد. لذا در ادامه کار به منظور شناخت تهدیدات ناشی از کارکردهای اجتماعی فضای سایبر و تعیین وضعیت آن‌ها یک گروه ۱۶ نفره متناسب با مهارت‌ها و دانش ایشان در حوزه‌های سایبری و امنیتی انتخاب گردید. از آنجا که ویژگی افراد انتخاب شده به گونه‌ای بود که با مباحث سایبری، جامعه‌شناسی و امنیتی آشنا و مسلط بودند لذا امکان اجماع در یک فضای بین رشته‌ای برای این تحقیق فراهم بود. در ادامه نتایج بخش نظری تحقیق، برای اعتبارسنجی و اخذ نظرات حجم نمونه تعیین و نظرات ایشان در قالب پرسش‌نامه توزیع شده اخذ گردید.

اعتبارسنجی تحقیق

در این مرحله یافته‌های بخش نظری تحقیق بر اساس ارکان فضای سایبر و مؤلفه‌های مربوط به هرکدام از این ارکان مورد پرسش قرار گرفته شد و پس از اعتبارسنجی و بهره‌گیری از نرم‌افزار Spss، اعتبار تحقیق با تأییدی در حد ۸۷ درصد بر اساس آنچه که در ادامه شرح داده می‌شود مورد تأیید واقع شد. چراکه از تعداد کل گزینه‌های پرسش شده (حاصل ضرب ۱۶ پرسش‌نامه در ۳۴ مورد پرسش شده) یعنی $۱۶ * ۳۴ = ۵۴۴$ ، تعداد ۴۷۳ نظر، گزینه کاملاً موافق را برای ارکان و مؤلفه‌های مربوطه تأیید نمودند. در مرحله پایانی و به منظور نظرسنجی، اعضای گروه خبرگی پرسش‌نامه‌ای را که اعتبارسنجی شده بود دریافت نموده و نسبت به شناسایی و تعیین وضعیت مؤلفه‌ها بر اساس اولویت‌های سه‌گانه زیر اقدام نمودند.

- ۱- اولویت اول، شامل آن دسته از تهدیداتی می‌باشد که احتمال وقوع آن زیاد است.
- ۲- اولویت دوم، شامل آن دسته از تهدیداتی می‌باشد که احتمال وقوع آن متوسط است.
- ۳- اولویت سوم، شامل آن دسته از تهدیداتی می‌باشد که احتمال وقوع آن ضعیف است.

تجزیه و تحلیل داده‌ها

جدول شماره (۱): ویژگی‌های جمعیت‌شناختی پرسش‌شوندگان

درصد فراوانی	فراوانی	موارد	
۱۰۰	۱۶	مرد	جنسیت
۰	۰	زن	
۱۰۰	۱۶	جمع	
۰	۰	کارشناسی	میزان تحصیلات
۲۵	۴	کارشناسی ارشد	
۵۶	۹	دانشجوی دکتری	
۱۹	۳	دکتری	
۱۰۰	۱۶	جمع	
۶	۱	مدیریت بحران	رشته تحصیلی
۱۳	۲	مطالعات اجتماعی	
۲۵	۴	مطالعات امنیتی	
۵۶	۹	فضای سایبر	
۱۰۰		جمع	

بر اساس جدول شماره ۱ غالب پرسش‌شوندگان دارای مدرک دانشجوی دکتری با فراوانی ۵۶ درصد و پس از آن مدرک دکتری با فراوانی ۱۹ درصد می‌باشند. همچنین مشخص می‌شود که رشته مدیریت فضای سایبر با فراوانی ۵۶ درصد بیشترین سهم را از بین رشته‌های تحصیلی دارد که برای جامعه هدف این تحقیق مناسب و مطلوب می‌باشد.

جدول شماره (۲)

اولویت ۳	اولویت ۲	اولویت ۱	امتیاز با ضریب			فراوانی			مؤلفه تهدید	بعد
			اولویت ۳ (۱)	اولویت ۲ (۲)	اولویت ۱ (۳)	اولویت ۳	اولویت ۲	اولویت ۱		
۰	/۰۹	/۹۱	۰	۴	۴۲	۰	۲	۱۴	بستری برای اعمال قدرت دشمن	تهدید
/۱۴	/۱۱	/۷۵	۵	۴	۲۷	۵	۲	۹	نقض حریم خصوصی با فراگیر شدن اینترنت همه اشیاء	
/۰۲	/۰۹	/۸۹	۱	۴	۳۹	۱	۲	۱۳	اختلال در زیرساخت‌های مجموعه‌های خدمت‌رسان اجتماعی از قبیل (بانک‌ها، پالایشگاه‌ها، نیروگاه‌ها، سدها، شبکه‌های حمل و نقل و ترافیک، شبکه‌های توزیع برق، آب، گاز و...).	
/۰۴	/۱۹	/۷۷	۲	۸	۳۳	۱	۴	۱۱	انهدام و یا آسیب‌رسانی به تأسیسات صنعتی کشور (پالایشگاه‌ها، نیروگاه‌ها و ... با نفوذ در سیستم‌های رایانه‌ای و کنترلی آن‌ها	
/۱۷	/۶۲	/۲۱	۵	۱۸	۶	۵	۹	۲	تسری یافتن تهدیدات با توجه به بستر شبکه‌های	
/۳۰	/۳۷	/۳۳	۸	۱۰	۹	۸	۵	۳	ممانعت از استفاده از برخی سرویس‌های فضای سایبر به بهانه تحریم‌ها	
/۰۶	/۳۱	/۶۳	۲	۱۲	۲۴	۲	۶	۸	کمک‌آزمایی به نیروهای معارض در سطح جامعه	
/۰۹	/۴۰	/۵۱	۳	۱۴	۱۸	۳	۷	۶	بروز ضعف ساختاری فنی برای مدیریت یکپارچه	
۰	/۱۸	/۸۲	۰	۸	۳۶	۰	۴	۱۲	قطع ارتباط با مراکز نگهداری داده در مواقع حساس و ضروری	
/۲۱	/۵۷	/۲۲	۶	۱۶	۶	۶	۸	۲	وابستگی افراطی و مصرف‌گرایی اطلاعات	اطلاعاتی
/۰۵	/۲۰	/۷۵	۲	۸	۳۰	۲	۴	۱۰	جمع‌آوری اطلاعات اجتماعی و فرهنگی جامعه	
/۰۳	/۱۹	/۷۸	۱	۸	۳۳	۱	۴	۱۱	انگاره‌سازی و هنجارسازی معارض در جامعه	

بعد	مؤلفه تهدید	فراوانی			امتیاز با ضریب			درصد از کل امتیاز		
		اولویت ۱	اولویت ۲	اولویت ۳	اولویت (۱)	اولویت (۲)	اولویت (۳)	اولویت ۱	اولویت ۲	اولویت ۳
امنیت	شبیه‌سازی الگوهای رفتاری جامعه	۱۳	۳	۰	۳۹	۶	۰	۸۷	۱۳	۰
	حمله به بانک‌های اطلاعاتی دستگاه‌ها و نهادهای خدمات‌رسان اجتماعی در سطح کشور	۱۱	۴	۱	۳۳	۸	۱	۷۸	۱۹	۰/۳
	دست‌کاری و مخدوش نمودن اطلاعات موجود در فضای سایبر	۷	۶	۳	۲۱	۱۲	۳	۵۹	۳۳	۰/۸
	ایجاد محدودیت در دسترسی به اطلاعات	۶	۵	۵	۱۸	۱۰	۵	۵۵	۳۰	۰/۱۵
	افکارسنجی جامعه	۱۳	۲	۱	۳۹	۴	۱	۸۷	۰/۹	۰/۴
	فضاسازی کاذب و پخش شایعات	۱۴	۲	۰	۴۲	۴	۰	۹۱	۰/۹	۰
	تصویرسازی امنیتی از جامعه	۷	۷	۲	۲۱	۱۴	۲۰	۳۹	۲۵	۰/۳۶
	پایش و کنترل اجتماعی به صورت متمرکز	۱۰	۲	۴	۳۰	۴	۴	۷۸	۱۱	۰/۱۱
	جعل هویت و کلاهبرداری	۱۰	۶	۰	۳۰	۱۲	۰	۷۱	۲۹	۰
	امکان توانایی رهگیری افراد در فضای سایبر	۱	۱۳	۲	۳	۲۶	۲	۰/۹	۸۴	۰/۷
امنیت ملی / اقتصادی	امکان پیش‌بینی رفتار افراد	۱۲	۴	۰	۳۶	۸	۰	۸۲	۱۸	۰
	انجام عملیات‌های روانی و ادراکی	۱۳	۳	۰	۳۹	۶	۰	۸۷	۱۳	۰
	ورود غیر قانونی به حریم خصوصی افراد	۹	۷	۰	۲۷	۱۴	۰	۶۶	۳۴	۰
	شبکه‌سازی و گروه‌سازی معارضین در سطح جامعه	۱۲	۴	۰	۳۶	۸	۰	۸۲	۱۸	۰
	بستری مناسب و تسهیل‌کننده برای فعالیت‌های تروریسم سایبری	۱۱	۵	۰	۳۳	۱۰	۰	۷۵	۲۵	۰
	تضعیف سرمایه‌های اجتماعی	۹	۶	۱	۲۷	۱۲	۱	۶۸	۲۲	۰
	جعل هویت در فضای سایبر و شیوع زندگی آواتاری	۷	۸	۰	۲۱	۱۶	۰	۶۲	۳۸	۰
	دائمه‌سازی و تغییر سبک زندگی به‌خصوص در جوامع شرقی	۱۴	۲	۰	۴۲	۴	۰	۹۱	۹	۰
	جهانی‌سازی فرهنگی و تسخیر فضای اجتماعی کشورها	۱۶	۰	۰	۴۸	۰	۰	۱۰۰	۰	۰
	جمع	۲۹۶	۱۴۶	۵۳	۸۸۸	۲۹۲	۵۳	۷۲	۲۴	۴

جدول شماره (۳)

درصد از کل امتیاز			درصد فراوانی از امتیاز کل	امتیاز کل	امتیاز با ضریب			فراوانی			بعد فضای سایر
اولویت ۳	اولویت ۲	اولویت ۱			اولویت ۳ (۱)	اولویت ۲ (۲)	اولویت ۱ (۳)	اولویت ۳	اولویت ۲	اولویت ۱	
۷/	۲۴/	۶۹/	۲۷/۵	۳۴۱	۲۵	۸۲	۲۳۴	۲۵	۴۱	۷۸	فیزیکی
۶/	۲۲/	۷۲/	۳۴/۵	۴۳۱	۲۵	۹۴	۳۱۲	۲۵	۴۷	۱۰۴	اطلاعاتی
۰۶/	۲۵/	۷۴,۴/	۳۸	۴۶۴	۳	۱۱۶	۳۴۵	۳	۵۸	۱۱۵	انسانی/شناختی

در جدول شماره ۲، فراوانی خام از داخل پرسش نامه‌های توزیع شده استخراج می‌شود. امتیاز با ضریب، از ضرب فراوانی در رقم اهمیت هر وضعیت محاسبه شده است به نحوی که برای اولویت ۱ ضریب ۳، برای اولویت ۲، ضریب ۲ و برای اولویت ۳ ضریب ۱ را تعریف می‌نماییم. سپس از جمع امتیاز ستون‌های سه‌گانه، امتیاز کل را محاسبه نموده‌ایم. درصد از کل، عددی است که از نسبت امتیاز با ضریب هر ردیف به امتیاز کل به دست می‌آید. تهدیداتی که در اولویت ۱ احصاء شده‌اند از نظر خبرگان، دارای قطعیت بالا ارزیابی شده‌اند و بایستی در تدوین راهبردهای امنیتی جمهوری اسلامی ایران به آن‌ها توجه جدی شود.

بر اساس جدول شماره ۳ مشخص گردید که از نظر خبرگان، به واسطه شرایط و ویژگی‌هایی که این فضا دارد تهدیدات آن در هر سه رکن فضای سایر برای جمهوری اسلامی ایران مخاطره‌آمیز می‌باشد. به گونه‌ای که تهدیدات حوزه انسانی و شناختی با ۳۸ درصد، حوزه اطلاعاتی با ۳۴/۵ درصد و حوزه فیزیکی و زیرساختی با ۲۷/۵ درصد به ترتیب در اولویت ۱ تا ۳ می‌باشند. از طرفی در رکن انسانی ملاحظه می‌گردد که تهدیدات در اولویت اول و دوم می‌باشند و اولویت سوم تقریباً صفر می‌باشد. لذا بیانگر این واقعیت است که تهدیدات این حوزه بسیار خطرناک‌تر از حوزه‌های دیگر می‌باشد.

بر اساس آنچه که در جدول شماره ۲ به دست آمده است می‌توان اذعان نمود که در بعد فیزیکی عمده‌ترین تهدیدی که متوجه جمهوری اسلامی ایران می‌باشد و خبرگان با ۹۱ درصد از کل آن را در اولویت ۱ بیان نموده‌اند، استفاده دشمن از بعد فیزیکی و زیرساختی

فضای سایبر برای اعمال قدرت و انجام مانور در فضای اجتماعی جامعه می باشد. همچنین اولویت‌های بعدی به ترتیب اختلال در زیرساخت‌های مجموعه‌های خدمات‌رسان اجتماعی با ۸۹ درصد و دیگری امکان قطع ارتباط با مراکز نگهداری داده در مواقع حساس و ضروری می باشد. از آنجا که این بستر به لحاظ ساختاری و فنی در اختیار جمهوری اسلامی ایران نمی‌باشد با ۸۲ درصد از کل، مورد تأیید و تأکید خبرگان قرار گرفته است. از طرفی در رکن اطلاعاتی، ملاحظه می‌شود که مؤلفه‌های فضا سازی کاذب و پخش شایعات با ۹۱ درصد، افکارسنجی جامعه و شبیه‌سازی الگوهای رفتاری جامعه هر کدام با ۷۸ درصد در درجه اهمیت ۱ قرار گرفته‌اند.

همچنین در رکن انسانی، مؤلفه جهانی سازی فرهنگی و تسخیر فضای اجتماعی کشورها با ۱۰۰ درصد و ذائقه سازی و تغییر سبک زندگی به خصوص در جوامع شرقی با ۹۱ درصد در اولویت ۱ می‌باشند.

نتیجه‌گیری و پیشنهادها

الف. نتیجه‌گیری

در این تحقیق از حیث نظری، به این نتیجه رسیدیم که: فضای سایبر تمام ابعاد و زوایای حیات انسان را تحت تأثیر قرار داده است. به گونه‌ای که بخش عمده‌ای از فعالیت‌ها و تعاملات اجتماعی در کلیه سطوح، اعم از افراد، مؤسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس، یا خود، بخشی از فضای سایبری را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره برداری می‌شوند. بیشتر تعاملات اجتماعی از طریق این فضا انجام می‌گیرد؛ به عبارت دیگر فضای سایبر یک بُعد در کنار سایر ابعاد حیات اجتماعی انسان، مانند اقتصاد، فرهنگ، سیاست، نظامی‌گری به شمار نمی‌آید، بلکه به نوعی بر تمامی آن‌ها مسلط است. از طرفی امروزه به علت زیست جوامع به‌طور عام و جمهوری اسلامی ایران به‌طور خاص، در محیط پرتلاطم منبعث از تأثیر کاربردهای اجتماعی فزاینده فضای سایبر، بایستی

در تدوین راهبردهای امنیتی به تهدیدات متأثر از کاربردهای اجتماعی این فضا توجه جدی شود. همچنین از حیث روشی در این پژوهش به این نتیجه رسیدیم که بر اساس تحلیل اظهار نظر خبرگان و کارشناسان جامعه آماری مدنظر، کاربردهای اجتماعی فضای سایبر در شرایط فعلی، در تمام ارکان مدل سه‌لایه‌ای مطرح شده برای فضای سایبر برای کشور ما مخاطره‌آمیز می‌باشد و این مخاطرات بیشتر جنبه ایجابی و انسان‌محور می‌باشد.

لذا برای مدیریت این مخاطرات بایستی به دنبال اعمال حاکمیت سایبری در راستای منافع و ارزش‌های جمهوری اسلامی ایران به منظور حفاظت از زیرساخت‌ها و فرآیندهایی که بر بستر فضای سایبر فعال هستند، باشیم.

ب. پیشنهادها

۱) پیشنهادهای اجرایی

۱/۱- سامان‌دهی و مدیریت یکپارچه فضای سایبر کشور و پرهیز از اعمال سیاست‌های مقطعی و کوتاه‌مدت.

۱/۲- نهادسازی و ایجاد ساختارهای مناسب جهت ورود هوشمندان در جنگ رسانه‌های اجتماعی به‌عنوان صحنه اصلی کارکردهای اجتماعی - شناختی فضای سایبر

۱/۳- تسریع در راه‌اندازی شبکه ملی اطلاعات

۱/۴- با توجه به یافته‌های به‌دست‌آمده مبنی بر اینکه عمده تهدیدات فضای سایبر انسان‌محور می‌باشد. به نظر می‌رسد که وزارت علوم و تحقیقات و فناوری نسبت به راه‌اندازی رشته‌های مربوط به این حوزه در سطح تحصیلات تکمیلی اهتمام ویژه به عمل آورد

۱/۵- آگاهی بخشی به جامعه در ارتباط با تهدیدات متأثر از کاربردهای فضای سایبر در حوزه‌های مختلف اجتماعی، اقتصادی و ...

۲) پیشنهادهای پژوهشی

۲/۱- انجام پژوهش‌های مرتبط با موضوع مذکور در سطح ملی و با جامعه خبرگی جامع‌تر

۲/۲- تبیین ابعاد، مؤلفه‌ها و شاخص‌های هرکدام از تهدیدات سایبری با درصد اهمیت بالا

در ارکان مختلف فضای سایبری جمهوری اسلامی ایران و یافتن راهکارهای مقابله با آن.

فهرست منابع و مآخذ

الف. منابع فارسی

- امام خامنه‌ای (دامت برکاته)، (۱۳۹۷)، بیانات در اجتماع بسیجیان در ورزشگاه آزادی تهران.
- ایزدی، فواد و ماه‌پیشانیان، مهسا، (۱۳۹۰)، راهکارها و راهبردهای ایالات متحده برای جنگ سایبر تهران، خبرگزاری فارس، معاونت پژوهشی و آموزشی گزارش راهبردی، شماره ۲.
- یوزان، باری، (۱۳۷۸)، دولت‌ها، مردم و هراس مترجم: ناشر، تهران، پژوهشکده مطالعات راهبردی.
- تامپسون، جان، (۱۳۸۰)، رسانه‌ها و مدرنیته: نظریه اجتماعی رسانه‌ها، مسعود اوحدی، تهران، سروش.
- درویشی، فرهاد، (۱۳۸۷)، پروژه تحقیقاتی جنگ‌های مدرن، بررسی تفاوت‌های آن با جنگ‌های پیشین، بررسی عام فناوری در جنگ‌های مدرن با تحولات مورد انتظار در جنگ و فناوری نظامی در دو دهه آینده.
- کاستلز، مانوئل، (۱۳۸۰)، عصر اطلاعات: ظهور جامعه شبکه‌ای، احمد علیقلیان و افشین خاک‌باز، تهران، طرح نو.
- نای، جوزف، (۱۳۹۰)، آینده قدرت، رضا مراد صحرائی، تهران، حروفیه.
- یوسفی، جعفر؛ روشنی، مرتضی، (۱۳۹۳)، استفاده‌های اطلاعاتی - امنیتی جریان تکفیر از شبکه‌های اجتماعی مجازی (فیس‌بوک و توییتر)، فصلنامه پژوهش‌های حفاظتی و امنیتی دانشگاه امام حسین (ع)، سال سوم، شماره ۱۱.

ب. منابع انگلیسی

- Adam Sadilek and John Krumm, "Far Out: Predicting Long- Term Human Mobility, Association for the Advancement of Artificial Intelligence, 2012, <http://research.microsoft.com/en-us/um/people/jckrumm/>
- Bughin, J., Byers, A. H., Chui, M. (2011). How business uses social technologies, McKinsey Quarterly, November 2011, access online 16 Sep. 2012, url: http://www.mckinseyquarterly.com/newsletters/chartfocus/2012_05.html
- Chui, M., Manyika, J., Bughin, J., Dobbs, R., Roxburgh, Ch., Sarrazin, H., Sands, G., Westergren, M. (2012). The Social Economy: Unlocking Value and Productivity Through Social Technologies, McKinsey Global Institute Report.
- Clay Shirky, Here Comes Every body: The Power of Organizing without Organizations (New York: Penguin Press, 2008), 11-21
- De Gennaro T. (2010). Social Technologies Will Penetrate IT Management Tools, Forrester Research.

- Derksen, M., Vikkelsø, S., Beaulieu, A. (2012). Social technologies: Cross-disciplinary reflections on technologies in and from the social sciences, *Theory Psychology*, vol. 22, no. 2, p. 139-147.
- FTC, Internet of Things: Privacy & Security in a Connected World, Staff Report (Washington, DC: FTC, 2015), <http://www.ftc.gov/system/files/documents/reports>
- Gibson, William, *Burning Chrome*, Eos Publishers, New York, NY, 2003 Edition, 224 pages and William Gibson, *Neuromancer*, 20th Edition, Ace Publishers, New York, NY, 2004, 384 pp. In the latter book, Gibson defined cyberspace as: “a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts.”
- Geoffrey Parker, Marshall Van Alstyne, and Sangeet Paul Choudary, *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*, 2016, <https://www.overdrive.com/search?q=747D962F-32B3-4F05-9126-A09E659AB96C>
- Janna Anderson and Lee Rainie, *Digital Life in 2025* (Washington, DC: Pew Research Center, 2014), 5, http://www.pewinternet.org/files/2014/03/PIP_Report_Future_of_the_Internet_Predictions_031114.pdf.
- Leibetseder, B. (2011). A Critical Review on the Concept of Social Technology. *Social Technologies*, 1(1), p 7–24.
- Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. McKinsey Global Institute Report, May 2013.
- Michael Chui, Markus Loffler, and Roger Roberts, “The Internet of Things, *McKinsey Quarterly*, March 2010, http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things
- McKinsey Global Institute et al., *The Social Economy: Unlocking Value and Productivity Through Social Technologies* (McKinsey Global Institute, 2012).
- Skaržauskienė, A; Tamošiūnaitė, R.; Žalėnienė I. (2013). Defining Social technologies. Proceedings of the 4th international conference on Information systems management and evaluation, RMIT University Vietnam, Ho Chi Ming City, Vietnam 13-14 May 2013 / edited by Blooma John, Mathews Nkhoma, Nelson Leung. [Sonning Common]: Academic Conferences and Publishing International, 2013