مقاله پژوهشی:
چالش‌های راهبردی حکمرانی با گسترش فضای سایبر

احسان کیان‌خواه[1]

تاریخ دریافت:۱۳۹۷/۰۹/۱۶ تاریخ پذیرش: ۱۳۹۷/۱۲/۸

چکیده

فضای سایبر با فناوری‌های جذاب و فریبنده خود بدون هیچ مقاومتی در بین نخبگان اجرایی و آحاد مردم در حال نفوذ به همه ارکان جامعه است. به علت توانمندسازی و قدرت‌سازی فضای سایبر تمام زیرساخت‌های حیاتی کشور با سرعت بالایی در حال سایبری شدن در ماده، صورت و غایت است. این سرعت بالا و بی‌مهابا بودن در استخدام فناوری‌های سایبری منجر به شکل‌گیری چالش‌ها و موانعی در استحکام درون‌زای حکمرانی شده است. این تحقیق با روش ترکیبی، ابتدا چالش‌های حکمرانی را به‌صورت توصیفی و تحلیلی اکتشاف نموده و سپس با مراجعه به خبرگان این حوزه و پیمایش نظرات و تحلیل با معادلات ساختاری اکتشاف نموده است. هژمونی آمریکایی در مدیریت و کنترل فضای سایبر، شناسایی و نظارت فراحاکمیتی بر توانمندی‌های اقتدارافزای جامعه، تهدیدات و تهاجمات سایبری، پذیرش الگوی رفتاری و سبک زندگی فراملی و فرافرهنگی و مهندسی و مدیریت فرهنگی فراملی و فرهنگ منحط و اباحه‌گر چالش‌های راهبردی حکمرانی عرصه جهانی‌سازی سایبری است. فهم صحیح گسترش سلطه‌افکنی غرب با فضای سایبر مبنایی کلیدی برای جهت‌دهی سیاست‌های گسترش فضای سایبر خواهد بود.

کلیدواژه‌ها: چالش‌های راهبردی حکمرانی، فضای سایبر، هژمونی.

---

۱. دانش‌آموخته دکتری مدیریت راهبردی فضای سایبر دانشگاه عالی دفاع ملی ehsan@kiankhah.com

مقدمه

انسان‌ها، اشیا و چیزها در حال اتصال به شبکه‌ای جهانی هستند. با گسترش سریع ارتباطات پهن باند[1] و عمومی شدن IPV6 که قابلیت افزوده شدن حدود (۲ ^۱۲۸) [2] دستگاه به‌طور هم‌زمان را به شبکه اینترنت دارد[3]، گستره‌ای از اتصالات متنوع با رشد شگفت‌انگیزی در حال شکل یافتن است. این اتصالات گسترده جهانی، منجر به رشد اینترنت اشیا[4] و اتصال هر چیز در هر مکان و هر زمان با هر وسیله‌ای در پیرامون ما خواهد شد. در سال ۲۰۰۳ میلادی، ساکنین زمین ٦/۳ میلیارد نفر بودند و از این بین ۵۰۰ میلیون دستگاه به اینترنت متصل بود؛ اما این وضعیت تا سال ۲۰۲۰ میلادی که جمعیت کره زمین به ۷/٦ میلیارد نفر خواهد رسید، به ۵۰ میلیارد دستگاه افزایش می‌یابد (ایوانس[5]، ۲۰۱۱). این تجمیع انسان، حیوان و اشیا نمایشی از یکپارچگی کامل دنیای واقعی و فضای سایبر در اینترنت آینده است (باکلی[6]، ۲۰۰٦).

فضای سایبر از حد برقراری ارتباط موقت که با اتصال[7] کاربر شروع می‌شد و با انجام فعالیت‌های مورد نیاز کاربر قطع ارتباط[8] صورت می‌گرفت، به یک ارتباط دائمی تبدیل شده است گویی که جهانی برای زیست در حال شکل گرفتن است. این زیست‌گون که بر پایه اینترنت اشیا، رایانش ابری و اینترنت همراه، در حال توسعه و گسترش یافتن است، به علت ماهیت فناورانه سایبر و خاستگاه شکل‌گیری و گسترش آن، منجر به شکل‌گیری چالش‌هایی برای حکمرانی شده است. لذا دغدغه و مسئله اصلی این تحقیق، شناسایی و اکتشاف چالش‌های راهبردی این هژمونی نوظهور است.

---

1. Broadband
2. 340,282,366,920,938,000,000,000,000,000,000,000,000,000
۳. در مقابل IPV4 که (۲ ^۳۲) [3] میزان ارتباط هم‌زمان را فراهم می‌آورد.
4. Internet of things (IOT)
5. Evans
6- Buckley
7. Online
8. Offline

از آنجایی که لحظه به لحظه بر تسلط و هژمونی سایبر بر جوامع به‌ویژه کشور ما در حال افزایش است، شناسایی و کشف چالش‌های راهبردی حکمرانی کشور، برای مدیریت آینده جامعه، اهمیت حیاتی دارد. از طرفی این تحقیق تلاش دارد، با شناسایی عوامل مرتبط با نفوذ و هژمونی سایبری به آگاهی‌بخشی جامعه علمی و اجرایی و برون‌رفت از اعتماد بدون پشتوانه به فناوری‌های عصر سایبر، کمک نماید.

هدف اصلی این تحقیق «اکتشاف چالش‌های حکمرانی با گسترش فضای سایبر» است. در این راستا پژوهش حاضر گام‌های زیر را برای کشف این چالش‌ها برداشته است:

(۱) چیستی حکمرانی،

(۲) فضای سایبر و قابلیت‌های آن،

(۳) اکتشاف چالش‌های راهبردی فضای سایبر بر حکمرانی.

از برخی کارهای پژوهشی و تحقیقات مرتبط با این حوزه می‌توان به «چالش‌آفرینی اینترنت اشیا بر ارکان امنیت ملی کشور» (کیان‌خواه و کریمی‌قهرودی، ۱۳۹٤)، «تهدیدات سایبری و تأثیر آن بر امنیت ملی» (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱) و «تأثیر فضای مجازی بر امنیت ملی جمهوری اسلامی و ایران و ارائه راهبرد» (قدسی، ۱۳۹۲) اشاره نمود. کیان‌خواه و کریمی قهرودی با بررسی اینترنت اشیا و فناوری‌های مرتبط با آن چالش امنیت ملی را با روش پیمایشی استخراج نموده‌اند. این چالش‌ها در سه حوزه حاکمیت، جغرافیا و مردم و سبک زندگی طبقه‌بندی شده است. آن‌ها معتقدند اینترنت اشیا، داده‌های عظیم، رایانش ابری و داده‌کاوی در کنار مزایای زیادی که دارد، چالش‌های جدیدی را متوجه امنیت ملی جمهوری اسلامی ایران خواهند کرد. خلیلی و نورعلی‌وند در تحقیق خود معتقد هستند که فضای سایبر مفهوم امنیت را تغییر داده است و امنیت ملی دیگر صرفاً در ارتباط با مرزهای جغرافیایی نیست، بلکه افت کیفیت شهروندان نوعی تهدید امنیت ملی است. از میان رفتن بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، تغییر ماهیت تهدید و گستردگی آسیب‌پذیران از تأثیرات فضای سایبر بر امنیت ملی است. در پژوهش دیگر، قدسی، به بررسی تأثیر فضای مجازی بر امنیت ملی در حوزه‌های اجتماعی – فرهنگی، سیاسی،

امنیت و روان‌شناختی پرداخته است. سه تحقیق فوق تأثیر فضای سایبر بر امنیت ملی را از نگاه‌های مختلف بررسی نموده است، در راستای پژوهش‌های مذکور، پژوهش حاضر تلاش نموده است، با توجه به ویژگی‌های فزاینده فضای سایبر و هژمونی پدیدآمده، چالش‌های دولت و هویت ملی را شناسایی نماید.

روش تحقیق

نوع پژوهش حاضر توسعه‌ای و آینده‌نگرانه است و روش تحقیق آن ترکیبی از توصیفی- تحلیلی و کمی است. در ابتدا اطلاعات مورد نیاز برای این پژوهش از طریق بررسی منابع، کتب و مقاله‌های پژوهشی، جمع‌آوری‌شده و سپس مورد مداقه و تحلیل قرار گرفته است. به این ترتیب که با توصیف فضای سایبر و ارکان دولت ملی، مجموعه‌ای از چالش‌های راهبری با تبیین و استدلال اکتشاف شده است. در گام دوم با روش کمی نتایج یافته‌شده در معرض نظر خبرگان قرار گرفته و نتایج با مدل‌سازی معادلات ساختاری و با نرم‌افزار SmartPLS تحلیل شده است. برای محاسبه حداقل نمونه لازم در روش PLS، از نظر بارکلای و همکاران (۱۹۹۵ م) استفاده شده است (داوری و رضازاده، ۱۳۹۲). بر اساس این دیدگاه تعداد نمونه با ضرب ۱۰ در بیشترین تعداد شاخص مدل اصلی پژوهش، مشخص می‌شود (همان). با این فرض حجم نمونه برای این مدل تحقیق، برابر با ۳۰ است که از بین متخصصان حوزه سایبر و امنیت ملی انتخاب شده‌اند و دارای مدرک کارشناسی ارشد و دکترا هستند. نتایج بر اساس این حجم نمونه مورد ارزیابی قرار گرفته است.

چیستی حکمرانی

حکمرانی[1] بیان شیوه و حالت حکومت کردن است. حکومت و دولت[2] ابزار و نتیجه حکومت کردن را ترسیم می‌کنند. حکمرانی به مجموعه‌ای از فرآیندها اشاره دارد که

1. Governance
2. Government

با قدرت، اقتدار و نفوذ، سیاست‌ها و رویه‌هایی را برای حکومت کردن در دست می‌گیرد. وادی حکمرانی، وادی هدایت و کنترل است و با خلق و بازتولید قوانین، هنجارهای اجتماعی و اقدامات ساختاریافته در ارتباط است. از طرفی، حکمرانی نیازمند جهت و تنظیم غایت است، یعنی حکمرانی برای هدف و غرضی شکل می‌گیرد. همان‌طور که در حکمرانی (حاکمیت) شرکتی[1]، هدف تنظیم روابط بین سهامدار و هیئت‌مدیره است تا بتوان حداکثر منفعت و ارزش پایدار را برای سهامدار تحقق بخشید. به‌طور کلی ویژگی حکمرانی می‌تواند فرآیندمحور، یعنی توجه به اثربخشی فرآیند، کل‌نگر، یعنی توجه به تمام فعل و انفعالات سیستم و پدیده، پیش‌بینی‌پذیر، یعنی درک بیرونی درست از عکس‌العمل حکمرانی در شرایط متفاوت، پاسخگویی، یعنی بیان هم علت و هم دلیل تصمیم و مسئولیت‌پذیری در اقدامات، مسئله‌محور، یعنی انضمامی و ناظر به مکان و زمان مشخص و در نهایت جهت‌دار، یعنی هدایت و کنترل برای دستیابی به تعالی و ارتقای مشخص، باشد.

روی دیگر حکمرانی قدرت، نفوذ و اقتدار است. قدرت ملی به‌عنوان مفهومی ژئوپلیتیکی، صفت جمعی افراد یک ملت یا ویژگی کلی یک کشور را منعکس می‌کند که برآیند توانایی‌ها و مقدورات آن ملت یا کشور محسوب می‌شود (حافظ‌نیا و دیگران، ۱۳۸۲: ۵۱). بارزترین وجه اعمال حاکمیت از سوی بازیگران و نهادهای سیاسی حکومتی، حاکمیت در قلمروی جغرافیایی کشورهاست که به فضای ملی موسوم است؛ چنین حاکمیتی عبارت از استقلال عمل و حق تصمیم‌گیری کشورها و حکومت‌ها در سیاست‌های داخلی و خارجی خود است (انوری، ۱۳۸۲: ۸۳۷). مرز مشخص‌کننده محدوده حاکمیت جغرافیایی است. مرز به‌عنوان خطی فرضی است که محدوده سرزمینی کشور را ترسیم می‌کند و اهمیت آن در این است که مشخص‌کننده محدوده حاکمیت کشور است (بلدسو بوسچک، ۱۳۷۵: ۱۸۷).

قدرت وقتی در قالب یک جامعه یا ملت نگریسته شود و برآیندی از توانایی های مادی و معنوی آن ملت محسوب شود، جنبه‌ای ملی پیدا می‌کند. به عبارت دقیق‌تر، مجموعه انسان‌هایی که تشکیل ملتی را داده که در کل یک کشور سازمان سیاسی پیدا کرده‌اند، دارای

1. Corporate Governance

قدرتی می‌باشند که از برآیند قوای ترکیب‌شده آن‌ها به دست می‌آید و می‌توان آن را قدرت ملی آن کشور و ملت دانست (حافظنیا و دیگران، ۱۳۷۸: ۵). از طرفی، ملت‌ها بر پایه هویت مشترک، احساس تعلق مشترک و علایق و منافع مشترک پدید می‌آیند و پدیده‌ای واقعی هستند که نمی‌توان آن‌ها را انکار کرد؛ ویژگی‌های بنیادین تشکیل ملت، یعنی هویت، احساس تعلق و منافع مشترک از ویژگی‌های ذاتی نوع بشر و انسان است (حافظنیا، ۱۳۹۰: ۱۲۸). به عبارت دیگر چارچوب جغرافیایی مرزها که خصلتی نمادین دارند، دربرگیرنده افرادی هستند که به‌طور کلی شباهت‌هایشان بیشتر از تفاوت‌های آن‌هاست. اساساً همین شباهت‌هاست که به‌عنوان شاخص‌هایی برای تعریف هویت ملی آن‌ها به‌عنوان عضویت در یک ملت و کشور خاص به کار می‌آید؛ هویت نه‌تنها ارتباط اجتماعی را ممکن می‌کند، بلکه به زندگی افراد هم معنا می‌بخشد (حافظنیا، ۱۳۹۰: ۱۲۵).

حکمرانی در واقع، قدرت برتری است که در حیطه دولت کشور، اراده‌ای فراتر از آن وجود ندارد، به‌گونه‌ای که در مقابل اعمال اراده و اجرای اقتدارش مانعی نمی‌پذیرد و از هیچ قدرت دیگری تبعیت نمی‌کند. این قدرت و اقتدار حاصل‌شده بر پایه ملت دارای هویت مشترک شکل‌گرفته که در پهنه جغرافیایی خاصی زیست می‌کنند. حکمرانی با ساختارهای اقتصادی، فرهنگی و سیاسی، اعمال قدرت پیدا کرده و درونداد و برونداد ساختارهای اداره کشور، جریان اطلاعات و دانش راهبردی در حرکت جامعه و ملت را شکل می‌دهد. این اقتدار درونی و هویت ملی و مشترک با گسترش فضای سایبر در حال به چالش کشیده شدن است.

فضای سایبر

فضای سایبر با فناوری جذاب و اغواگر خود، هژمونی را در حال پدید آوردن است که مبتنی بر دانش و اطلاعات درونی، فضای تفوق و برتری نوینی را شکل داده است. فضای سایبر از دیدگاه سخت‌افزاری شبکه‌ای جهانی از رایانه‌های به‌هم‌پیوسته است که از طریق کانال‌های ارتباطی پرسرعت تارعنکبوتی شکل، اطلاعات را جابه‌جا می‌کند. این شبکه که

توسط وزارت دفاع آمریکا شکل گرفته، بستر هیجان‌انگیزی را ایجاد نموده که قابلیت ارائه خدمات متنوع، سریع و جذاب را دارد. ارتباطات سریع قابلیت ارسال پیام؛ ارائه سرویس‌های ارتباطی و تبادل اطلاعات با فرمت‌های مختلف از خدمات متنوع این ابرشبکه است. اینترنت قابلیت‌های ویژه‌ای را برای تجارت الکترونیکی، بازاریابی، تبلیغات و بانکداری الکترونیکی پدید آورده است (موتالا، ۲۰۰۷: ۱۵). خدمات قابل ارائه روی شبکه اینترنت به علت قابلیت ذاتی و فضای قابل رشد شبکه رو به افزایش است. هر حرفه‌ای در حال طرح‌ریزی اطلاع‌رسانی، ارائه خدمات برخط و فروش الکترونیکی بر اساس ویژگی‌های کسب‌وکار خود در شبکه اینترنت است. اینترنت به‌عنوان یکی از جلوه‌های فضای سایبر به‌سرعت در حال گسترش است. سامانه‌های محاسباتی پنهان و توکار[1] در حال قرارگیری در تمام اشیا و محیط‌ها است. هر شیئی که اطراف ما قرار گرفته به‌گونه‌ای قابلیت قراردهی سیستم پردازش و هوشمندسازی را دارد. اینترنتِ اشیا[2] در حال گسترش است و هر چیز و شیئی در حال گرفتن IP [3] و نشانه‌دار شدن است و هویتی جدید و مجازی را در شبکه برای خود شکل داده که قابل شناسایی و تمایز است.

در سطح معنایی فضای سایبر، فضایی اجتماعی شکل‌گرفته با زیرساخت رایانه‌ای است. فضای سایبر برای توصیف هر مفهومی است که در ارتباط با شبکه‌های رایانه‌ای، فناوری اطلاعات، اینترنت و جامعه اطلاعاتی به کار برده شده و افراد و کاربران این فضا تجربه اجتماعی از تعامل، تبادل و اشتراک‌گذاری اطلاعات، کسب‌وکار، بازی و تفریح و بحث‌های گروهی که به‌صورت غیر فیزیکی است به دست می‌آورند. این قابلیت‌ها، بدون هیچ‌گونه حرکت، جابه‌جایی و مصرف انرژی است. با شکل‌گیری فضای سایبر و رشد سریع آن مفاهیم عرصه زندگی نیز به سمت تغییر ماهوی گام برمی‌دارند. همه‌چیز از هویت، فرهنگ، حکمرانی، روابط و تعاملات خصوصی و گروهی تغییر می‌یابد. این جذابیت هیجان‌انگیز برای انسان موجب پیوند زدن این فضا با خیال و وهم شده است. فضای سایبر واقعیت را

1. Embedded
2. The Internet of things
3. Internet Protocol

به درون قلب و نفس انسان‌ها برده که در آنجا به هر شکل که بخواهد تغییر داده و یا از نو می‌سازد، بدون اینکه محدودیت مادی بر آن اثر گذارد. فضای سایبری یکی از ویژگی‌های زندگی مدرن است که در آن افراد و جوامع در سراسر جهان با هم مرتبط شده و معاشرت و همکاری می‌نمایند (وزارت دفاع آمریکا، ۲۰۱۱). توانمندی فضای سایبر در ایجاد یا تغییر ذائقه اجتماعی و ذخیره و بهره‌برداری از اطلاعات و دانش موجود در فضا، قدرت و هژمونی سایبری را شکل داده که جوامع و ملت‌ها را تحت تأثیر خود قرار داده است.

استنباط چالش‌های راهبردی حکمرانی با گسترش فضای سایبر

با بررسی ویژگی‌های فضای سایبر و عمق و گستره نفوذ آن و کارکرد حکمرانی، مجموعه‌ای از چالش‌های راهبردی قابل استنباط است. این چالش‌ها بر اساس شواهد تبیین شده است.

۱. هژمونی آمریکایی در مدیریت و کنترل فضای سایبر

هژمونی آمریکایی در مدیریت و کنترل فضای سایبر به دو علت پیشینه تاریخی در ایجاد و احاطه و رصد فضای سایبر وجود و توسعه یافته است. تبارشناسی اینترنت به‌صورت مستقیم به هژمونی و سلطه آمریکا توسط وزارت دفاع برمی‌گردد و تأثیرات این اصل و نسب در ساختار و محتوای این شبکه جهانی مشهود است (بل، ۱۳۸۹: ۱۶۹). باید به خاطر سپرد که اینترنت یک فناوری خنثی و بی‌طرف نیست؛ بلکه همانند هر فناوری دیگری، پیش‌داوری‌ها و تعصب‌های کسانی که آن را طراحی کرده‌اند (ارتش آمریکا) در این فناوری نهفته است (ابو، ۱۳۸۵: ۱۳۵). این مدل کنترل فضای ارتباطی را کوپف این‌گونه بیان می‌دارد: ایالات‌متحده، هدف محوری سیاست خارجی خود را در عصر ارتباطات باید پیروزی در نبرد بر سر جریان اطلاعات جهانی و تسلط بر امواج قرار دهد؛ همانند حاکمیت بریتانیا بر دریاها (روث کوپف[1]، ۱۹۹۷: ۳۷). از طرفی خصوصیت تمرکززدایی‌شده

1. Rothkopd,David

اینترنت که مورد تحسین بسیار فراوانی قرار می‌گیرد از یک هدف آنارشیستی ناشی نمی‌شود، بلکه از یک استراتژی نظامی بدوی سر برآورده است (ابو، ۱۳۸۵: ۱۷۱).

آیکان که متعلق به سازمان ملل و وزارت بازرگانی ایالات‌متحده آمریکا است، حفظ وضعیت عملیات اینترنت را با مدیریت سلسله‌مراتب نام‌گذاری اینترنتی و تخصیص IP مدیریت می‌کند. آیکان چشم‌انداز خود را یک جهان، یک اینترنت[1] (آیکان، ۲۰۱۵) تعریف نموده است. هر دستگاهی، برای اتصال به اینترنت نیازمند IP معتبری است که توسط سلسله‌مراتب تحت مدیریت آیکان که با مرجع شماره‌های واگذارشده اینترنت[2] (آیانا) اعمال می‌شود، تخصیص داده شده است. این شرکت با مراکز قاره‌ای[3] خود محدوده‌های IP را به شرکت‌های مورد تقاضا واگذار می‌کند.

سازه و کار مدیریت نام‌های اینترنتی عمومی[4] و کشوری[5] نیز آن آیکان انجام‌شده و اعطا و سلب مجوز توسط آیکان صورت می‌گیرد. اطلاعات دامنه‌ها و IPهای مرتبط در سرورهای ریشه[6] نگهداری می‌شود. سیزده سرور نام دامنه که متعلق به ۱۲ سازمان است (از حرف A تا M نام‌گذاری شده است). در ۳۰۰ نقطه از کره زمین با IP های هر یاب[7] پخش‌شده است (سرورهای دارای آدرس‌های هر یاب، سرورهایی با آدرس‌های IP یکسان است که بهترین و نزدیک‌ترین آن‌ها به درخواست پاسخ می‌دهد). عمده این سرورها تحت حاکمیت شرکت‌های آمریکایی است (پایگاه سرورهای ریشه[8]، ۲۰۱۵).

---

1. One World, One Internet
2. Internet Assigned Numbers Authority (IANA)
3. African Network Information Center (AFRINIC), American Registry for Internet Numbers (ARIN), Asia-Pacific Network Information Centre (APNIC), Latin America and Caribbean Network Information Centre (LACNIC), Roseau IP Europeans Network Coordination Centre (RIPE NCC)
4. Com,.Net,.Org…

۵. ازجمله دامنه‌ی ir. که مجوز آن را پژوهشگاه فیزیک و ریاضی گرفته است.

6. Root Servers, http://www.root-servers.org
7. any cast
8. root-servers.org

ایالات متحده با ایجاد و راه‌اندازی آژانس امنیت ملی[1] در سال ۱۹۴۸ میلادی بـه سـمت تسلط و کنترل فضای ارتباطات الکترومغناطیس گام برداشت. «سین گـالانگر» در یادداشـتی در پایگاه اطلاع‌رسانی «آرتچنیکا» می‌نویسد: آژانس امنیت ملی آمریکا در «برنامه پریسـم[2]»، در حال گردآوری داده‌ها و یافتن ارتباطات بین آن‌ها است. آژانس امنیـت ملـی آمریکـا بـا آنالیز داده‌های عظیم به دنبال استثنائات است. با دسترسی بـه ایـن اسـتثنائات، اف. بـی.آی[3] شروع به تعمیق و یافتن ابعاد مسئله می‌کند . واقعیت آن است که آژانس امنیت ملی آمریکـا قابلیت گردآوری داده‌های شبکه‌های تلفنی و اینترنتی را مدت‌هاست که کسـب کـرده و بـا همکاری شرکت‌های بزرگ نرم‌افـزاری بـالأخص دو شـرکت «گوگـل» و «یـاهو» در حـال پالایش و آنالیز داده‌های عظیم و متنوع اینترنتی اسـت. «مـارک هرشـبرگ» در مصـاحبه بـا پایگاه اطلاع‌رسانی «ساینتیفیک آمریکن» تصریح می‌کند که آژانـس امنیـت ملـی آمریکـا در پروژه داده عظیم خود به دنبال «سیگنال‌های خاص»[4] می‌گردد. به این ترتیب، سیگنال‌هـایی در رفتار [سایبری] افراد وجود دارد که ردیابی و طبقه‌بندی می‌شـود. بنـا بـر اطلاعـاتی کـه ادوارد اسنودن در اختیار رسانه‌ها قرار داده است، شرکت مایکروسافت که ویندوزهایش در اکثر رایانه‌ها مورد استفاده قرار می‌گیرند نیز از سال ۲۰۰۷ میلادی اطلاعات کاربران خود را در اختیار آژانس امنیت ملی آمریکا قرار داده است. این اطلاعات می‌تواند به آژانـس امنیـت ملی آمریکا کمک کند تا حتی از سد پروتکل امن[5] نیز بگذرد.

آژانس امنیت ملی آمریکا اکنون این امکان را یافتـه اسـت تـا بـا جمـع‌آوری اطلاعـات و پست‌های شهروندان کشورهای مختلف و آنالیز آن‌ها، رویکردهای افکار عمـومی و الگوهـای مختلف فکری بخش‌های مختلف جوامع انسانی را شناسایی کند. آمریکایی‌هـا پـس از آنـالیز

1. National Security Agency (NSA)
2. PRISM program
3. FBA (Federal Bureau of Investigation)

٤. به‌طور مثال، اگر به نوجوانانی که قصد خودکشی دارند دقت شود، پیش از این اقدام مدتی را در خصوص آن فکـر می‌کنند. نشانه‌هایی در آن‌ها وجود دارد که افراد حرفه‌ای برای تشخیص آن‌ها آموزش دیده‌اند. مثلاً ممکن اسـت پـیش از خودکشی با دوستان خود خداحافظی کنند.

5. Secure Sockets layer (SSL)

نمودار هم می‌توانند گروه‌های انسانی مخالف خود را شناسایی کنند و آن‌ها را تحت پایش قرار دهند و هم می توانند نیروهای خاص را در کشورهای مختلف شناسایی کرده و روی آن‌ها سرمایه‌گذاری کنند. از سوی دیگر، با جریان‌سازی در فضای سایبر می‌توانند، رویکردهایی را به نفع گروه‌های سیاسی خاصی تغییر دهند و اجتماعاتی را برای تأثیرگذاری بر روندهای جامعه تغییر دهند. این جریان‌سازی در شبکه‌های اجتماعی کارایی خود را به نحوی ملموس‌تر نشان می‌دهد. آنالیز داده‌های عظیم توانایی افکارسازی را در شبکه‌های اجتماعی و رسانه‌های جمعی به‌صورت هدفمند، با کاهش ضریب اشتباه و نتایج ناخواسته، شکل داده است. این تبارشناسی، مدیریت ساختار و کنترل محتوا به‌وضوح هژمونی و سلطه آمریکا را در اینترنت و فضای سایبر به تصویر کشیده است. هرچه فضای سایبر با این ساختار گسترش پیدا کند، بیشتر و بیشتر به هژمونی آمریکایی کمک خواهد کرد.

۲) شناسایی و نظارت فراحاکمیتی بر توانمندی‌های اقتدارافزای جامعه

جغرافیای کشور دربردارنده سرمایه‌های انسانی، فیزیکی، اقتصادی و سایبری است. این سرمایه‌ها که دارای طبقه‌بندی‌های آشکار یا پنهان است و در پیکره کشور پراکنده شده است. مراکز نظامی، مراکز تجمع سرمایه‌های انسانی مختلف، محل قرارگیری زیرساخت‌های فنی، سایبری و اقتصادی ازجمله این سرمایه‌ها در بستر جغرافیا است. عناصر اقتدارافزای کشور که با همگرایی درونی ابعاد انسانی، سیاسی، اقتصادی، فناورانه شکل و استحکام می‌یابد، با گسترش فضای سایبر این عوامل با چالش‌های نوین و پیچیده‌ای روبه‌رو خواهند شد. شناسایی، ره‌گیری و انهدام سرمایه‌های ملی در این عصر برای کشورهای مسلط بر فضای فنّاورانه ساده‌تر خواهد شد. گسترش اینترنت اشیا که نمادی از هژمونی گسترده سایبری است، موجب کاهش حفاظت از سرمایه‌های ملی خواهد شد، کیان‌خواه و کریمی قهرودی (۱۳۹٤ ه.ش) معتقد هستند که این کاهش اقتدار در چند جنبه مختلف خواهد بود:

(۱) شناسایی نقاط حیاتی و حساس کشور با رصد و پایش سرمایه‌های انسانی، سرمایه‌های فیزیکیِ سایبری‌شده؛

(۲) شناسایی سرمایه‌های انسانی حیاتی و حساس بر اساس میزان مراجعه به نقاط حیاتی و حساس؛

(۳) شناسایی زیرساخت‌های حیاتی و حساس و مهم سایبری؛

(٤) در معرض تهدید قرار گرفتن سرمایه‌های ملی با دست‌کاری اشیاء سایبری برای آسیب رساندن و انفجار.

گسترش فضای سایبر موجب کاهش حفاظت از سرمایه‌های انسانی، سرمایه‌های فیزیکی و اقتصادی و کاهش حفاظت از سرمایه‌های سایبری خواهد شد. دیگر نیازی به به‌کارگیری گروه‌های ویژه‌ای برای عملیات تروریستی نیست، بلکه فناوری هم قابلیت رصد و نظارت را پدید می‌آورد و هم قابلیت تخریب و انفجار را به‌صورت بالقوه خواهد داشت. در حقیقت عناصر اقتدارآفرین در معرض شناسایی، نظارت و تغییر بوده و به‌تبع آن دیگر قدرت درون‌زا و پایدار تداوم نخواهد یافت.

۳) تهدیدات و تهاجمات سایبری

تهاجمات سایبری با تنوع، انعطاف‌پذیری و خسارت‌های قابل تأمل، حاکمیت ملی و اقتدار کشور را تهدید می‌کند. تهاجمات سایبری طیف گسترده‌ای از هکتیویسم[1]، جاسوسی سایبری[2] و جرائم سایبری[3] تا سایبر تروریسم[4] و جنگ سایبری[5] را در بردارد. هکتیویسم صورتی از فعالیت‌ها برای تغییرات اجتماعی است که تحت شبکه‌های رایانه‌ای شکل می‌گیرد. هکتیویسم فعالیتی سیاسی است که از فصل مشترک اعتراضات عمومی (تظاهرات، اعتصاب و فعالیت‌های مشابه در فضای عمومی) و ارتباطات رایانه‌ای[6] شکل گرفته است(نایر، ۲۰۱۰: ۱۰۲). سایبر تروریسم، فعالیتی است که گروهی از مردم با استفاده از رایانه برای خرابکاری و از بین بردن زیرساخت فیزیکی و مالی یا الکترونیک یک ملت یا گروهی

1. Hactivism
2. Cyber intelligence
3. Cybercrime
4. Cyber terrorism
5. Cyber warfare
6. Computer-mediated communication (CMC)

از ملت برای مقاصد سیاسی انجام می‌شود (همان: ۱۰۳). مهم‌ترین مسئله در تروریسم سایبری، هدف قرار گرفتن زیرساخت‌های اساسی کشورهاست که امنیت آن‌ها را به خطر انداخته و در کوتاه‌مدت تولید بحران می‌کند؛ زیرا زیرساخت‌هایی؛ نظیر انرژی، آب، برق، گاز و صنعت وابستگی زیادی به فناوری اطلاعات و شبکه اینترنت دارند؛ تروریسم سایبری فرصت‌های جدیدی را برای تروریسم‌ها فراهم کرده که برخی از ویژگی‌های آن، هدف قرار دادن تعداد بیشتری از مردم، استفاده از گروه‌های رایانه‌ای ناشناخته در سطح بین‌المللی، نداشتن محدودیت جغرافیایی، پنهان ماندن هویت، تبلیغ و عضوگیری بین‌المللی و گسترش دامنه تروریسم به مسائل مالی، بانکی، اقتصادی و خدمات شهری است (حافظ‌نیا، ۱۳۹۰: ۲۶۷-۲۶۸). جنگ سایبری، بالاترین سطح و پیچیده‌ترین نوع از تهاجم سایبری است که علیه منافع ملی سایبری کشورها انجام‌شده و شدیدترین پیامدها را به همراه خواهد داشت. ویژگی این نوع از تهاجم سایبری، تلقی جنگ علیه منافع ملی توسط دولت‌ها است (سازمان پدافند غیرعامل، ۱۳۹۳). تهاجمات سایبری، چالش ملموس حاکمیت ملی در فضای سایبر است. هرچه زیرساخت‌های حیاتی کشور (برق، آب، گاز، کشاورزی و...) بیشتر به سمت سایبری شدن حرکت کند، تهاجمات گسترده‌تر و همراه با خسارات فلج‌کننده و جبران‌ناپذیر برای کشور در سطح فیزیکی – سایبری شکل خواهد گرفت. این تهاجمات قابلیت مختل نمودن اقتصاد و ثبات سیاسی – امنیتی کشور را داشته و حتی توانمندی فروپاشی و ناکارآمدی تمام ارکان حاکمیتی کشور را دارد.

٤) مهندسی و مدیریت فرهنگی فراملی

با شروع تعاملات کاربر با فضای سایبر، پروسه بی‌وقفه آپلود - دانلود[1] با موضوعات متنوع و مرتبط با داده‌های جغرافیایی طیف گسترده‌ای از داده‌ها را فراهم آورده که تجزیه‌وتحلیل آن‌ها ایجادکننده قدرتی سایبری در هدایت و مدیریت جوامع

۱. هر رفتاری در ارتباط با شبکه در پروسه آپلود – دانلود قرار دارد. به این معنی که هر ارتباطی با شبکه از قبیل وب‌گردی، جستجو در اینترنت، گشت و گذار در رسانه‌های اجتماعی در حال ارسال و دریافت داده است.

است. توانمندی‌ای که داده‌کاوی، هوش مصنوعی و پردازش‌های بـرخط رویـدادههـای عظیم تجمیع‌شده از رفتارهای سایبری انسان‌هـا در جوامـع و جغرافیاهـای مختلـف را ایجاد می‌کند، الگوهایی را برای تغییر هویت، ارزش‌ها و ذائقه‌های جوامع برای دستیابی به اهداف فرهنگی، اقتصادی و سیاسی هموار نموده و قدرت جدیدی را شکل می‌دهد. این قدرت سایبری با آنـالیز داده‌هـای مـرتبط بـا طـرز تفکـر، مسـائل و دغدغـه‌هـای اجتماعی، سیاسی و اقتصادی بر اساس موقعیت جغرافیایی و مناسبات قومیتی، توانـایی تغییر ارزش‌ها، سبک زندگی، اعتقادات، انگیزه‌هـای دینـی، سیاسـی و اقتصـادی و بـه معنای دقیق‌تر فرهنگ؛ شامل منش، بینش و کنش جامعه را بـا فضـای سـایبر دارد. بـر اساس دلایل زیر هدایت و مدیریت فرهنگی جامعه از اختیار حاکمیت ملی خارج شده و فراملی و فراحاکمیتی شده است. اولین دلیل شکل‌گیـری ایـن وضـعیت در هژمـونی آمریکا که در ساختار و محتوای فضای سایبر ریشه دوانـده و در آیکـان و NSA نهفتـه است، قابل ردیابی است که در بخش چالش‌های حاکمیت ملی توضیح داده شد. دومین دلیل برای شکل‌گیـری مهندسـی و مـدیریت فراملـی و فراحـاکمیتی فرهنگـی جامعـه، شبکه‌سازی گسترده توسط رسانه‌های اجتماعی نوین است. رسانه‌های اجتماعی سایبری تحت اشراف،حمایت و نظارت قدرت‌های استعماری به‌صورت گسترده در حـال رشـد است. این رشد گسترده که به همراه خود انواع داده‌های مرتبط با رفتار سایبری انسان‌ها را به ارمغان می‌آورد، با خوشه‌بندی و دسته‌بندی گروه‌های مرجع و کشف ذائقـه‌هـا و توان کمی و کیفی آن‌ها، قابلیت مهندسی و مدیریت رفتـار و هویـت جوامـع و امکـان ایجاد ناپایداری و شکل‌دهی به انقلاب‌های سـایبری را دارد. در حقیقـت بـا گسـترش بسترهای سخت و نرم فضای سایبر، صـاحبان فنـاوری (اعـم از هژمـونی آمریکـایی و اَبَرسرویس‌های جهانی) و حاکمان بلامنازع این فضا شده و بر اساس سطح و گستردگی نفوذ خود با مهندسی و مدیریت فرهنگ و فرهنگی، بهـره‌کشـی و بـرده‌داری مـدرن را شکل داده‌اند.

۵) پذیرش الگوی رفتاری و سبک زندگی فراملی

با انعطاف‌پذیری سایبری در مکان، زمان و تعامل عوامل هویت‌ساز فردی و اجتماعی در حال میل به خارج از مرزها و تعلقات فرهنگی – اجتماعی است. جمله مشکل داره کاستلز معتقد است، این عصر هرگز موضوعی فناورانه نبوده، بلکه دگرگونی اجتماعی و فرآیند تغییر آن که فناوری در آن یک عامل جدایی‌ناپذیر از گرایش‌های اجتماعی، اقتصادی، فرهنگی و سیاسی است، نقطه عطف این عصر به شمار می‌رود (بل، ۱۳۹۰: ۱۱۷). به‌واسطه گسترش فناوری اطلاعات و ارتباطات، فضایی به وجود آمده است که پایه‌های تشکیل‌دهنده ملت مانند فرهنگ و هویت ملی را به‌تدریج متحول می‌کند (حافظ‌نیا، ۱۳۹۰: ۱۲۵). این هویت در بستری شبکه‌شده، رشد و قوام می‌یابد. سایبری شدن انسان و بازتعریف او در فضای سایبر، انسان فنّاورانه‌ای را شکل می‌دهد که مزین و وابسته به فناوری سایبر خواهد بود. گجت‌های پوشیدنی، موجب بروز و ظهور انسان در فضایی به غیر از فضای طبیعی شده است. این ظهور سایبری به علت وجود مجموعه فناوری‌های پوشیدنی و نظارتی بر رفتار و فکر انسان سایبری‌شده نظارت و کنترل دارد. با شکل‌گیری داده‌های عظیم در حیطه‌های رفتاری و گسترش تکنیک‌های داده‌کاوی بر خط، مجموعه رفتار و سکنات این انسان را پیش‌بینی‌پذیر نموده است. انسان شکل‌یافته از بدن، حواس و تفکر تحت تأثیر این فضای عالم‌گونه به انسانی سایبری بدل شده که احوالات خاص خود را پیدا کرده است.

قابلیت‌های فضای سایبر حس تحرک بی‌سابقه‌ای را به درون فضای اجتماعی تزریق کرده است؛ حس تحرک بدان معناست که در این فضا امکان تغییر طبقه، نژاد و جنسیت برای افراد وجود دارد؛ فرد در هر لحظه آنی می‌تواند جنس، نژاد و طبقه اجتماعی خود را پنهان سازد و با ویژگی‌های کاذب جنسیتی و نژادی، هویتی جدید برای خود تعریف کند و بر اساس آن به تعامل با هویت‌های واقعی یا سایبری دیگر بپردازد. در این چارچوب، گذر زمان و قرار گرفتن فرد به دفعات متعدد در این فضا و تعامل با هویت سایبری موجب می‌شود تا هویت مجازی در فرد نهادینه گردد و فرد آن را به‌عنوان یکی از هویت‌های واقعی خود همچون هویت‌های خود جهان واقعی بپندارد؛ فضای سایبر به شکل‌گیری

هویت‌های جدید در قالب شبکه‌های اجتماعی کمک کرده است که ارتباط چندانی با هویت‌های ریشه‌ای دنیای واقعی آن‌ها ندارد؛ در هویت دیجیتالی دیگر تنها سرزمین، زبان بومی و محلی، کشور، فرهنگ ملی و در حوزه موضوعات مختلف افراد را در اجتماعات سایبری تعیین نمی‌کند، بلکه منافع مقطعی، محدود و در حوزه موضوعات مختلف افراد را دور هم جمع می‌کند و هویت آن‌ها را می‌سازد (حافظ‌نیا، ۱۳۹۰: ۱۲٦-۱۳٦). به این ترتیب با نفوذ سایبر به همه ارکان زندگی با سرویس‌هایی که سبک زندگی‌ای متفاوت با سبک زندگی شکل‌گرفته از فرهنگ و آداب‌ورسوم جامعه در طول سال‌ها و قرن‌ها را ترویج می‌کند، هویت و رفتار رسوخ‌یافته جدیدی را شکل می‌دهد که به‌جای ریشه داشتن در فضای جغرافیایی پیرامونی، در فضایی خارج از عناصر فرهنگی متعلق به جامعه خود ریشه دارد. در حقیقت کاربر که به انسان معلق در فضای سایبر بدل شده و با رویت عناصر مرتبط با سبک زندگی فراملی که با جذابیت فناورانه مزین شده است، خود را در آن فضا پنداشته و هویت جدیدی را برای خود شکل می‌دهد که در تناقض با هویت فردی و اجتماعی جامعه خود است.

٦) فرهنگ منحط و اباحه‌گر

در جامعه پیش از مدرن، بنیان شخصیت آدمی بر دو ساحت تن و جان استوار بود، روح تفکر بر اعتبار شخصیت انسان می‌افزود، اینک روزگاری فرارسیده که واقعیت ذاتی و ماهوی انسان در قبال شیء‌ت و سودمندی اقتصادی او از یاد رفته و فناوری انسان را به بردگی سوق داده است (لاکوست، ۱۳۷۵: ۸۳). این عقلانیت ابزاری که تجسم عینی آن فناوری است، در برهه‌ای از زمان به آزادی انسان از سیطره کار سخت و طاقت‌فرسا و چیرگی بر طبیعت انجامید ولی امروزه باعث شیء‌گونگی انسان شده و به ناظری بر عملکرد آدمی بدل گشته است و آفریده در مقابل آفریننده قد علم کرده است (رحیم‌پور، ۱۳۸۳: ٦۳). ایجاد انگیزه کاذب برای ادامه زندگی و بی‌هدفی که ثمره دوری از خدا که هدف اصلی خلقت انسان

است[۱] و خالی نمودن زندگی از مخلوق بودن چه به‌صورت نمایان و یا چه به‌صورت پنهان‌شده در توهمات و خیالات باطلی که ظاهری قدسی دارد و از حقیقت به دور است، موجب سوق دادن انسان به نهیلیسم و پوچ‌گرایی شده است. این انسان مدرن هویتش را از تمایلات غریزی و لذت‌جویانه که غیر قابل مقاومت و اجتناب‌ناپذیر است، اخذ نموده و از هویت آخرت‌گرای خود غافل شده است. انسان دیگر به خالق و مسئولیت خود در مقابل او توجه ندارد و به بی‌هویتی و فراموشی خود دچار می‌شود، «وَ لَا تَكُونُواْ كَالَّذِينَ نَسُواْ اللَّهَ فَأَنسَئهُمْ أَنفُسَهُمْ أُوْلَئكَ هُمُ الْفَاسِقُون؛ و همچون کسانی نباشید که خدا را فراموش کردند و خدا نیز آن‌ها را به خودفراموشی گرفتار کرد، آن‌ها فاسق‌اند»(حشر/ ۱۹). ماشینی شدن زندگی انسان، غفلت انسان از مسئولیت دنیوی و اخروی و تغییر سبک زندگی جامعه به سبک زندگی غربی، ثمره حضور گسترده و بدون برنامه اینترنت اشیاء در زندگی خواهد بود و انسان انقلابی را تحت برنامه خود به سمت سبک زندگی غربی سوق خواهد داد.

فضای سایبر با این شرایط موتور محرک جهانی شدن و نظم نوین جهانی غرب و آمریکایی شده است. مقام معظم رهبری می‌فرمایند: «گفتمان پیوستن به نظم نوین جهانی؛ یعنی سیاهی‌لشکر آمریکا شدن! این جهانی‌شدن، اسمش جهانی‌شدن است؛ اما باطنش آمریکایی شدن است. معنایش این است که ملت ایران علی‌رغم مجاهدت‌هایی که کرده، علی‌رغم پرچم‌هایی که بر قلّه‌های پیروزی کوبیده، علی‌رغم بیداری عظیمی که در ملت‌های مسلمان به وجود آورده، باید دوباره مثل دوران قبل از انقلاب، سیاهی‌لشکر و عمله و ابزار تأمین منافع آمریکایی‌ها شود. هدف به‌صورت لخت و پوست‌کنده، جز این چیز دیگری نیست؛ اما می‌خواهند در زیر نام‌های زیبای جهانی‌شدن و تحوّل و پیشرفت – این هدف را پنهان کنند» (مقام معظم رهبری، ۱۳۷۹/۱۲/۰۹). تعبیر دیگر از نظم نوین جهانی جاهلیت مدرن است که در پی کشاندن انسان به وضعیت منحط جاهلیت کهن است. مقام معظم رهبری می‌فرمایند: «استعمار و تحقیر ملّت‌ها و غارت منابع مالی ملّت‌ها و فاسد کردن منابع انسانی ملّت ها، ناشی از آن حاکمیت جاهلیت است. وقتی جاهلیت حاکم شد، شما می بینید

---

۱. «وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ» (ذاریات/۵۶)

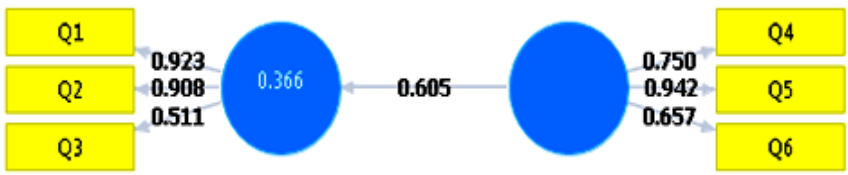
ملت‌های بسیاری در سطح جهان در زیر چکمه استعمار لِه می‌شوند، منابع آن‌ها غارت می‌شود، خودِ آن‌ها تحقیر می‌شوند، سال‌ها عقب می‌افتند، ملت‌های استعمارزده، بعضی ده‌ها سال عقب افتادند، بعضی قرن‌ها عقب افتادند» (امام خامنه‌ای، ۱۳۹۵/۰۲/۱۶). فضای سایبر بستر نرم وقوع حاکمیت جاهلیت مدرن و امپریالیسم فرهنگی غرب شده است. حاکمیت شهوت و غضب به‌وضوح در لایه‌های فضای سایبر قابل شهود است.

تأیید یافته‌های پژوهش

داده‌های حاصل از اخذ پرسشنامه از ۳۰ نفر از متخصصین امنیت ملی جمع‌آوری‌شده و در نرم‌افزار SmartPLS، مدل تحلیل اولیه برای محاسبه بارهای عاملی با ۵۰۰ نمونه اجرا شده است. بارهای عاملی شاخص‌های بیش از ۰.٤ است و درنتیجه شاخص‌های مورد تأیید است (شکل ۲ و جدول ۱).

جدول ۱. چالش‌های راهبردی حکمرانی با گسترش فضای سایبر

چالش‌های راهبردی حکمرانی با گسترش فضای سایبر	
Q1	هژمونی آمریکایی در مدیریت و کنترل فضای سایبر
Q2	شناسایی و نظارت فراحاکمیتی بر توانمندی‌های اقتدارافزای جامعه
Q3	تهدیدات و تهاجمات سایبری
Q4	پذیرش الگوی رفتاری و سبک زندگی فراملی
Q5	مدیریت و مهندسی فرهنگی فراملی
Q6	فرهنگ منحط و اباحه‌گر



شکل ۱. مدل تحقیق

در جدول زیر گزارش روایی و پایایی مدل قرار گرفته است.

جدول ۲. گزارش روایی و پایایی

	AVE	Composite Reliability	Cronbachs Alpha
چالش‌های راهبردی حکمرانی	۰/۶۳۶۵	۰/۸۳۵	۰/۷۱۸۵

همان‌گونه که در جدول ۱ مشاهده می‌شود، ضریب آلفای کرونباخ همه ابعاد بالاتر از ۰/۷ و قابل قبول است و معیار پایایی ترکیبی[1] بالای ۰.۷ که از پایایی مدل روایت می‌کند. برای روایی مدل فورنل و لدرکر (۱۹۸۱ م) مقدار مناسب برای AVE[2] را ۵٪ به بالا معرفی کرده‌اند که بر اساس نتایج تمامی مقادیر عددی بالاتر از ۰/۵ است که روایی همگرای مناسب مدل را نشان می‌دهد. با توجه به نتایج (شکل ۳) مدل نهایی و مورد تأیید قرار گرفته است.

نتیجه‌گیری

فضای سایبر با سرعت بالایی در حال پیش رفتن است. سرویس‌های مکان‌محور در حال رصد توانمندی‌های اقتدارافزای جامعه در پوشش جذابیت فناوری است. شبکه‌های اجتماعی به ابرگراف تعاملات و روابط جامعه دست پیدا کرده‌اند و کسی دیگر از رصد پنهان نیست. محتواهای نادقیق و مغرضانه به مراجع کاذب معتبرشده در فضای سایبر تبدیل شده است. موتورهای جستجو در حال جهت‌دهی به فکر و اندیشه کاربر و مهندسی و مدیریت جامعه هستند. مرورگرها همه تعاملات و ارتباطات کاربران و جوامع را رصد می‌کنند و سرویس‌های ابری در حال متمرکز ساختن داده‌ها هستند و اینترنت اشیاء به رصد همه رفتارها می‌پردازد و این مجموعه رصدها و کنترل‌ها در شبکه‌ای به وسعت جهان در حال تبدیل شدن به تابلوی بزرگی است که کوچک‌ترین تحرکات در آن قابل رصد، پایش و اشراف است.

جنگ نرم و ناتوی فرهنگی غرب با بستر فضای سایبر ملموس شده است. با این حال برخی این جنگ همه‌جانبه را در پوشش فناوری‌های جذاب و فریبنده سایبری نمی‌بینند.

1. Composite Reliability
2. Average variance extracted (AVE)

فضای سایبر با قدرت مهندسی افکار و تغییر ذائقه‌ها و توأمانی با تغییر سبک زندگی جامعه اسلامی با جنگ نرم و شبیخون فرهنگی به دنبال سلطه و تغییر جامعه اسلامی است.

به خدمت گرفتن هر پدیده نیازمند فهم دقیق آن است و توجه بـه مصـالح و مفاسـد آن دارد. درجه پیچیدگی فهم پدیده‌ها بر اساس کارایی و وسعت آثار آن متفاوت است. فضـای سایبر در کنار تحولات مطلوب و پرشتاب آن، دارای مفاسد است کـه موجـب چـالش‌هـای کلیدی برای حکمرانی کشور شده است.

این تحقیق به اکتشاف چالش‌های راهبردی حکمرانی با گسترش فضای سایبر پرداخته است.

(۱) هژمونی آمریکایی در مدیریت و کنترل فضای سایبر،

(۲) شناسایی و نظارت فراحاکمیتی بر توانمندی‌های اقتدارافزای جامعه،

(۳) تهدیدات و تهاجمات سایبری،

(٤) پذیرش الگوی رفتاری و سبک زندگی فراملی و فرافرهنگی،

(۵) مهندسی و مدیریت فرهنگی فراملی،

(٦) فرهنگ منحط و اباحه‌گر، چالش‌های راهبردی گسترش فضای سایبر است.

توجه به این چالش‌های راهبردی، موجب مقابله فعالانه بـا ایـن چـالش‌هـا شـده و قابلیـت آینده‌نگاری هنجاری فضای سایبر برای مقابله با این موانع را فراهم می‌آورد. برای غلبـه بـر ایـن چالش‌ها چارچوبی برای ترسیم حکمرانی نوین نیازمند ترسیم است. فهم و حذف چـالش‌هـای راهبری راه را به سمت ترسیم اهداف حکمرانی مطلوب فضای سایبر همکار می‌کنـد. راه‌انـدازی شبکه ملی اطلاعات، رگولاتوری و تنظیم قوانین بومی و هم‌راستا را ارتباطات سـایبری جهـانی، ساخت تجهیزات بومی برای ستون فقرات و هسته شبکه بـومی، مهندسـی فرهنـگ و مهندسـی فرهنگی ناظر به فضای سایبر و طراحی هنجارهای سایبر مبتنی بـر الگـوی اسـلامی – ایرانـی و پیشرفت و زنجیره ارزش در دستیابی تعالی روحی و جسمی و...

(٦) استقرار نظامات بازار مجازی اسلامی مبتنی بر نظام ارزشی اسلام و اقتصاد مقـاومتی از راهکارهای مهار چالش‌های راهبردی حکمرانی با گسترش فضای سایبر اسـت. عـدم توجـه بـه این چالش‌های راهبردی منجر به وابسته و سلطه کفار بر نظام اسلامی خواهد شد.

فهرست منابع ومآخذ

الف) منابع فارسی

۱. قرآن کریم، ترجمه آیت‌الله مکارم شیرازی.
۲. امام خامنه‌ای، پایگاه حفظ و نشر آثار http://farsi.khamenei.ir
۳. اِبو، بوسا (۱۳۸۵)، امپریالیسم سایبر، ترجمه دکتر پرویز علوی، انتشارات ثانیه.
٤. انوری، حسن (۱۳۸۲). فرهنگ فشرده سخن (۱)، تهران، نشر سخن.
۵. بل دیوید، (۱۳۸۹) درآمدی بر فرهنگ سایبر (۲۰۰۱)، ترجمه مسعود کوثری، حسین حسنی، چاپ اول، انتشارات جامعه شناسان.
٦. بل دیوید (۱۳۹۰)، نظریه‌پردازان فرهنگ سایبری ۲۰۰۷، ترجمه مهدی شفیعیان، چاپ اول، انتشارات دانشگاه امام صادق (علیه‌السلام).
۷. بلدسو، رابرت و بوسچک، بولسلاو (۱۳۷۵)، فرهنگ حقوق بین‌الملل، ترجمه علیرضا پارسا، تهران، قومس.
۸. سازمان پدافند غیرعامل (۱۳۹۳)، سند راهبردی سازمان پدافند غیرعامل.
۹. داوری، علی؛ رضازاده، آرش (۱۳۹۲)، مدل‌سازی معادلات ساختاری با نرم‌افزارPLS ، تهران، انتشارات جهاد دانشگاهی.
۱۰. روث کوپف، دیوید (۱۹۹۷)، امپریالیسم فرهنگی در پاریس؟، نشریه فارین پالیسی، ۱۰۷ صفحه ۳۸-۵۳. دیده‌شده در امپریالیسم سایبر نوشته بوسا ابو.
۱۱. قدسی، امیر (۱۳۹۲)، تأثیر فضای مجازی بر امنیت ملی ج.ا.ایران و ارائه راهبرد (با تأکید بر ایفای نقش سرمایه اجتماعی)، مجله راهبرد دفاعی، زمستان ۱۳۹۲، دوره ۱۱، شماره ٤٤ .
۱۲. کیان‌خواه احسان؛ کریمی‌قهرودی، محمدرضا (۱۳۹٤)، چالش‌آفرینی اینترنت اشیاء بر ارکان امنیت ملی کشور، فصلنامه امنیت ملی، دانشگاه عالی دفاع ملی، شماره ۱٦، سال چهارم.
۱۳. لاکوست، ژان (۱۳۷۵)، فلسفه در قرن بیستم، ترجمه رضا داوری اردکانی، تهران، انتشارات سمت. دیده‌شده در کتاب «نقدی بر مبانی معرفت‌شناسی اومانیستی» نوشته مریم صانع پور (۱۳۸۸)، تهران، انتشارات کانون اندیشه جوان.
۱٤. حافظ نیا، محمدرضا و دیگران (۱۳۸۲)، تحلیل مبانی جغرافیایی قدرت ملی جمهوری اسلامی ایران، نشریه علوم جغرافیایی دانشگاه تربیت‌معلم.
۱۵. حافظ‌نیا محمدرضا (۱۳۹۰)، جغرافیای سیاسی فضای مجازی، انتشارات سمت.
۱٦. خلیلی‌پور رکن‌آبادی، علی؛ نورعلی‌وند، یاسر (۱۳۹۱)، تهدیدات سایبری و تأثیر آن بر امنیت ملی، فصلنامه امنیت ملی، تابستان.

ب) منابع انگلیسی

1. Buckley J. Ed. (2006). The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, New York, 2006.
2. DOD, (2011), Department Of Defense Strategy For Operating In Cyberspace, http://www.defence.gov.
3. Evans Dave (2011). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything Cisco, April 2011,
4. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
5. Fornell, C. & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18 (1): 39-50.
6. ICANN (2015). https://www.icann.org/en/system/files/files/ecosystem-06feb13-en.pdf
7. Information Society, European Commission (2012). "Glossary and Acronyms," URL: http://ec.europa.eu /information_ society/tl/help/glossary/index_en.htm, Visited: 2012-01-12.
8. Mutula,Stephen M. and Wamukoya Justus M. (2007) Web Information Management, UK: Cahndos Publication
9. NayarPramod (2010). An Introduction new media and cybercultures, Wily – BLACKWELL
10. Root Server (2015). http://root-servers.org.