

نقش کاربرست دانش سایبرنتیک در ارتقای کیفیت حکمرانی (۱): از حکمرانی بر فضای سایبر تا حکمرانی با فضای سایبر



لله الحمد لله الرحمن الرحيم

تاریخ انتشار: ۱۴۰۴/۰۹/۱۳

شماره مسلسل: ۲۱۱۶۴



مرکز پژوهش‌های
مجلس شورای اسلامی

عنوان گزارش:

نقش کاربر بست دانش سایبرنتیک در ارتقای کیفیت حکمرانی (۱):
از حکمرانی بر فضای سایبر تا حکمرانی با فضای سایبر

نوع گزارش: طرح / لایحه □ راهبردی ■ نظارتی □ پیش‌نویس قانونی □

نام دفتر:

دفتر مطالعات بنیادین حکمرانی (گروه سیاست‌پژوهی و آزمایشگاه حکمرانی)

تهیه و تدوین:

کاظم فولادی قلعه (عضو هیئت علمی دانشگاه تهران)، فاطمه دیانت (گروه سیاست‌پژوهی و آزمایشگاه حکمرانی)

مدیر مطالعه:

حسین بابایی مجرد (عضو هیئت علمی پژوهشگاه فرهنگ و اندیشه اسلامی)

ناظر علمی:

مهدی عبدالحمید

اظهار نظر کننده:

ابوالقاسم رجبی (گروه مخابرات و فناوری اطلاعات)

اظهار نظر کننده خارج از مرکز:

رحیم خانی‌زاد (عضو هیئت علمی دانشگاه علم و صنعت)

گرافیک و صفحه‌آرایی:

ستایش افشاریان

ویراستار ادبی:

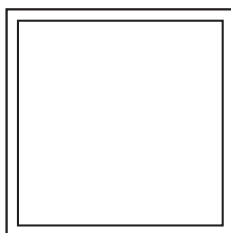
اکرم وحدانی‌فر

واژه‌های کلیدی:

۱. اطلاعات
۲. ارتباطات
۳. محاسبات
۴. دانش سایبرنتیک
۵. فضای سایبر

تاریخ شروع مطالعه:

۱۴۰۳/۰۵/۱۵



فهرست مطالب

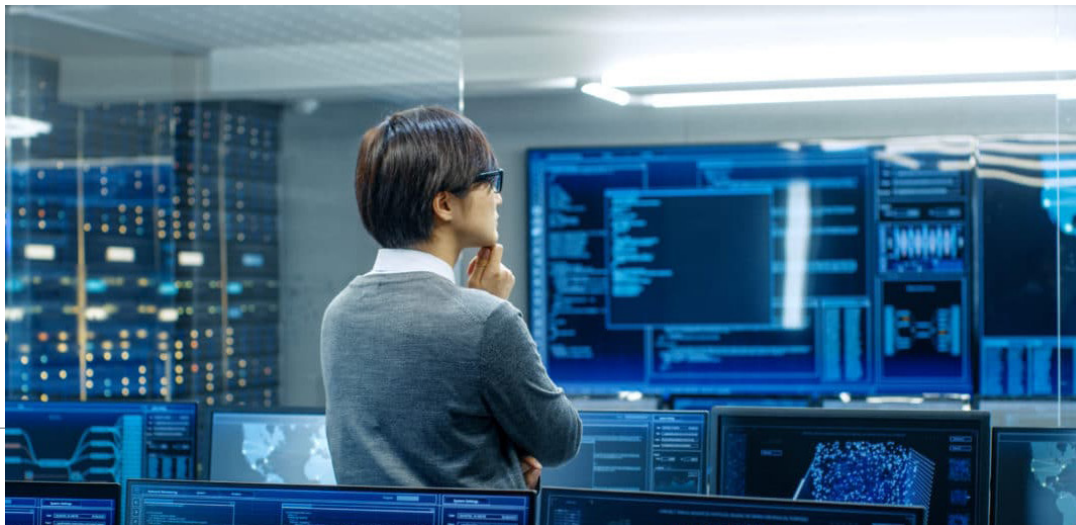
چکیده.....	۶
خلاصه مدیریتی.....	۷
۱. مقدمه.....	۹
۲. پیشینه پژوهش.....	۱۰
۳. دانش سایبرنتیک و حکمرانی.....	۱۴
۴. فضای سایبر.....	۱۸
۵. جایگاه سیستم‌های سایبرنتیکی در سطوح پیچیدگی سیستم‌ها.....	۱۹
۶. قدرت سایبری و امنیت فضای سایبر.....	۲۲
۷. حدود دانش سایبرنتیک.....	۲۴
۸. تعاملات حکمرانی و فضای سایبر.....	۲۶
۹. جمع‌بندی و نتیجه‌گیری.....	۲۸
۱۰. پیوست.....	۳۶
منابع و مأخذ.....	۴۰

فهرست جداول

جدول ۱. پیشنهاد توصیه سیاستی.....	۳۲
جدول ۲. پیوست. اهم قوانین و مقررات مرتبط با فضای سایبر در کشور.....	۳۶

فهرست اشکال

شکل ۱. هم‌پوشانی علوم در دانش سایبرنتیک [۱].....	۱۷
شکل ۲. کاربردپذیری و اعتبار در دانش سایبرنتیک [۱۵].....	۱۷
شکل ۳. فضای گسترش‌یافته در طول زمان.....	۱۸
شکل ۴. جایگاه سیستم‌های سایبرنتیکی در میان سطوح مختلف پیچیدگی سیستم‌های فیزیکی [۲۱].....	۲۰
شکل ۵. جایگاه امنیت سایبر در ارکان فضای سایبر.....	۲۳



نقش کاربست دانش سایبرنتیک در ارتقای کیفیت حکمرانی (۱): از حکمرانی بر فضای سایبر تا حکمرانی با فضای سایبر

چکیده



در دنیای امروزی و همگام با رشد فناوری، مفاهیمی همچون شبکه‌های اجتماعی، هوش مصنوعی، جرائم سایبری، رایانش ابری، زنجیره بلوکی، رمزارزها، اینترنت اشیا، واقعیت افزوده، هم‌زادهای دیجیتال و ربات‌ها به مفاهیمی پربسامد تبدیل شده‌اند. تصمیم‌گیری کارا در هریک از این حوزه‌ها، دانش و اشراف دقیق نسبت به موضوعات مطرح شده را ایجاب می‌کند. فضای سایبر به عنوان مفهومی بالادستی، از این قاعده مستثنا نیست و به دلیل تغییرات پرسرعت فناوری، به روزرسانی سریع این اشراف اطلاعاتی، گریزناپذیر است. با وجود اهمیت و اثربخشی فضای سایبر بر گستره وسیعی از تصمیمات حاکمیتی، در اظهارنظرهای برخی از تصمیم‌گیران و مسئولان حوزه فضای سایبر، صرفاً به بخشی از این فضا پرداخته شده که نتیجه آن، احصا نشدن تمام فرصت‌ها و تهدیدات این فضا به‌ویژه در اثر تغییرات سریع فناوری و در پی آن ناکامی در دستیابی به اهداف مندرج در اسناد بالادستی بوده است. این گزارش به عنوان اولین گزارش از سلسله گزارش‌های «نقش کاربست دانش سایبرنتیک در ارتقای کیفیت حکمرانی» ابتدا می‌کوشد به ارائه تعریفی جامع از فضای سایبر و معرفی ارکان اصلی در این فضا به همراه حدود توانمندی‌های فضای سایبر و مؤلفه‌های مؤثر در امنیت آن بپردازد تا با کمک تعریف ارائه شده، تصمیم‌گیری در این فضا متوجه بخش مشخصی از آن نشود و در ادامه الزامات و پیشنهادهایی برای حکمرانی کارا در فضای سایبر ارائه می‌شود. در گزارش‌های بعدی با توجه به مؤلفه‌های احصا شده، دیدگاه‌های مختلف درباره نسبت این فضا با انسان، جامعه و حاکمیت از زوایای مختلف فلسفی و آینده‌پژوهانه تبیین، و رویکردهای تعامل با آن بررسی می‌شود.



بیان / شرح مسئله

فضای سایبر^۱ کلان مفهومی است که به موضوعاتی همچون شبکه‌های اجتماعی، کلاهبرداری‌های فضای مجازی، امنیت سایبری، هوش مصنوعی، واقعیت افزوده^۲، واقعیت مجازی^۳، ربات‌ها و غیره ارتباط پیدا می‌کند. نهادهای قانونگذار برای حل و فصل مسائل ایجاد شده در هریک از موضوعات این کلان مفهوم، به مباحث این فضا ورود می‌کنند. محدود بودن دیدگاه‌های نهادهای تصمیم‌گیر و قانونگذار نسبت به فضای سایبر، سبب درک مسائل از زوایای مشخصی شده است که گاهی این ادراکات ناقص سبب می‌شود تصمیمات جامع مناسب اتخاذ نشود. ادراکات ناقص، ضربه‌پذیری از محدوده‌های به‌خوبی درک نشده این فضا را افزایش می‌دهد و امنیت ملی را با خطر مواجه می‌کند. هدف اصلی این گزارش ارائه تعریفی جامع از فضای سایبر و معرفی ارکان اصلی در این فضا به همراه حدود فضای سایبر و مؤلفه‌های مؤثر در امنیت آن است. با بینش حاصل از این تعریف، تصمیم‌گیرنده می‌تواند به ابعاد و قابلیت‌های فضای سایبر، حدود اثربخشی آن در بهبود حکمرانی و الزامات حکمرانی بر این فضا پی ببرد و متناسب با مسئله مورد بحث، نقاط مورد نیاز برای قانونگذاری یا اصلاح قوانین قبلی بر بستر قابلیت‌های این فضا را شناسایی، و ساختارها و قوانین جدید را به گونه‌ای طراحی و تدوین کند تا بیشترین کارایی را در پی داشته باشد. این گزارش می‌کوشد از این طریق از صحت و کفایت قانونگذاری در این فضا محافظت شود.

نقطه‌نظرات / یافته‌های کلیدی

دانش سایبرنتیک، دانش سلطه بر پدیده‌ها و کنترل امور یک مجموعه (یا سازمان یا کشور) و ایجاد حاکمیت^۴ با وجود دانش و اطلاعات ناقص درباره محیط و بازیگران است. فضایی که مبتنی بر به‌کارگیری این دانش پدید می‌آید، فضای سایبر نامیده می‌شود که با توجه به مطالعات صورت گرفته بر چهار رکن استوار است و عبارت‌اند از: رکن اطلاعات، رکن کنترل، رکن ارتباطات و رکن محاسبات. رکن اطلاعات به محتوایی اطلاق می‌شود که در فضای سایبر به گردش درمی‌آید؛ رکن کنترل به تغذیه هدفمند و جهت‌مند اطلاعات گفته می‌شود؛ رکن ارتباطات وظیفه انتقال اطلاعات را برعهده دارد و رکن محاسبات نیز به پردازش اطلاعات اشاره دارد.

با مرور قوانین و مصوبات صورت گرفته در فضای سایبر، می‌توان آنها را در دو دسته «حکمرانی بر فضای سایبر» و «حکمرانی با فضای سایبر» تحلیل کرد. متأسفانه تمرکز دیدگاه به فضای سایبر از زاویه مسائل زیرساختی و امور فناورانه همچون مسائل مخابراتی و امنیت شبکه و اطلاعات، سبب شناخت ناقص از توانمندی‌های گسترده این فضا شده است که نه فقط بهره‌مند نشدن از تمام قابلیت‌های این فضا را در پی دارد، بلکه احتمال آسیب‌پذیری حاکمیت از سوی موضوعات صرف نظر شده را افزایش می‌دهد. نتایج بررسی‌ها نشان می‌دهند که رکن کنترل فضای سایبر، رکن مغفول مانده این فضا است و فضای سایبر اغلب بدون در نظر گرفتن روح دانش سایبرنتیک مورد توجه قرار گرفته است. از دانش سایبرنتیک می‌توان برای اداره برخی از امور جامعه بهره برد؛ به گونه‌ای که اطلاعات و فرامین در مدارها به گردش درآیند و سیستم تحت مطالعه و عناصر موجود در آن با مقایسه وضع موجود و وضع مطلوب، به صورتی چابک تصمیمات لازم را اتخاذ و اجرایی کند. لازمه چنین رویکردی، تحول و تغییر در سازوکارهای ایجاد تصمیم است؛ به گونه‌ای که از اتکای صرف به اعلام دستور از سطح بالاتر سازمان به سطح پایین‌تر آن، سیستم مورد مطالعه خود به سمتی حرکت و اصلاح رفتار کند که ملاحظات و خواسته‌های مدیریت سازمان را در نظر گیرد و اهداف کلی تعیین شده برای مجموعه را تحقق بخشد. از این رو شناسایی جامع این فضا و بهره‌مندی از قوت‌ها و آگاهی از ضعف‌ها و فرصت‌ها و تهدیدهای موجود، می‌تواند به بهره‌مندی از ظرفیت‌های پنهان این فضا برای حکمرانی کارا تر بر مسائل کمک کند.

1. Cyberspace
2. Augmented Reality (AR)
3. Virtual Reality (VR)
4. Sovereignty



پیشنهاد راهکارهای تقنینی، نظارتی یا سیاستی

راهکارهای پیشنهادی برای تقویت و حفاظت حاکمیت فضای سایبر می‌توانند در سه سطح راهکارهای مرتبط با «حکمرانی بر فضای سایبر»، راهکارهای مرتبط با «حکمرانی با فضای سایبر» و راهکارهای مرتبط با پیوند این دو سطح ارائه شوند:

۱ تقویت زیرساخت‌های نرم‌افزاری هریک از ارکان و مؤلفه‌های فضای سایبر در همراهی با تقویت زیرساخت‌های سخت‌افزاری آن از طریق وضع هنجارهای قانونی؛

۲ قاعده‌مندسازی فعالیت کسب‌وکارها و حضور کاربران از طریق وضع قوانین و مقررات و همچنین تسهیلگری برای صنعت کاران و فعالان به منظور استقلال یافتن و بومی‌سازی فناوری‌ها در فضای سایبر و در راستای امنیت بخشیدن به انجام دادن فعالیت‌ها در این فضا؛

۳ کاهش فاصله محتوایی و زمانی قانون با نیازهای جامعه در فضای سایبر؛

۴ سرعت بخشیدن به وضع و همگام‌سازی قوانین و دستورالعمل‌ها با تغییرات فضای سایبر به منظور پر کردن خلأهای قانونی، به‌روزرسانی مستمر آنها، بهبود در مقررات موجود، کاهش تأثیرپذیری از نظام‌های قانونی و حقوقی کشورهای پیشرو و تقویت بخشی حاکمیت ملی؛

۵ شرح دقیق وظایف و اختیارات سازمان‌ها و نهادهای تصمیم‌گیر و اجرایی در فضای سایبر با رویکرد انسجام‌بخشی و هماهنگی آنان در این فضا به منظور جلوگیری از نابسامانی و هم‌پوشانی اقدامات؛

۶ متقاعدسازی ذی‌نفعان و مشروعیت‌بخشی به تصمیمات اتخاذ شده در خط‌مشی‌گذاری‌های فضای سایبر؛

۷ پذیرش، باورمندسازی و اطمینان‌بخشی کاربران نسبت به حضور در فضای سایبر داخلی و نهادهای تصمیم‌گیر در آن؛

۸ اهتمام جدی بر هوشمندسازی فرایندهای تصمیم‌سازی در راستای پیاده‌سازی حکمرانی داده‌مبنا و پیگیری و نظارت بر اجرای بند «پ» ماده (۱۰۷) قانون برنامه پنج‌ساله هفتم پیشرفت؛

۹ بهره‌گیری از قابلیت‌های دانش سایبرنتیک در حکمرانی مبتنی بر اصول اخلاقی مطرح شده در نظام جمهوری اسلامی (حکمرانی با فضای سایبر) و در طرح‌ریزی چگونگی رسیدن از وضع موجود به وضع مطلوب مورد نظر حاکمیت؛

۱۰ استفاده از تحلیلگران و مشاورانی با نگرشی سیستمی همراه سایر متخصصان در بررسی طرح‌ها و لوایح در کمیسیون‌های تخصصی مجلس شورای اسلامی و در امور تصمیم‌سازی؛

۱۱ توجه به نقش نظارتی مجلس و در نظرگیری فرایند خط‌مشی‌گذاری به مثابه چرخه که این راهکار با هوشمندسازی فرایند نظارتی و هدایت مجدد از طریق نظارت تسریع می‌شود؛

۱۲ اهتمام بر توسعه آزمایشگاه‌های خط‌مشی‌گذاری در نهادهای تنظیم‌گر؛

۱۳ بهره‌گیری از سهولت فراهم شده توسط فضای سایبر برای درگیر کردن حداکثری ذی‌نفعان، بررسی مسئله از ابعاد مختلف و ایجاد شفافیت در جامعه؛

۱۴ تکمیل مباحث فلسفی، نظری و عملی فضای سایبر و تربیت نیروی متخصص در این زمینه از طریق راه‌اندازی رشته‌های جدید یا گنجانیدن درس‌هایی همچون آشنایی با دانش سایبرنتیک، مباحث ویژه در فضای سایبر و مهندسی سایبرنتیک کاربردی که به‌طور مشخص در سرفصل‌های رسمی درس‌های رشته‌های دانشگاهی مهندسی و خط‌مشی‌گذاری وجود ندارند.

۱. مقدمه

پسوند «سایبر» اصطلاحات جدیدی را از قبیل سیستم سایبری، فضای سایبر، تهدیدات سایبر، امنیت سایبر، ارتش سایبری و جنگ سایبری به وجود آورده است و شامل مواردی می‌شود که به نحوی مرتبط با اتوماسیون، رایانه، واقعیت مجازی، اینترنت و غیره باشند [۱]. در این ارتباط، فضای سایبر به فضایی گفته می‌شود که متأثر از دانش سایبرنتیک باشد و اطلاعات در آن به منظور کنترل و سلطه بر جامعه هدف جریان داشته باشد [۱-۳]. حکمرانی نیز به نحوه حکومت کردن و شیوه اعمال قدرت اشاره دارد. تعاملات فضای سایبر و حکمرانی در مواجهه با یکدیگر در سه حیطه قابل بررسی اند: حیطه اول، تأثیرات حکمرانی بر فضای سایبر؛ حیطه دوم، نحوه اداره امور کشور و حکمرانی با فضای سایبر و حیطه سوم، تعاملات رفت و برگشت میان این دو (اثر گذاری هر حیطه بر حیطه دیگر). حیطه حکمرانی با فضای سایبر خود شامل دو قسم می‌شود: قسم اول، حکمرانی با استفاده از قابلیت‌های ابزاری فضای سایبر و قسم دوم، آثار کاربست دانش سایبرنتیک بر حکمرانی.

۱-۱. حکمرانی بر فضای سایبر

نقش‌های متفاوتی برای حکمرانی بر فضای سایبر تعریف می‌شود که می‌توان به مواردی نظیر خط‌مشی‌گذاری، قانونگذاری، ارزیابی، نظارت، محاکمه، تربیت و آموزش نیروی انسانی، تقویت علمی متخصصان و نخبگان، هدایت، فرهنگ‌سازی و ترویج، حمایت و توسعه فضای کسب و کار، سامان‌دهی مجوزها و پروانه‌ها و تنظیمگری اشاره داشت.

این حکمرانی بیشتر به موضوعات زیر ساختی فضای سایبر از قبیل تبیین، تنظیم و مدیریت روابط و منافع بازیگران و ذی‌نفعان فضای سایبر، به‌ویژه در بخش‌های ارتباطاتی و فناوری اطلاعات می‌پردازد. سهم ارتباطات و فناوری اطلاعات (فاوا) در قوانین این حوزه به قدری پررنگ است که حکمرانی بر فضای سایبر را می‌توان حکمرانی فاوامحور نیز نامید (هر چند «سایبر» مفهومی در سطح بالاتر است).

در این گونه حکمرانی دولت‌ها می‌کوشند از طریق وضع قوانین، مقررات، تنظیم‌گری‌ها یا مقررات‌زدایی‌ها و اجرایی کردن خط‌مشی‌ها، اهداف و مقاصد کشور خود را در زمینه تأمین نیازهای اساسی، رعایت حقوق کلیه افراد، جلوگیری از فعالیت‌های سوداگرانه، امنیت اجتماعی، صیانت از حریم شخصی و حفظ کرامت انسانی و نظایر آن برآورده کنند. تعیین دستورالعمل‌های سطح خدمات دسترسی، ضوابط برای حکمرانی بر داده، ضوابط بر انواع سکوها^۱ و ضوابط بر فرایندهای جمع‌آوری، ذخیره‌سازی، نگهداری، استفاده و بازیابی داده‌های شخصی شهروندان، می‌تواند در این حیطه تعریف شود. از نتایج حکمرانی صحیح بر فضای سایبر، تسلط کشور بر تأمین تجهیزات و ابزارهای سخت‌افزاری و نرم‌افزاری فضای سایبر، محتوا، سکوها و توسعه شبکه ملی اطلاعات خواهد بود. برای نمونه، سکوها براساس محصول قابل ارائه، به سکوهای حوزه پرداخت، حوزه خدمات رمارز، حوزه مدیریت مالی، حوزه حمل و نقل، حوزه خرده‌فروشی، حوزه شبکه‌های تعاملی و پیام‌رسان‌ها، حوزه اشتراک محتوای رسانه‌ای، حوزه رویدادها و جلسات بر خط، حوزه انتشارات و کتاب‌فروشی بر خط، حوزه آموزش و پرورش، حوزه تبلیغات، حوزه نیازمندی‌های بر خط، حوزه نیازهای شغلی، حوزه اشتراک و نمایش فیلم، حوزه بازی‌های بر خط، حوزه سلامت و درمان، حوزه توسعه نرم‌افزار و حوزه تحلیل داده (جمع‌آوری، محاسباتی و جست‌وجو)، دسته‌بندی می‌شوند. گستردگی انواع محصولات ارائه شده در این سکوها خود نشان از آن دارد که ضوابط و قانونگذاری صحیح در هر مورد، بر چه حجم قابل توجهی از اقتصاد، فرهنگ، روابط اجتماعی و فناوری تأثیرگذار است و از دیگر سو، نبود قوانین کافی یا قوانین ضد و نقیض تا چه حد می‌تواند بلا تکلیفی در مسیر پیشرفت اقتصادی و فرهنگی کشور ایجاد کند.



۱-۲. حکمرانی با فضای سایبر

۱-۲-۱. حکمرانی با استفاده از قابلیت‌های ابزاری فضای سایبر

حکمرانی مطلوب نیازمند شفافیت حداکثری و مشارکت حداکثری است که این امر می‌تواند از طریق امکاناتی که فضای سایبر فراهم می‌کند، تحقق یابد. با توجه به نیاز روزافزون جامعه به فضای سایبر و آثار و پیامدهای آن در زندگی اجتماعی، حاکمیت در این رویکرد تلاش می‌کند با استفاده از قابلیت‌های ابزاری فضای سایبر، اقداماتی را در راستای رسانش سریع فرمان‌ها و اطلاعات به مخاطبان، گسترش دادن دامنه مخاطبان و سهولت در اجرای خط‌مشی‌های خود به کار بندد.

این نوع حکمرانی به دنبال پیوند زدن فضای سایبر به فضای فیزیکی و گسترش دامنه حکمرانی به فضای گسترش یافته ناشی از این پیوند است. حاکمیت با استفاده از قابلیت‌های ابزاری فضای سایبر می‌کوشد با قوانین و مقررات وضع شده موجود، به مدیریت این فضای گسترش یافته بپردازد و به اهداف و اولویت‌های خود در حوزه‌های مختلف سیاسی، اقتصادی، اجتماعی، زیست‌محیطی، فرهنگی و فناوریانه دست یابد. صدور اینترنتی مجوزها، سامانه‌های خدمات‌رسانی برخط، آموزش از راه دور، توسعه شبکه‌های اجتماعی بومی، سامانه‌های ارزشیابی و رصد فساد و در نهایت بروز و ظهور دولت الکترونیک می‌توانند از خروجی‌های کنونی حکمرانی با استفاده از قابلیت‌های ابزاری فضای سایبر قلمداد شوند. البته که در آینده و با ورود فناوری‌های جدید، بهره‌مندی از سایر ابزارهای تسهیل‌کننده برای خدمات‌رسانی بیشتر به جامعه قابل انتظار است.

۱-۲-۲. حکمرانی با کاربرست دانش سایبرنتیک

این نوع حکمرانی می‌کوشد دانش سایبرنتیک را در جهت طرح‌ریزی و برنامه‌ریزی اقدامات در راستای رسیدن به اهداف مشخص شده به کار گیرد. در ایران کاربرست این قسم از حکمرانی نسبت به دو مورد قبلی بسیار کمتر است و نبود شناخت و بهره‌گیری از این دانش در تصمیم‌سازی، نه فقط دستیابی به راه‌حل‌های بهینه برای رویارویی با مسائل مختلف پیش آمده در کشور را دشوار می‌کند و کشور را در حل و فصل به موقع بحران‌ها ناتوان می‌گرداند، بلکه احتمال آسیب دیدن کشور را در برخی از مسائل و از سوی دیگر کشورهای متخاصم افزایش می‌دهد. نتیجه حکمرانی با کاربرست دانش سایبرنتیک، افزایش چابکی و هوشمندی در انتخاب گزینه‌ها و تصمیمات بهینه و طراحی اقدامات و استراتژی‌های کارا خواهد بود.

گزارش پیش‌رو قصد دارد با مروری بر مصوبات مجلس شورای اسلامی و مطالعات انجام شده در فضای سایبر، جهت‌گیری موجود مجلس شورای اسلامی ایران را در قبال فضای سایبر استخراج کند. همچنین با ارائه تعریفی جامع و واقع‌بینانه از فضای سایبر و شفاف‌سازی محدوده اثرگذاری آن، نقاط مورد نیاز برای ورود به منظور برطرف کردن خلأهای قانونگذاری را نمایان، و پیشنهادهایی را برای پر کردن این شکاف‌ها ارائه کند.

۲. پیشینه پژوهش

۲-۱. پیشینه مطالعات پژوهشی مرتبط

در گزارش‌های متعددی از مرکز پژوهش‌های مجلس شورای اسلامی به فضای سایبر توجه شده است که در مواردی از آنها برداشت کلی از فضای سایبر، کنترل جوامع از طریق رساندن اطلاعات به جامعه هدف و تغییر ذهنیت‌ها، نگرش‌ها، ذائقه‌ها و ارزش‌های جامعه از طریق آن و ترویج سبک زندگی متعارض با سبک زندگی ایرانی اسلامی بوده است. در گزارش‌هایی با عناوین «بررسی بخش دوم لایحه بودجه سال ۱۴۰۳ کل کشور - حوزه رسانه و فضای مجازی» (با شماره مسلسل ۱۹۷۴۴ و شماره ثبت ۹۵۰ ارائه شده توسط دفتر مطالعات آموزش و فرهنگ در اردیبهشت‌ماه ۱۴۰۳)، «ارزیابی میزان عملکرد قانون بودجه ۱۴۰۲ در حوزه رسانه و فضای مجازی» (با شماره مسلسل ۱۹۵۵۵ ارائه شده توسط دفتر مطالعات آموزش و فرهنگ در دی‌ماه ۱۴۰۲)، «بررسی ابعاد مسئله تنظیم‌گری خدمات رسانه‌ای صوت و تصویر فراگیر در فضای مجازی و ارائه پیش‌نویس قانونی» (با کد موضوعی ۲۷۰ و شماره مسلسل ۱۹۲۵۴ ارائه شده توسط دفتر مطالعات آموزش و

فرهنگ در شهریورماه ۱۴۰۲)، «بررسی لایحه برنامه هفتم توسعه- حوزه رسانه و فضای مجازی و ارائه احکام پیشنهادی» (با کد موضوعی ۲۷۰ و شماره مسلسل ۱۹۰۵۲ و شماره ثبت ۹۱۰ ارائه شده توسط دفتر مطالعات آموزش و فرهنگ در تیرماه ۱۴۰۲)، «بررسی عملکرد قانون برنامه ششم توسعه در حوزه رسانه و فضای مجازی و درس آموخته‌هایی برای برنامه هفتم توسعه» (با شماره مسلسل ۱۹۰۴۳ ارائه شده توسط دفتر مطالعات آموزش و فرهنگ در تیرماه ۱۴۰۲)، «بررسی ابعاد مسئله اطلاعات، اخبار و محتوای خلاف واقع در فضای مجازی و ارائه پیش‌نویس قانونی» (با کد موضوعی ۲۷۰ و شماره مسلسل ۱۸۴۵۲ ارائه شده توسط دفتر مطالعات فرهنگ و آموزش در مهرماه ۱۴۰۱)، «بررسی چالش‌های توسعه زیست‌بوم فضای مجازی در حوزه کودک و نوجوان و ارائه بسته سیاستی» (با کد موضوعی ۲۷۰ و شماره مسلسل ۱۸۴۹۶ ارائه شده توسط دفتر مطالعات فرهنگ و آموزش در آبان‌ماه ۱۴۰۱)، «تأثیر شبکه‌های اجتماعی مجازی بر امنیت ملی» (با کد موضوعی ۲۶۰ و شماره مسلسل ۱۲۲۳۶ ارائه شده توسط دفتر مطالعات سیاسی در بهمن‌ماه ۱۳۹۰) و «مسئولیت چهره‌ها در شبکه‌های اجتماعی» (با کد موضوعی ۲۷۰ و شماره مسلسل ۱۸۳۴۸ ارائه شده توسط دفتر مطالعات فرهنگ و آموزش در مردادماه ۱۴۰۱) به‌طور غالب به فضای سایبر از بُعد رسانه‌ای و تبلیغاتی و ابزاری برای برقراری ارتباطات جمعی توجه شده است. همین برداشت ناکامل از فضای سایبر سبب شده است که حکمرانی فضای سایبر به اقداماتی همچون ارتقای سطح سواد خبری جامعه در شناسایی منبع پیام‌ها، مسدودسازی پیامدهای خبرهای دروغی و جعلی یا فیلترینگ محدود شود و تنزل یابد. در گزارش «الزامات مدیریت راهبردی امنیت عمومی در جمهوری اسلامی ایران» (با کد موضوعی ۲۶۰ و شماره مسلسل ۱۰۲۷۷ ارائه شده توسط دفتر مطالعات سیاسی در خردادماه ۱۳۸۹) فضای سایبر اغلب معادل بستری برای انتقال اطلاعات، گسترش رسانه‌ها در ابعاد وسیع و تغییر ذهنیت افراد در این فضا در نظر گرفته شده و تلاش شده است با شناسایی تهدیدات ایجاد شده با این برداشت، به ارائه راهکارهایی برای مواجهه با آن پرداخته شود. در این گزارش، عوامل متعددی در شکل‌گیری ناامنی عمومی مطرح می‌شوند که مهم‌ترین مؤلفه‌های منفی اثرگذار بر امنیت عمومی، در ریشه‌های ناامنی امنیتی، ریشه‌های ناامنی سیاسی، ریشه‌های ناامنی رسانه‌ای، ریشه‌های ناامنی روانی، ریشه‌های ناامنی ساختاری و ریشه‌های ناامنی اجتماعی جای می‌گیرند. در این مؤلفه‌ها فقط در ریشه‌های ناامنی رسانه‌ای (از لحاظ: ۱. عدم بهره‌وری بهینه از ظرفیت‌های رسانه‌ای تولید امنیت نرم، ۲. تنوع و تکثر تهدیدات سایبری امنیت عمومی مانند رسانه وب‌لاگ یا شبکه‌های اجتماعی مانند توئیتر و فیس‌بوک، ۳. افزایش ماهواره‌های صوتی-تصویری ضدانقلاب در محیط امنیت مجازی جمهوری اسلامی ایران و بهره‌گیری آنان از ترفندهای عملیات روانی مانند شایعه‌سازی) و در ریشه‌های ناامنی روانی (از نظر: ۱. شکل‌گیری ذهنیت تهدید در جامعه و ضعف پدافند رسانه‌ای برای مقابله با آفندهای عملیات روانی، ۲. ایجاد برخی مولدهای ناامنی ذهنی مانند شکل‌گیری ذهنیت بی‌عدالتی به دلیل ناکارآمدی نظام تولید، توزیع و مصرف) به موضوع فضای سایبر و آن هم از بُعد رسانه و انتقال اطلاعات پرداخته شده است و فقط در یک بند از ریشه‌های ناامنی ساختاری (از لحاظ: ۱. نبود ساختار سازمانی منسجم برای مدیریت و خنثی‌سازی آفندهای سایبری امنیت عمومی) نگاهی عمل‌گرایانه و کاربردی به حکمرانی بر فضای سایبر (البته آن هم به دلیل رویارویی با رسانه‌های معاند، انتقال اطلاعات و جاسوسی) همچون قانونمندسازی نظام جامع فیلترینگ وجود دارد.

برخی از تهدیدات فضای سایبر در گزارش اشاره شده، تخلیه بانک‌های اطلاعاتی کشور، نفوذ و خراب‌کاری در سایت‌های اینترنتی، شکستن یا عبور از فیلترینگ، مدیریت شبکه‌های اجتماعی با رویکرد تسریع و تسهیل وقوع و گسترش ناامنی داخلی، بسترسازی برای ارتباط امن تلفنی و دیتا برای مصاحبه با رادپوها و تلویزیون‌های بیگانه، شناسایی، جذب و سازمان‌دهی ایرانیان خارج از کشور، ارائه کدهای اشتباه از آمار تلفات و مجروحان آشوب‌های اجتماعی، انتقال غیرقانونی متهمان به خارج کشور با کمک گروهک‌های ضدانقلاب، انجام اقدامات ایدایی سایبری با هدف رخنه هکرها به اطلاعات طبقه‌بندی شده دیجیتال کشور و مختل‌سازی نظام مدیریت خدمات شهری از جمله سامانه سوخت‌رسانی با هدف ایجاد نارضایتی عمومی معرفی شده‌اند.

گزارش «تأملی بر فیلترینگ- برنامه اقدام برای تحقق برنامه سالم‌سازی فضای سایبر» (با کد موضوعی ۲۹۰ و شماره مسلسل ۸۹۴۷ ارائه شده توسط دفتر مطالعات ارتباطات و فناوری‌های نوین در اردیبهشت‌ماه ۱۳۸۷) به موضوع عاری‌سازی فضای سایبر از ناهنجاری‌های مجرمانه و منحرفانه در تمام ابعاد آن پرداخته شده است و همراه با الزامی دانستن اقدامات و تدابیر پیشگیرانه و ایجابی و وجود ارکان سلبی، اما تمرکز صرف بر تدابیر سلبی همچون فیلترینگ و نادیده انگاشتن دیگر گزینه‌های سالم‌سازی فضای سایبر را موجب نارسایی و تحت‌الشعاع قرار گرفتن مزایای این ابزار می‌داند.



در مجموعه گزارش‌های دیگری همچون «بررسی لایحه بودجه سال ۱۴۰۲ کل کشور» (۶۲): اعتبارات بخش فناوری اطلاعات و ارتباطات» (با کد موضوعی ۳۱۰ و شماره مسلسل ۱۸۷۶۹ ارائه شده توسط گروه فناوری اطلاعات و ارتباطات دفتر مطالعات انرژی، صنعت و معدن در بهمن‌ماه ۱۴۰۱) و «بررسی لایحه بودجه سال ۱۴۰۴ کل کشور» (۹): تبصره «۶» (حوزه صنعت، معدن و ارتباطات)» (با کد موضوعی ۳۱۰ و شماره مسلسل ۲۰۱۹۶ ارائه شده توسط گروه صنعت، معدن و صنایع معدنی و ارتباطات دفتر مطالعات انرژی، صنعت و معدن در آبان‌ماه ۱۴۰۳) به مسائلی همچون گسترش شبکه تار (فیبر) نوری، ساخت ماهواره‌های ارتباطی، توسعه خدمات پستی، شبکه ملی اطلاعات، سامانه‌ها، دولت الکترونیک، صنعت میکروالکترونیک، تجهیزات رایانشی و فضای ابری و همچنین سهم آنها در لایحه بودجه پرداخته شده است که می‌توان آنها را مرتبط با زیرساخت‌های اطلاعاتی و ارتباطاتی فضای سایبر دانست.

در این راستا، گزارش‌های دیگری نیز مرتبط با تأثیرات حکمرانی بر زیرساخت‌های فضای سایبر جای می‌گیرند. در گزارش «حریم خصوصی در فضای سایبر - حریم داده‌های الکترونیکی» (با کد موضوعی ۲۹۰ و شماره مسلسل ۸۰۶۹ ارائه شده توسط گروه ارتباطات و فناوری‌های نوین در آبان‌ماه ۱۳۸۵)، به موضوع حریم خصوصی داده‌های افراد در فضای سایبر پرداخته شده است. در گزارش «فساد در زنجیره تأمین داده‌های فضای مجازی» (با شماره مسلسل ۱۹۷۲۲ ارائه شده توسط دفتر مطالعات آموزش و فرهنگ در فروردین‌ماه ۱۴۰۳)، به موضوع دسترسی، جمع‌آوری، ذخیره‌سازی، پردازش، افشای غیرمجاز و حتی امحای داده‌ها و الزامات حقوقی برای ارتقای امنیت داده‌ها و جلوگیری از بروز فساد پرداخته شده است.

گزارش‌های دیگری نیز با تأثیرات حکمرانی بر ابزارهای جدیدی، که فضای سایبر در اختیار کاربران خود قرار داده است، مرتبط‌اند. گزارش‌هایی با عناوین «ارز مجازی: قانونگذاری در کشورهای مختلف و پیشنهاد برای ایران» (با کد موضوعی ۲۸۰ و شماره مسلسل ۱۶۰۴۲ ارائه شده توسط معاونت پژوهش‌های زیربنایی و امور تولیدی دفتر مطالعات ارتباطات و فناوری‌های نوین در شهریورماه ۱۳۹۷)، «مقدمه‌ای بر تنظیمگری رمزینه‌ارزها در اقتصاد ایران» (با کد موضوعی ۲۲۰ و شماره مسلسل ۱۵۹۳۲ ارائه شده توسط معاونت پژوهش‌های اقتصادی دفتر مطالعات اقتصادی در تیرماه ۱۳۹۷)، «فناوری واقعیت مجازی، کاربردها و الزامات حقوقی آن» (با کد موضوعی ۲۸۰ و شماره مسلسل ۱۵۷۳۵ ارائه شده توسط دفتر مطالعات ارتباطات و فناوری‌های نوین معاونت پژوهش‌های زیربنایی و امور تولیدی در بهمن‌ماه ۱۳۹۶) و «متاورس (فراجهان): چالش‌ها و الزامات توسعه و به‌کارگیری» (با شماره مسلسل ۱۹۳۸۰ ارائه شده توسط دفتر مطالعات انرژی، صنعت و معدن در آبان‌ماه ۱۴۰۲) به فناوری‌های جدید بروز یافته در فضای سایبر نظیر ارز مجازی، رمزارز، واقعیت مجازی، اینترنت اشیا^۱ و... پرداخته‌اند و کوشیده‌اند با تبیین این فناوری‌ها، مقررات لازم برای مواجهه با مسائل پیش آمده در آنها را تدوین کنند. برای نمونه در گزارش «اینترنت اشیا: چارچوب مقررات گذاری امنیت سایبری و مقررات گذاری داده در اینترنت اشیا برای ایران» (با کد موضوعی ۳۱۰ و شماره مسلسل ۱۷۰۱۲ ارائه شده توسط معاونت پژوهش‌های زیربنایی و امور تولیدی دفتر مطالعات انرژی، صنعت و معدن در اردیبهشت‌ماه ۱۳۹۹) به ملاحظات قانونگذاری پیرامون فناوری اینترنت اشیا و برقراری امنیت سایبری در این زمینه پرداخته شده است.

گزارش «مروری بر معاهده‌های فراملی سایبری» (با کد موضوعی ۲۸۰ و شماره مسلسل ۱۵۸۶۵ ارائه شده توسط دفتر مطالعات ارتباطات و فناوری‌های نوین معاونت پژوهش‌های زیربنایی و امور تولیدی در خردادماه ۱۳۹۷) فضای سایبر را ناشی از پیوند گسست‌ناپذیر فناوری‌های ارتباطی و اطلاعاتی می‌داند که به مرور هرچه در مسیر تکاملی خویش پیش می‌رود، قلمرو حاکمیتی را تحت الشعاع توانمندی‌های خود قرار می‌دهد و در حال زدودن این ویژگی از شخصیت کشورهاست. با فراتر رفتن دامنه موضوعات از قلمرو حاکمیت‌های ملی و قوانین داخلی کشورها، نیاز به معاهده‌های فراملی بیشتری احساس خواهد شد. براساس این گزارش، معاهده‌ها به سه دسته معاهده‌های فیزیکی، معاهده‌های سایبری و معاهده‌های مشترک تقسیم می‌شوند و می‌توان این گونه استنباط کرد که این گزارش فضای حکمرانی گسترش یافته امروزی را در سه بخش فضای فیزیکی و فضای سایبر و فضای مشترک میان این دو قابل بررسی می‌داند. شایان ذکر است در این گزارش تدوین معاهده‌های فراملی سایبری از موضوعاتی است که باید به‌نحوی صورت پذیرد که علاوه بر حفظ منافع کشورها و در امان ماندن از تهدیدهای فضای سایبر، تحمیل دیدگاه‌ها و خواسته‌های یک یا چند کشور مسلط صورت نپذیرد و به این ترتیب این گزارش در حیطه مطالعات حکمرانی بر فضای سایبر جای می‌گیرد.

در این میان، مطالعات اندکی به تأثیرات فضای سایبر در ارتقای حکمرانی (حکمرانی با فضای سایبر) پرداخته‌اند. برای نمونه، در گزارش

«ضرورت تأمین رایانک (تبلت) دانش آموزی برای آموزش مجازی» (با شماره مسلسل ۱۷۱۷۱ ارائه شده توسط دفتر مطالعات آموزش و فرهنگ در شهریورماه ۱۳۹۹) به نحوی به تبیین نقش قابلیت‌های فضای سایبر در تسهیلگری ارائه خدمات آموزشی پرداخته شده است. با جمع‌بندی مطالعات صورت گرفته حوزه‌های حکمرانی بر فضای سایبر و حکمرانی با فضای سایبر، می‌توان از منظر کارشناسان، نقش‌آفرینی فضای سایبر را در سه دسته اصلی ۱- محتوایی و رسانه‌ای، ۲- زیرساختی- فاوا محور و ۳- عملکردی و ابزاری به‌منظور تسهیلگری تحلیل کرد.

۲-۲. سوابق تقنین به‌همراه آسیب‌شناسی

با بررسی روند مهم‌ترین قوانین و مصوبات انجام شده در زمینه فضای سایبر و رویکردهای مختلف حاکمیت درباره این فضا، که در جدول بخش پیوست آورده شده است، مشاهده می‌شود که تا نیمه اول دهه ۱۳۸۰ رویکرد غالب مجلس شورای اسلامی به حکمرانی بر فضای سایبر اختصاص داشته است و قوانین و مقررات به توسعه لایه‌های مختلف زیرساخت از قبیل محتوا، توسعه دسترسی به شبکه و خدمات ارتباطی ارتباط دارد. در این سال‌ها، سهم اقتصاد دیجیتال اغلب به لایه هسته، شامل بخش‌های خدمات ارتباطی و اطلاعاتی و تجهیزات سخت‌افزاری و نرم‌افزاری، محدود بوده است. با تصویب [قانون برنامه چهارم توسعه](#) در سال ۱۳۸۳ و توجه به قابلیت‌های فضای سایبر در اداره امور کشور در برنامه‌های توسعه برای اولین بار، به‌مرور از نیمه دوم دهه ۱۳۸۰ و با تأسیس دفترهای پیشخوان خدمات دولت، شکل‌گیری تجارت الکترونیک و بانکداری الکترونیک، اقدامات حاکمیت به‌سمت ایجاد دولت الکترونیک و حکمرانی با فضای سایبر پیش می‌رود. دهه ۱۳۹۰ را می‌توان دهه آغازین آزادسازی بازار ارتباطات و شکل‌گیری انواع سکو (پلتفرم)های اقتصادی- اجتماعی- فرهنگی و شکوفایی فضای مجازی دانست. در این دهه ضربه نفوذ اینترنت افزایش و حجم اقتصاد دیجیتال به بخش‌های بیشتری توسعه می‌یابد [۳]. همسو با سوابق مطالعات پژوهشی صورت گرفته، غالباً برداشت کلی حاکمیت از تهدیدات فضای سایبر، کنترل جوامع از طریق رساندن اطلاعات به جامعه هدف و تغییر در نگرش و ذهنیت آنها بوده است و با این برداشت در سال ۱۳۹۵ و با شروع مجلس دوره دهم، فراکسیون «رسانه، مطبوعات و فضای مجازی» شکل می‌گیرد. با آغاز سال ۱۳۹۶ و تصویب [قانون برنامه ششم توسعه](#)، به حکمرانی با فضای سایبر و امنیت آن و افزایش ظرفیت‌های قدرت نرم و تقویت امکانات در دفاع و جنگ سایبری به‌طور جدی توجه می‌شود. همچنین به کارکرد فناوری اطلاعات در شفافیت و مبارزه با فساد در نظام‌های اداری نیز اشاره می‌شود. در آبان‌ماه ۱۳۹۸ شورای اجرایی فناوری اطلاعات، تشکیل می‌شود که هدف اصلی آن استقرار و توسعه دولت الکترونیک و ایجاد بسترهای گسترش کاربردهای فناوری اطلاعات و ارتباطات در کشور در زمینه‌های اجتماعی- اقتصادی- فرهنگی و به‌کارگیری فناوری اطلاعات در خدمات عمومی است.

در آبان‌ماه ۱۴۰۱، با تصویب [قانون مدیریت داده‌ها و اطلاعات ملی \(مدام\)](#) در مجلس شورای اسلامی، گام مهمی در تبیین راهبردهای کلان نظام تولید، نگهداری، پردازش، دسترسی، یکپارچه‌سازی، تبادل و امنیت داده‌ها و اطلاعات ملی با هدف افزایش قدرت حکمرانی، سامان‌دهی و انسجام‌بخشی به نظام تبادل داده‌ها و اطلاعات، گسترش تبادل اطلاعات میان دستگاه‌ها و نهادها و تسهیل دسترسی به اطلاعات پایه برای کسب‌وکارهای بخش خصوصی برداشته شد. با تدوین موادی همچون ماده (۱۰۷) در [قانون برنامه هفتم توسعه](#) با عنوان «هوشمندسازی و دولت الکترونیک»، به نظر می‌رسد این برنامه توسعه نیز در راستای تقویت زیرساخت‌ها، تکمیل و توسعه شبکه ملی اطلاعات، تأمین محتوا، استقرار نظام حکمرانی داده‌مبنا و ارتقای قدرت و امنیت سایبری گام بردارد.

با آنکه در اهداف کلان سند راهبردی جمهوری اسلامی ایران در فضای مجازی- اهداف و اقدامات کلان، مصوب شهریورماه ۱۴۰۱ شورای عالی فضای مجازی، به بهینه‌سازی و افزایش کارآمدی نظام تصمیم‌گیری و ارتقای سطح هوشمندی در نظامات ملی (از قبیل نظام آموزش، سلامت و بهداشت، حمل‌ونقل، تجارت، امور قضایی، انتظامی، گردشگری، پولی و بانکی و سایر خدمات شهری) اشاره شده است، آنچه از مجموعه قوانین و مقررات برداشت می‌شود آن است که بیشتر قوانین در حیطه حکمرانی بر فضای سایبر جای گرفته و بهره‌گیری از قابلیت‌های این فضا در بهبود حکمرانی، فقط تا بخش‌های ابزاری آن فضا و به‌منظور تسهیلگری همچون توسعه دولت الکترونیک و ارتقای خدمات‌رسانی عمومی محدود شده است. این در صورتی است که هر نوع انتقال اطلاعات و ارسال فرمان به‌منظور کنترل و تسلط بر یک مجموعه در فضای سایبر قابل بررسی است. برای نمونه، در [قانون](#)



سامان‌دهی صنعت خودرو مصوب ۱۶ خردادماه ۱۴۰۱ مجلس شورای اسلامی یا در **قانون حمایت از خانواده و جوانی جمعیت** مصوب ۱۹ آبان‌ماه ۱۴۰۰ مجلس شورای اسلامی یا در **قانون توسعه حمل‌ونقل عمومی و مدیریت مصرف سوخت** مصوب ۱۸ آذرماه ۱۳۸۶ مجلس شورای اسلامی یا در **قانون سامان‌دهی و حمایت از تولید و عرضه مسکن** مصوب ۲۵ اردیبهشت‌ماه ۱۳۸۷، با آنکه در راستای سامان‌دهی و راهبری جامعه مورد نظر به‌سوی اهداف تعیین شده و حکمرانی بر مسائل مورد نظرند و به‌طور مشخص به کاربرست دانش سایبرنتیک برای طراحی خط‌مشی‌ها نیاز دارند، بهره‌گیری از اصول دانش سایبرنتیک در آنها دیده نمی‌شود. با آنکه خروجی برخی بندهای قوانین مدون شده با نیت رسیدن به اهداف مطلوب نگارش شده‌اند، بدون کاربرست دانش سایبرنتیک ممکن است با تحقق اهداف تعیین شده در تضاد باشند. برای نمونه، در قانون سامان‌دهی صنعت خودرو، به‌دلیل آنکه شماره‌گذاری خودروها و موتورسیکلت‌ها مشروط به ارائه گواهی اسقاط توسط خودروسازان و موتورسیکلت‌سازان شده، افزایش قیمت خودروهای اسقاطی را در پی داشته است؛ یا افزایش قیمت خودروهای اسقاطی، به‌واسطه آنکه واردکنندگان خودرو و موتورسیکلت موظف‌اند به‌ازای واردات هر خودرو و موتورسیکلت به تناسب مصرف و نوع سوخت، علاوه‌بر پرداخت عوارض گمرکی، گواهی اسقاط خودروی معادل را دریافت کنند؛ یا تعیین سقف واردات خودرو بدون تأثیر ملموس بر تنظیم قیمت بازار یا بدون تأثیر ملموس در ارتقای کیفیت تولید خودروهای داخلی، نمونه‌هایی از جمله نابسامانی‌های ایجاد شده در اثر به‌کار نگرفتن دانش سایبرنتیک در برنامه‌ریزی‌ها و قانونگذاری‌هاست.

۳. دانش سایبرنتیک و حکمرانی

حکمرانی در فضای سایبر یکی از چالشی‌ترین حوزه‌های پیش‌روی حاکمیت‌هاست و موفقیت در آن نیازمند شناختی صحیح از این پدیده، چالش‌های پیش‌روی آن و راهکارهای رویارویی با آن است. واژه یونانی سایبرنتیک، که ریشه آن به واژه «کوبرنه‌تیس» در یونان باستان بازمی‌گردد و از نظر لغوی به‌معنای سکان‌داری کشتی است، ابتدا توسط افلاطون^۱ به‌معنای علم «اداره دولت-شهر» به کار برده شد. این مفهوم در دوره مدرن، حدود ۲۰۰۰ سال پس از افلاطون، در قالب همین واژه اما با املای فرانسوی در آثار امپیر^۲ دانشمند و فیلسوف فرانسوی، با عنوان «علم حاکمیت مدنی» (۱۸۳۴) در کتاب «فلسفه علم» وی تعریف شد و پس از او ترنتوفسکی^۳ (۱۸۴۳) از آن با عنوان «هنر چگونگی حکومت بر یک ملت» یاد کرد. در قرن بیستم، بوگدانوف^۴ (۱۹۲۵) در کتابی به نام «تکنولوژی»^۵ اصولی را برای سازمان‌دهی انواع سیستم‌ها (که امروزه به‌عنوان نظریه سیستم‌ها شناخته می‌شود) مطالعه کرد و به پایه‌گذاری بخشی از این علم کمک کرد. در اواخر دهه ۱۹۴۰ این مفهوم توسط وی‌نر^۶، دانشمند آمریکایی، به‌عنوان دانش کنترل و ارتباطات در حیوان و ماشین معرفی شد (۱۹۴۸) و نویسنده در کتاب «سایبرنتیک» تا حدی پیش رفت که با نگاه فنی و رویکردی عمل‌گرایانه، زمینه‌های شکل‌گیری یک حکومت جهانی توسط این علم را نه‌فقط محتمل، بلکه ضروری می‌دانست [۲]. با مطالعه تاریخچه دانش سایبرنتیک [۴ و ۵] مشخص می‌شود، تنوع تعاریف دانش سایبرنتیک از نگاه دانشمندان حوزه سایبرنتیک بسیار زیاد بوده است؛ به‌خصوص آنکه این مقوله با گذر زمان و پیشرفت تکنولوژی تغییر می‌کند و آن‌گونه نیست که صاحب‌نظران این حوزه بر تعریف خاصی توافق کرده باشند. این تعاریف با یکدیگر متفاوت‌اند، اما متضاد نیستند و صرفاً برخی از تعاریف جامع‌تر و برخی محدودترند [۴] یا برخی از تعاریف بیشتر بر بخش ارتباطاتی یا برخی بیشتر بر بخش کنترلی یا برخی بر اطلاعات یا برخی بر سیستم مورد مطالعه تمرکز کرده‌اند. مرور تعاریف مختلف از دانش سایبرنتیک از آن نظر ارزشمند است که جنبه‌های مختلفی را که این دانش می‌تواند به آنها ورود کند، مشخص می‌کند.

1. Plato
2. Andre-Marie Ampere (A. Ampere)
3. B. Trentowsky
4. A. Bogdanov
5. Tektology
6. Norbert Wiener (N. Wiener)

در این راستا، کولموگروف^۱ علم سایبرنتیک را علم مطالعه سیستم‌ها با ماهیت‌ها و طبیعت‌های مختلف تعریف کرده است که قادر بر دریافت، ذخیره و پردازش اطلاعات به‌منظور بهره‌برداری از آنها برای کنترل کردن است [۴]. اشبی^۲، پایه‌گذار حوزه بایولوژیکال سایبرنتیک، سایبرنتیک را هنر راهبری و سکان‌داری می‌داند. از منظر او، سایبرنتیک با تمام انواع رفتارها، تا آنجا که عادی، معین یا قابل بازتولید و تکرار باشند، سروکار دارد (به آن معنا که رفتارها کنترل‌پذیر باشند)؛ همچون ماشین‌های واقعی که می‌توانند الکترونیکی، مکانیکی، عصبی یا حتی اقتصادی باشند. از دیدگاه اشبی، سایبرنتیک در واقع روشی برای مواجهه علمی با سیستم‌هایی است که پیچیدگی در آنها بالاست و باید از آن صرف‌نظر شود [۶]. گرگوری بیتسون^۳ آن را شاخه‌ای از ریاضیات می‌داند که با مسائل مربوط به کنترل، بازگشتی بودن (حلقه تکرار) و اطلاعات درگیر است و بر فرم‌ها و الگوهای که به‌هم مرتبط‌اند تمرکز دارد [۷]. استفورد بیر^۴، پایه‌گذار سایبرنتیک مدیریتی، سایبرنتیک را هنر سازمان‌دهی مؤثر می‌داند [۸]. کوفینگال^۵ سایبرنتیک را هنر ایمنی‌بخش و تضمین عملیات کارآمد تعریف می‌کند؛ درحالی‌که پسک^۶ آن را هنر و علم تشخیص، یادگیری و دست‌کاری استعاره‌های^۷ قابل دفاع^۸ [۹] و به‌عبارتی همان مدل‌سازی‌های پدیده‌ها و سیستم‌ها برای شناخت، اشراف و کنترل معرفی می‌کند. ارنست ون گلیسرزفلد^۹ سایبرنتیک را هنر ایجاد تعادل در جهان محدودیت‌ها و امکان‌ها تعریف کرده است؛ همچون علم مدیریت که به‌دنبال تخصیص منابع محدود به نیازهای نامحدود و اعمال حاکمیت است [۱۰]. متیوران^{۱۰} سایبرنتیک را علم و هنر فهمیدن [۱۱] و باتکووسکی^{۱۱} آن را علمی ترکیبی از علوم کنترل، اطلاعات و سیستم‌ها [۴]، موویسیو^{۱۲} آن را نظامی از دیدگاه‌هایی که حکمران باید برای کنترل مؤثر حوزه‌اش دارا باشد [۴] و اسکات^{۱۳} آن را هنر تعامل در شبکه‌های پیچیده پویا همچون جامعه در نظر گرفته است [۱۲].

همان‌طور که از مجموعه تعریف‌ها مشخص است، تقریباً در همه تعاریف به‌نحوی به موضوع کنترل و سیستم اشاره شده است. در دانش سایبرنتیک، سازوکار سلطه بر یک پدیده یا سازوکار سلطه و اداره امور از طریق یک پدیده مورد بحث قرار می‌گیرد. این سلطه با استفاده از روش «کنترل» تحقق می‌یابد. در هریک از شاخه‌های دانش سایبرنتیک روی پدیده‌ای خاص همچون X تمرکز می‌شود و چگونگی سلطه بر X یا چیز دیگری از طریق X بررسی می‌شود. اگر X کنترل‌پذیر باشد، در این صورت امکان سلطه بر آن یا از طریق آن فراهم می‌شود. برای این منظور نیاز است که منطق حاکم بر X شناسایی شود که این دانش X -logy نام دارد و رفته‌رفته با شناخت X می‌توان سازوکارهای تحقق برای سلطه (سلطه بر X یا سلطه از طریق X (کنترل X)) را کشف کرد که در این صورت به دانش X -Cybernetics می‌انجامد. هدف نهایی این دانش سلطه است. با استفاده از این دانش می‌توان قواعدی برای سلطه بر X یا سلطه از طریق X را کشف و طراحی کرد و برای اجرا در اختیار مدیران و مجریان قرار داد. البته واژه دیگری نیز به‌صورت $Cyber-X$ به‌معنای توسعه کارکرد X از طریق فضای سایبر وجود دارد که گاهی به‌اشتباه به‌جای واژه X -Cybernetics یا بالعکس به کار برده می‌شود.^{۱۴}

1. A. Kolmogorov
2. W. Ashby
3. Gregory Bateson
4. S. Beer
5. L. Couffignal
6. G. Pask
7. Metaphors
8. Defensible
9. E. Glasersfeld
10. H. Maturana
11. A. G. Butkovsky
12. N. Moiseev
13. R. Ascott

۱۴. برای توضیح بیشتر، هنگامی که از $Cyber-Economy$ صحبت می‌شود، در واقع از قابلیت‌های فضای سایبر برای توسعه علم اقتصاد استفاده می‌شود و کلیدواژه‌هایی از قبیل رمزارز، بیمه مجازی و فینتک در این فضا متولد می‌شوند (دانش اقتصاد سایبر). درحالی‌که وقتی از $Econo-Cybernetics$ سخن به میان می‌آید که از علم اقتصاد برای تسلط و اداره امور یا از علم برای سلطه بر اقتصاد استفاده شود.



همان‌طور که اشاره شد، سایبرنتیک دانش حاکمیت بر پدیده‌ها از طریق سازوکار کنترل است و این کنترل از طریق اشراف بر جریان اطلاعات محقق می‌شود. دانش سایبرنتیک نیازمند مطالعه دو بخش در کنار یکدیگر است: بخش اول، سیستم مورد مطالعه یا کنترل‌شونده است که کنترل‌کننده تصمیم به کنترل آن دارد و بخش دوم، سیستم کنترل‌کننده که در اختیار کنترل‌کننده است. هدف به کارگیری دانش سایبرنتیک پیروی کردن کنترل‌شونده از دستورهای کنترل‌کننده است و هرچه فرمان کنترل‌کننده به میزان بیشتری اجرایی شود، قابلیت کنترل و ضریب نفوذ کنترل‌کننده بیشتر ارزیابی می‌شود. از این منظر، حکومت می‌تواند نوع خاصی از نفوذ و سلطه باشد. از طرفی هر نفوذ و سلطه‌ای الزاماً حکومت نیست و به بیانی اگر سلطه بر مبنای حکمت صورت پذیرد، نمای حکومت می‌یابد. ذکر این نکته خالی از لطف نیست که ریشه واژه لاتینی گاورنمنت^۱ (حکومت)، به واژه «کوبرنه تیس» در یونان باستان بازمی‌گردد و در واقع ریشه کلمات گاورنمنت و سایبرنتیک واژه‌ای مشترک است و هر دو به نحوه و شیوه حکومت کردن (حکمرانی)^۲ بازمی‌گردند؛ حتی قرن‌ها قبل از آنکه تکنولوژی فضای مجازی وجود داشته باشد!

دانستن این ارتباط (دانش سایبرنتیک یا به نحوی معادل دانش حکمرانی)، برای فهم چرایی آنکه حوزه فضای مجازی تا به این اندازه، حتی به اندازه انقلاب اسلامی در فرمایش‌های رهبر معظم انقلاب اسلامی (مدظله العالی)، با اهمیت دانسته شده [۱۳] و قوی شدن در آن برای کشور حیاتی برشمرده شده است [۱۴]، بسیار راهگشاست.

سایبرنتیک به واسطه برقراری ارتباطات در دنیای امروزی، قابلیت جمع‌آوری داده در ابعاد وسیع را دارد و به کمک تحلیل این داده‌ها می‌تواند اقدامات کنترلی برای رسیدن به اهداف تعریف شده بر محدوده تحت مطالعه خود را طراحی کند. با جمع‌بندی تمام نقاط اشتراک تعاریف ارائه شده از دانش سایبرنتیک توسط صاحب‌نظران این حوزه، ارکان و ابعاد دانش سایبرنتیک را می‌توان شامل چهار رکن اصلی اطلاعات، کنترل، ارتباطات و محاسبات دانست [۴ و ۱۵]. رکن اطلاعات به محتوایی اطلاق می‌شود که در فضای سایبر به گردش درمی‌آید. رکن کنترل به تغذیه هدفمند و جهت‌مند اطلاعات گفته می‌شود. رکن ارتباطات وظیفه انتقال اطلاعات را برعهده دارد و رکن محاسبات نیز به پردازش اطلاعات می‌پردازد [۲ و ۴].

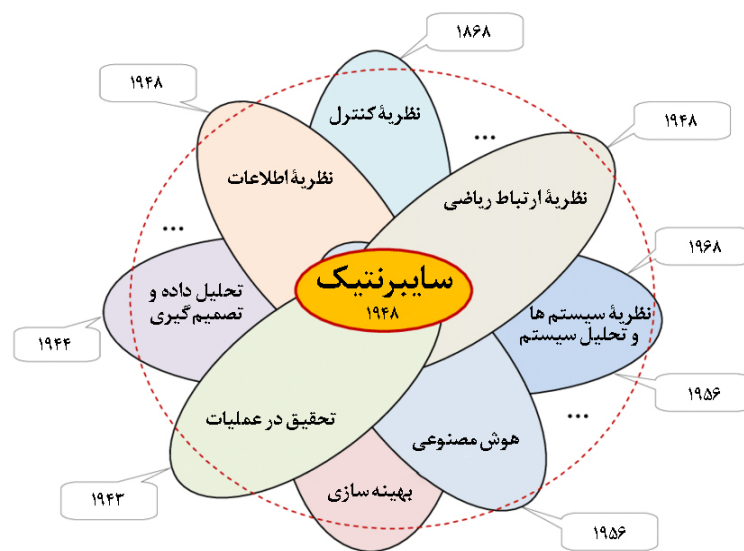
حکمرانی نیز چند ویژگی مهم دارد که در بسیاری موارد، همسویی با ارکان دانش سایبرنتیک در آن دیده می‌شود. حکمرانی غایت‌محور است و برای هدفی یا منظوری یا تحقق امری شکل می‌گیرد (هم در حکمرانی و هم در دانش سایبرنتیک، تصویرسازی و آینده‌پردازی صحیح و تعیین حالت مطلوب به منظور طرح‌ریزی و سازمان‌دهی برای رسیدن به آن اهمیت ویژه‌ای دارد). حکمرانی ویژگی هدایتگری دارد و سازوکارهایی را برای جهت‌دهی به منابع برای تحقق اهداف فراهم می‌آورد (اهمیت ارتباطات و فرمان). حکمرانی و هدایتگری به کنترل و ارزیابی مستمر نیاز دارد تا میزان انحراف از مسیر را شناسایی و اصلاح کند (اهمیت کنترل). همچنین حکمرانی نیازمند سازوکاری برای ارزیابی و اولویت‌بندی اقدامات برای تحقق بهینه اهداف است (اهمیت محاسبات، دریافت و پردازش اطلاعات). حکمرانی به مبنای متقن و دقیق و تبیین اصول و ارزش‌های اساسی نیاز دارد. حکمرانی به هم‌گراسازی و هم‌راستاسازی اقدامات برای ایجاد حداکثر هم‌افزایی و هماهنگی نیاز دارد. ویژگی و تمایز اساسی حکمرانی در این عصر ابتنا بر غرق بودن در داده و جریان تحلیل و کاوش است (اهمیت محاسبات). در واقع حکمرانی بدون داده مؤثر و مرتبط عملاً ابزاری بدون خاصیت و کور است [۱۶].

دانش سایبرنتیک به تدریج مرزهای علوم را از بین می‌برد و زمینه‌ساز پیوند آنها با یکدیگر می‌شود. این دانش می‌تواند میان علوم مختلف وحدت و یکپارچگی به وجود آورد؛ به طوری که مرزهای بین رشته‌های مختلفی همچون اقتصاد، مخابرات، جامعه‌شناسی، روان‌شناسی و... به مرور ناپدید شوند و علوم با یکدیگر ارتباط یابند. برای مثال، اگر موضوع قرارداد و معاهده‌ای، مبارزه با جرائم مالی الکترونیکی میان دو کشور باشد، به دلیل ماهیت کیفری آن، قوه قضائیه و وزارت دادگستری، به دلیل درگیر بودن زیرساخت و کاربردهای ارتباطی و فناوری اطلاعات، وزارت ارتباطات و فناوری اطلاعات، به دلیل ماهیت اقتصادی و مالی و بازرگانی، وزارت اقتصاد و دارایی یا وزارت صنعت، معدن و تجارت، به دلیل جنبه‌های امنیتی آن، وزارت اطلاعات و سایر نهادهای ذی‌ربط مانند وزارت کشور و نیروی انتظامی و به دلیل ماهیت روابط خارجی دو کشور، وزارت امور خارجه درگیر خواهند شد.

1. Government
2. Governance

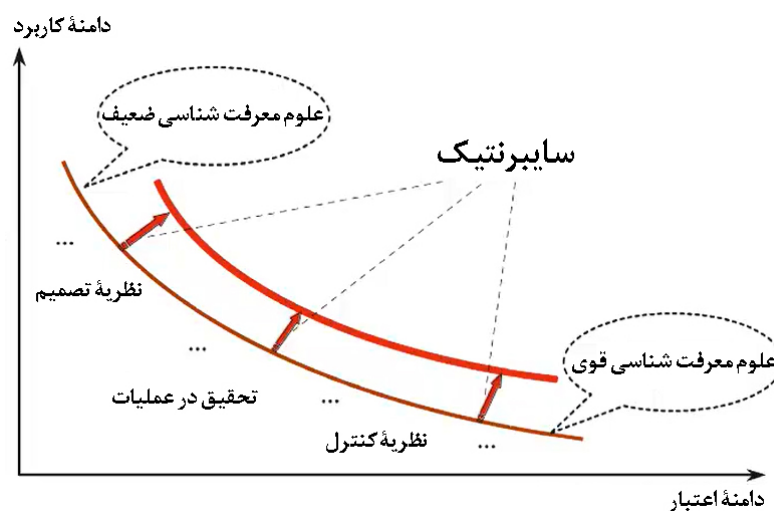
در واقع دانش سایبرنتیک دانش عظیم^۱ به هم پیوسته‌ای^۲ است که ویژگی بارز آن چندرشته‌ای^۳ و میان رشته‌ای^۴ بودن آن است. ویژگی جهان شمول بودن دانش سایبرنتیک فارغ از رشته‌ها و علوم مورد مطالعه، موضوعی است که در کتاب «سایبرنتیک از گذشته تا آینده» [۱] به صورت شکل ۱ ترسیم شده است.

شکل ۱. هم پوشانی علوم در دانش سایبرنتیک [۱]



همان طور که در کتاب «سایبرنتیک از گذشته تا آینده» [۱۷] اشاره شده است، در معرفت شناسی قوی، جواب‌ها دقیق تر و حوزه کاربرد محدودتر (اعتبار بالا) و در معرفت شناسی ضعیف، حوزه کاربرد وسیع تر و جواب‌ها مبهم تر (کاربردپذیری بالا) است. دانش سایبرنتیک با به کارگیری علوم مختلف در کنار یکدیگر می تواند نقطه آغازین برای رسیدن به جواب‌های دقیق در کنار کاربردپذیری بالا باشد و آن همان چیزی است که حکومت‌ها به دنبال پیشینه سازی آن اند تا تمام پدیده‌ها تحت فرمانشان قرار گیرد.

شکل ۲. کاربردپذیری و اعتبار در دانش سایبرنتیک [۱۵]



1. Super Science
2. Interconnected
3. Multi-Deciplinary
4. Inter-Deciplinary

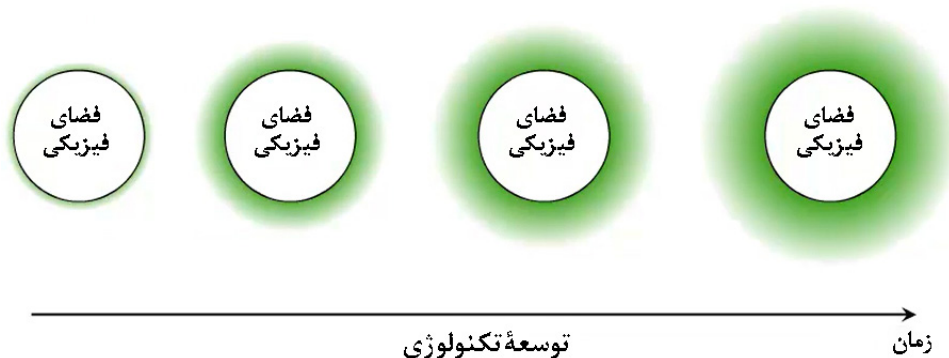
۴. فضای سایبر



پدیده‌ها به دو دسته اکچوال^۱ (پدیده‌هایی مرتبط با ماده و انرژی) و ویرچوال^۲ (پدیده‌هایی مرتبط با اطلاعات) تقسیم پذیرند. پدیده‌ها در هر فضایی، لزوماً صد درصد اکچوال یا صد درصد ویرچوال نیستند و هر پدیده می‌تواند شامل طیفی از ماده، انرژی و اطلاعات در درون خود باشد و به بیانی طیفی از اکچوال و ویرچوال را به همراه داشته باشد. گاهی به اشتباه برای جایگزین واژه «فضای سایبر»، واژه‌های «فضای مجازی» یا «فضای ویرچوال» به کار رفته و در نتیجه آشفتگی واژگانی و مفهومی ایجاد شده است. مجازی در تعبیر فارسی به معنای آن چیزی است که واقعی نیست و در مقابل واقعیت قرار دارد؛ اما اصطلاح فضای مجازی به فضایی اطلاق می‌شود که در آن اشتراک و تبادل اطلاعات و تعاملات تعداد زیادی از بازیگران و ارتباطات راه دور وجود دارد. ویرچوال در لغت به واقعیتی گفته می‌شود که غیرقابل لمس (ناملموس) است و فضای ویرچوال به فضا و واقعیت‌هایی اشاره دارد که ملموس نیستند. در حالی که فضای سایبر محدود به این موارد نیست و فراتر از ویژگی‌های اشاره شده، به فضایی گفته می‌شود که متأثر از دانش سایبرنتیک، اطلاعات در آن به منظور کنترل و سلطه بر جامعه هدف جریان داشته باشد [۲]. این فضا با آنکه محدود به کاربرست تکنولوژی نیست، ارکان آن بسیار متأثر از پیشرفت فناوری است؛ به گونه‌ای که می‌توان آن را در گذشته منطبق بر فضای فیزیکی دانست که امروزه دامنه فضای سایبر به دلیل رشد تکنولوژی در ارکان و مؤلفه‌های دانش سایبرنتیک (شامل اطلاعات، کنترل، ارتباطات و محاسبات)، گسترش یافته و به فراتر از فضای فیزیکی گام نهاده است. این فضا رفته رفته ارتباط تنگاتنگی با زندگی انسان‌ها برقرار می‌کند که با توسعه هر چه بیشتر علم و فناوری و فراگیری قدرت ارتباطی و کنترلی، هر روزه لایه‌های مختلفی از واقعیت توسط آن به نمایش گذاشته می‌شود.

در واقع فضای سایبر، فضایی دوم و مستقل از فضای فیزیکی نیست که انسان بتواند زیست جداگانه‌ای در آن داشته باشد. فضای سایبر در امتداد فضای فیزیکی قرار دارد و توانایی گسترش ظرفیت‌های فضای فیزیکی را داراست [۱۸]. بنابراین مطابق شکل ۳ فضای حکمرانی گسترش یافته امروزی در دو بخش فضای فیزیکی و فضای سایبر و مشترک میان این دو (برای نمونه سامانه‌های سایبر فیزیکی، اینترنت اشیا و سایبورگ^۳) (موجودات زنده‌ای با هر دو اجزای ارگانیکی و سایبرنتیکی) که در فضای مشترک جای خواهند گرفت قابل بررسی است.

شکل ۳. فضای گسترش یافته در طول زمان



مأخذ: یافته‌های پژوهش.

در فضای گسترش یافته، معنای قلمرو سرزمینی حاکمیت متحول می‌شود و قلمرو حاکمیت در فضای گسترش یافته علاوه بر مرزهای فیزیکی جغرافیایی به تسلط و کنترل بر فضای سایبر نیز باز می‌گردد. حکمرانی در دنیای امروزی با گسترش قلمروهای حاکمیتی، آمیخته به فضای سایبر و فناوری‌های نوظهور است و این فضا می‌تواند فرصت‌های جدیدی را برای تحقق جامعه آرمانی و تمدنی کشورها فراهم

1. Actual
2. Virtual
3. Cybernetic Organism (Cyborg)

آورد. از این رو حاکمیت در فضای سایبر به یکی از ابعاد جدید حاکمیت ملی تبدیل می‌شود و حکمرانی بر فضای سایبر، حیطه‌ای منفک از حیطه حکمرانی بر فضای فیزیکی نیست و به مرور فضای سایبر هر چه در مسیر تکاملی خویش پیش می‌رود، قلمرو حاکمیتی را بیشتر تحت الشعاع توانمندی‌های خود قرار می‌دهد و قلمروهای سرزمینی را از شخصیت کشورها می‌زداید [۱۹].

از آنجا که شالوده فضای سایبر بر ارتباطات و انتقال اطلاعات و فرامین به منظور کنترل استوار است و امروزه قابلیت تعاملات در سطح جهانی وجود دارد؛ لذا امروزه فضای سلطه و حاکمیتی فقط به مرزهای داخلی کشورها و دولت‌های حاکم بر آن محدود نمی‌شود و بازیگران خارج از سیستم‌های دولتی متعارف نیز مجال ایفای نقش خواهند یافت؛ به بیانی دیگر، در دنیای امروزی دولت‌ها تنها منبع تأمین‌کننده و تهدیدکننده امنیت نیستند. با این حال، مفهوم دولت در دنیای کنونی همچنان از نفوذ گسترده و قدرتمندی برخوردار است؛ اما باید توجه داشت که گسترش فضای سایبر با سرعت زیادی در حال وقوع است و به دلیل ویژگی‌هایی نظیر ناملموس بودن، ساختارهای غیرمتمرکز و وجود بازیگران دیگری خارج از مرزهای فیزیکی یک کشور، در آینده قدرت در یک کشور فقط محدود به دولت نخواهد بود و حکمرانی بر چنین فضایی حاکمیت‌ها را با چالش‌های جدی روبه‌رو می‌کند.

دانش بررسی این فضای گسترش یافته نیز محدود به دانش‌های خاصی چون اقتصاد، سیاست، کشاورزی یا بهداشت نیست و فضای گسترش یافته دانش مختص به خود و همه‌شمولی را طلب می‌کند؛ از این رو دانش سایبرنتیک می‌تواند به عنوان بستر و زیرساختی برای به کارگیری سایر دانش‌ها و مشرف بر آنها به شمار آید.

هر علم، فناوری یا تکنیکی نیز که به نحوی به توسعه هر یک از ارکان فضای سایبر مرتبط باشد، در حقیقت به فضای سایبر مرتبط خواهد شد. در همین راستا در کتاب «جنگ سایبری (ایجاد پایه و اساس علمی)» [۲۰]، با تمرکز بر جنبه‌های مختلف جنگ سایبری، به فنون علمی پرداخته شده است که می‌تواند برای تحلیل چالش‌های مرتبط با حوزه جنگ سایبری مانند نظریه بازی‌ها، مدل سازی شناختی، بهینه سازی، پروفایل سازی خودکار، کاوش پروفایل‌های پنهان در شبکه‌های اجتماعی و تجزیه و تحلیل داده‌های عظیم به کار روند.

۵. جایگاه سیستم‌های سایبرنتیکی در سطوح پیچیدگی سیستم‌ها

به مجموعه‌ای از اجزا، که با یکدیگر ارتباط دارند و ارتباطات میان آنها هدفمند است، سیستم می‌گویند. سیستم‌ها را می‌توان از دیدگاه‌های مختلفی، در دسته‌بندی‌های متفاوتی قرار داد:

سیستم خطی / غیر خطی؛

سیستم پویا^۱ / سیستم ایستا^۲؛

سیستم بسته^۳ / باز^۴؛

سیستم پایدار^۵ / ناپایدار^۶؛

سیستم زنده^۷ / غیرزنده^۸.

1. Dynamic

2. Static

۳. سیستم‌های بسته بیشتر به سیستم‌های مکانیکی در فیزیک و علوم تجربی اطلاق می‌شوند. سیستم‌های بسته با استفاده از نیروهای داخلی و بدون ارتباط با محیط خارج به کارشان ادامه می‌دهند و به محیط خارج از خود وابسته نیستند. سیستم‌های بسته از محیط تأثیر نمی‌پذیرند و تعاملی با محیط اطراف ندارند. سیستم‌های بسته قادر به حفظ یا کاهش سطح سازمان خود هستند.

۴. در سیستم‌های باز، برخلاف سیستم‌های بسته، هم عامل ورودی به محیط و هم عامل خروجی از محیط وجود دارد و اجزا در تعامل با محیط، خدمت ارائه می‌دهند. در نظریه سیستم‌ها فقط در صورتی افزایش نظم و کاهش آنتروپی در سیستم به وقوع می‌پیوندد که سیستم بسته نباشد و عاملی از بیرون بتواند بر آن اعمال شود.

5. Stable

6. Unstable

۷. سیستم‌هایی که می‌توانند بقای خود را حفظ کنند؛ همانند موجودات تک سلولی، گیاهان، حیوانات، انسان‌ها، سیستم‌های اجتماعی و فراتر از سیستم‌های اجتماعی.

۸. سیستم‌های غیرزنده که روابطی میان آنها شکل گرفته باشد؛ همچون موجودیت ساعت که روابط مکانیکی میان اجزای آن برقرار است یا سیستم‌های سایبرنتیک که با گردش اطلاعات در مدار، قابلیت رساندن سیستم به هدف غایی را دارند.

معمولاً در تحلیل مسائل، مشکل از آنجا آغاز می‌شود که برای افزایش کارایی یک سیستم، صرفاً بر درستی کارکرد اجزای سیستم تمرکز می‌شود و از تأثیراتی که اجزا بر یکدیگر و ساختار بر رفتار اجزا دارد و بالعکس، غفلت می‌شود. نظریه سیستم‌ها نظریه‌ای برای درک و تحلیل کلیت جهان هستی و وقایع و منظومه‌های درون آن است که توان تصمیم‌سازی، تصمیم‌گیری و کنترلگری را به شکل چشمگیری افزایش داده و به عنوان یک روش میان‌رشته‌ای تحولات زیادی را در بستر سازمان‌ها رقم زده است. این تفکر به پدیده‌ها نه به صورت فرایندی خطی، بلکه به صورت فرایندی بازخوردی می‌نگرد و برای تصمیم‌گیری از شناسایی الگوها و رویکردهای روندگرا و نه صرفاً تمرکز بر نتایج و رفتارهای اجزا و رویکردهای واقعه‌گرا بهره می‌جوید. نظریه سیستم‌ها با ایجاد تفکری کل‌نگرانه در مدیریت سازمان‌ها و کسب و کارها، نقش بسیار مهمی در پیدایش نظام سایبرنتیکی و الگوی مدیریت جامع آن داشته است. سایبرنتیک رویکردی در حوزه نظریه پیچیدگی سیستم‌هاست که براساس ارکان اطلاعات، کنترل، ارتباطات و محاسبات شکل می‌گیرد و الگویی سیستماتیک برای درک سیستم و افزایش کارایی آن به شمار می‌آید. این الگو، که بازخورد نام دارد، مفهومی زیربنایی در تفکر سیستمی و نظریه سیستم‌هاست. در حقیقت رفتار سایبرنتیکی در سازمان مشابه نگرش مدیریت سیستمی است. دانش نظریه سیستم‌ها و سایبرنتیک از نظر زمانی نیز تقریباً با یکدیگر بروز و ظهور یافته و توسعه علم در آنها با همکاری یکدیگر شکل گرفته است؛ به گونه‌ای که کاربردهای آنها در تحلیل برخی موضوعات، جدایی‌ناپذیر است. طبق طبقه‌بندی بولدینگ برای سیستم‌ها و با تأکید بر تعریف نظریه جامع سیستم‌ها [۲۱]، سیستم‌های سایبرنتیکی از نظر پیچیدگی، فراتر از محدوده سیستم‌های مکانیکی و در انتهای محدوده سیستم‌های غیرزنده و پیش از محدوده سیستم‌های زنده جای می‌گیرند

شکل ۴. جایگاه سیستم‌های سایبرنتیکی در میان سطوح مختلف پیچیدگی سیستم‌های فیزیکی [۲۱]



سیستم‌های پیچیده ویژگی‌هایی از قبیل تنوع^۱ متغیرها و تصادفی بودن^۲ دارند. با افزایش ابعاد مسئله در سیستم‌های پیچیده، دستیابی به راه‌حل‌های مواجهه با مسئله دشوارتر می‌شود و زمان یافتن راهکار برای رویارویی با سؤالات، نه به صورت خطی، بلکه به صورت نمایی افزایش می‌یابد. سیستم‌های پیچیده معمولاً سیستم‌های خطی^۳ تغییرناپذیر با زمان^۴ (LTI)^۵ نیستند و ممکن است روابط میان اجزای آنها در طی زمان تغییر یابد. شکل‌گیری علوم چندرشته‌ای و بین‌رشته‌ای همچون فیزیک اقتصاد و بیومکانیک به منظور تقابل با همین غامض بودن مسائل سیستم‌های پیچیده صورت گرفته است. یک سیستم ممکن است از نگاه کلان و با ساده‌سازی‌هایی، سیستمی ساده، و از نگاه خرد و جزئی‌نگرانه، سیستمی پیچیده به شمار آید. برای نمونه، یک میز می‌تواند با نگاهی تقلیل‌گرایانه و با در نظر گرفتن عناصر

1. Variety
2. Random

۳. سیستم‌های خطی سیستم‌هایی‌اند که خروجی‌شان برای ترکیبی خطی از ورودی‌ها برابر با ترکیبی خطی از پاسخ به تک‌تک آن ورودی‌ها باشد.
۴. سیستم‌های تغییرناپذیر با زمان نیز سیستم‌هایی‌اند که خروجی‌شان به اینکه ورودی چه زمانی اعمال شود، بستگی ندارد. به آن معنا که گذشت زمان تأثیری در جواب سیستم نداشته باشد و با هر بار دادن ورودی مشخص به سیستم، جوابی مشخص حاصل شود؛ به عبارتی با هر بار روشن شدن ماشین تراش، تراشکاری انجام شود.
5. Linear Time Invariant (LTI)

تشکیل دهنده آن از قبیل پایه‌ها، الوار و سطح شیشه‌ای میز و میخ، سیستمی ساده، و با در نظر گرفتن اجزای اتم‌های تشکیل دهنده آن، سیستمی پیچیده و زنده محسوب شود. بنابراین، تحلیل سیستم بستگی به حد در نظر گرفتن جزئیات دارد؛ از این رو می‌توان برای قدم‌های اولیه در شناخت سیستم‌های پیچیده با دید کلان به سیستم مورد نظر ورود یافت و به مرور و پس از فائق آمدن به اجزای آن، دیدی خردتر به اجزای تشکیل دهنده آن داشت. شایان ذکر است ساده‌سازی‌هایی که برای فهم راحت‌تر و توسعه علم انجام شده و می‌شود، پس از گذشت زمان به اشتباه به گزاره‌ای صحیح تبدیل نشود و سبب در نظر گرفتن جهان واقعی به شکل جهانی ساده نگردد.

مسائل دنیای واقعی فقط با یک کنترل کننده و یک کنترل شونده سروکار ندارند و چندین کنترل کننده و کنترل شونده در چیدمان‌های سلسله‌مراتبی^۱ یا چیدمان‌های متداخل^۲ دارند. تسلط بر سیستم‌های پیچیده، مستلزم به کارگیری از سیستم‌های سایبرنتیکی یا سیستم‌های سایبرنتیکی مرتبه دوم و مراتب بالاتر یا متداخل است. بنابراین در تحلیل یک سیستم این نکته اهمیت دارد که بتوان بر این پیچیدگی‌ها فائق آمد یا آنکه از آنها صرف نظر کرد؛ در حالی که به شناخت از سیستم خللی وارد نشود و کارایی روندها در آن تضمین شود.

دانش سایبرنتیک با رفتارهایی از سیستم سروکار دارد که منظم، معین و قابل بازتولید باشند. این دانش روشی علمی برای رویارویی با سیستم‌هایی است که پیچیدگی در آنها برجسته باشد و روش مؤثری برای مطالعه، شناخت و کنترل سیستم‌هایی است که پیچیدگی در آنها زیاد، اما نه به اندازه پیچیدگی موجودات زنده مختار باشد. موضوعاتی همچون هوش مصنوعی در سیستم‌های سایبرنتیکی قرار می‌گیرند که با سیستم‌هایی با ساختارهای ایستا و مکانیکی انطباق ندارند و در سیستم‌های زنده نیز جای نمی‌گیرند.

بنابراین اولین قدم در تحلیل سیستم‌ها از منظر دانش سایبرنتیک، شناسایی متغیرهای درون‌زا و برون‌زای سیستم مورد مطالعه و پس از آن تعیین مرز و مشخص کردن متغیرهای کنترل شونده و کنترلی است. شناخت زیست‌بوم مسئله و یافتن اجزا و ارتباطات و قواعدی که میان عناصر و اهمیت هر رابطه وجود دارد، مقدمه‌ای بر شناخت متغیرهای کنترلی است که تصمیم‌گیرنده از طریق آنها می‌تواند قدرت جهت‌دهی به سیستم را بیابد.

متغیر کنترل متغیری برون‌زا است که از طریق اعمال آن به عنوان ورودی به سیستم، می‌توان رفتار سیستم را تغییر داد. عامل کنترل در سیستم‌های سایبرنتیکی به صورت عامل کاهنده آنتروپی در راستای خواسته کنترل‌گر عمل می‌کند. البته باید در نظر داشت که متغیری از متغیرهای برون‌زا انتخاب شود که در دسترس باشد و قابلیت انتخاب میان حالات و گزینه‌های مختلف برای آن متغیر از سوی تصمیم‌گیرنده امکان‌پذیر باشد. با این توضیح می‌توان به چرایی اجرایی نشدن برخی از دستورهای پی برد که یا متغیرهای کنترلی مربوط به آن موضوع به درستی شناسایی نشده و اعمال قدرت بر متغیری است که نقشی در جهت‌دهی به سیستم ندارد یا آنکه در صورت تشخیص متغیر کنترلی، تأثیر قدرت کنترل‌گر به اندازه کافی نیست و اثر سایر متغیرهای کنترلی که توسط سایر صاحبان قدرت کنترل می‌شوند، نادیده انگاشته شده است. بنابراین سؤال اصلی آن است که آیا کنترل کننده در تعیین متغیرهای کنترلی خود دچار خطا شده است؟ یا تا چه حد قدرت کنترل کنترل شونده را داراست؟ هر میزان حاکمیت قدرت خود را بر تعداد بیشتری از متغیرهای کنترل حفظ کند، به گونه‌ای که سایر ذی‌نفعان امکان تغییر آنها را نداشته باشند، نفوذ قدرت و اعمال تصمیمات و رسیدن به اهداف، برای او هموارتر خواهد شد.

در ادامه می‌توان برای تحلیل سیستم‌های پیچیده از انواع مدل‌سازی‌ها فراخور هدف بهره گرفت. مدل‌سازی، تقلیدی از یک پدیده یا نظام است که به منظور درک و تحلیل ابعاد مختلف آن صورت می‌پذیرد. آزمایشگاه‌های حکمرانی به دلیل جمع‌آوری داده و تحلیل آنها از طریق تکنیک‌های علوم داده و داده‌کاوی و به دلیل استفاده از ابزارهای مدل‌سازی نظیر شبیه‌سازی، محاسبات تکاملی و بهینه‌سازی برای مشاهده نتایج اعمال ورودی بر خروجی و به دلیل بهره‌برداری از نتایج آنها در یافتن کنش مناسب در سیستم و کنترل آن، با دانش سایبرنتیک پیوند خورده است. این موضوع در شناخت هر چه بیشتر آزمایشگاه‌های حکمرانی و کاربرد آن در فضای سایبر و متقابلاً شناخت هر چه بیشتر آزمایشگاه‌های فضای سایبر و کاربرد آن در ارتقای حکمرانی کمک کننده خواهد بود.

۱. سلسله‌مراتب در کنترل وجود دارد و این چیدمان، سیستم‌های سایبرنتیکی مراتب بالاتر را شکل می‌دهد.

۲. در چیدمان‌های متداخل، ممکن است با آنکه یک سیستم کنترل کننده باشد، اما در داخل بخشی از آن، سیستم کنترل شونده دیگری وجود داشته باشد و بالعکس.

3. Data

4. Information



۶. قدرت سایبری و امنیت فضای سایبر



اگر بتوان قدرت^۱ را با «توان تحمیل اراده‌ها بر دیگری» یا «توان تغییر به‌منظور ایجاد اثر دلخواه» تعریف کرد، می‌توان ارتباط تنگاتنگ آن با موضوع کنترل را دریافت. در واقع کنترل هنگامی صورت می‌پذیرد که اراده‌ای توسط بخش کنترل‌کننده بر بخش کنترل‌شونده اعمال شود. البته قدرت به‌صورت افزایش نفوذ اراده و کاهش آسیب‌پذیری نیز تعریف می‌شود؛ به آن معنا که قدرت برگرفته از قدرت نفوذ دولت یا قدرت رهبری آن بر جهان یا قدرت نظامی یا قدرت اقتصادی و نفوذ مالی یا قدرت کشور برای تأمین نیازهای اساسی (نظیر امنیت، آموزش، سرپناه، بهداشت) یا امکانات دیگر برای افراد جامعه است. قدرت یک حاکمیت، توانایی برای انجام امور خود یا وادار کردن افراد برای انجام آن است و منابع آن می‌تواند شامل قدرت در این حوزه‌ها باشد:

۱. حوزه‌های اقتصادی،
۲. حوزه‌های اجتماعی،
۳. حوزه‌های سیاسی،
۴. حوزه‌های فرهنگی،
۵. حوزه‌های زیست‌محیطی،
۶. حوزه‌های فناوریانه،
۷. حوزه‌های فضایی،
۸. حوزه‌های نظامی-امنیتی.

قدرت از منظر صلابت قابل تقسیم به قدرت سخت (تغییر رفتار با تهدید و اجبار مستقیم و از طریق روش‌های سخت نظامی و خشونت)، قدرت نیمه‌سخت (تغییر رفتار با قوانین تشویقی و تنبیهی) و قدرت نرم (توانایی تغییر رفتار و شکل‌دهی به ترجیحات افراد از طریق اقناع یا جذابیت آفرینی و ارضا) است. قدرت پدیده‌ای متغیر و به‌شدت پویا و دارای ساختاری عمیق و چندلایه است و دگرگونی در هریک از لایه‌های قدرت سبب تغییر در ماهیت آن لایه و در نهایت قدرت کل خواهد شد. باوجود توفیق‌های بسیار خوب کشور در به‌کارگیری و خودکفایی از فناوری‌های قدرت، به‌خصوص قدرت سخت، به‌کارگیری فناوری‌های قدرت نیمه‌سخت و نرم با کاستی‌هایی روبه‌رو است. بهره‌گیری هرچه بیشتر از فناوری‌های قدرت نیمه‌سخت و نرم، موجب تصمیم‌گیری‌های دقیق‌تر، سریع‌تر و بهینه‌تر خواهد شد و قدرت کلی کشور را افزایش خواهد داد.

دانش سایبرنتیک به‌دنبال آن است که تا حد ممکن به‌صورت قدرتی غیر از قدرت سخت، سلطه خود را بر جامعه هدف خود تحمیل کند. در رکن کنترل، که از ارکان دانش سایبرنتیک به حساب می‌آید، اهداف کنترلی می‌تواند به‌صورت فعال^۲ و غیرفعال^۳ در سیستم‌ها دنبال شود. اهداف کنترل عبارت‌اند از:

۱. پایدارسازی^۴ شامل تنظیم‌گری^۵ (از طریق هنجارسازی و استانداردسازی)، جبران‌سازی^۶ و جلوگیری از انحراف، حفاظت^۷، هدایت^۸،
۲. بهینه‌سازی^۹؛
۳. اجرای برنامه‌ها^{۱۰}؛
۴. ردگیری و پیگیری^{۱۱}.

1. Power

۲. دستیابی به هدف با حفظ ساختار موجود و فقط با کمک متغیرهای کنترلی.

۳. دستیابی به هدف با تغییر ساختار موجود یا متغیرهای پیرامون سیستم و علاوه‌بر متغیرهای کنترلی درون سیستم.

4. Stabilization

5. Regulation

6. Compensation

7. Protection

8. Guidance

9. Optimization

10. Program Running

11. Tracking

تقویت دانش سایبرنتیک در سیستم‌های تحت مدیریت سبب می‌شود که تصمیمات به دلیل همراه شدن با موضوعاتی از قبیل یادگیری، تکرارپذیری و سنجش پیش از اقدام، به صورت مؤثر و کارا در دنیای فیزیکی قابل تحقق باشند و سیستم با دقت بالاتری به سوی اهداف تصمیم‌گیر حرکت کند و رفته رفته قدرت حکمران افزایش یابد. قدرت در هریک از ارکان و مؤلفه‌های فضای سایبر نیز منجر به قدرت در این فضا خواهد شد. به همین دلیل نیز هوش مصنوعی، که در محاسبات کارایی دارد و قدرت تحلیل را افزایش می‌دهد، از اجزای قدرت محسوب می‌شود. با همین استدلال، کاستی و ضعف در هریک از ارکان چهارگانه این فضا می‌تواند به نقاط ضعف برای همان رکن و سایر ارکان فضای سایبر و همچنین نقاط تهدیدی برای ضربه دیدن از سوی تهدیدکنندگان به حساب آید و خسارات قابل توجهی را به دولت‌ها وارد آورد. در این خصوص، وابستگی شدید جوامع به زیرساخت‌ها و شبکه‌های مبتنی بر فناوری اطلاعات و ارتباطات، شکل جدیدی از آسیب‌پذیری را در جامعه پدید آورده است و باعث می‌شود تا در زمان درگیری‌ها اهداف جدیدی ایجاد شوند [۲۰]. کشورهای معاند و گروه‌های تروریستی و تبه‌کار می‌توانند با ایجاد اختلال در زیرساخت‌های حیاتی یک کشور، چه در بخش‌های دولتی و چه خصوصی، از قبیل سامانه‌های حمل و نقل و کنترل ترافیک هوایی و جاده‌ای، سامانه‌های سوخت‌رسانی و توزیع انرژی از جمله خطوط گازرسانی، نیروگاه‌های برق و تأسیسات هسته‌ای، سیستم‌های مالی و بانکی، بخش‌های امداد رسانی و نهادهای آموزشی، از راه دور و بدون شلیک حتی یک گلوله، آن کشور را فلج کنند. این امر موجب شده است علاوه بر زمین، هوا، دریا و فضا، فضای سایبر نیز به عنوان حوزه نبرد جدیدی مطرح شود [۲۲]. همچنین نبود مصون‌سازی زیرساخت‌ها، دسترسی به داده‌های شخصی، افشای اطلاعات محرمانه، احتمال صورت‌نپذیرفتن صحیح محاسبات، امکان سوگیری پاسخ‌های حاصل از فناوری‌های نوظهوری همچون هوش مصنوعی، نبود مدلی متقن از مسئله، اعمال فرمان‌های نادرست به سیستم یا اعمال نشدن پس‌خور در تصمیم‌گیری می‌تواند از نقاط ضعف در این فضا به شمار آید که امنیت این فضا را خدشه‌دار می‌کند. در حال حاضر، جنگ سایبری به عنوان بخشی از خط‌مشی‌های راهبردی فناوری اطلاعات در کشورهای مختلف مطرح است. از این رو با توجه به اهمیت این دانش، ممکن است عامدانه بر دستیابی به حوزه‌های جدید و تأثیر گذار از کارکردهای این دانش محدودیت اعمال شود تا از تهدید سایر حکومت‌ها جلوگیری به عمل آید. در این راستا استقلال فناوری‌ها در فضا سایبر و بومی‌سازی آنها راهگشا خواهد بود. شایان ذکر است، نظریه‌های امنیت، ذیل نظریه‌های سیستم نمود می‌یابند و این به آن معناست که امنیت را نمی‌توان به عنوان جزئی از اجزای سیستم در نظر گرفت، بلکه شایسته است امنیت سایبر را به عنوان مفهومی بالادستی در تمام اجزای فضای سایبر لحاظ کرد (شکل ۵).

شکل ۵. جایگاه امنیت سایبر در ارکان فضای سایبر



مأخذ: یافته‌های پژوهش.

با وجود اهمیت بالای تأمین امنیت فضای سایبر در بخش‌های زیرساختی و معماری آن، امنیت فضای سایبر موضوعی فراتر از امنیت اطلاعات و امنیت شبکه است که با مسائل فناورانه و تکنولوژیکی ارتباط دارد و اگر منظور حاکمیت فقط امنیت اطلاعات و امنیت شبکه باشد، صرفاً به بخشی از امنیت فضای سایبر توجه شده است که غالباً فواید محصور است. روح حاکم بر دانش سایبرنتیک جایی است که چگونگی رسیدن از وضع موجود به وضع مطلوب در آنجا طرح‌ریزی می‌شود؛ وضع مطلوب در هر جامعه نیز با توجه به خواست و هدف و ارزش جمعی آن جامعه تعیین می‌شود. بنابراین تعیین منفعلانه وضع مطلوب یک جامعه یا تلاش برای ارتقای رتبه در شاخص‌هایی جهانی که درباره اتخاذ آنها به عنوان شاخص‌های کلیدی آن جامعه، مطالعات و بررسی پیشینی صورت‌نپذیرفته است، می‌تواند از موضوعاتی باشد که در صورت کاربریست دانش سایبرنتیک توسط دیگران، جامعه را به جهت مدنظرشان سوق دهد و امنیت آن را به مخاطره اندازد. برقراری بستر امن



در فضای گسترش یافته سایبر به تمام ارکان و فرایندهای این فضا، حتی به تعیین ارزش‌ها، اهداف و آرمان‌های سیستم تحت مطالعه و نحوه تصمیم‌گیری سیستم وابسته است و خلل در هر یک از این بخش‌ها، به امنیت فضای گسترش یافته خدشه وارد می‌کند. بنابراین لازم است برای تأمین امنیت به تمام زیست‌بوم فضای سایبر توجه شود.

۷. حدود دانش سایبرنتیک



دانش سایبرنتیک و فلسفه مدیریت، از شاخه‌های کاربردی نظریه کنترل محسوب می‌شوند؛ به‌طوری‌که مباحث حوزه کنترل و حوزه مدیریت، ارتباط تنگاتنگی با یکدیگر دارند و کنترل یکی از قدم‌های مهم در اصول مدیریت کلاسیک (از میان قدم‌های برنامه‌ریزی، سازمان‌دهی، هماهنگی، رهبری و کنترل) به شمار می‌آید [۲۳ و ۲۴]. تصور از قابلیت‌های این دانش به حدی است که امروزه استفاده از دانش سایبرنتیک در پدیده‌های شناختی و روان‌شناختی برای کنترل و مدیریت جوامع انسانی و سلطه بر حاکمیت‌های محلی، بستر ساز رسیدن به نظم نوین جهانی مورد نظر نظام سلطه و مفهوم جهان تک‌حکومتی در جهان امروزی شده است.

با تحلیل اطلاعات کاربران در فضای سایبر می‌توان گروه‌های اجتماعی مخالف و خاص در هر کشوری را شناسایی و سپس بر آنها برای پیشبرد اهداف تصمیم‌گیران سرمایه‌گذاری کرد. همچنین می‌توان با جریان‌سازی در فضای سایبر، رویکردهایی را به نفع گروه‌های سیاسی خاص یا اجتماعی را برای تأثیرگذاری بر روندهای جامعه تغییر داد. تحلیل کلان‌داده‌ها، توانایی افکارسازی در شبکه‌ها و رسانه‌های اجتماعی را به صورت هدفمند و با هدف کاهش ضریب خطای پیش‌بینی و نتایج ناخواسته افزایش می‌دهد [۲۵].

تحلیل داده‌های مرتبط به منظور خوشه‌بندی و دسته‌بندی گروه‌های مرجع و شناسایی مسائل و دغدغه‌های اجتماعی، سیاسی و اقتصادی بر اساس موقعیت‌های جغرافیایی و مناسبات قومیتی و کشف ذائقه‌ها و بافتن فرایند تفکر، می‌تواند توانایی تغییر ارزش‌های جامعه، سبک زندگی، اعتقادات، انگیزه‌های دینی، سیاسی و اقتصادی و به معنای دقیق‌تر فرهنگ جامعه را افزایش دهد. امروزه با خلأهای حکمرانی بر فضای سایبر، غالباً هدایت و مدیریت فرهنگی جوامع از اختیار حاکمیت‌های ملی خارج، و به موضوعی فراملی و فراحاکمیتی تبدیل شده است [۲۵].

امروزه پا از این موضوعات فراتر گذاشته شده است و تلاش می‌شود از دانش سایبرنتیک برای کنترل اذهان انسان‌ها استفاده شود. ردپای قدم‌های ابتدایی این کنترل را می‌توان در شکل‌گیری سیستم‌های اعتبار اجتماعی^۱ مشاهده کرد [۲۶] که سعی شده است با امتیازدهی فعالیت‌های انسانی در جامعه، نظارت^۲ بر جامعه و تصمیم‌گیری درباره افراد صورت پذیرد. ایده‌پردازی در استفاده از این دانش تا آنجا پیش می‌رود که گروهی از انسان‌ها بتوانند بر نحوه تفکر سایر انسان‌ها با ابزارهای سخت یا نرم، کنترل یابند و آنها را در حوزه شناختی دچار اختلال کنند (جنگ‌های شناختی رسانه‌ای^۳ می‌توانند در دسته ابزارهای نرم قلمداد شوند).

همان‌طور که قبلاً اشاره شد، انسان سیستمی پیچیده محسوب می‌شود که همچنان قادر به شناسایی تمام ابعاد وجود خود نیست. شناخت ناقص از تمام ابعاد انسان، سبب شناخت ناقص متغیرهای درونی و بیرونی و پیرو آن شناخت ناقص متغیرهای کنترلی می‌شود. بنابراین قضاوت‌های ناقصی از رفتارهای انسان شکل می‌گیرد که تصمیمات اتخاذ شده بر اساس این قضاوت‌ها و بدون تصمیم‌گیرنده انسانی و ملاحظات انسانی، به خطا خواهند رفت.

پاسخ به آن دسته از پرسش‌هایی که آیا کاربست دانش سایبرنتیک روزی به جایگاهی خواهد رسید که انسان قدرت کنترل بر تفکر انسان دیگری را داشته باشد؟ یا آیا این دانش اجازه حذف کردن موجودات زنده‌ای را که از منظر متغیرهای عملکردی (برای مثال در سیستم‌های ارزیابی اعتبار اجتماعی افراد)، رتبه قابل قبولی ندارند و برای سیستم مورد مطالعه هزینه‌زا هستند، خواهد داد یا خیر؟ و آیا این گونه اقدامات در دنیای آینده، پذیرفته شده خواهد بود یا خیر؟ نگرانی از آینده جهان را صرفاً با چنین نگاه‌های به‌ظاهر منطقی افزایش می‌دهد.

1. Social Credit System

2. Monitoring

۳. هدف جنگ شناختی رسانه‌ای، تهاجم به باورها و از بین بردن امیدها، نیروها و سرمایه‌ها (از قبیل اجتماعی، سیاسی و مالی) و شکست دشمن از طریق از بین بردن اعتماد ملت‌ها به نسبت به حاکمیت‌ها و نهادهای سیاسی و مشروعیت‌زدایی از آنهاست.

در اندیشه قرآنی، همان گونه که در آیه ۳ سوره شریفه اعلی «وَالَّذِي قَدَّرَ فَهَدَى»؛ «همان کسی که اندازه گرفت و سپس هدایت کرد» آمده، به اهمیت اندازه گیری و برنامه ریزی برای هدایت جامعه اشاره شده است؛ اما همچنین در آیه ۲۵۶ سوره شریفه بقره «لَا إِكْرَاهَ فِي الدِّينِ قَدْ تَبَيَّنَ الرُّشْدُ مِنَ الْغَيِّ فَمَنْ يَكْفُرْ بِالطَّاغُوتِ وَيُؤْمِنْ بِاللَّهِ فَقَدْ اسْتَمْسَكَ بِالْعُرْوَةِ الْوُثْقَى لَا انْفِصَامَ لَهَا وَاللَّهُ سَمِيعٌ عَلِيمٌ»؛ «در دین هیچ اجباری نیست. راه از بیراهه به خوبی آشکار شده است. پس هر کس به طاغوت کفر ورزد و به خدا ایمان آورد، به یقین به دستاویزی استوار، که آن را گسستن نیست، چنگ زده است و خداوند شنوای داناست» بیان شده است که مابه ازای کارکرد نهایی سایبرنتیک در تمدن غرب در حوزه شناختی برای حکمرانی در اسلام، پذیرفته شده نیست. در اندیشه قرآنی مفهوم حاکمیت به این معناست که روش زندگی انسان ها به اختیار و خواست خود آنها صورت می پذیرد و رفتارهای انسان ها و به خصوص حاکمیت در حوزه شناختی متأثر از اقناع و اغوا و در راستای اجرای خواسته ها و تمایلات حاکمان نیست. حکومت در اندیشه اسلامی، جایگزینی عالی تر نسبت به مفهوم سایبرنتیک (فضای کنترل) خواهد بود و در آن اختیار از انسان ها سلب نمی شود. امروزه اشراف دانشی انسان ها همچنان بر سیستم های زنده وجود ندارد و از این رو در تقسیم بندی های سیستم ها، تسلط بر سیستم های بیولوژیکی و اکولوژیکی و فراتر از آن برای انسان مقدور نیست. البته در قرآن به صورت تلویحی به این نکته اشاره شده است؛ آنجا که در آیه ۸۵ سوره شریفه اسراء بیان می دارد: «وَيَسْأَلُونَكَ عَنِ الرُّوحِ قُلِ الرُّوحُ مِنْ أَمْرِ رَبِّي وَمَا أُوتِيتُمْ مِنَ الْعِلْمِ إِلَّا قَلِيلًا»؛ «و درباره روح از تومی پرسند بگو روح از [سنخ] فرمان پروردگار من است و به شما از دانش جز اندکی داده نشده است». مطلبی که امکان شناخت کامل و تسلط انسان بر بُعد روحانی خویش را غیر ممکن می داند که به معنای ناتوانی انسان در تسلط بر خود و ناکارآمدی دانش سایبرنتیک در حوزه شناختی موجودات زنده است.

به طریقی دیگر در آیه ۷۳ سوره شریفه حج «يَا أَيُّهَا النَّاسُ ضَرْبٌ مَثَلٌ فَاسْتَمِعُوا لَهُ إِنَّ الَّذِينَ تَدْعُونَ مِنْ دُونِ اللَّهِ لَنْ يَخْلُقُوا ذُبَابًا وَلَوْ اجْتَمَعُوا لَهُ»؛ «ای مردم مثلی زده شده است گوش به آن فرا دهید، کسانی را که غیر از خدا می خوانید هرگز نمی توانند مگس بیافرینند هر چند برای این کار دست به دست هم بدهند»، به ناتوانی مخلوقات در آفرینش اشاره شده است. امام علی (ع) نیز در خطبه ۱۸۶ نهج البلاغه می فرماید: «وَلَوْ اجْتَمَعَ جَمِيعُ حَيَوَانِهَا مِنْ طَيْرِهَا وَبَهَائِمِهَا... وَأَجْناسِهَا وَمُتَبَدِّلَةِ أَمَمِهَا، وَآكِيَسِهَا، عَلَى أَحْدَاثٍ بَعُوضَةٍ مَا قَدَّرَتْ عَلَى إِحْدَاثِهَا، وَلَا عَرَفَتْ كَيْفَ السَّبِيلِ إِلَى إِجَادِهَا، وَتَحْخَرَتْ عُقُولُهَا فِي عِلْمِ ذَلِكَ»؛ «اگر همه موجودات زنده جهان، اعم از پرندگان و چهارپایان... و تمام انواع گوناگون جانداران، اعم از آنها که کم هوش اند و آنها که زیرک و باهوش اند، همگی گرد آیند، هرگز قدرت بر ایجاد پشه ای را ندارند؛ هیچ گاه طریق ایجاد آن را نتوانند شناخت و عقول آنها در راه یافتن به اسرار آفرینش این موجود حیران می ماند».

بنابراین آنچه از ادبیات دینی استنباط می شود، آن است که انسان با به کارگیری دانش سایبرنتیک هیچ گاه به تمامی بر سیستم های زنده و بیولوژیکی سلطه نخواهد یافت. انسان نیز موجودی زنده است و موجودات زنده با درجه بالایی از پیچیدگی و عناصر و روابط متنوع، فراتر از سیستم های سایبرنتیکی قرار می گیرند؛ بنابراین دامنه اشراف دانش سایبرنتیک به سلطه بر انسان نمی انجامد و توانایی های کنترلی برای انسان فقط در سطح سیستم های سایبرنتیکی محدود می شود. تاکنون نیز هیچ سیستم زنده ای توسط انسان به طور کامل تحت کنترل قرار نگرفته یا ساخته نشده است. انسان تاکنون توانسته است فقط با انجام اقداماتی همچون دست کاری ژنتیکی، روی موجودات زنده تغییر ایجاد کند. در ادبیات دینی ادعای کارکرد بی نقص دانش سایبرنتیک در کنترل موجودات زنده بی معناست و در نتیجه اتکای بی چون و چرا بر کاربری دانش سایبرنتیک برای کنترل سیستم های بیولوژیکی و اکولوژیکی، همواره به راه حل بهینه و صحیح منتج نمی شود.

شایان ذکر است که حکمرانی با فضای سایبر و اشراف بر دانش سایبرنتیک، به معنای قبول تمام اصول و اتکای محض به آن در تمام ابعاد حکمرانی نیست. همانند اشراف بر دانش مکانیکی که به معنای داشتن دید مکانیکی به تمام اجزای عالم و واگذار کردن تمام ساز و کارهای حکمرانی بر آنها نیست. تسلط بر دانش مکانیکی و به کارگیری آن در علوم فنی - مهندسی به منظور توانمندسازی و رشد کشورها کاملاً قابل پذیرش است؛ همان طور که دامنه بهره گیری از دانش مکانیک در محدوده سیستم های مکانیکی تعریف می شود، دامنه بهره گیری از دانش سایبرنتیک نیز در محدوده سیستم های سایبرنتیک خواهد بود و نمی توان انتظار اثربخشی این دانش را در سیستم های بیولوژیکی و اکولوژیکی داشت. از طرفی همان طور که استفاده نکردن از دانش مکانیکی در محدوده سیستم های مکانیکی منجر به عقب افتادگی فاحش کشور در سیستم های مکانیکی همچون صنایع خودروسازی و ساختمان سازی خواهد شد، بهره مند نشدن از دانش سایبرنتیک در سیستم های سایبرنتیکی نیز به ضعف کشور در نظام هایی همچون سیستم تولید و توزیع دارو و انرژی خواهد انجامید. اهمیت دانش سایبرنتیک در حکمرانی به دلیل بهره گیری از قابلیت های آن در راستای تصمیم گیری سنجیده و چابک در امور اجرایی کشور (نظیر مدیریت منابع آبی،



تخصیص ارز، کاهش آلاینده‌گی، کاهش اتلاف منابع و بهینه‌سازی انجام فعالیت‌ها) بر مبنای اصول اخلاقی و انسانی مطرح شده در اندیشه دینی و فرهنگ ملی و با هدف پیشرفت جامعه و تحقق بخشیدن به آرمان‌های آن و خنثی نمودن تهدیدات احتمالی دشمنان است؛ دشمنانی که تلاش دارند از این فضا برای نفوذ و اعمال اراده خود بر ملت‌ها استفاده کنند.

بنابراین به کارگیری دانش سایبرنتیک در مسائل مدیریتی، در حال حاضر بالاترین سطح از تلاش انسانی در به کارگیری تمام توانمندی‌های او برای رویارویی با مسائلی در سطح سیستم‌های سایبرنتیکی است و راه‌حل پیشنهادی این دانش فقط با توجه به اقتضائات علم موجود صورت پذیرفته است. به بیانی دیگر، کاربرست دانش سایبرنتیک در شرایط کنونی، کامل‌ترین ساختار موجود برای حل مسئله و نه الزاماً ساختاری کامل و مفید برای حل آن است.

۸. تعاملات حکمرانی و فضای سایبر



به دلیل ماهیت تغییراتی که توسط فناوری‌های ارتباطاتی و محاسباتی در حال شکل‌گیری است، فضای زیستی به صورت فضایی توسعه‌یافته و ترکیبی از فضای فیزیکی و فضای سایبر درآمده است. در دنیای امروزی، روش‌های سنتی حکومت کردن که صرفاً قابل اجرا و استوار بر فضای فیزیکی‌اند، به تدریج سست می‌شوند. حاکمیت ملی در آینده به فضای سایبر، که به طور مداوم در حال گسترش است، تسری خواهد یافت. در این فضا تعداد فزاینده‌ای از بازیگران خارج از مرزهای رسمی کشور در فرایند اداره کردن دولت حضور خواهند داشت که می‌توانند شبکه‌ای از بازیگران به هم مرتبط و چندسطحی را تشکیل دهند. این فضای توسعه‌یافته جدید، روش‌های ارتقایافته جدیدی را برای حاکمیت بر خود مطالبه می‌کند.

در فضای گسترش‌یافته، معنای قلمرو سرزمینی متحول می‌شود و قلمرو حاکمیت در این فضا علاوه بر مرزهای فیزیکی جغرافیایی به تسلط و کنترل بر فضای سایبر نیز بازمی‌گردد؛ بنابراین هرگونه ضعف در این فضا، حاکمیت ملی را به خطر خواهد انداخت و هرگونه اهمال و کوتاهی در قدرتمندی در این زمینه، مترادف با کاهش قلمرو کشور به حساب خواهد آمد و از دست دادن قدرت و نفوذ در این فضا به اندازه از دست دادن خاک کشور دردناک خواهد بود.

این گزارش، نقطه کلیدی در تصمیم‌گیری صحیح در فضای سایبر را بر خورداری از دیدگاه و تعریفی صحیح از فضای سایبر می‌داند. نبود تعریفی جامع و صحیح از فضای سایبر یکی از علل نابسامانی در خط‌مشی‌گذاری صحیح در فضای سایبر است. برداشت‌های متعدد و گاه مبهم از مفهوم فضای سایبر، خط‌مشی‌ها و تصمیمات گاه متناقض را در پی خواهد داشت. از این رو گزارش تلاش کرده است در گام نخست با تبیین فضای سایبر و ارائه تعریفی همه‌شمول از آن و ارائه قابلیت‌ها و محدودیت‌های این فضا برای رویارویی با مسائل پیچیده حکمرانی، در جهت شفاف‌سازی نگاه تصمیم‌گیر گام بردارد. در ادامه این گزارش در راستای انتظام‌بخشی به خط‌مشی‌های فضای سایبر، تعاملات حیطة حکمرانی و فضای سایبر را در سه حیطة حکمرانی بر فضای سایبر، حیطة حکمرانی با فضای سایبر و حیطة ارتباطات متقابل آن دو قابل بررسی می‌داند.

حکمرانی بر فضای سایبر به معنای حکمرانی و اعمال قدرت بر هریک از مؤلفه‌های این فضا شامل اطلاعات، کنترل، ارتباطات و محاسبات است [۱۵]. حکمرانی بر فضای سایبر غالباً معادل حکمرانی بر زیرساخت‌های فضای سایبر (در بخش‌های اطلاعاتی، ارتباطاتی، محاسباتی یا امنیتی) در نظر گرفته شده است و قانونگذاران بیشتر به وضع قوانین و مقررات برای نظارت بر کارکرد مؤلفه‌های فضای سایبر بالاخص در حوزه فاوا پرداخته‌اند.

به دلیل ابعاد مختلف زیرساختی در فضای سایبر از قبیل کلان‌داده‌ها^۱ و اطلاعاتی که از تحلیل آنها ظهور می‌یابند، نحوه دسترسی به داده یا تبعیض در دسترسی به آنها، فضای ذخیره ابری و رایانش ابری، که به منظور نگهداری اطلاعات و تسهیل محاسبات، چه در بخش کنترل‌کننده و چه در بخش کنترل‌شونده، توسعه یافته‌اند، توسعه الگوریتم‌های محاسباتی، هوش مصنوعی، سیستم‌عامل‌ها

و فناوری‌های ارتباطاتی، شاخه‌های مختلفی از حاکمیت نیز از قبیل حاکمیت داده و اطلاعات، حاکمیت فضای ذخیره داده و فضای الکترومغناطیسی و حاکمیت فناوری ارتباطاتی شکل گرفته است. البته که درباره شاخه‌ها و اشکال حاکمیت بر فضای سایبر (حاکمیت فضای سایبر) و تنظیم روابط موجود در آن، دیدگاه‌های متفاوتی در میان کشورهای گوناگون وجود دارد که قابل بحث است؛ اما هدف غایی هریک از دیدگاه‌های مرتبط با حکمرانی بر فضای سایبر، کاهش، مهار یا اجتناب از تهدیدات و استفاده هرچه بیشتر از قابلیت‌های این فضا است.

موضوعاتی که به تصمیم‌گیری در مواجهه با فضای سایبر شناخته می‌شوند، معمولاً با زمینه‌سازی و پیاده‌سازی، ایجاد استانداردها، قوانین، سازمان‌دهی، هماهنگی و فرهنگ‌سازی در جنبه‌های زیرساختی این فضا مرتبط‌اند. در حال حاضر، به‌منظور حفاظت از فضای سایبر اقدامات مختلفی از قبیل وضع مقررات و هنجارهای قانونی برای ذخیره‌سازی داده و نحوه دسترسی به آن و رایانش ابری، نظارت بر شبکه‌های اجتماعی، نظام‌مندسازی صنعت محتوای اینترنتی، جلوگیری از انتشار اطلاعات ناهنجار و تبهکارانه، حفاظت از داده‌های شبکه، سنجش امنیت شبکه، حفظ حریم خصوصی، مالکیت فکری، مقابله با خرابکاری‌ها و سرقت اطلاعات، مقابله با جرائم بانکی در این فضا، حفاظت نظامی، سامان‌دهی خدمات میزبانی، پشتیبانی فنی، گسترش همکاری‌های بین‌المللی و تعاملات به‌هم‌پیوسته و مشترک، و آموزش صورت می‌پذیرد.

حکمرانی با فضای سایبر نیز به‌معنای اعمال حاکمیت از طریق هریک از مؤلفه‌های فضای سایبر نظیر اطلاعات، کنترل، ارتباطات و محاسبات است. غالباً در حکمرانی با فضای سایبر، فضای مجازی به‌صورت یک ابزار و قابلیت در نظر گرفته می‌شود که می‌تواند گستره و عمق امکانات دولت‌ها را تغییر دهد و فرصت‌های بدیعی را بیافریند [۱۵]. در حکمرانی با فضای سایبر همگام با توسعه فناوری‌ها، حاکمیت برای انجام وظایف و پیگیری اوامر خود از قابلیت‌های فضای سایبر مدد می‌جوید و با انتقال سریع اطلاعات، تسهیل در گردآوری اطلاعات و ابلاغ آنی دستورها، مدت‌هاست زمینه‌سازی برای حضور قابل لمس خود را در فضای سایبر آغاز کرده است. میزان پیشرفت حکمرانی با استفاده از قابلیت‌های ابزاری فضای سایبر را می‌توان از میزان تحقق دولت الکترونیک در لایه‌های مختلف برآورد کرد. در این رویکرد توسعه فناوری‌های اطلاعاتی و ارتباطاتی، به‌عنوان هدف در نظر گرفته می‌شود.

از این‌رو، در دورانی که با حجم زیادی از اطلاعات همراه شده، موضوعاتی همچون حکمرانی با داده و محاسبات که با تحلیل داده، داده‌کاوی، پردازش زبان طبیعی، هوش مصنوعی و کاربرد آن در شناسایی مشکلات و ارائه راه‌حل‌ها مرتبط است، صدور اینترنتی مجوزها، سامانه‌های خدمات‌رسانی برخط، آموزش از راه دور، توسعه شبکه‌های اجتماعی بومی، سامانه‌های ارزشیابی و رصد فساد و درنهایت بروز و ظهور دولت الکترونیک در حیطه حکمرانی با فضای سایبر جای می‌گیرند.

مرور اسناد مصوب مرتبط با حکمرانی با فضای سایبر نشان از آن دارد که قانونگذاران اغلب به وضع قوانین و مقررات برای استفاده از قابلیت‌های این فضا به‌ویژه ارتباطات و فناوری اطلاعات در تسهیل وظایف حاکمیت در ارائه خدمات به شهروندان پرداخته‌اند و از دیگر مؤلفه‌های فضای سایبر غفلت شده است. به بیانی، حکمرانی با استفاده از قابلیت‌های ابزاری فضای سایبر قسمی از حکمرانی با فضای سایبر است که معادل حکمرانی با فضای مجازی و به‌معنای دقیق‌تر حکمرانی با ابزارهای فضای سایبر و بدون کاربست معنا و روح این دانش در حکمرانی است.

در حکمرانی با فضای سایبر و با استفاده از کاربست دانش سایبرنتیک، توسعه فناوری‌های اطلاعاتی و ارتباطاتی، نه به‌عنوان هدف، بلکه به‌عنوان تسهیلگر برای مدیریت و جهت‌دهی جامعه نقش‌آفرینی می‌کند. مرور اقدامات صورت‌گرفته، بیشتر نشان از مواجهه و رویکرد انفعالی کشور در این زمینه دارد که اغلب از فقدان شناخت کافی از دانش سایبرنتیک و قابلیت‌های فضای سایبر ناشی می‌شود. در ادامه راهکارهایی با توجه به ظرفیت‌های عرصه قانونگذاری برای بهبود حکمرانی در مواجهه با فضای سایبر به‌منظور حفظ حاکمیت ملی و ارتقای قدرت در این فضا ارائه می‌شود.

۹. جمع‌بندی و نتیجه‌گیری

۹-۱. پیشنهادها در راستای ارتقای حکمرانی بر فضای سایبر

۱ کارکرد فضای سایبر با فرض تمایل حضور کاربران در فضای سایبر است. از آنجایی که فضای سایبر، فضایی کنترلی است، حضور انسان در این فضا با روحیه آزادی‌خواهانه او در تعارض است؛ لذا باورمند به این فضا و اعتماد به آن، عامل بسیار مهمی برای تمایل افراد جامعه به ورود به این فضا به‌شمار می‌رود. تمایلی که به‌دلایل: الف) ضرورت حضور آنان نظیر وابستگی به خدمات فضای سایبر (همچون اشتراک‌گذاری محتوا میان تعداد زیادی از کاربران و با سرعت بالا) یا ب) جذابیت حضور ناشی از اعتماد، امنیت و تجربه خوب شکل می‌گیرد. هرچه اعتماد کاربران به اثربخشی فضای سایبر بیشتر شود، میزان حضور آنان در این فضا افزایش می‌یابد. اطمینان‌بخشی به کاربران از افشا نشدن اطلاعات آنان و اتخاذ رویکردهای حفظ حریم خصوصی، می‌تواند به رفع نگرانی‌ها و ارتباط بیشتر آنان با این فضا بینجامد. در این راستا قاعده‌مندسازی دسترسی به داده‌های خصوصی، عمومی و کلان‌داده‌ها و اعمال حاکمیت و حفاظت از امنیت داده‌های ملی و دولتی (دولت الکترونیک) در برابر نفوذ و دست‌اندازی غیرمجاز، حفاظت از امنیت اطلاعات شخصی کاربران و حفاظت از حریم خصوصی، امضاهای الکترونیک و شواهد الکترونیکی مؤثر خواهد بود. یکی از اقدامات در این زمینه می‌تواند تصویب قانون حمایت از داده‌های شخصی و حفاظت از حریم خصوصی باشد.

۲ احساسات، راحتی، رضایت و به‌طور کلی تجربه خوب کاربران از فضای سایبر نیز عامل مهم دیگری است که به انگیزه کاربران برای حضور در فضای سایبر منجر می‌شود. استفاده از اجزای مناسب در طراحی فضای سایبر^۱، به‌نحوی که تأمین‌کننده نیازهای کاربران و ایجادکننده تجربیات خوب باشند^۲، می‌تواند به این امر کمک کند. برای نمونه، تولیدات باکیفیت محتوا در ایجاد تجربه بهتر کاربران مؤثر است یا ایجاد سند صیانت از کودکان و نوجوانان در فضای مجازی به‌منظور حفاظت از آنان در شبکه را می‌توان از اقدامات انجام شده در این راستا نام برد.

۳ امنیت حضور در فضای سایبر همانند امنیت حضور در فضای فیزیکی موضوع دیگری است که افراد را به ورود و فعالیت در این فضا تشویق می‌کند. وجود قوانین حقوقی و کیفری فعالان در خصوص حمایت از عرضه‌کنندگان کالا و خدمات (نظیر نحوه رسیدگی به شکایات تولیدکنندگان محتوا از نقض حقوق تکثیر محتوای تولید شده یا نحوه پیگیری کارآفرینان در مواجهه با سوءاستفاده از اطلاعات) و همچنین حمایت از مصرف‌کنندگان و کاربران این فضا، می‌تواند به رونق کسب‌وکارهای قابل شکل‌گیری در فضای سایبر همچون سکوها و پیاده‌سازی هرچه بیشتر دولت الکترونیک کمک کند.

۴ قوانین و مقررات وضع شده باید ملزومات امنیت‌بخشی به زیرساخت‌های فضای سایبر را برای فعالان این فضا فراهم آورد. اعتماد کاربران به زیرساخت‌های این فضا، موجب مشارکت آنان در این فضا، رونق و وسعت فضای گسترش‌یافته خواهد شد. ایجاد چارچوب قضایی فضای سایبر، به‌گونه‌ای که موضوعاتی همچون مدیریت اطلاعات اینترنتی، مدیریت شبکه‌های اجتماعی، حفاظت از امنیت سامانه‌های اطلاعاتی و ارتباطی در برابر رخنه در شبکه، مقابله با جرائم سایبری (جاسوسی، تخریب و...)، مدیریت نام دامنه، دفاع از کاربران شبکه در برابر مسائل نوپدید، حفاظت از امنیت سامانه‌های کنترل صنعتی و تجارت الکترونیک، دفاع از مالکیت فکری و سایر حوزه‌ها را دربر گیرد و برای هریک از موضوعات، قوانین و مقررات مورد نیاز تهیه و تدوین شود، کمک‌کننده خواهد بود. در این راستا، اصلاح برخی مفاد قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای یا تصویب قانون جامع حقوق (و وظایف) عرضه‌کنندگان خدمات فناوری اطلاعات و سکوها یا اصلاح برخی مفاد قانون جرائم رایانه‌ای می‌تواند راهگشا باشد.

۵ استقلال فناوری‌ها در فضای سایبر و بومی‌سازی آنها به‌منظور امنیت بخشیدن به این فضا راهگشاست. اختصاص بودجه یا تسهیلگری قوانین و مقررات در راستای فعالیت سازمان‌ها، شرکت‌ها و کسب‌وکارهای مرتبط با فضای سایبر با اولویت شرکت‌های نوآور دانش‌بنیان، می‌تواند به تمایل حضور آنان و رونق بخشی فضای سایبر و پیشرفت کشور در این فضا کمک‌کننده باشد.

۶ شکل‌گیری فناوری‌های جدید و توسعه کاربردهای آن در سالیان اخیر در زندگی روزمره و در بخش‌های مختلفی نظیر صنعت، کشاورزی و کسب‌وکار، نشان از روند پویای فضای سایبر دارد که با وجود اقدامات شایان برای قانونگذاری، به دلیل چابکی این فضا و سرعت بالای توسعه فناوری‌ها، وضع برنامه‌ها و قوانین در فضای سایبر، فاصله موضوعی و زمانی قابل ملاحظه‌ای با نیازهای جامعه دارد. برای نمونه، یکی از این فاصله‌های محتوایی و زمانی را می‌شود در نبود تناسب میان آموزش نیروی انسانی با نیاز کنونی بازار کار مشاهده کرد. نمونه دیگر خلأها و کاستی‌هایی است که در سازوکارهای قانونی و نظارتی برای جلوگیری از فساد در زنجیره تأمین داده وجود دارد که همچنان جامعه با سوءاستفاده در داده دست به گریبان است. نمونه بعدی ضوابط و قوانین مربوط با نحوه تعامل جامعه در مواجهه با فناوری‌های جدید نظیر خودروهای هوشمند و پزشکی هوشمند است و پاسخ به پرسش‌هایی همچون آنکه در صورت وقوع خطا مسئولیت برعهده چه شخصی خواهد بود؟، با ابهام روبه‌روست. نمونه دیگر در تنظیم مقررات سکوها و تغییر مناسبات اجتماعی، ارزش‌ها و هنجارها توسط آنهاست که نیاز است با دقت و سرعت بیشتری تعاملات کشورها، سازمان‌ها و اشخاص با سکوهای ملی و فراملی مشخص شود؛ درحالی‌که برای پاسخ به سؤالاتی از قبیل آنکه: اگر کاربری در یک کشور در هنگام ارسال و دریافت داده از سکوهای کشورهای دیگر استفاده کند، لازم است از قوانین کدام کشور پیروی کند؟ و آیا آنکه سکوها تا چه حد حق بهره‌مندی از داده‌های کاربران خود را خواهند داشت؟، زمان قابل توجهی گذشته است.

این فاصله محتوایی و زمانی قانون با نیازهای جامعه، که غالباً از رویکرد دو فضایی و نه رویکرد امتدادی به فضای سایبر ناشی می‌شود، گاهی به حدی می‌رسد که به دلیل نبود قانون و دستورالعمل‌های کافی نمی‌توان درباره درستی یا نادرستی موضوعات رخ داده در فضای سایبر قضاوتی انجام داد و حل موضوعات پیش‌آمده موکول به زمان دیگری می‌شوند و به علت فقدان نص صریح قانون، افراد خاطی از مجازات مصون می‌مانند. از این منظر، تصویب قانون جامع (حقوق و) وظایف عرضه‌کنندگان خدمات فناوری اطلاعات و سکوها یا اصلاح برخی مفاد قانون جرائم رایانه‌ای، راهگشاست.

۷ فعالیت و توسعه محدوده‌ای از فضای سایبر، پیش از فراهم شدن زیرساخت‌های قانونی و حقوقی، احتمال تأثیرپذیری بیشتر از نظام‌های قانونی و حقوقی کشورهای پیشرو و تضعیف حاکمیت ملی را در پی دارد. در این راستا، سرعت بخشیدن و همگام‌سازی وضع قوانین و دستورالعمل‌ها با تغییرات فضای سایبر به منظور پر نمودن خلأهای قانونی، به‌روزرسانی مستمر آنها و بهبود در مقررات موجود با کسب نظر تمام ذی‌نفعان در کشور، راهگشا خواهد بود. انجام این مهم منجر به کاهش تعارضات در میان ذی‌نفعان، هم‌راستایی اقدامات آنان و بهره‌مندی از مزایای تصمیم‌گیری مشارکتی نیز خواهد شد.

۸ باتوجه به تحولات سریع در عرصه فناوری، فضای سایبر کشور از مشکلاتی زیرساختی نظیر کمبود ابررایانه‌ها برای انجام محاسبات پیچیده، نبود تطابق فعالیت‌های مراکز علمی و دانشگاهی با نیازهای صنعت سایبر، مصرف‌کننده بودن از فضای ابری و ابزارهای هوش مصنوعی خارجی رنج می‌برد. از این‌رو تقویت زیرساخت‌های سخت‌افزاری و نرم‌افزاری هریک از ارکان و مؤلفه‌های فضای سایبر (شامل بخش‌های اطلاعات، کنترل، ارتباطات و محاسبات) از طریق وضع هنجارهای قانونی و تنظیمگری عادلانه ضرورت دارد. قوانین و مقررات، لازم است موجبات تأمین و ارتقای کیفیت زیرساخت‌های سخت‌افزاری و نرم‌افزاری فضای سایبر به‌ویژه زیرساخت‌های انسانی (توسعه مهارت‌های عمومی دیجیتال، بازنگری در درس‌های دانشگاهی باتوجه به تحولات فناوری و تربیت نیروی انسانی متخصص، ماهر و متعهد برای ارکان فضای سایبر)، زیرساخت‌های پردازشی، زیرساخت‌های مخابراتی و شبکه ملی اطلاعات، زیرساخت‌های حقوقی و مالکیت فکری، زیرساخت‌های تولید محتوای غنی، زیرساخت‌های بهره‌برداری از داده‌ها و چگونگی ارتباطات میان دستگاه‌ها برای دسترسی به داده‌های یکدیگر را فراهم آورد. برای نمونه، تصویب قانون مدیریت داده‌ها و اطلاعات ملی (مدام) (مصوب ۱۰ آبان‌ماه ۱۴۰۱) در راستای تقویت بُعد اطلاعات فضای سایبر است یا تصویب قانون ملی هوش مصنوعی می‌تواند با توسعه این فناوری به تقویت رکن محاسبات این فضا کمک کند.

۹ باتوجه به نداشت نهادی انجام شده در گزارش «مروری بر مفاهیم و نهادهای مرتبط با فضای مجازی و ارائه چشم‌انداز تقنین و نظارتی مجلس دوازدهم» (با شماره مسلسل ۲۰۳۹۴ و کد موضوعی ۳۱۰ ارائه شده توسط گروه مخابرات و فناوری اطلاعات دفتر مطالعات انرژی، صنعت و معدن در بهمن‌ماه ۱۴۰۳) مشخص می‌شود کشور در سطح نهادی با تراکم در لایه سیاستگذاری کلان



و ناهماهنگی و اجرا نکردن مصوبات نهادهای سیاستگذار ازسوی خود این نهادها مواجه است. مقررات غیرمتمرکز و ناهماهنگ در سازمان‌ها و نهادهای مختلف، موجب نابسامانی و اجرای ضعیف خط‌مشی‌ها و قوانین موجود شده است. یکی از عوامل ایجاد این شرایط، تعدد نهادهای متولی در فضای سایبر و شرح وظایف، گاهی هم‌پوشان است. به‌منظور حکمرانی مؤثر بر فضای سایبر، پیشنهاد می‌شود شرح دقیق وظایف و اختیارات سازمان‌ها و نهادهای تصمیم‌گیرنده و اجراکننده، با رویکرد هماهنگی آنان در این فضا و به‌منظور جلوگیری از هم‌پوشانی و نابسامانی اقدامات انجام پذیرد.

۱۰. برای حکمرانی بر هر حوزه‌ای، نیاز است در قدم ابتدایی شئون حکمرانی توسط آحاد آن حوزه پذیرفته شود. نگرش و اعتماد کاربران به نهادهای تصمیم‌گیر در پذیرش شئون و تصمیمات حکمران مؤثر است. این موضوع که در مرحله متقاعدسازی ذی‌نفعان و مشروعیت بخشی به تصمیمات، قبل از پیاده‌سازی هر تصمیم در چرخه خط‌مشی‌گذاری مطرح است و به فضای فیزیکی یا فضای سایبر محدود نیست، گاهی به حدی در فرایند تصمیم‌گیری فضای سایبر نادیده گرفته می‌شود که باوجود تصمیمات راهبردی همچون توسعه پیام‌رسان‌های داخلی، با بی‌رغبتی جامعه و درنهایت شکست برنامه‌ها روبه‌رو می‌شود یا برای نمونه در طرح صیانت، به‌دلیل بی‌اعتمادی شدید کاربران و نگرانی آنان از اعمال محدودیت‌های بیشتر، تصمیم‌گیران را به بازنگری تصمیمات وادار می‌کند. ازاین‌رو رعایت الزامات فرایند خط‌مشی‌گذاری در فضای سایبر همچون فضای فیزیکی توصیه می‌شود.

۲-۹. پیشنهادها در راستای ارتقای حکمرانی با فضای سایبر

۱. همان‌طورکه در بخش قبل اشاره شد، کارکرد فضای سایبر و اثربخشی حکمرانی با این فضا، با فرض تمایل حضور کاربران در فضای سایبر است که کاملاً متأثر از نحوه حکمرانی بر فضای سایبر خواهد بود. حیطه حکمرانی با فضای سایبر، محدوده‌ای جدا و مستقل از حیطه حکمرانی بر فضای سایبر نیست و هماهنگی همگون میان این دو حیطه در کارایی هریک از آنها اثرگذار است. کارایی حکمرانی با فضای سایبر به کارایی هریک از ارکان فضای سایبر باز خواهد گشت؛ موضوعی که برای تحقق آن، به تنظیم روابط میان عوامل نیازمند است و بدون قوانین و مقررات و تنظیم‌گری شایسته بر فضای سایبر، حکمرانی با ابزارهای موجود در فضای سایبر دچار اختلال خواهد شد. درنتیجه حکمرانی با فضای سایبر، در گام ابتدایی نیازمند تحقق حکمرانی کارآمد بر اطلاعات، بر ارتباطات و بر محاسبات است؛ لذا ضروری است اثربخشی خط‌مشی‌ها و قوانین اتخاذ شده در فضای سایبر، فراتر از آن فضا و به‌عنوان مواردی زمینه‌ساز برای حکمرانی با فضای سایبر در نظر گرفته شود و در تدوین اسناد بر هماهنگی کردن راهبردهای دو حوزه دقت کافی صورت پذیرد.

۲. حداکثر بهره‌برداری از ظرفیت‌ها و قابلیت‌های ابزاری فضای سایبر در راستای تحقق اهداف مورد نظر حاکمیت، همچون ارتقای سطح شفافیت از طریق بستر رسانه‌های اجتماعی، تسهیل ارائه خدمات به شهروندان و رفع دغدغه‌ها و افزایش رضایت‌مندی آنان از طریق بهبود مستمر سامانه‌های دولت الکترونیک، ارتقای انسجام اجتماعی و میزان مشارکت سیاسی از طریق فرهنگ‌سازی و انتقال مفاهیم با ابزارهای ارتباطی فضای سایبر.

۳. به‌دلیل فهم ناقص از فضای سایبر و یکسان در نظر گرفتن آن با معنای فضای ناملموس یا فضای مجازی و غیرواقعی، اقدامات مرتبط حکمرانی با فضای سایبر به موضوعاتی از قبیل هوشمندسازی و خودکارسازی سامانه‌ها،^۱ توسعه هوش مصنوعی، به‌کارگیری

۱. برای مثال، سازمانی با تعداد زیادی کارمند جای خود را به سامانه‌ای یا چندین سرویس هوشمند بدهد یا چندین وزارتخانه با هم تلفیق شوند تا شرایط کاراتر و اثربخش‌تری را مبتنی بر هوش مصنوعی و هوشمندسازی اشیا برای ارائه خدمت به مردم شکل دهند.

از اینترنت اشیا، واقعیت افزوده، واقعیت مجازی، همزادهای دیجیتال^۲ و زنجیره بلوکی^۳ محدود می شود. در حالی که بهره‌مندی از فضای سایبر موضوعی فراتر از به کارگیری این دست موارد است و اگرچه هریک از این موارد گشایشی بر کاربست دانش سایبرنتیک به وجود خواهد آورد،^۱ در واقع توجه و رشد در این موارد بدون توجه به روح حاکم بر دانش سایبرنتیک و نقش تعالی بخش آن در حکمرانی و نحوه تصمیم‌گیری‌ها، تنها زیرساخت‌های یک حکمرانی مطلوب را (توسعه فناوری‌های اطلاعات، توسعه شبکه، توسعه مخابرات، نرم‌افزارها، برنامه‌های کاربردی،^۴ سیستم‌های عامل، سخت‌افزارهای محاسباتی و رایانه و...) فراهم می‌آورد و به خودی خود نتیجه‌ای در ارتقای سطح حکمت در حکمرانی نخواهد داشت.

به‌طور مشابه، امنیت فضای سایبر نیز موضوعی فراتر از امنیت اطلاعات و امنیت شبکه است (که مرتبط با مسائل فناورانه است) و اگر برداشت حاکمیت فقط امنیت اطلاعات و امنیت شبکه باشد، صرفاً به بخشی از امنیت فضای سایبر پرداخته است. روح حاکم بر دانش سایبرنتیک در واقع آنجایی بروز می‌یابد که چگونگی رسیدن از وضع موجود به وضع مطلوب مورد نظر حاکمیت طرح‌ریزی می‌شود.

استفاده نکردن از قابلیت‌های دانش سایبرنتیک، به‌حدی زیان‌بار است که باوجود حکمرانی بر تمام زیرساخت‌های فضای سایبر و انجام اقدامات سلبی و بازدارنده، احتمال سلطه سایر کشورها و تضعیف حاکمیت ملی با بهره‌گیری از دانش سایبرنتیک از میان نمی‌رود و تحقق امنیت سایبر بدون فهم این دانش و روح حاکم بر آن خدشه‌پذیر خواهد بود. به‌منظور تصمیم‌گیری‌های کارا و مواجهه فعالانه‌تر در راستای حفظ حاکمیت ملی در فضای گسترش‌یافته و بهره‌وری بیشتر در عملکرد سیستم‌ها، اقدام در راستای کاربست دانش سایبرنتیک در سیستم‌های تحت مدیریتی پیشنهاد می‌شود که از راهکارهای عملیاتی آن می‌تواند بهره‌گیری از تحلیلگران و مشاورانی با نگرشی سیستمی همراه سایر متخصصان مرتبط برای بررسی طرح‌ها و لوایح در کمیسیون‌های تخصصی مجلس شورای اسلامی یا اهتمام بر توسعه آزمایشگاه‌های خط‌مشی‌گذاری در نهادهای تنظیمگر به‌منظور ارزیابی پیشینی آنها باشد. **۴** همچون تقویت دیدگاه مکانیکی، که ضرورتی برای رویارویی با مسائل فنی و مهندسی است، تقویت دیدگاه سایبرنتیک در کشور نیز ضرورتی در حل مشکلات مدیریتی با رعایت تمام اصول انسانی و اخلاقی در مبانی دینی و فرهنگی است. بهره‌مند نشدن از این دانش یا هراس از آن، علاوه بر استفاده نکردن از قابلیت‌های آن در حل مشکلات، سبب متوجه نبودن تحت سلطه قرار گرفتن هنگام سلطه سایر حکومت‌ها یا نداشتن توانایی مقابله کارآمد در برابر آنها خواهد شد. تکمیل مباحث فلسفی، نظری و عملی فضای سایبر در عصر حاضر و آینده و تربیت نیروی متخصص در این زمینه از طریق راه‌اندازی رشته‌های جدید یا گنجاندن درس‌هایی همچون آشنایی با دانش سایبرنتیک و فناوری‌های آن، مباحث ویژه در فضای سایبر و مهندسی سایبرنتیک کاربردی که به‌طور مشخص در سرفصل‌های رسمی درس‌های رشته‌های دانشگاهی مهندسی و خط‌مشی‌گذاری وجود ندارند، می‌تواند راهگشا باشد.

۵ حکمرانی با آنکه شیوه و نحوه حکومت کردن است و دولت و مجلس به‌عنوان بخشی از حکمرانان جامعه، نهادهایی برای مقررات‌گذاری و تنظیمگری محسوب می‌شوند، دامنه آن لزوماً محدود به تشکیل ساختارهایی سلسله‌مراتبی و با نگاهی «از بالا به پایین» یا مبتنی بر نهادهای دولتی نیست. افراد جامعه در نگاه حاکمیت می‌توانند به‌صورت کاربر یا کنشگر در ساختارهای شبکه‌ای و مشارکتی ظاهر شوند. فضای سایبر همانند سایر عرصه‌های فضای فیزیکی، نیازمند حکمرانی عادلانه بر آن است و همراه با سازمان‌دهی از بالا به پایین نهادهای دولتی، می‌تواند با تدارک دیدن بسترهای ایفای نقش فعالانه و کنشگرانه برای مردم و تقویت مشارکت مردمی و تعامل و هم‌افزایی گروه‌های تخصصی و نهادهای مدنی و ظرفیت‌های بومی، دستیابی جامعه به‌سوی اهداف تعیین شده در اسناد بالادستی را تحقق ببخشد. حکمران می‌تواند از طریق سهولت فراهم شده توسط فضای سایبر، با درگیر کردن حداکثری ذی‌نفعان یک مسئله، علاوه بر ایجاد شفافیت، با بررسی مسئله از ابعاد مختلف و تلاش برای جاری کردن نگرش سیستمی موجبات اتخاذ تصمیمات سنجیده را فراهم آورد.

۱. برای نمونه، فناوری زنجیره بلوکی به‌معنای دفتر کل توزیع شده قابلیت ثبت و نگهداری هر رویداد و اطلاعاتی را مبتنی بر اعتماد عمومی دارد یا اینترنت اشیا می‌تواند اطلاعات ارزشمندی را از ابزارهای پیرامون انسان به‌منظور کنترل بهتر بر آنها در اختیار قرار دهد یا هوش مصنوعی می‌تواند با قدرت محاسباتی بالا به بهبود تصمیمات کمک کند.

2. Infrastructure
3. Application



جدول ۱. پیشنهاد توصیه سیاستی

ملاحظات	زمان بندی اجرا (کوتاه مدت، میان مدت، بلند مدت)	دستگاه معین	دستگاه متولی	الزامات و قیود اجرایی	توصیه سیاستی	نوع توصیه		ردیف
						اصلاح **	تداوم *	
	میان مدت	مرکز ملی فضای مجازی، وزارت اقتصاد و دارایی، معاونت علمی و فناوری ریاست جمهوری	وزارت ارتباطات و فناوری اطلاعات، وزارت علوم، تحقیقات و فناوری، وزارت آموزش و پرورش، وزارت فرهنگ و ارشاد اسلامی	توسعه فناوری‌های پیشرفته، ارتقای مهارت‌های عمومی دیجیتال و توسعه منابع انسانی متخصص	تقویت زیرساخت‌های نرم‌افزاری هریک از ارکان و مؤلفه‌های فضای سایبر در همراهی با تقویت زیرساخت‌های سخت‌افزاری آن از طریق وضع هنجارهای قانونی		*	۱
	میان مدت	وزارت صنعت، معدن و تجارت، سازمان صنفی رایانه‌ای، وزارت اقتصاد و دارایی، معاونت علمی و فناوری ریاست جمهوری	مجلس شورای اسلامی	اصلاح برخی مفاد قانون حمایت از حقوق پدیدآوران نرم‌افزارهای رایانه‌ای، تصویب قانون جامع حقوق (و وظایف) عرضه‌کنندگان خدمات فناوری اطلاعات و سکوها، اصلاح برخی مفاد قانون جرائم رایانه‌ای	قاعده‌مندسازی فعالیت کسب‌وکارها و حضور کاربران از طریق وضع قوانین و مقررات یا تنظیمگری‌های موضوعی		*	۲
	میان مدت	مجلس شورای اسلامی، وزارت اقتصاد و دارایی، معاونت علمی و فناوری ریاست جمهوری	وزارت صنعت، معدن و تجارت، سازمان نظام صنفی رایانه‌ای	توسعه فناوری‌های پیشرفته بومی، حمایت مادی و معنوی از صنایع نوآور دانش‌بنیان در این زمینه و کاهش وابستگی به فناوری‌های خارجی	تسهیل‌گری برای صنعت‌کاران و فعالان به منظور استقلال یافتن و بومی‌سازی فناوری‌ها در فضای سایبر و در راستای امنیت بخشیدن به انجام دادن فعالیت‌ها در این فضا		*	۳

ردیف	نوع توصیه		توصیه سیاستی	الزامات و قیود اجرایی	دستگاه متولی	دستگاه معین	زمان بندی اجرا (کوتاه مدت، میان مدت، بلند مدت)	ملاحظات
	اصلاح**	تداوم*						
۴		*	کاهش فاصله محتوایی و زمانی قانون با نیازهای جامعه در فضای سایبر	تصویب قانون جامع (حقوق و) وظایف عرضه کنندگان خدمات فناوری اطلاعات و سکوها، اصلاح برخی مفاد قانون جرائم رایانه ای	مجلس شورای اسلامی، شورای عالی فضای مجازی	تمام دستگاه های اجرایی	میان مدت	
۵		*	کاهش تأثیرپذیری از نظام های قانونی و حقوقی کشورهای پیشرو و تقویت بخشی حاکمیت ملی	سرعت بخشیدن به وضع و همگام سازی قوانین، دستورالعمل ها و استانداردها با تغییرات فضای سایبر به منظور پر نمودن خلأهای قانونی، به روزرسانی مستمر آنها، بهبود در مقررات موجود	مجلس شورای اسلامی، شورای عالی فضای مجازی	تمام دستگاه های اجرایی	میان مدت تا بلند مدت	
۶		*	کاهش نزاحات میان نهادهای تنظیمگر و جلوگیری از هم پوشانی و نابسامانی اقدامات	شرح دقیق وظایف و اختیارات نهادهای تصمیم گیر و اجرایی در فضای سایبر با رویکرد هماهنگی اقدامات	مرکز ملی فضای مجازی	تمام دستگاه های اجرایی و تصمیم ساز مرتبط	میان مدت تا بلند مدت	
۷		*	متقاعدسازی ذی نفعان و مشروعیت بخشی تصمیمات اتخاذ شده در خط مشی گذاری های فضای سایبر	تولید محتوا برای همفکری و تولید محتوای آموزشی برای ترویج	وزارت فرهنگ و ارشاد اسلامی، سازمان صدا و سیما، شورای عالی حوزه های علمیه	شورای عالی فضای مجازی	کوتاه مدت	



ردیف	نوع توصیه		توصیه سیاستی	الزامات و قیود اجرایی	دستگاه متولی	دستگاه معین	زمان بندی اجرا (کوتاه مدت، میان مدت، بلند مدت)	ملاحظات
	اصلاح **	تداوم *						
۸	*		پذیرش، باورمندسازی و اطمینان بخشی کاربران نسبت به حضور در فضای سایبر داخلی و نسبت به نهادهای تصمیم گیر در آن	تصویب قانون حمایت از داده‌های شخصی و حفاظت از حریم خصوصی، طراحی شاخص‌هایی برای سنجش باورمند و اطمینان کاربران نسبت به فضای سایبر داخلی و همچنین نسبت به نهادهای تصمیم گیر، سنجش مستمر این شاخص‌ها و بهبود آن	مجلس شورای اسلامی، شورای عالی فضای مجازی	وزارت فرهنگ و ارشاد اسلامی، سازمان صدا و سیما، شورای عالی حوزه‌های علمیه، قوه قضائیه	کوتاه مدت تا میان مدت	
۹		*	گسترش ظرفیت‌ها و قابلیت‌های ابزاری فضای سایبر در راستای تحقق ارتقای سطح شفافیت و تسهیل ارائه خدمات به شهروندان	توسعه رسانه‌های بومی اجتماعی و بهبود مستمر سامانه‌های دولت الکترونیک	وزارت ارتباطات و فناوری اطلاعات، سازمان فناوری اطلاعات ایران	مجلس شورای اسلامی، شورای عالی فضای مجازی	میان مدت	
۱۰		*	اهتمام جدی بر هوشمندسازی فرایندهای تصمیم سازی در راستای حکمرانی داده مینا	پیگیری و نظارت بر اجرای بند «پ» ماده (۱۰۷) قانون برنامه پنج ساله هفتم پیشرفت	مجلس شورای اسلامی	تمام دستگاه‌های تصمیم گیر	میان مدت	
۱۱		*	بهره گیری از قابلیت‌های دانش سایبرنتیک در حکمرانی و طرح ریزی چگونگی رسیدن از وضع موجود به وضع مطلوب مورد نظر حاکمیت	استفاده از تحلیلگران و مشاورانی با نگرشی سیستمی همراه سایر متخصصان در بررسی طرح‌ها و لوایح در کمیسیون‌های تخصصی	مجلس شورای اسلامی، مجمع تشخیص مصلحت نظام	تمام دستگاه‌های تصمیم گیر	میان مدت	

ردیف	نوع توصیه		توصیه سیاستی	الزامات و قیود اجرایی	دستگاه متولی	دستگاه معین	زمان بندی اجرا (کوتاه مدت، میان مدت، بلند مدت)	ملاحظات
	اصلاح**	تداوم*						
۱۲	*		اهتمام بر توسعه آزمایشگاه های خط مشی گذاری در نهادهای تنظیمگر	الزام نمودن دستگاه های تصمیم ساز به راه اندازی آزمایشگاه های خط مشی گذاری مرتبط با فعالیت، در نظر گرفتن سازوکار امتیازدهی برای ارزیابی طرح ها و لوایح قانونی وصول شده	مجلس شورای اسلامی	تمام دستگاه های تصمیم ساز	کوتاه مدت تا میان مدت	
۱۳	*		در نظرگیری فرایند خط مشی گذاری به مثابه چرخه و توجه به نقش نظارتی مجلس	هوشمندسازی فرایند نظارتی مجلس	مجلس شورای اسلامی	مجلس شورای اسلامی	میان مدت	
۱۴	*		تکمیل مباحث فلسفی، نظری و عملی فضای سایبر در عصر حاضر و آینده و تربیت نیروی متخصص در این زمینه	راه اندازی رشته های جدید یا گنجاندن دروسی همچون آشنایی با دانش سایبرنتیک و فناوری های آن، مباحث ویژه در فضای سایبر و مهندسی سایبرنتیک کاربردی که به طور مشخص در سرفصل های رسمی درس های رشته های دانشگاهی مهندسی و خط مشی گذاری وجود ندارند.	وزارت علوم، تحقیقات و فناوری	شورای عالی انقلاب فرهنگی	میان مدت	

* تداوم یا تقویت آیتمها یا اقدامات

** اصلاح رویه ها یا ایجاد سازوکارها

مأخذ: یافته های پژوهش.



۱۰. پیوست



جدول ۲ پیوست. اهم قوانین و مقررات مرتبط با فضای سایبر در کشور

تاریخ	عنوان	حیطه
اسفندماه ۱۳۳۱	اساسنامه شرکت سهامی تلفن ایران (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
دی‌ماه ۱۳۴۸	قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات)
خردادماه ۱۳۵۰	قانون تأسیس شرکت مخابرات ایران (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
اسفندماه ۱۳۵۰	اساسنامه شرکت مخابرات ایران (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
خردادماه ۱۳۵۲	اساسنامه شرکت سهامی خدمات ماشین‌های محاسب الکترونیکی (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر محاسبات)
دی‌ماه ۱۳۵۲	قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات)
دی‌ماه ۱۳۵۵	قانون کنوانسیون بین‌المللی ارتباطات دور (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
آذرماه ۱۳۶۰	قانون حمل‌ونقل و مبادله محصولات و مرسولات پستی وزارت پست و تلگراف و تلفن توسط مؤسسات و شرکت‌های خصوصی حمل‌ونقل بار و مسافر (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
تیرماه ۱۳۶۱	قانون خط‌مشی کلی و اصول برنامه‌های سازمان صدا و سیما جمهوری اسلامی ایران (مصوبه مجلس شورا)	حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
مهرماه ۱۳۶۲	اساسنامه سازمان صدا و سیما جمهوری اسلامی ایران (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات) حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
اسفندماه ۱۳۶۵	اساسنامه دانشگاه نیمه‌حضوری و آموزش از راه دور (مصوبه شورای عالی انقلاب فرهنگی)	حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
اردیبهشت‌ماه ۱۳۶۷	قانون (اساسنامه) شرکت پست جمهوری اسلامی ایران (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
مردادماه ۱۳۷۱	اساسنامه مرکز سنجش از دور ایران (مصوبه هیئت‌وزیران)	حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
بهمن‌ماه ۱۳۷۲	قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نمایند (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات)
بهمن‌ماه ۱۳۷۴	اساسنامه شرکت سهامی خاص خدمات هوایی پست و مخابرات (پیام) (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
بهمن‌ماه ۱۳۷۴	اساسنامه شرکت سهامی مخابرات استان‌ها (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
آذرماه ۱۳۷۵	اساسنامه مؤسسه آموزش از راه دور (مصوبه شورای عالی انقلاب فرهنگی)	حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
فروردین‌ماه ۱۳۷۹	قانون برنامه سوم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
فروردین‌ماه ۱۳۷۹	قانون مطبوعات (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات)
دی‌ماه ۱۳۷۹	قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات)

تاریخ	عنوان	حیطه
تیرماه ۱۳۸۲	تغییر وزارت پست و تلگراف و تلفن به وزارت ارتباطات و فناوری اطلاعات	حکمرانی بر فضای سایبر (بر ارتباطات)
آذرماه ۱۳۸۲	قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
دی ماه ۱۳۸۲	قانون تجارت الکترونیک (مصوبه مجلس شورا)	حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
تیرماه ۱۳۸۳	اساسنامه شرکت مادر تخصصی مخابرات ایران (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
شهریورماه ۱۳۸۳	قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات) حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
شهریورماه ۱۳۸۳	اساسنامه شرکت ارتباطات زیرساخت (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر ارتباطات)
شهریورماه ۱۳۸۳	اساسنامه شرکت ارتباطات سیار (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر ارتباطات)
شهریورماه ۱۳۸۳	اساسنامه شرکت ارتباطات داده ها (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر ارتباطات)
بهمن ماه ۱۳۸۳	اساسنامه شورای عالی فضای (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
اسفندماه ۱۳۸۳	آیین نامه اجرایی مربوط به وظایف و طرز کار کمیسیون تنظیم مقررات ارتباطات (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر ارتباطات)
اردیبهشت ماه ۱۳۸۴	قانون اجازه اجرای موافقت نامه پروانه شبکه و خدمات ارتباطات سیار (مجلس شورای اسلامی)	حکمرانی بر فضای سایبر (بر ارتباطات)
خردادماه ۱۳۸۴	اساسنامه شورای عالی فناوری اطلاعات (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر اطلاعات) حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
تیرماه ۱۳۸۴	اساسنامه سازمان فضایی ایران (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
خردادماه ۱۳۸۵	اساسنامه بنیاد ملی بازی های رایانه ای (مصوبه شورای عالی انقلاب فرهنگی)	حکمرانی بر فضای سایبر (بر اطلاعات) حکمرانی با فضای سایبر (با اطلاعات)
آبان ماه ۱۳۸۶	قانون ثبت اختراعات، طرح های صنعتی و علائم تجاری (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات)
دی ماه ۱۳۸۶	قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت های غیرمجاز می نمایند (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات)
اسفندماه ۱۳۸۶	آیین نامه نظام بانکداری الکترونیکی (مصوبه هیئت وزیران)	حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
خردادماه ۱۳۸۷	اساسنامه سازمان فضایی ایران (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
شهریورماه ۱۳۸۷	اساسنامه شرکت ارتباطات زیرساخت (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر ارتباطات)
دی ماه ۱۳۸۷	اساسنامه شرکت فناوری اطلاعات ایران (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
بهمن ماه ۱۳۸۷	قانون انتشار و دسترسی آزاد به اطلاعات (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات)
اردیبهشت ماه ۱۳۸۸	قانون صیانت از حریم مسیرهای شبکه کابل فیبر نوری شبکه مادر مخابراتی کشور (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)



تاریخ	عنوان	حیطه
خردادماه ۱۳۸۸	قانون جرائم رایانه‌ای (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات، ارتباطات و محاسبات)
شهریورماه ۱۳۸۸	اساسنامه مرکز توسعه تجارت الکترونیک (مصوبه هیئت وزیران)	حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
دی‌ماه ۱۳۸۹	قانون برنامه پنج‌ساله پنجم توسعه جمهوری اسلامی ایران (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات) حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
تیرماه ۱۳۹۱	اساسنامه مرکز ملی فضای مجازی کشور (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات، ارتباطات و محاسبات)
مردادماه ۱۳۹۱	قانون عضویت دولت جمهوری اسلامی ایران در اتحادیه بین‌المللی مخابرات هوانوردی (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر ارتباطات)
خردادماه ۱۳۹۲	اصول و سیاست‌های حاکم بر مجوز خدمات سلامت در فضای مجازی (مصوبه شورای عالی فضای مجازی)	حکمرانی با فضای سایبر (با اطلاعات و محاسبات)
آبان‌ماه ۱۳۹۲	قانون اجازه تعیین و وصول حق امتیاز فعالیت بخش غیردولتی در زمینه پست و مخابرات (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
دی‌ماه ۱۳۹۲	الزامات حاکم بر تحقق شبکه ملی اطلاعات (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
مهرماه ۱۳۹۳	قانون آیین دادرسی الکترونیکی (مصوبه مجلس شورا)	حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
اسفندماه ۱۳۹۳	توسعه فضای مجازی سالم، مفید و ایمن (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات)
آذرماه ۱۳۹۵	سند تبیین الزامات شبکه ملی اطلاعات (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
فروردین‌ماه ۱۳۹۶	قانون برنامه پنج‌ساله ششم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات) حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
مردادماه ۱۳۹۶	سیاست‌ها و اقدامات سامان‌دهی پیام‌رسان‌های اجتماعی (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
شهریورماه ۱۳۹۷	اساسنامه قانون دفاتر خدمات الکترونیک قضایی (مصوب قوه قضائیه)	حکمرانی با فضای سایبر (با اطلاعات، ارتباطات و محاسبات)
مهرماه ۱۳۹۷	الزامات حاکم بر اینترنت اشیا در شبکه ملی اطلاعات (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات، ارتباطات و محاسبات و کنترل)
مردادماه ۱۳۹۸	تصویب‌نامه در خصوص استفاده از رمز ارزها (مصوب هیئت وزیران)	حکمرانی بر فضای سایبر (بر محاسبات)
شهریورماه ۱۳۹۸	نظام هویت معتبر در فضای مجازی کشور (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات)
آبان‌ماه ۱۳۹۸	اساسنامه شورای اجرایی فناوری اطلاعات (مصوب هیئت وزیران)	حکمرانی با فضای سایبر (با اطلاعات، ارتباطات و محاسبات)

تاریخ	عنوان	حیطه
مهرماه ۱۳۹۹	طرح کلان و معماری شبکه ملی اطلاعات (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات، ارتباطات و محاسبات)
بهمن ماه ۱۳۹۹	الزامات پیشگیری و مقابله با نشر اطلاعات، اخبار و محتوای خبری خلاف واقع در فضای مجازی (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (اطلاعات)
تیرماه ۱۴۰۰	سند صیانت از کودکان و نوجوانان در فضای مجازی (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات)
تیرماه ۱۴۰۰	تصویب نامه درخصوص تبادل اطلاعات مورد نیاز بین سامانه تدارکات الکترونیکی دولت (ستاد) و سامانه خدمات غیرحضوری سازمان تأمین اجتماعی (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر اطلاعات) حکمرانی با فضای سایبر (با اطلاعات، ارتباطات و محاسبات)
مهرماه ۱۴۰۰	الزامات سامانه های الکترونیکی آموزش و پرورش و شبکه آموزشی دانش آموز (شاد) (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات) حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
شهریورماه ۱۴۰۱	سند راهبردی جمهوری اسلامی ایران در فضای مجازی - اهداف و اقدامات کلان (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات، ارتباطات و محاسبات) حکمرانی با فضای سایبر (با اطلاعات و ارتباطات، محاسبات و کنترل)
آبان ماه ۱۴۰۱	قانون مدیریت داده ها و اطلاعات ملی (مصوبه مجلس شورا)	حکمرانی بر فضای سایبر (بر اطلاعات)
آذرماه ۱۴۰۱	آیین نامه استخراج رمزداری ها (مصوبه هیئت وزیران)	حکمرانی بر فضای سایبر (بر محاسبات)
مردادماه ۱۴۰۲	اساسنامه اصلاح شده سازمان فرهنگ و ارتباطات اسلامی (مصوبه هیئت وزیران)	حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)
بهمن ماه ۱۴۰۲	دستورالعمل سامان دهی خدمات میزبانی در فضای مجازی کشور (مصوبه شورای عالی فضای مجازی)	حکمرانی بر فضای سایبر (بر اطلاعات)
تیرماه ۱۴۰۳	قانون برنامه پنج ساله هفتم پیشرفت جمهوری اسلامی ایران	حکمرانی بر فضای سایبر (بر اطلاعات و ارتباطات) حکمرانی با فضای سایبر (با اطلاعات و ارتباطات)



منابع و مأخذ

- [1] Novikov, D.A., (2015), Cybernetics: from past to future. Vol. 47, Springer, pp. 14.
- [2] Wiener, N., (2019), Cybernetics: or Control and Communication in the Animal and the Machine. MIT press.
- [۳] فیروزآبادی، سیدابوالحسن و جواد احمدآبادی آزادی، (۱۳۹۹)، «تحلیل پیشینه حکمرانی فضای مجازی جمهوری اسلامی ایران»، دانش سیاسی، دوره ۱۶، شماره ۲، صص. ۵۹۸-۵۶۳.
- [4] Novikov, D.A., (2015), Cybernetics: from past to future. Vol. 47, Springer, pp. 4.
- [5] Umpleby, S.A., (2008), "A short history of cybernetics in the United States: The origin of cybernetics", österreichische zeitschrift für geschichtswissenschaften, Vol. 19, No. 4, pp. 28-40.
- [6] Ashby, W.R., (1956), An introduction to cybernetics.
- [7] Bateson, G., (1971), "The cybernetics of 'self': A theory of alcoholism", Psychiatry, Vol. 34, No. 1, pp. 1-18.
- [8] Beer, S., (1972), "Cybernetics—a systems approach to management", Personnel Review, Vol. 1, No. 2, pp. 28-39.
- [9] Pask, G., (1975), Cybernetic theory of cognition and learning.
- [10] Von Glasersfeld, E., (2019), Cybernetics, experience, and the concept of self, in A Cybernetic Approach To The Assessment Of Children, Routledge. pp. 67-113.
- [11] Maturana, H.R., (1988), "The notions of cybernetics", Continuing the conversation, Vol. 13, No. 7.
- [12] Ascott, R., (1994), "The architecture of cyberception", Leonardo Electronic Almanac, Vol. 2, No. 8.
- [13] <https://farsi.khamenei.ir/others-dialog?id=19272>.
- [14] <https://farsi.khamenei.ir/speech-content?id=47637>.
- [۱۵] لک‌زایی، علی و کاظم فولادی قلعه، (۹ تا ۱۱ آبان ۱۴۰۲)، «نسبت قلمرو حکمرانی با فضای سایبر»، در مجموعه مقالات دومین کنفرانس ملی فضای سایبر، دانشگاه تهران، صص. ۶۹۳-۷۰۱.
- [16] <https://iict.ac.ir/1402/08/hciberi/>.
- [17] Novikov, D.A., (2015), "Cybernetics: from past to future", Vol. 47, Springer, pp. 16.
- [18] Xu, G., et al., (2006), "Dual relations in physical and cyber space", Chinese Science Bulletin, Vol. 51, pp. 121-128.
- [۱۹] فانگ، بین‌شینگ، (۱۳۹۹)، حاکمیت فضای سایبری (اندیشه‌هایی پیرامون ایجاد جامعه‌ای با آینده مشترک در فضای سایبر)، ترجمه محمدرضا کریمی قهرودی و وحید زارعی، جلد ۲، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.
- [۲۰] جاجودیا، سوشیل، (۱۳۹۷)، جنگ سایبری (ایجاد پایه و اساس علمی)، ترجمه حوزه نوآوری آرایه‌های دفاعی، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.
- [21] Wilby, J., (2006), "An essay on Kenneth E. Boulding's General Systems Theory: the skeleton of science". Systems Research and Behavioral Science: The Official Journal of the International Federation for Systems Research, Vol. 23, No. 5, pp. 695-699.
- [۲۲] دفرماندهی آموزش و دکتترین ارتش ایالات متحده، (۱۳۹۸)، ارتش سایبری ۲۰۵۰، ترجمه محمدرضا کریمی قهرودی و وحید زارعی، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.
- [23] Novikov, D.A., (2015), Cybernetics: from past to future. Vol. 47, Springer, pp. 22.

[24] Novikov, D.A., (2015), Cybernetics: from past to future. Vol. 47, Springer, pp. 24.

[۲۵] کیان خواه، احسان، (اسفند ۱۳۹۸)، «چالش‌های راهبردی حکمرانی با گسترش فضای سایبر»، امنیت ملی، دوره ۹، شماره ۳۴، صص. ۱۷۴-۱۵۳.

[26] Wang, J., et al., (2023), "Envisioning a credit society: social credit systems and the institutionalization of moral standards in China", Media, Culture & Society, Vol. 45, No.3, pp. 451-470.

گزیده سیاستی

فضای سایبر دارای چهار رکن اطلاعات، کنترل، ارتباطات و محاسبات است و حکمرانی بر فضای سایبر به معنای حکمرانی بر هریک از مؤلفه‌های این فضا و حکمرانی با فضای سایبر به معنای اعمال حاکمیت بر جامعه از طریق هریک از مؤلفه‌های فضای سایبر است.



مرکز پژوهش‌های مجلس شورای اسلامی

تهران، خیابان پاسداران، روپروی پارک نیاوران (ضلع جنوبی، پلاک ۸۰۲)

تلفن: ۷۵۱۸۳۰۰۰ صندوق پستی: ۱۵۸۷۵-۵۸۵۵ پست الکترونیک: mrc@majles.ir

وبسایت: rc.majles.ir