فصلنامه علمی
مطالعات قدرت نرم

چالش‌های امنیتی در فضای سایبری ایران

خلیل سلیمانی[۱] خسرو مزرعی[۲] عبدالرضا بای[۳]

۴۳
دوره ۱۵، شماره ٤، پیاپی ٤۳
زمستان ۱٤۰٤
مقاله پژوهشی
تاریخ دریافت:
۱٤۰٤-۰۶-۰۶
تاریخ پذیرش:
۱٤۰٤-۱۲-۰۵
صص: ۱۸-۱
شاپا چاپی: ۲۳۲۲-۵۵۹۹
رتبه علمی
ب
بررسی صحت گواهی در :
JOURNALS.MSRT.IR

چکیده

با گسترش روزافزون فناوری‌های دیجیتال و وابستگی فزاینده زیرساخت‌های حیاتی به فضای سایبری، امنیت سایبری به یکی از اولویت‌های اساسی در سطح ملی و بین‌المللی تبدیل شده است. ایران نیز، به‌عنوان یکی از کشورهای در حال توسعه در حوزه فناوری اطلاعات، با چالش‌های پیچیده و چندلایه‌ای در زمینه امنیت سایبری مواجه است. این مقاله به بررسی نظام‌مند چالش‌های اصلی امنیت سایبری در ایران می‌پردازد و تلاش دارد تا با رویکردی تحلیلی، ابعاد مختلف این چالش‌ها را از منظر زیرساختی، حقوقی، فرهنگی و فناورانه مورد واکاوی قرار دهد. مطالعه حاضر نشان می‌دهد که ضعف در هماهنگی نهادی، نبود سیاست‌گذاری جامع، کمبود نیروی انسانی متخصص، تهدیدات فزاینده سایبری از سوی بازیگران دولتی و غیردولتی، و همچنین سطح پایین آگاهی عمومی از مهم‌ترین عوامل تهدیدکننده امنیت فضای مجازی ایران هستند. همچنین مشخص شد که در کنار پیشرفت‌های قابل‌توجه در ایجاد مراکز پاسخ‌گویی به حوادث سایبری و تقویت برخی نهادهای نظارتی، هنوز شکاف‌های قابل‌توجهی در مدیریت بحران‌های سایبری، توسعه زیرساخت‌های بومی و تدوین قوانین به‌روز وجود دارد. در پایان، راهکارهایی نظیر تقویت همکاری‌های بین‌نهادی، تدوین چارچوب‌های قانونی جامع، سرمایه‌گذاری در آموزش سایبری، و بهره‌گیری از فناوری‌های نوین مبتنی بر هوش مصنوعی پیشنهاد شده‌اند.

واژه‌های کلیدی:

امنیت سایبری، فضای مجازی ایران، تهدیدات سایبری، زیرساخت‌های حیاتی، قدرت نرم

۱. دانشجوی دکتری علوم سیاسی – سیاستگذاری عمومی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی، آزادشهر، گلستان، ایران
۲. استادیار، گروه علوم سیاسی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی، آزادشهر، گلستان، ایران.
(نویسنده مسئول) Kh.mazrai@iau.ac.ir
۳. استادیار، گروه علوم سیاسی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی، آزادشهر، گلستان، ایران.

مقدمه و بیان مسأله

با ورود به عصر دیجیتال، وابستگی جوامع به فناوری‌های اطلاعات و ارتباطات به طور چشمگیری افزایش یافته است؛ به گونه‌ای که فضای سایبری به یکی از ارکان حیاتی زیرساخت‌های ملی تبدیل شده است. ایران نیز در مسیر توسعه فناوری‌های دیجیتال گام‌های مهمی برداشته است، اما همزمان با این پیشرفت‌ها، چالش‌های امنیتی متعددی در این حوزه ظهور کرده‌اند که می‌توانند تهدیدی جدی برای ثبات سیاسی، اقتصادی و اجتماعی کشور محسوب شوند. این چالش‌ها که هم از عوامل داخلی و هم خارجی نشأت می‌گیرند، نیازمند شناسایی دقیق و راهکارهای عملی است. مسأله کلیدی که در این مطالعه بررسی می‌شود، درک عمیق و همه‌جانبه از موانع و تهدیدهای امنیت سایبری در ایران است؛ مسأله‌ای که نه تنها پیچیدگی‌های فناورانه دارد، بلکه ابعاد نهادی، حقوقی و فرهنگی نیز در آن نقش اساسی ایفا می‌کنند. در شرایطی که حملات سایبری سازمان‌یافته و روزافزون بازیگران دولتی و غیردولتی فضای مجازی کشور را هدف قرار می‌دهد، ضعف هماهنگی میان نهادهای مسئول، کمبود نیروی انسانی متخصص و خلأهای قانونی، کار را برای مقابله مؤثر دشوار کرده است. افزون بر این، سطح پایین آگاهی عمومی و کمبود سرمایه‌گذاری در آموزش سایبری، نقاط ضعف دیگری هستند که به افزایش آسیب‌پذیری فضای مجازی منجر می‌شوند. از این رو، این مقاله با رویکردی تحلیلی، تلاش می‌کند تا چالش‌های امنیتی فضای سایبری ایران را در قالب ابعاد مختلف بررسی و با ارائه راهکارهای نوین و مستدل، بستری برای تقویت امنیت ملی در بستر فناوری‌های نوین فراهم آورد.

با وجود مطالعات متعدد درباره ابعاد فنی، حقوقی و راهبردی امنیت سایبری در ایران، ادبیات موجود دچار پراکندگی تحلیلی است و کمتر به تبیین منسجم ارتباط میان چالش‌های نهادی داخلی و ظرفیت بازدارندگی سایبری پرداخته است. نوآوری این پژوهش در سه سطح قابل بیان است: نخست، در سطح نظری، با تعمیم نظریه بازدارندگی از سطح بین‌المللی به حکمرانی داخلی و نشان دادن تأثیر کاستی‌های ساختاری بر بازدارندگی سایبری؛ دوم، در سطح تحلیلی، با سازمان‌دهی چالش‌های پراکنده در قالب الگویی منسجم و چندبعدی؛ و سوم، در سطح روشی، با تلفیق شاخص‌های بین‌المللی، اسناد سیاستی و پژوهش‌های دانشگاهی برای ارائه یک چارچوب تحلیلی بومی. بر این اساس، مقاله فراتر از یک مرور تجمیعی، چارچوبی تحلیلی برای فهم پیوند میان حکمرانی سایبری و بازدارندگی ملی ارائه می‌دهد.

گسترش وابستگی زیرساخت‌های حیاتی، نظام مالی، ارتباطات و خدمات عمومی به فناوری‌های دیجیتال، امنیت سایبری را به یکی از ارکان بنیادین امنیت ملی کشورها تبدیل کرده است. در ایران نیز طی دو دهه اخیر توسعه شتابان زیرساخت‌های ارتباطی و نفوذ گسترده فناوری‌های دیجیتال، همزمان با افزایش تهدیدات سایبری، اهمیت این حوزه را دوچندان ساخته است. با این حال، مواجهه سیاستی و نهادی با این تحولات، عمدتاً واکنشی، پراکنده و فاقد انسجام راهبردی بوده است. بررسی ادبیات پژوهش نشان می‌دهد که مطالعات انجام شده در ایران عموماً در یکی از سه سطح متمرکز بوده‌اند: نخست، مطالعات فنی و مهندسی در حوزه

امنیت شـــبکه و حفاظت اطلاعات؛ دوم، پژوهش‌های حقوقی در زمینه تنظیم‌گری و قانون‌گذاری ســـایبری؛ و ســـوم، تحلیل‌های راهبردی مقایسه‌ای درباره رویکرد ایران و سایر کشورها.

با وجود این تلاش‌ها، یک خلأ دانشی اساسی همچنان باقی است: تاکنون مطالعه‌ای که به‌صورت یکپارچه و با رویکردی نهادی ـــ سیاستی، چالش‌های ساختاری امنیت سایبری ایران را در چارچوب نظری بازدارندگی تحلیل کند و نسبت این چالش‌ها را با ظرفیت بازدارندگی و تاب‌آوری ملی تبیین نماید، کمتر مورد توجه قرار گرفته است. به بیان دیگر، مسئله صرفاً شناسایی تهدیدات ســـایبری نیســـت، بلکه درک این نکته اســـت که چرا با وجود اســـناد، نهادها و اقدامات متعدد، امنیت ســـایبری ایران همچنان با آسیب‌پذیری‌های پایدار مواجه است. مسئله اصلی پژوهش حاضر آن است که چالش‌های امنیت سایبری ایران صرفاً ناشی از تهدیدات خارجی نیستند، بلکه ریشه در کاستی‌های نهادی، ساختاری، آموزشی و سیاستی دارند که بر ظرفیت بازدارندگی سایبری کشور اثر می‌گذارند. فقدان راهبرد یکپارچه، تعدد مراکز تصمیم‌گیری، کمبود سرمایه انسانی تخصصی، وابستگی فناورانه و کاهش اعتماد عمومی، مجموعه‌ای از عوامل درهم‌تنیده‌اند که کارآمدی نظام حکمرانی سایبری را تحت تأثیر قرار داده‌اند.

بر این اساس، پرسش تحلیلی پژوهش چنین صورت‌بندی می‌شود:

چالش‌های امنیتی فضای سایبری ایران در ابعاد مختلف چه هستند و چه راهبردهایی می‌تواند به کاهش آسیب‌پذیری و تقویت تاب‌آوری ملی در برابر این تهدیدات کمک کند؟

پاسخ به این پرسش مستلزم عبور از رویکردهای صرفاً فنی یا توصیفی و حرکت به سوی تحلیلی میان رشته‌ای است که بتواند پیوند میان حکمرانی سایبری، سیاست‌گذاری عمومی و امنیت ملی را روشن سازد. پژوهش حاضر در پی آن است که با بهره‌گیری از چارچوب نظری بازدارندگی و روش تحلیل نهادی ـــ سیاستی، این خلأ دانشی را پوشش داده و تصویری منسجم از موانع ساختاری امنیت سایبری ایران ارائه دهد.

سوالات پژوهش

سوال اصلی پژوهش حاضر این است که چالش‌های امنیتی فضای سایبری ایران در ابعاد مختلف چه هستند و چه راهبردهایی می‌تواند به کاهش آسیب‌پذیری و تقویت تاب‌آوری ملی در برابر این تهدیدات کمک کند؟

پیشینه تحقیق

تحقیقاتی که در این راستا صورت گرفته است به شرح ذیل می‌باشد:

احسان کیان‌خواه(۱۳۹۸) در مقاله‌ای با موضوع چالش‌های راهبردی حکمرانی با گسترش فضای سایبری با هدف بررسی اثر گسترش فضای سایبری بر حکمرانی در ایران به این نتیجه رسیده است که زیرساخت‌های ایران به سرعت به فضای سایبری منتقل می‌شوند اما نبود ساختار حکمرانی منسجم، وابستگی به فناوری خارجی و ضعف در هماهنگی نهادی، چالش‌های اصلی هستند.

محمدر ضا حسینی(۱۴۰۲) در مقاله‌ای با عنوان الگوی مقررات گذاری در فضای سایبر: ارائه چارچوب جامع تنظیم‌گری برای محیط ملی با هدف طراحی الگویی برای قانون‌گذاری در حوزه سایبر در ایران به این نتیجه رسیده است که پیشنهاد چارچوبی شامل تنظیم مقررات در سه سطح: دولت، بخش خصوصی و نهادهای مدنی؛ خلأ بزرگ، نبود نهاد تخصصی یکپارچه برای تنظیم‌گری است.

محمدکاظم صیاد و همکاران(۱۳۹۹) در مقاله‌ای با عنوان تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات متحده آمریکا و جمهوری اسلامی ایران با هدف تحلیل رویکردهای امنیتی دو کشور در مواجهه با تهدیدات سایبری به این نتیجه رسیده است که ایران بیشتر بر دفاع و مقابله متمرکز است در حالی‌که آمریکا سیاست‌های پیش‌دستانه، تهاجمی و بین‌المللی را دنبال می‌کند. ضعف ایران، ناهماهنگی نهادی و کمبود سرمایه‌گذاری فناورانه است.

محمدرضا کریمی قهرودی و همکارن(۱۴۰۱) در مقاله‌ای با عنوان ارائه مدلی برای ارزیابی امنیت سایبری جمهوری اسلامی ایران با هدف ارائه مدل برای سنجش سطح امنیت سایبری کشور به این نتیجه رسیده است که ایران در سطح متوسط قرار دارد؛ بیشترین تهدید از ناحیه زیرساخت‌های مالی و انرژی است. نیاز فوری به تدوین شاخص‌های بومی امنیت سایبری وجود دارد.

چارچوب نظری

نظریه بازدارندگی

با گسترش فناوری‌های سایبری، تهدیداتی همچون جاسوسی و حملات علیه زیرساخت‌های حیاتی افزایش یافته است. در این چارچوب، بازدارندگی سایبری به‌عنوان بخشی از الگوی دفاع ملی مطرح می شود که می‌تواند با ایجاد چارچوبی پیشگیرانه، زمینه کاهش احتمال وقوع حملات پیش از آغاز آن‌ها را فراهم آورد.

نظریه بازدارندگی به‌جای جنگیدن، با ایجاد اثر روانی بر طرف مقابل، او را از اقداماتی که ممکن است هزینه‌زا یا زیان‌بار باشد منصرف می‌کند و هدف اصلی آن حفظ صلح است.(رحیمی‌روشن،۱۳۹۶:۸۲) بازدارندگی وضعیتی راهبردی است که در آن واحدها با اتکا به تهدید متقابل، امکان حمله مستقیم را از یکدیگر سلب می‌کنند. تحقق این وضعیت به قدرت و توان راهبردی طرفین وابسته است؛ زیرا قدرت زمانی معنا می‌یابد که در قالب تهدید قابل‌اعمال بازنمایی شود. بنابراین، متغیرهای مختلف نظام بین‌الملل و چرخه قدرت در شکل‌دهی به معادله تهدید متقابل نقش تعیین‌کننده‌ای دارند. در مجموع، بازدارندگی را می‌توان گونه‌ای تکامل‌یافته از نظریه موازنه قوا تلقی کرد.(قاسمی،۱۳۹۱:۱۱۰) از منظر واقع‌گرایی، انسان ذاتاً قدرت‌طلب است و برای دستیابی به منافع بیشتر از هیچ تلاشی فروگذار نمی‌کند. در چنین شرایطی، نبود قدرت دفاعی طرف مقابل موجب تشدید تمایل به تجاوز می‌شود و اصول اخلاقی یا تعهدات بین‌المللی قادر به مهار آن نیستند. مورگنتا بر این باور است که منشأ رفتار بشر قدرت‌طلبی ذاتی اوست و صلح تنها زمانی حاصل می‌شود که قدرت‌ها بتوانند از خود دفاع کنند. بنابراین، ریشه نظریه بازدارندگی را باید در مکتب رئالیسم جست‌وجو کرد، نظریه‌ای که در برابر آرمان‌گرایی قرار دارد و بر نقش تهدید در تأمین امنیت در نظام بین‌الملل آنارشیک

تأکید می‌ورزد. بازدارندگی در ساده‌ترین تعریف، جلوگیری از اقدام حریف از طریق تهدید به تحمیل هزینه‌های سنگین است. این نظریه پس از جنگ جهانی دوم و به‌ویژه با ظهور سلاح‌های هسته‌ای اهمیت یافت، زیرا ترس ناشی از قدرت تخریب این سلاح‌ها به عاملی برای حفظ صلح در نظام دوقطبی تبدیل شد. در این چارچوب، بازدارندگی بر ایجاد ترس و افزایش هزینه‌های احتمالی طرف مقابل برای منصرف کردن او از اقدام خصمانه استوار است.(هلالات،۱۴۰۰)

فضای سایبری

اصطلاح سایبری برگرفته از واژه یونانی «سایبرنتیک» به معنای راهبری است و در فارسی غالباً معادل فضای مجازی به‌کار می‌رود. فضای سایبری حاصل تعامل فناوری‌های اطلاعات و ارتباطات بوده و بر پایه داده‌ها، سیگنال‌ها و شبکه‌های ارتباطی شکل می‌گیرد. این فضا بستری نظام‌مند برای تبادل مستمر اطلاعات میان شبکه‌های آنلاین است و فرهنگی نوین پدید می‌آورد که نه تنها روابط اجتماعی را بازنمایی می‌کند، بلکه خود به عرصه‌ای برای شکل‌گیری و تداوم این روابط تبدیل می‌شود.(اختیاری‌امیری و همکاران،۱۴۰۰:۶۳) به نوعی این فضا می‌تواند عامل اساسی در فرهنگ سازی و هویت سازی و به تبع آن تأثیر مهمی در روند اجتماعی شدن افراد داشته باشد.(پاسبان،۱۴۰۲:۱۹)

فضای سایبری به‌عنوان نسل نوین روابط اجتماعی، با وجود عمر کوتاه خود، جایگاهی گسترده در زندگی افراد یافته و امکان برقراری ارتباط فراملی میان گروه‌های مختلف را فراهم آورده است. خانواده‌های ایرانی نیز در کنار رسانه‌های مدرن و شبکه‌های ماهواره‌ای با این فضا مواجه‌اند که هر یک بخشی از فرآیند تأثیرگذاری فرهنگی را بر عهده دارند. واژه «سایبر» ریشه در اصطلاح یونانی سایبرنتیک دارد که به مفاهیم کنترل، سیستم‌های رایانه‌ای پیشرفته و واقعیت‌های مصنوعی اشاره دارد و حتی در مفهوم «سایبورگ» به پیوند انسان و فناوری دلالت می‌کند. نفوذ این فضا نه تنها سبک زندگی را دگرگون ساخته، بلکه ساختار روابط بین‌الملل را نیز متحول کرده و عرصه‌ای نو از قدرت مبتنی بر تعاملات اقتصادی، فرهنگی و اجتماعی به وجود آورده است. ارتقای فضای سایبری به سطح میدان پنجم نبرد پس از زمین، دریا، هوا و فضا بیانگر پویایی و چالش‌های امنیتی و راهبردی ناشی از جنگ‌های سایبری است.(مرادی و همکاران،۱۴۰۱:۵۵)

فضای سایبری قلمرویی مبتنی بر علوم و فناوری‌های الکترونیک و ارتباطات است که در آن داده‌ها ذخیره، پردازش و مبادله می‌شوند. این فضا با تکیه بر شبکه‌ها و فناوری اطلاعات، یا بر اساس بازنمایی‌های تخیلی فاقد واقعیت عینی و یا بر پایه شبیه سازی‌های مبتنی بر واقعیت طراحی و بازآفرینی می‌گردد.(مقدسی‌لیچاهی و همت،۱۳۹۷: ۱۰۷). به‌عبارت دیگر می‌توان گفت فضای سایبری، فضایی است که در آن فعالیت‌های گوناگون در ابعاد داده‌ورزی و اطلاع رسانی، ارتباطات و ارائه خدمات، مدیریت و کنترل از طریق سازوکارهای الکترونیکی و مجازی انجام می‌پذیرد.(صدری و کروبی ،۱۳۸۴:۵۸) به عبارت دیگر فضای سایبری استعاره‌ای برای تشریح سرزمین غیرفیزیکی،تشکیل شده توسط سیستم‌های کامپیوتری است. برخلاف فضای حقیقی، سیر و گشت

در این سرزمین بدون هیچگونه حرکت فیزیکی مقدور است، تنها با حرکت موشواره با فشردن کلیدی در صفحه کلید.(عبدالله خانی و حسینی،۱۳۹۴:۵۱)

امنیت سایبری

امنیت سایبری به عنوان یکی از ابعاد نوین امنیت، نخستین بار در اواخر دهه ۱۹۶۰ و همزمان با شکل‌گیری شبکه‌های رایانه‌ای مطرح شد و در آغاز بر حفاظت از داده‌ها و منابع رایانه‌ای متمرکز بود. با گسترش اینترنت و افزایش وابستگی به ارتباطات دیجیتال، این مفهوم ابعاد گسترده‌تری به خود گرفت و اهمیت روزافزونی یافت. در ایران نیز شورای عالی فضای مجازی در مصوبه «توسعه فضای مجازی سالم، مفید و امن» بر تولید و توزیع محتوای ایمن و ممانعت از انتشار داده‌های مضر تأکید کرده است. در سطح جهانی، امنیت سایبری به مجموعه‌ای از قوانین، سیاست‌ها، دستورالعمل‌ها و راهکارهای فناورانه اطلاق می‌شود که هدف آن مقابله با تهدیداتی چون هک، تخریب داده‌ها، حملات سایبری و نقض حریم خصوصی است. این حوزه نه تنها شامل امنیت اطلاعات و سامانه‌ها می شود، بلکه امنیت کاربران، زیر ساخت‌های حیاتی و امنیت ملی را نیز دربر می‌گیرد. بر این اساس، امنیت سایبری در عصر انقلاب صنعتی چهارم به موضوعی کلیدی در تعامل با رژیم‌های بین‌المللی، نهادهای غیردولتی و فرایندهای جهانی‌شدن تبدیل شده و در اسناد راهبردی کشورها به عنوان ضرورتی حیاتی برای مقابله با تهدیدات نوین در فضای دیجیتال مورد تأکید قرار گرفته است.(نگهدار و همکاران،۱۴۰۲: ۱۰۱ـ۱۰۰)

امنیت سایبری به مجموعه اقداماتی اطلاق می‌شود که با هدف حفاظت از داده‌ها، شبکه‌ها، سامانه‌های دیجیتال و زیرساخت‌های رایانه‌ای در برابر تهدیدات مجرمانه و خرابکارانه انجام می‌گیرد. این مفهوم که در اسناد و سیاست‌های ملی دولت‌ها نیز به‌کار می‌رود، ارتباط نزدیکی با امنیت اینترنت داشته و ابعاد مختلفی همچون محرمانگی، یکپارچگی، دسترس‌پذیری و کنترل دسترسی را دربر می‌گیرد. محرمانگی شامل حفاظت از داده‌ها و صیانت از حریم خصوصی است؛ یکپارچگی بر صحت داده‌ها و عملکرد صحیح سامانه‌ها تأکید دارد؛ دسترس‌پذیری ناظر بر تضمین خدمات مستمر برای کاربران مجاز است؛ و در نهایت، کنترل دسترسی به تعیین سطح مجوزها و شرایط استفاده از منابع و محتوای دیجیتال مربوط می‌شود. بر این اساس، امنیت سایبری را می‌توان چارچوبی جامع برای مدیریت تهدیدات در فضای مجازی دانست که پیوندی مستقیم با سیاست‌گذاری کلان و قواعد حقوقی در سطح ملی و بین‌المللی دارد.(حقی و کارگری،۱۴۰۱: ۱۳ـ۱۲)

تهدید سایبری

تهدیدات سایبری به‌عنوان پدیده‌ای نوین همزمان با گسترش فناوری اطلاعات و اینترنت جهانی مطرح شده و به دلیل ماهیت پیچیده و چندبعدی خود، شناخت و مقابله با آن اهمیت ویژه‌ای دارد. این تهدیدات می‌توانند امنیت ملی را در ابعاد مختلف تحت تأثیر قرار داده و با آسیب به زیرساخت‌های حیاتی، پیامدهای گسترده‌ای بر زندگی شهروندان و ثبات کشور به همراه داشته باشند. در ایران نیز حملات سایبری عمدتاً متوجه بخش‌های مالی، هسته‌ای و نظامی بوده و اختلال یا افشای داده‌ها در این حوزه‌ها

می‌تواند نتایج فاجعه‌باری ایجاد کند. ازاین‌رو ارتقای امنیت سایبری، ایجاد سازوکارهای دفاعی کارآمد و بهره‌گیری از راهبرد بازدارندگی سایبری ضرورتی اجتناب‌ناپذیر است. طراحی نظام جامع پدافند سایبری باید با هدف پایش، رصد و مدیریت به‌موقع تهدیدات انجام گیرد تا زمینه خنثی‌سازی حملات و حفاظت از سرمایه‌های ملی سایبری فراهم شود.(خیاطیان‌یزدی و همکاران،۱۴۰۰: ۱۷۱ــ۱۷۰) نشت اطلاعات، سرقت داده‌های حیاتی و آسیب‌پذیری شبکه‌های اطلاع‌رسانی از مهم‌ترین چالش‌های امنیتی فضای سایبری به شمار می‌روند که در صورت بی‌توجهی حکومت‌ها می‌توانند تهدیدی جدی علیه منافع ملی باشند. اینترنت به‌عنوان بستر اصلی فضای سایبری، ضمن تسهیل دسترسی گسترده کاربران، به یکی از عوامل کلیدی در شکل‌گیری تهدیدات سایبری تبدیل شده و پیامدهای آن به‌ویژه در ارتباط با امنیت ملی و زیر ساخت‌های حیاتی کشورها ـــ به‌خصوص کشورهای درحال‌توسعه ـ اهمیت فزاینده‌ای یافته است.(موسی‌زاده وهمکاران،۱۴۰۰:۴۹)

حملات سایبری

پیشرفت فناوری موجب ظهور نوعی نوین از حملات تحت عنوان حملات سایبری شده است که ماهیتی متفاوت از حملات فیزیکی دارند. این حملات با بهره‌گیری از ضعف‌های ذاتی فضای سایبری شکل می‌گیرند، اما همچنان درباره تعریف و ماهیت دقیق آنها اجماع نظری در میان دولت‌ها و سازمان‌های بین‌المللی وجود ندارد. حملات سایبری، عملیات‌های خصمانه‌ای مبتنی بر مؤلفه‌های کامپیوتری‌اند که با هدف اخلال در کارکرد سامانه‌های هدف، کاستن از دسترسی‌پذیری و کارایی آنها، تزریق اطلاعات نادرست به‌منظور تضعیف فرایند تصمیم‌سازی کاربران و یا سرقت داده‌ها طراحی و اجرا می‌شوند. حملات سایبری از چند جهت با حملات متعارف تفاوت دارند: نخست، ناشناس بودن عاملان که ردیابی و شناسایی آنها را دشوار می‌سازد و مرزهای مکانی و فاصله را بی‌اثر می‌کند؛ دوم، هزینه اندک اجرای این حملات در مقایسه با جنگ‌های سنتی که انگیزه مهاجمان را افزایش می‌دهد؛ و سوم، ماهیت شبکه‌ای و توزیع‌شده مهاجمان که آنان را در برابر اقدامات تلافی‌جویانه مقاوم کرده و ظرفیت خودترمیمی‌شان را تقویت می‌کند.(برقعی،۱۳۹۳:۸۷)

قدرت سایبری

تحولات سیاست خارجی آمریکا نشان می‌دهد که راهبردهای قدرت در طول زمان تغییرات معناداری را تجربه کرده‌اند. در دوره جرج بوش، استفاده از قدرت سخت برای کسب مشروعیت بین‌المللی در دستور کار قرار گرفت، اما این رویکرد در پایان با ناکامی مواجه شد. با روی کار آمدن باراک اوباما، تأکید بر قدرت نرم افزایش یافت و ایالات متحده تلاش کرد با بهره‌گیری از ابزارهای فرهنگی، رسانه‌ای و فناوری، شبکه‌ای گسترده از متحدان جدید ایجاد کند. در این میان، قدرت سایبری به‌عنوان یکی از مهم‌ترین منابع نوظهور قدرت، جایگاهی میان قدرت سخت، نیمه‌سخت و نرم یافته است. این نوع قدرت به‌ویژه در شرایط کنونی که اطلاعات و فناوری‌های ارتباطی با سرعتی بی‌سابقه در حال گسترش‌اند، اهمیت ویژه‌ای دارد. قدرت نرم نیز که بر توانایی متقاعدسازی دیگران به‌جای اجبار استوار است در فضای سایبری کارآمدتر از هر زمان دیگری به کار گرفته می‌شود. صاحب‌نظران

قرن بیست‌ویکم را «عصر اینترنت و داده» می‌نامند و بر این باورند که تغییر بنیادین از قدرت فیزیکی به قدرت سایبری در حال وقوع است. جوزف نای، نظریه‌پرداز برجسته روابط بین‌الملل، فضای سایبری را «کلید قدرت در قرن بیست‌ویکم» معرفی می‌کند. این تحولات، بازتاب مستقیم «انقلاب اطلاعاتی» یا به تعبیر برخی، «انقلاب صنعتی سوم» است که بر پایه پیشرفت‌های رایانه‌ای، ارتباطی و نرم‌افزاری بنا شده و هزینه‌های تولید، پردازش، انتقال و جستجوی اطلاعات را به‌شدت کاهش داده است.

از منظر حکمرانی، فضای سایبری برای دولت‌ها بستر جدیدی از ابزارهای کنترلی و راهبردی فراهم ساخته است که مهم‌ترین آن‌ها عبارتند از:

- اعمال نفوذ بر ابزارهای تولید اطلاعات از جمله نرم‌افزارهای پردازشی؛
- کنترل دسترسی به فضای مجازی و شاه‌راه‌های اطلاعاتی؛
- بهره‌برداری از محتوای پیام‌ها و داده‌های کاربران؛
- ذخیره‌سازی و مدیریت اطلاعات در مقیاس فراملی؛
- هدایت فنی و تخصصی زیرساخت‌های اینترنت جهانی.

این موارد نشان می‌دهد که قدرت سایبری نه تنها ابزاری برای افزایش نفوذ در عرصه بین‌المللی است، بلکه به یکی از ارکان اصلی سیاست‌گذاری امنیتی دولت‌ها در جهان معاصر بدل شده است.(جعفری،۱۳۹۸:۱۱۶)

روش تحقیق

این پژوهش با رویکرد کیفی و مبتنی بر تحلیل اسنادی نظام‌مند انجام شده است. داده‌های تحقیق شامل اسناد سیاستی، قوانین و مقررات، مقالات علمی منتشرشده، گزارش‌های رسمی داخلی و بین‌المللی و شاخص‌های جهانی مرتبط با امنیت سایبری بوده‌اند. چارچوب کلی پژوهش توصیفی ـ تحلیلی است، اما فرایند تحلیل داده‌ها بر اساس روش تحلیل مضمون و با رویکرد تحلیل نهادی ـــ سیاستی صورت گرفته است. هدف از به‌کارگیری این روش، شناسایی و تبیین نظام‌مند چالش‌های ساختاری امنیت سایبری ایران و بررسی پیامدهای آن در سطح حکمرانی و امنیت ملی بوده است.

معیار استخراج یافته‌ها به شرح زیر تعیین شد:

- تکرار موضوع: هر چالشی که در بیش از یک منبع مورد اشاره قرار گرفته بود، به عنوان یافته اولیه ثبت شد.
- اهمیت و اثرگذاری: موضوعاتی که مستقیماً بر امنیت ملی، زیرساخت‌های حیاتی، اعتماد عمومی یا تاب‌آوری سایبری اثرگذار بودند، در اولویت استخراج قرار گرفتند.
- قابلیت تحلیل نهادی ـــــ سیاستی: تنها موضوعاتی در نظر گرفته شدند که امکان تحلیل در قالب چارچوب نظری بازدارندگی و ابعاد نهادی، حقوقی و فناورانه را داشتند.

- تطابق با شاخص‌های بین‌المللی: یافته‌ها با شاخص‌ها و گزارش‌های معتبر جهانی (مانند شاخص کیفیت زندگی دیجیتال، شکاف مهارت‌های دیجیتال) هم‌سنجی و صحت‌سنجی شدند.

با استفاده از این معیارها، استخراج یافته‌ها به صورت **سیستماتیک، شفاف و مستند** انجام شد. هر یافته، بر اساس منابع معتبر داخلی یا بین‌المللی مستند شده و قابلیت تحلیل و ارائه راهکارهای عملیاتی را داراست.

یافته‌های پژوهش

امنیت سایبری در ایران به‌دلیل گسترش وابستگی به زیرساخت‌های دیجیتال به یکی از حوزه‌های حیاتی امنیت ملی تبدیل شده است. یافته‌های این پژوهش نشان می‌دهد که چالش‌های امنیتی فضای سایبری صرفاً فنی نیستند، بلکه ابعاد نهادی، حقوقی، فرهنگی و حتی بین‌المللی را نیز در بر می‌گیرند. بررسی‌ها حاکی از آن است که ضعف در هماهنگی نهادی، خلأهای قانونی، کمبود نیروی متخصص، سطح پایین آگاهی عمومی و فشارهای ژئوپلیتیکی از مهم‌ترین عوامل آسیب‌پذیری کشور در این حوزه‌اند.

یافته‌های پژوهش نشان می‌دهد که جمهوری اسلامی ایران با مجموعه‌ای از آسیب‌پذیری‌های ساختاری و نهادی در حوزه امنیت سایبری مواجه است که شرح ذیل می‌باشد:

۱ـ چالش پیچیدگی فضای سایبری همراه با دیدگاه سنتی نسبت به امنیت در آن

فضای سایبری به دلیل ماهیت پویا، پیچیده و غیرقابل پیش‌بینی خود، کنترل‌پذیری محدودی دارد. در چنین فضایی لزوماً کنترل در دست دولت‌ها نیست و چندان هم روشن نیست چه چیزی فرصت است و چه چیزی تهدید. با این حال، نگاه سنتی و دولت‌محور به امنیت که عمدتاً نظامی‌زده است، امکان شناسایی دقیق تهدیدها و فرصت‌های این فضا را محدود می‌سازد. در ایران، این رویکرد منجر به سیاست‌هایی چون فیلترینگ گسترده و کاهش سرعت اینترنت شده است که نتیجه آن عقب‌ماندگی فناورانه و وابستگی به نرم‌افزارها و سخت‌افزارهای خارجی است.(ترابی،۱۳۹۷: ۱۷۴).

۲ـ چالش کاربر محوری در فضای سایبری

اصطلاح کاربر بودن در فضای سایبری معمولاً به استفاده افراد از سخت‌افزار و نرم‌افزار اشاره دارد، اما این مفهوم را می‌توان به سطح کشورها نیز تعمیم داد. بسیاری از دولت‌ها در این حوزه عمدتاً مصرف‌کننده‌اند و نقشی در شکل‌گیری ساختارها و قواعد کلان آن ندارند؛ وضعیتی که نگرانی‌های امنیتی قابل توجهی ایجاد کرده است. حتی متحدان آمریکا در اروپا نیز در این زمینه دغدغه دارند و خواهان بومی‌سازی بخشی از زیرساخت‌ها هستند. در ایران نیز طرح شبکه ملی اطلاعات و سیاست‌هایی چون محدودسازی برخی شبکه‌های خارجی در همین چارچوب قابل تبیین است، هرچند میزان اثرگذاری آن‌ها بر کاهش آسیب‌پذیری‌ها همچنان محل بحث است. ایران بیشتر مصرف‌کننده فناوری‌های دیجیتال است تا تولیدکننده. اتکا به نرم‌افزارها و سخت‌افزارهای وارداتی، خطر نفوذ بدافزارها و تجهیزات جاسوسی را افزایش داده است. گزارش‌هایی نظیر یافته‌های شرکت کسپرسکی در سال ۱۳۹۴، میزان بالای آلودگی گوشی‌ها و دستگاه‌های دیجیتال ایرانیان را نشان می‌دهد. این وابستگی، یکی از آسیب‌پذیری‌های بنیادین

کشور در فضای سایبری به شمار می‌رود.(ترابی،۱۳۹۷: ۱۷۵) از طرفی دیگر یکی از معضلات اساسی در حوزه نرم‌افزارهای داخلی، تولید ابزارهایی است که بیشتر «شکل بومی» دارند تا محتوای واقعی بومی. این نرم‌افزارها در عمل بر پایه کدهای متن‌باز خارجی بنا شده‌اند، اما به دلیل نبود فرآیند مستمر برای ارتقا و به‌روزرسانی، به مرور زمان دچار ضعف‌های جدی می‌شوند. تغییرات محدود و غیرکار شنا سی که روی آن‌ها اعمال شده، نه‌تنها سطح ایمنی را افزایش نداده، بلکه احتمال بروز خطاها، نا سازگاری‌ها و رخنه‌های امنیتی را بیشتر کرده است. بر این اساس، ضروری است که برای کاهش این آسیب‌پذیری‌ها، راهبردی بلندمدت و چندلایه طراحی شود. حمایت هدفمند از بخش خصوصی برای تقویت نوآوری، ایجاد بسترهای حمایتی برای استارت‌آپ‌های بومی فعال در عرصه فناوری اطلاعات و تو سعه برنامه‌های آموز شی در حوزه تربیت نخبگان سایبری از جمله اقدامات کلیدی به شمار می‌روند. تنها با چنین رویکردی است که می‌توان آینده‌ای امن‌تر و پایدارتر در عرصه حکمرانی سایبری برای کشور ترسیم کرد.

۳ـ ضعف اعتماد عمومی نسبت به دولت در حوزه سایبری

بی‌اعتمادی کاربران به سیاست‌های سایبری داخلی باعث گرایش گسترده به استفاده از شبکه‌های اجتماعی خارجی و فیلترشکن‌ها شده است. این وضعیت علاوه بر تهدید امنیت اطلاعات داخلی، موجب افزایش آسیب‌پذیری در برابر بازیگران خارجی نیز می‌گردد. ناکامی سیاست‌های محدودکننده در این حوزه ضرورت بازسازی اعتماد متقابل میان حاکمیت و جامعه را برجسته می‌سازد (ترابی،۱۳۹۷: ۱۷۶). بر اساس گزارش سال ۲۰۲۳ «شاخص کیفیت زندگی دیجیتال» شرکت سورفشارک، جایگاه ایران طی دوره ۲۰۲۰ تا ۲۰۲۳ روندی نزولی داشته و امتیاز کلی آن به ۰,۳۴ رسیده است. این شاخص شامل پنج بعد اصلی مقرون‌به‌صرفه بودن، کیفیت و زیرساخت اینترنت، دولت الکترونیک و امنیت الکترونیک است. افت هم‌زمان ایران در تمامی این زیرشاخص‌ها بیانگر ضعف در دسترسی پایدار و امن به خدمات دیجیتال و کاهش استانداردهای زیست دیجیتال شهروندان است. پیامد چنین شرایطی بروز م شکلاتی چون نقض حریم خ صو صی، محدودیت در د ستر سی به خدمات، کاهش انبا شت داده و در نهایت افت جذابیت استفاده از فضای مجازی است. این روند به شکل مستقیم بر اعتماد عمومی به نهادهای دولتی در حوزه سایبری اثر می‌گذارد و موجب تقویت شکاف میان دولت و کاربران در فضای مجازی می‌شود. (اخوان و همکاران،۱۴۰۳:۱۷)

برای نمونه در این زمینه یافته‌های نظرسنجی ایسپا در بهمن ۱۴۰۲ نشان می‌دهد که بخش عمده کاربران ایرانی همچنان به استفاده از پیام‌رسان‌ها و شبکه‌های اجتماعی خارجی گرایش دارند؛ به‌گونه‌ای که ۴۶,۵ درصد از اینستاگرام، ۳۵,۳ درصد از واتساپ و ۳۴,۶ در صد از تلگرام ا ستفاده می‌کنند، در حالی که سهم پیام‌ر سان‌های داخلی مانند ایتا (۲۵,۲ در صد)، روبیکا (۲۴,۱ در صد) و بله (۸,۷ درصد) به‌مراتب پایین‌تر است. این اختلاف آشکار، ریشه در محدودیت‌های فنی، کمبود قابلیت‌های کاربرپسند، ضعف در اعتمادپذیری و نیز محدودیت در برقراری ارتباط جهانی پیام‌ر سان‌های داخلی دارد. در نتیجه، کاربران تمایل بی شتری به ا ستفاده از پلتفرم‌های خارجی با وجود فیلترینگ نشان می‌دهند. چنین رفتاری بیانگر کاهش اعتماد عمومی به ظرفیت‌ها و سیا ست‌های دولت در ساماندهی فضای سایبری است و نشان می‌دهد که محدودیت‌ها نه‌تنها کارآمدی نداشته، بلکه خود عاملی برای تقویت

بی‌اعتمادی و روی‌آوردن مردم به ابزارهای غیررسمی (مانند فیلترشکن‌ها) شده است.(همان: ۱۸) راه برون‌رفت از این وضعیت، نه در سیاست‌های محدودکننده، بلکه در ایجاد راهبردی متوازن میان استفاده از ظرفیت‌های شبکه‌های اجتماعی و کاهش تهدیدات آن‌هاست. تحقق چنین رویکردی نیازمند بازسازی اعتماد عمومی نسبت به حاکمیت است. در صورتی که این سرمایه اجتماعی ترمیم نشود، هرگونه اقدام سخت‌گیرانه در فضای سایبری می‌تواند پیامدهایی معکوس داشته و به گسترش بحران منجر شود و ضعف اعتماد عمومی با کاهش همکاری کاربران در سیاست‌های امنیت سایبری، موجب تضعیف بازدارندگی انکاری و کاهش تاب‌آوری ملی در برابر حملات سایبری می‌شود.

۴ـ نبود چارچوب راهبردی یکپارچه برای مدیریت فضای سایبری

یکی از مهم‌ترین چالش‌هایی که کشور ما در عرصه فضای سایبری با آن مواجه است، فقدان یک راهبرد منسجم، کارآمد و بلندمدت به شمار می‌رود. این موضوع به معنای نبود مطلق اسناد و برنامه‌های مرتبط با حوزه سایبری در ایران نیست؛ بلکه مسئله اصلی را می‌توان در عدم وجود بسترهای نهادی، حقوقی و اجرایی مناسب برای طراحی، تصویب و به‌ویژه عملیاتی‌سازی یک راهبرد جامع دانست. ریشه این ضعف را می‌توان در ورود دیرهنگام ایران به عرصه فضای سایبری و همچنین عدم همسویی ساختارهای دولتی و اجتماعی با تحولات شتابان ناشی از انقلاب دیجیتال و فناوری‌های نوین جستجو کرد. علاوه بر این، می‌توان به تعویق و ناتمام‌ماندن پروژه‌هایی همچون شبکه ملی اطلاعات نیز به‌عنوان نمونه‌ای بارز از مشکلات ساختاری در مسیر تحقق حکمرانی سایبری اشاره نمود.(موحدی صفت و همکاران،۱۴۰۲:۷۸). ایران تاکنون فاقد راهبردی جامع و کارآمد در حوزه سایبری بوده و اقدامات نهادهای متولی عمدتاً جزیره‌ای و پراکنده است. این وضعیت، هم‌افزایی ملی را کاهش داده و فرصت‌ها را از بین برده است. تدوین یک راهبرد ملی مبتنی بر شناخت فرصت‌ها و تهدیدها، تقسیم وظایف نهادی، تقویت بخش خصوصی و توسعه همکاری‌های علمی و بین‌المللی ضروری به نظر می‌رسد.(ترابی،۱۳۹۷: ۱۷۷).

افزون بر این، تداخل وظایف، تعدد نهادهای تصمیم‌گیر و تصدی‌گری‌های بی ضابطه در تقسیم کار نهادی میان دستگاه‌های حاکمیتی و ذی‌نفعان مختلف، بویژه بخش خصوصی، به تشدید نابسامانی‌ها انجامیده است. برای نمونه در حوزه فیلترینگ، علی‌رغم وجود سازوکار رسمی، ورود نهادهای متعدد به فرایند تصمیم‌گیری موجب افزایش پیچیدگی و سردرگمی شده است. همچنین در اجرای سند صیانت از کودکان و نوجوانان در فضای مجازی نیز تصدی‌گری پراکنده دستگاه‌های دولتی مانع شکل‌گیری چرخه منسجم تولید محتوا و خدمات بومی برای این گروه سنی شده است. از سوی دیگر، خلأها و موانع قانونی و نیز ضعف در اجرای قوانین مصوب از دیگر چالش‌های مهم‌اند. شواهدی مانند عملکرد قانون برنامه ششم توسعه در حوزه رسانه و فضای مجازی نشان می‌دهد که مشکلاتی نظیر بی‌توجهی دستگاه‌های اجرایی، تأخیر در تصویب آیین‌نامه‌ها، پراکندگی اطلاعات عملکردی، کمبود منابع مالی و فقدان شاخص‌های ارزیابی مناسب، مانع تحقق اهداف بوده است. همچنین در حوزه مقابله با نشر اکاذیب و اطلاعات نادرست، اگرچه قوانین موجود تدوین شده‌اند، اما ضعف ضمانت‌های اجرایی و بازدارندگی کافی همچنان این حوزه را آسیب‌پذیر

نگاه داشته است.(اخوان و همکاران،۱۴۰۳:۱۱) نبود چارچوب راهبردی یکپارچه در حوزه امنیت سایبری، مستقیماً مؤلفه «اعتبار تهدید» در نظریه بازدارندگی را تضعیف می‌کند. زیرا در غیاب تقسیم کار نهادی روشن و پاسخ هماهنگ، بازیگران مهاجم نسبت به توان واکنش مؤثر کشور دچار تردید نمی‌شوند. در نتیجه، بازدارندگی تنبیهی فاقد انسجام عملیاتی شده و ظرفیت هزینه‌سازی کاهش می‌یابد. برای عبور از این چالش، نیاز به راهبردی جامع وجود دارد که نه‌تنها تهدیدهای امنیتی و فناورانه را شناسایی کند، بلکه فرصت‌های اقتصادی، فرهنگی و علمی را نیز به خدمت بگیرد. این راهبرد باید مبتنی بر نگاه بلندمدت بوده و ابعادی همچون تعیین مرجع واحد تصمیم‌گیری، ایجاد مراکز پژوهشی تخصصی، تربیت نخبگان سایبری، گسترش آموزش‌های مرتبط در سطوح مختلف، تنظیم تقسیم کار ملی میان نهادها، و ایجاد هماهنگی میان دولت، دانشگاه و بخش خصوصی را دربر گیرد.

۵ـ عدم تطابق با تغییرات ناشی از انقلاب سایبری

ساختارهای سیاسی، نظامی و اداری کشور همچنان در چارچوب‌های سنتی عمل می‌کنند و کمتر با تحولات سایبری سازگار شده‌اند. این در حالی است که کشورهایی چون آمریکا اصلاحات جدی در ساختارهای اطلاعاتی و امنیتی خود برای مقابله با تهدیدات سایبری انجام داده‌اند. برای ایران نیز بازنگری ساختاری، آموزش تخصصی نیروی انسانی و جذب نخبگان سایبری پیش شرط‌های اساسی ارتقای تاب‌آوری در این حوزه محسوب می شود.(ترابی،۱۳۹۷: ۱۷۸). از آغاز ورود و گسترش فضای مجازی در ایران، نگاه حاکم نسبت به این فناوری غالباً بدبینانه بوده و به‌رغم گذشت چند دهه، این نگرش چندان اصلاح نشده است. در نتیجه سیاست‌گذاری‌ها بیشتر رویکردی سلبی و از بالا به پایین داشته‌اند تا ایجابی و مشارکتی. این نوع سیاست‌گذاری عمدتاً بر کنترل و محدودیت (مانند فیلترینگ و سامانه‌های نظارتی) متمرکز بوده که همواره با مقاومت جامعه مدنی روبه‌رو شده است. برخورد صرفاً سلبی نه تنها ناکارآمدی خود را نشان داده بلکه با ماهیت پویای فضای سایبری نیز در تضاد است. به همین دلیل، ضرورت حرکت به‌سوی سیاست‌های ایجابی همچون آموزش و ارتقای سواد رسانه‌ای، بومی‌سازی محتوا و جلب مشارکت اجتماعی بیش از پیش احساس می شود. چنین رویکردی می‌تواند تعادلی میان نگاه بالا به پایین و پایین به بالا ایجاد کند و هم‌زمان دولت و جامعه را در فرآیند سیاست‌گذاری دخیل نماید. تجربه سایر کشورها نشان می‌دهد که موفقیت در مدیریت فضای مجازی مستلزم تمرکز بر نوآوری، حمایت از پژوهش و توسعه، ایجاد دانشگاه‌های پژوهش‌مدار، ارتقای همکاری‌های بین‌المللی، و مشارکت بخش خصوصی است. اما در ایران همچنان شکاف میان اهداف کلان امنیتی و الزامات توسعه‌ای به‌عنوان نشانه‌ای از عدم تطابق با تغییرات ناشی از انقلاب سایبری باقی مانده است. بنابراین یافته‌ها نشان می‌دهد که تمرکز بیش از حد بر سیاست‌های بازدارنده و امنیت‌محور، موجب ناهماهنگی با نیازهای واقعی جامعه و تحولات سریع فناوری شده است. راهکار اساسی، بازنگری در فرایند سیاست‌گذاری و حرکت به سمت ترکیب سیاست‌های ایجابی و مشارکتی است تا از یک‌سو امنیت ملی حفظ شود و از سوی دیگر، بستر رشد نوآوری و تعامل سازنده در فضای مجازی فراهم گردد.(درویش‌زاده،۱۴۰۲:۴۱)

۶ـ کمبود توان آموزشی، آگاهی عمومی و نیروی انسانی متخصص در جامعه در فضای سایبری

یکی از عوامل تمایزبخش کشورها در مواجهه با تحولات فناوری اطلاعات و ارتباطات، سطح دانش و آگاهی تخصصی و راهبردی آن‌ها ست. کشورهایی که توانسته‌اند فضای سایبری را به‌مثابه یک زیست‌بوم نوین درک کنند، معمولاً با تکیه بر دانش عمیق و نیروهای متخصص، برنامه‌ریزی منسجم و هماهنگ را دنبال کرده‌اند. در مقابل، کمبود آموزش عمومی، آگاهی سازنده و نیروی انسانی متخصص در ایران، مانع شکل‌گیری چنین تلاش‌های ساختارمندی شده و ظرفیت بهره‌گیری از فرصت‌های فضای سایبری را به میزان قابل توجهی کاهش داده است. (دهقانی و همکاران،۱۹۹:۱۴۰۲) فضای سایبری در ایران با کاستی‌های جدی دانشی روبه‌روست که این امر به ضعف درک و تحلیل جامع در حوزه‌های مرتبط منجر شده است. هرچند به دلیل سابقه‌ی رشته‌هایی همچون مهندسی کامپیوتر و فناوری اطلاعات، بُعد فنی وضعیت بهتری دارد، اما سایر ابعاد علمی همچنان مغفول مانده‌اند. در حالی که دانشگاه‌های معتبر جهان با ایجاد رشته‌هایی مانند «مطالعات سایبر» و «مطالعات اینترنت» در پی گسترش دانش میان‌رشته‌ای هستند، نظام دانشگاهی ایران اقدام مؤثری در این زمینه نداشته است. تنها برخی مراکز آموزشی با رویکرد دفاعی، مانند دانشگاه عالی دفاع ملی، رشته‌هایی محدود و عمدتاً امنیت‌محور ایجاد کرده‌اند. این تمرکز یک‌جانبه موجب شده کمبود آموزش عمومی و فقدان نیروی متخصص در حوزه‌های غیردفاعی همچنان به‌عنوان یک چالش اساسی باقی بماند. ترکیب مدیران و سیاست‌گذاران حوزه سایبری در ایران، که اغلب دارای پیشینه فرهنگی و نظامی هستند، سبب غلبه رویکرد امنیتی بر حکمرانی فضای مجازی شده است. این تمرکز یک‌جانبه نه تنها مانع از توجه به ابعاد آموزشی، آگاهی‌بخشی عمومی و تربیت نیروی متخصص شده، بلکه قدرت راهبردی کشور در بهره‌گیری جامع از ظرفیت‌های فضای سایبری را نیز محدود ساخته است.(همان:۲۰۰) گزارش جهانی «شکاف مهارت‌های دیجیتال» در سال ۲۰۲۱ نشان می‌دهد که ایران در میان ۱۳۴ کشور در جایگاه ۸۱ قرار گرفته و امتیاز کلی ۴,۴ را به دست آورده است. بررسی جزئیات این شاخص گویای آن است که عملکرد کشور در برخی حوزه‌ها به‌ویژه در «نهادهای توسعه مهارت‌های دیجیتال» (رتبه ۸۲، امتیاز ۴,۰)، «پشتیبانی دولتی» (رتبه ۸۹، امتیاز ۳,۵) و «پاسخگویی دیجیتال» (رتبه ۷۳، امتیاز ۴,۵) کمتر از سطح میانگین جهانی بوده است. در عین حال، رتبه بسیار پایین ایران در «عرضه، تقاضا و رقابت‌پذیری» (رتبه ۱۱۰، امتیاز ۴,۲) به‌عنوان یکی از چالش‌های کلیدی مطرح است، چراکه می‌تواند مستقیماً بر کیفیت و تنوع محتوای دیجیتال و خدمات آنلاین اثر منفی بگذارد. در مقابل، در برخی حوزه‌ها وضعیت نسبتاً مطلوب‌تری مشاهده می‌شود؛ به‌طور خاص در شاخص «اخلاق و صحت داده» ایران با رتبه ۶۱ و امتیاز ۶,۴ عملکرد بهتری نسبت به سایر حوزه‌ها داشته و در شاخص «شدت تحقیق» نیز با رتبه ۳۵ و امتیاز ۵,۲ جایگاه قابل قبولی را کسب کرده است. مقایسه منطقه‌ای نتایج نشان می‌دهد که ایران از کشورهای همسایه و رقیب مانند امارات متحده عربی (رتبه ۲)، عربستان سعودی (۲۸) و عمان (۲۵) عقب‌تر است، در حالی که جایگاه آن در مقایسه با کشورهایی مانند ترکیه (۷۹) و کویت (۶۷) نزدیک‌تر به وضعیت موجود است. این داده‌ها بیانگر آن است که برای ارتقای کیفیت محتوای دیجیتال و افزایش توان رقابتی در فضای مجازی، توجه به حمایت‌های دولتی، تقویت نهادهای مهارت‌آفرینی دیجیتال و افزایش ظرفیت بازار ضروری است. (اخوان و همکاران،۱۷:۱۴۰۳)

۷ـ چالش ضعف ساختاری در هماهنگی نهادی و رویکردهای پاسخگویی

این بحث این را بیان می‌کند که امنیت سایبری صرفاً یک مسئله فنی یا وابسته به دولت‌های مقطعی نیست، بلکه بخشی بنیادین از امنیت ملی و حافظ زیر ساخت‌های حیاتی کشور، حریم خصوصی شهروندان و اعتماد عمومی به فضای دیجیتال محسوب می‌شود. تهدیدات سایبری ماهیتی فرادولتی دارند و بدون توجه به تقویم سیاسی، به‌صورت مستمر توسط بازیگران متنوعی همچون گروه‌های سازمان‌یافته یا هکرهای مستقل دنبال می‌شوند. تغییر رویکرد یا جابه‌جایی منابع انسانی و سازمانی همزمان با تغییر دولت‌ها، موجب ناپایداری و ایجاد خلأهای امنیتی می‌شود؛ وضعیتی که مهاجمان سایبری به‌خوبی از آن بهره‌برداری می‌کنند. همچنین، تنوع دیدگاه‌های دولتی نسبت به حفاظت از داده‌ها و حریم خصوصی می‌تواند اعتماد عمومی را تضعیف نماید. بر این اساس، نهادهای مسئول امنیت سایبری نیازمند ثبات ساختاری، استقلال حرفه‌ای و برنامه‌ریزی بلندمدت هستند. تجارب کشورهای پیشرفته نیز نشان می‌دهد که ایجاد نهادهای تخصصی و غیرسیاسی در این حوزه، تضمین‌کننده استمرار چارچوب‌های حفاظتی و حفظ سرمایه انسانی متخصص است. در نتیجه، امنیت سایبری باید به‌عنوان بخشی پایدار از امنیت ملی و نه تابعی از سیاست‌های کوتاه‌مدت، مورد توجه قرار گیرد. سیاسی‌شدن امنیت سایبری از مهم‌ترین چالش‌های تضعیف‌کننده امنیت ملی به شمار می‌رود. در ایران نیز بروز این پدیده در برخی مقاطع، پیامدهایی جدی به همراه داشته است. نخست، وابستگی تصمیم‌ها و ساختارهای امنیتی به تغییرات سیاسی موجب بی‌ثباتی مدیریتی، موازی‌کاری نهادی و اتلاف منابع می شود و برنامه‌ریزی بلندمدت را مختل می سازد. دوم، کاهش اعتماد عمومی از پیامدهای مستقیم سیاسی‌سازی است؛ زیرا شهروندان زمانی که سیاست‌های مرتبط با حریم خصوصی و کنترل داده‌ها را ناشی از ملاحظات سیاسی بدانند، همکاری خود را کاهش داده و به استفاده از پلتفرم‌های خارجی یا ابزارهای غیررسمی روی می‌آورند. از سوی دیگر، در فضای سیاسی‌شده، امنیت سایبری گاه به ابزاری برای کنترل اجتماعی تقلیل می‌یابد و این امر باعث غفلت از تهدیدات واقعی و فنی می‌شود. همچنین، کاهش انگیزه و مهاجرت متخصصان یکی دیگر از پیامدهای جدی است که کشور را از سرمایه انسانی حیاتی محروم می‌کند. در مجموع، یافته‌ها نشان می‌دهد که استمرار این روند می‌تواند امنیت سایبری را از یک سپر دفاعی ملی به یک نقطه‌ضعف ساختاری تبدیل کند. راهکار مؤثر، ایجاد ساختاری تخصصی، مستقل و ملی است که خارج از فضای رقابت‌های سیاسی عمل کرده و ثبات، انسجام و پاسخگویی را در این حوزه تضمین نماید.(خبرگذاری آنا:۱۴۰۴)

با توجه به مطالب گفته شده در جدول ذیل می‌توان پیوند نظریه بازدارندگی با یافته‌های تحقیق را مشاهده کرده که به شرح ذیل می‌باشد:

یافته پژوهش	بعد چارچوب بومی (نهادی/اجتماعی/فناورانه)	تأثیر بر بازدارندگی سایبری	توضیح/پیامد سیاستی
پیچیدگی فضای سایبری و نگاه سنتی به امنیت	نهادی	کاهش بازدارندگی تنبیهی	ضرورت تغییر رویکرد دولت‌محور به سیاست‌های منعطف و ایجابی
ضعف بومی‌سازی زیرساخت و نرم‌افزارها	فناورانه	کاهش بازدارندگی تنبیهی و تاب‌آوری	حمایت از نوآوری و استارتاپ‌های داخلی
ضعف اعتماد عمومی	اجتماعی	کاهش بازدارندگی انکاری	بازسازی اعتماد از طریق آموزش و شفافیت
نبود چارچوب راهبردی یکپارچه	نهادی	تضعیف بازدارندگی تنبیهی	تدوین راهبرد ملی جامع و بلندمدت
عدم تطابق با تحولات انقلاب سایبری	نهادی/فناورانه	کاهش تاب‌آوری	اصلاح ساختارهای تصمیم‌گیری و جذب نخبگان
کمبود نیروی انسانی متخصص و آگاهی عمومی	اجتماعی/فناورانه	کاهش بازدارندگی انکاری و تاب‌آوری	سرمایه‌گذاری در آموزش و رشته‌های میان‌رشته‌ای
ضعف هماهنگی نهادی و پاسخگویی	نهادی	کاهش بازدارندگی تنبیهی	ایجاد نهاد مستقل، تخصصی و پایدار

نتیجه‌گیری و پیشنهادات

یافته‌های این پژوهش نشان می‌دهد که امنیت سایبری در ایران صرفاً یک موضوع فناورانه نیست، بلکه ابعاد نهادی، حقوقی، فرهنگی و حتی اجتماعی و سیاسی را نیز در بر می‌گیرد. چالش‌هایی همچون ضعف هماهنگی نهادی، نبود راهبرد جامع و یکپارچه، کمبود نیروی انسانی متخصص، بی‌اعتمادی عمومی به سیاست‌های سایبری، وابستگی فناورانه به خارج و ناتوانی در تطبیق با تحولات ناشی از انقلاب دیجیتال، از مهم‌ترین موانع در مسیر ارتقای امنیت سایبری کشور هستند. افزون بر این، شدت یافتن حملات سایبری و گسترش تهدیدات پیچیده از سوی بازیگران دولتی و غیردولتی، ضرورت بازاندیشی در سیاست‌ها و راهبردهای امنیت سایبری ایران را دوچندان کرده است. بنابراین می‌توان نتیجه گرفت که مواجهه مؤثر با تهدیدات و مخاطرات نوظهور در این عرصه، مستلزم اتخاذ رویکردی جامع، آینده‌نگر و میان‌رشته‌ای است که بتواند ضمن ارتقای انسجام نهادی، راه را برای ایجاد اعتماد عمومی و ارتقای تاب‌آوری سایبری در سطح ملی هموار سازد.

با توجه به تحلیل‌های صورت‌گرفته، پیشنهادهای زیر می‌تواند به بهبود وضعیت امنیت سایبری در ایران کمک نماید:

- تدوین راهبرد ملی یکپارچه: ایجاد سندی جامع و بلندمدت در حوزه امنیت سایبری با تقسیم وظایف روشن میان نهادهای مسئول، و پرهیز از موازی‌کاری نهادی

- تقویت سرمایه انسانی: سرمایه‌گذاری در آموزش تخصصی، ایجاد رشته‌های میان‌رشته‌ای مرتبط با مطالعات سایبری، و تربیت نخبگان در حوزه‌های فنی، حقوقی و اجتماعی
- ارتقای آگاهی عمومی: توسعه برنامه‌های آموزش عمومی و سواد رسانه‌ای با هدف افزایش درک شهروندان از تهدیدات و مسئولیت‌های فردی در فضای مجازی
- بومی سازی زیر ساخت‌ها و فناوری‌ها: حمایت هدفمند از بخش خصوصی و استارتاپ‌ها برای تولید نرم‌افزار و سخت‌افزار بومی و کاهش وابستگی به فناوری‌های خارجی
- ایجاد نهاد مستقل و غیرسیاسی: تشکیل سازمانی ملی و تخصصی در حوزه امنیت سایبری که از فضای سیاسی فاصله داشته و بتواند با ثبات و انسجام، اقدامات حفاظتی را دنبال کند
- تقویت همکاری‌های بین‌نهادی و بین‌المللی: افزایش تعامل میان دولت، دانشگاه‌ها و بخش خصوصی در سطح داخلی، و گسترش همکاری‌های علمی و فناورانه در سطح بین‌المللی برای بهره‌گیری از تجربیات موفق جهانی
- حرکت از سیاست‌های سلبی به ایجابی: جایگزینی رویکرد صرفاً محدودکننده با سیاست‌های ایجابی و مشارکتی، از طریق حمایت از تولید محتوای بومی، جلب مشارکت جامعه مدنی و تقویت اعتماد عمومی
- استفاده از فناوری‌های نوین: بهره‌گیری از ظرفیت‌های هوش مصنوعی، کلان‌داده و یادگیری ماشین در حوزه پایش، پیش‌بینی و مقابله با تهدیدات سایبری

فهرست منابع؛

۱. اختیاری‌امیری،رضا و تابعی،سیدمحمدصادق و دهرویه،عباس.(۱۴۰۰). "تلگرام و امنیت ملی جمهوری اسلامی ایران ". فصلنامه راهبرد سیاسی. سال پنجم. شماره۱. بهار. صص ۸۲ـ۵۵

۲. اخوان،منیژه و قاسمی‌نژاد،عبدالرحیم و فروزان‌فر،محمدمهدی.(۱۴۰۳). پویایی شناسی مسائل و نابسامانی های فضای مجازی در ایران. ماهنامه گزارش‌های کارشناسی مرکز پژوهش‌های مجلس شورای اسلامی. دوره۳۲. شماره ۴. صفحات ۳۱ـ۱

۳. برقعی، سیدمهدی.(۱۳۹۳). مروری بر امنیت سایبری؛ درس‌هایی برای جمهوری اسلامی ایران. فصلنامه علمی پژوهشی مطالعات انقلاب اسلامی. سال یازدهم. پاییز. صفحات ۱۰۴ـ۸۵

۴. پاسبان،ابوالفضل.(۱۴۰۲). "حاکمیت حقوقی دولت‌ها بری فضای مجازی و تأثیر آن بر امنیت ملی". نشریه علمی سیاست دفاعی. سال ۳۲. زمستان. صص ۴۸ـ۱۱

۵. ترابی،قاسم.(۱۳۹۷). "چالش‌ها و آسیب‌پذیری‌های جمهوری اسلامی ایران در فضای سایبر". فصلنامه مطالعات راهبردی. دوره ۲۱، شماره ۷۹. صص ۱۷۸ـ۱۷۳

۶. جعفری،افشین.(۱۳۹۸). حاکمیت بر فضای سایبر از منظر حقوق بین‌الملل و نظام حقوقی جمهوری اسلامی ایران. فصلنامه رهیافت انقلاب اسلامی. سال ۱۳. شماره ۴۹. صفحات ۱۳۲ـ۱۰۹

۷. حقی،مجید و کارگری،مهرداد.(۱۴۰۱). "ارائه مدل مفهومی دفاع سایبری امنیت محور جمهوری اسلامی ایران". فصلنامه مطالعات راهبردی فضای سایبر. سال اول. شماره۳. زمستان. صص ۳۲ـ۷

۸. خیاطیان‌یزدی،محمدصادق و رحیمی‌راد،زهره و فرتاش،کیارش و سعدآباد،علی.(۱۴۰۰). "علم و فناوری در الگوی اسلامی‌ـایرانی پیشرفت با رویکرد مصون سازی راهبردی ور منظومه پدافند غیرعامل". فصلنامه علمی مطالعات امنیت اقتصادی. سال اول. شماره چهارم. تابستان. صص ۱۸۲ـ۱۵۵

۹. خبرگذاری آنا.(۱۴۰۴). چندصدایی در حوزه سایبری؛ نقطه ضعف بزرگ برای ایران. کد خبر ۹۸۳۵۹۸. برگرفته از سایت https://ana.ir/fa/news/۹۸۳۵۹۸

۱۰. دهقان،علی‌اصغر و پوراحمدی‌میبدی،حسین و ناصری،مجتبی.(۱۴۰۲). ارزیابی و پیشنهادات سیاست‌گذاری فضای سایبر در جمهوری اسلامی ایران. پژوهش‌های روابط بین‌الملل. دوره ۱۳. شماره۳. صفحات ۲۱۷ـ۱۸۷

۱۱. دروش‌زاده، سیف‌الدین.(۱۴۰۲). واکاوی سیاستگذاری فناوری اطلاعات و فضای مجازی در ایران در عصر جهانی شدن. مجله بین‌المللی پژوهش ملل. دوره۹. شماره۹۵. صفحات ۳۵ـ۵۷

۱۲. رحیمی‌روشن،حسن.(۱۳۹۶). "بازدارندگی منطقه‌ای و تأمین امنیت جمهوری اسلامی ایران". فصلنامه سیاست و روابط بین‌الملل. سال اول. شماره اول. بهار و تابستان. صص ۹۹ـ۷۹

۱۳. صدری،سیدمحمدرضا و کروبی،محمدتقی.(۱۳۸۴). ابعاد حقوقی محیط سایبر در پرتو توسعه ملی. تهران: نشر بقعه

۱۴. عبدالله‌خانی،علی و حسینی،پرویز.(۱۳۹۴). "سنجش تهدیدات سایبری". فصلنامه امنیت ملی. سال۴، شماره۱۶، تابستان. صص ۸۲ـ۴۵

۱۵. قاسمی،فرهاد.(۱۳۹۱). "پیاز سازی مفهوم نظریه بازدارندگی منطقه‌ای و طراحی الگوهای آن بر اساس نظریه‌های چرخه قدرت و شبکه". فصلنامه راهبرد دفاعی. سال دهم. شماره ۳۸. تابستان. صص ۱۴۶ـ۱۰۳

۱۶. مرادی،محمدرضا و ولوی،محمدرضا و حسینی،محمدرضا و نوروزانی،شهرام.(۱۴۰۱). "اصول و قواعد دکترین سایبری جمهوری اسلامی ایران درذ حوزه دفاعی‌ـامنیتی". فصلنامه علمی راهبردی دفاعی. سال بیستم. شماره۷۹. پاییز. صص ۷۳ـ۴۴

۱۷. مقدسی‌لیچاهی،امیرحسین و همت،حمید.(۱۳۹۷). "ارائه الگوی امنیت در فضای سایبری جمهوری اسلامی ایران با رویکرد آینده پژوهانه". فصلنامه آینده پژوهی دفاعی. سال سوم، شماره۱۰. صص ۱۲۰ـ۱۰۳

۱۸. موسی‌زاده،سیدعلی و مهکویی،حجت و باقری‌چوکامی،سیامک.(۱۴۰۰). "ارائه مدل راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک". فصلنامه سیاست خارجی. دوره دهم. شماره چهارم. زمستان. صص ۷۰ـ۳۹

۱۹. موحدی‌صفت،محمدرضا و محمدی‌منفرد،حسن و آقایی،محسن.(۱۴۰۲). تأثیر فضای مجازی بر امنیت داخلی و راه کارهای جلوگیری از امنیتی شدن پدیده‌های اجتماعی. فصلنامه مطالعات و پژوهش‌های امنیت داخلی. سال یکم. شماره چهارم. زمستان. صص ۱۰۰ـ۷۲

۲۰. نگهدار،ایرج و پورقهرمان،بابک و بیگی،جمال.(۱۴۰۲). "سیاستگذاری جنایی در نقض امنیت سایبری و رهیافت‌های پیشگیری اجتماعی". فصلنامه سیاستگذاری عمومی. دوره۹. شماره۲. تابستان. صص ۱۵۲_۱۲۶

۲۱. هلالات،عماد.(۱۴۰۰). چهارچوب نظری مفهوم «بازدارندگی» در ادبیات علم روابط بین‌الملل. قابل دسترسی در: https://farhikhtegandaily.com/news/۷۰۶۴۵