فصلنامه علمی امنیت ملی
سال دهم، شماره سی‌وهفتم، پاییز ۱۳۹۹
مقاله ششم از صفحات ۲۱۶-۱۸۱

مقاله پژوهشی: احصاء، ارزیابی و تحلیل شکاف ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی

محمدرضا ولوی[۱]، حمیدرضا حسنی اصل[۲]، علی نیک‌نفس[۳]، علی دلگیر[۴]

تاریخ دریافت:۱۳۹۸/۰۲/۱۳ تاریخ پذیرش:۱۳۹۹/۰۴/۱۱

چکیده

امروزه با توجه به گسترش روزافزون فضای سایبری در حوزه‌های اقتصادی، سیاسی، فرهنگی و نظامی در سطح کشورها، تأثیرگذاری آن بر امنیت ملی غیر قابل انکار است. لذا یکی از محورهای اصلی تهدید امنیت ملی در عصر ارتباطات و جهانی‌شدن برای کشورها حوزه سایبر است. با توجه به اینکه بخش قابل توجهی از وقایع گذشته در حوزه سایبر ناظر به ایجاد ناامنی و تهدیدات امنیتی که قابلیت ایجاد اخلال در نظم عمومی جامعه به‌عنوان یکی از عناصر امنیت ملی را داشته، بوده است؛ وجود نظامی منسجم به‌منظور تعیین نقش حاکمیت، جهت‌دهی فعالیت‌های اجرایی و هماهنگی، نظارت و هدایت بخش‌های درگیر، جهت پایش روند تحولات فضای سایبری با رویکرد امنیت ملی بیش‌ازپیش ضروری به نظر می‌رسد. نظام رصد، پایش و هشداردهی سایبری کشور با رویکرد امنیت‌محور، ضمن مدیریت تهدیدات ملی و بین‌المللی با تسهیل امور و توانمندسازی حوزه‌های مختلف، زمینه‌ساز گسترش حوزه نفوذ در عرصه‌های مختلف می‌شود. بر این اساس هدف پژوهش پیش‌رو، احصاء ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی و تبیین شکاف بین وضعیت موجود و وضعیت مطلوب آن است. اولویت‌بندی پرداختن به هر یک از این ابعاد به‌منظور نیل به وضعیت مطلوب نیز بخش دیگری از اهداف این پژوهش است. با توجه به موضوع و هدف پژوهش، نوع تحقیق کاربردی- توسعه‌ای[۵]است و از نظر اجرا توصیفی-تحلیلی است. درنهایت ابعاد نظام به ترتیب اولویت فرهنگی، اجتماعی، دیپلماسی، دفاعی-امنیتی، اقتصادی، سیاسی و علم و فناوری احصاء می‌شود. تحلیل‌ها نشان می‌دهد که بین وضع مطلوب و وضع موجود ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی، تفاوت قابل توجهی وجود دارد.

کلیدواژه‌ها: نظام رصد پایش و هشداردهی، فضای سایبری، امنیت ملی، تحلیل شکاف.

۱. دانشیار و عضو هیئت علمی دانشگاه صنعتی مالک اشتر - valavi@mut.ac.ir
۲. دانشجوی دکترای مدیریت راهبردی امنیت سایبر، دانشگاه عالی دفاع ملی (نویسنده مسئول)- h.hasaniasl@sndu.ac.ir
۳. دانشجوی دکترای مدیریت راهبردی امنیت سایبر، دانشگاه عالی دفاع ملی- niknafs.a@sndu.ac.ir
۴. دانشجوی دکترای مدیریت راهبردی امنیت سایبر، دانشگاه عالی دفاع ملی- a.delgir@sndu.ac.ir

5.Applied – Development Research

مقدمه

مفهوم امنیت ملی، مفهوم بسیار پیچیده‌ای است و عوامل زیادی بر توانمندی دولت‌ها جهت دستیابی به اهداف امنیت ملی تأثیر می‌گذارند. این عوامل به‌طورکلی به دو دسته محسوس و نامحسوس تقسیم می‌شوند؛ عواملی مانند ثروت، جغرافیا، نیروی نظامی، زیرساخت‌های حمل‌ونقل، سیستم‌های ائتلاف و اتحاد، توانمندی‌های صنعتی و ... قابل اندازه‌گیری‌اند ولی عوامل دیگری؛ نظیر راهبرد ملی، توانمندی‌های سازمانی، دانش علمی فنی، توانمندی‌های رهبری، اراده و روحیه ملی، در بدو امر به دشواری قابل اندازه‌گیری هستند. در بیشتر موارد اهمیت نسبی عوامل تشکیل‌دهنده معادله امنیت ملی دولت‌ها ایستا نیستند بلکه در طی زمان دچار دگرگونی می‌شوند. درواقع همچنان که در عصر اطلاعات پیش می‌رویم، اهمیت عناصر نامحسوس و نرم قدرت ملی همانند تهدیدات سایبری نسبت به اهمیت عوامل محسوس و سنتی قدرت، به‌گونه‌ای قابل توجه در حال افزایش‌اند.

بیان مسئله

تهدیدات سایبری از ماهیتی متنوع، گسترده و منحصربه‌فرد برخوردارند. متنوع ازآن‌رو که این تهدیدات تمام حوزه‌های زندگی بشر را تحت تأثیر قرار داده‌اند و درنتیجه فقدان امنیت در فضای سایبری بسیار بالاست. طبیعتاً امنیت در فضای سایبر یکی از مؤلفه‌های اصلی امنیت ملی کشور است (ملائی،۱۳۹۷). حملات مخرب مهم با تأثیرات گسترده، تهدیدهای سایبری را به‌عنوان یکی از بدترین تهدیدهای منافع ملی به تصویر کشیده است تا جایی که ایالات‌متحده آمریکا اعلام کرده است که این حملات را به‌عنوان جنگ تلقی کرده و با آن برخورد فیزیکی خواهد کرد (خلیلی‌پور رکن‌آبادی و نورعلی وند، ۱۳۹۱).

جایگاه خاص جمهوری اسلامی ایران در ترتیبات منطقه‌ای و نظام بین‌الملل سبب شده تا نظام سلطه از فضای سایبری برای تحدید قدرت ملی به شکل فزاینده‌ای بهره‌برداری نماید. در این میان، به‌منظور ایجاد سازوکار مناسب برای تضمین امنیت و منافع ملی در این

فضا، شناخت ابعاد مختلف این مسئله به دغدغه بسیاری از صاحب‌نظران این حوزه تبدیل شده است (تقی‌پور و اسماعیلی،۱۳۹۷).

پنج قلمرو قدرت؛ یعنی سرزمین، آب، هوا، فضا و فضای سایبر تولید و کسب منابع و نفوذ را میسر می‌سازند که امروزه فضای سایبر پیشگام گسترش قدرت دیپلماسی، اطلاعاتی، نظامی و اقتصادی است .تمام انواع واحدها (دولت‌ها، شرکت‌ها، تروریست‌ها، سازمان‌های جنایی و گروه‌های غیرانتفاعی) همگی فعالیت‌های خود را در بستر فضای سایبر به پیش می‌برند (Rowland, Rice & Shenoi,2014:4).

در دوران معاصر، جهت‌گیری اولویت‌های راهبردی کشورها، برای نیل به قدرت فائقه، به سمت بهره‌برداری از فضای سایبر تغییر یافته و فناوری‌های پیشرفته سایبری، زمینه‌ساز تجدید بنای قدرت ملی در قالب قدرت سایبری شده است. ازجمله پیامدهای این تغییر بنیادین، تأثیر آن بر امنیت ملی کشورها است. فرایند جهانی‌شدن، ظهور جوامع شبکه‌ای و حملات سایبری سازمان‌یافته فرامرزی، از چالش‌های جدی و نوین در دستیابی و حفظ امنیت ملی است (هلیلی و همکاران، ۱۳۹۷).

اهمیت و ضرورت تحقیق

در طول تاریخ فناوری‌های جدید و نوظهور اطلاعاتی، قابلیت‌ها و توانمندی‌های جدیدی را در اختیار قرار داده و هم‌زمان محیط راهبردی را تغییر داده‌اند. ازاین‌رو دائماً تقاضا برای توسعه و پیشرفت این حوزه وجود داشته است. فناوری اطلاعات و ارتباطات و به‌طورکلی فضای سایبری به‌عنوان یکی از عوامل نامحسوس، به‌مثابه یک توانمندساز و تسهیل‌کننده، تأثیر به‌سزایی در امنیت ملی کشورها دارد.

با بررسی سناریوهای محتمل و مشخص کردن الگوهای شرایط مطلوب (اسناد بالادستی و فرمایشات امام خامنه‌ای(مدظله‌العالی)) مشخص شد که سناریوی مطلوب جمهوری اسلامی ایران؛ جزء سناریوهای محتمل نیست؛ این بدان معناست که روندهای کنونیِ فضای سایبر، به سمت الگوی مطلوب نظام اسلامی حرکت نمی‌کند و درصورتی‌که عزم عمومی برای

ایجاد روندها، استفاده از فرصت‌ها و مقابله با چالش‌ها نباشد؛ انتخاب آینده نظام در فضای سایبر، انتخاب بین بد و بدتر خواهد بود (اسماعیلی و ثنا قربانی، ۱۳۹۷).

برخورد منفعلانه با نوآوری‌های سریع و مکرر، بستری مطلوب برای تهدیدگران جمهوری اسلامی ایجاد خواهد کرد و در نقطه مقابل، تعامل فعالانه، ایجابی و مشارکتی در نوآوری‌های فضای سایبر، زمینه‌های فرصت‌آفرین برای جمهوری اسلامی ایران در برخواهد داشت (اسماعیلی و ثناقربانی، ۱۳۹۷).

بنابراین وجود نظامی جهت پایش روند تحولات فضای سایبری با رویکرد امنیت ملی بیش‌ازپیش ضروری به نظر می‌رسد. چراکه این فضا به دلیل گستردگی، تابع شرایط بحرانی قرار می‌گیرد و بنابراین تحلیل‌های رایج گذشته پاسخگوی حوزه حاکمیتی این فضا نمی‌باشد.

اهداف تحقیق

هدف اصلی

بررسی وضعیت و تحلیل شکاف ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی

اهداف فرعی

- احصاء ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی
- تبیین تأثیر تهدیدات فضای سایبر بر امنیت ملی
- بررسی وضعیت موجود و آینده مطلوب ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی

سؤالات تحقیق

سؤال اصلی

وضعیت موجود، آینده مطلوب و تحلیل شکاف ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی چگونه است؟

سؤالات فرعی

– ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی کدام است؟

– تأثیر تهدیدات فضای سایبر بر امنیت ملی چیست؟

– وضعیت موجود و آینده مطلوب ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی چگونه است؟

ادبیات و مبانی نظری

پیشینه تحقیق

تحقیقات گسترده‌ای در خصوص مخاطرات و تهدیدات حوزه سایبر و تأثیر آن بر امنیت ملی صورت گرفته است و کشورهای پیشرو در عرصه فناوری‌های سایبری جهت استحکام زیرساخت‌های سایبری خود به مطالعه و ایجاد ساختارها و یا نظام‌های یکپارچه‌ای جهت مواجهه با این موضوع پرداخته‌اند. رویکرد تحقیقات مرتبط انجام‌شده در حوزه فضای سایبر و مسائل امنیت ملی را می‌توان به دو دسته تقسیم کرد: تعدادی از پژوهش‌های صورت‌گرفته در رابطه با فضای سایبر معطوف به چالش‌ها، آسیب‌پذیری‌ها و تهدیدات این فضا و وجوب ایجاد نظامات سایبری جهت مواجهه با این چالش‌ها پرداخته‌اند. برای نمونه مقاله آقایان علی اسماعیلی و جلال ثناقربانی با عنوان «تبیین نسبت سناریوهای محتمل و مطلوب تهدیدات سایبری جمهوری اسلامی ایران» برای پاسخ به این سؤال که «نسبت میان سناریوهای محتمل و مطلوب تهدیدات سایبری علیه جمهوری اسلامی ایران چیست؟» با تأکید بر ضرورت محافظت از ارزش‌های اساسی، زیرساخت‌های حیاتی، اطلاعات ارزشمند ملی، لازمه این کار را، تولید یک تصویر درست از وضعیت خود، محیط پیرامونی و عوامل تأثیرگذار بر آینده می‌داند. مقاله «سنجش تهدیدات سایبری» آقایان عبدالله خانی و حسینی، به دنبال پاسخ به این سؤال است که وضعیت و میزان تهدیدات خطرناک امنیتی سایبری در چه حدی است؟ آقایان تقی‌پور و اسماعیلی در مقاله‌ای با عنوان «طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران» به

ضرورت ایجاد نظام دفاع سایبری به‌منظور کاهش آسیب‌پذیری‌ها، مقابله با تهدیدات، ایجاد بازدارندگی، ایجاد نگاه کل‌گرایانه و سیستمی در مقابل نگاه واکنشی تأکید نموده‌اند. در مقاله دیگری آقای علی ملائی و همکاران نسبت به احصاء «الگوی راهبردی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها» اقدام نموده و با بهره‌گیری از بازی پویای علامت‌دهی با اطلاعات ناقص و تعادل نش، راهبردهای مختلط در شش بعد و چهار مؤلفه اصلی وضع موجود، وضع مطلوب و تحلیل شکاف را معرفی می‌نمایند.

دسته دوم پژوهش‌های انجام‌شده، درصدد بررسی تبعات تلاقی فضای سایبر با زندگی واقعی و تأثیر آن بر امنیت ملی بوده‌اند. خلیلی‌پور رکن‌آبادی و نورعلی‌وند در مقاله‌ای با عنوان «تهدیدات سایبری و تأثیر آن بر امنیت ملی» در پی پاسخ‌گویی به این پرسش هستند که تهدیدهای سایبری چگونه بر امنیت ملی تأثیر می‌گذارند و این اثرگذاری در چه ابعادی خود را نمایان می‌سازد. درنهایت به این نتیجه می‌رسند که این پدیده امنیت ملی را ابعاد مفهوم امنیت، دولت‌محوری در امنیت، بُعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه، تحت تأثیر قرار داده است. در مقاله «تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن»، آقای موسوی و همکاران، فناوری‌های سایبری را یکی از الزامات و ابزارهای جهانی‌شدن می‌دانند که هم یک فرصت و هم یک تهدید به شمار می‌رود. از نظر ایشان تروریسم سایبری با هدف نابودسازی ساختارهای اساسی و حیاتی یک کشور به‌عنوان مصداق نقض امنیت ملی مطرح است. این جرم ازجمله مهم‌ترین جرائم فراملی در فضای مجازی می‌باشد. نوع پیشگیری، مقابله و مبارزه با این جرم، با نوع اقدامات کنترلی در سایر جرائم به‌کلی متفاوت می‌باشد. در جرم تروریسم سایبری، جرم فاقد محل وقوع می‌باشد. این جرم عموماً فرامرزی بوده و تهدیدی مستقیم علیه منافع و امنیت ملی کشور است. در این راستا لازم است تدابیر تقنینی، قضایی و اجرایی ویژه‌ای در سطح ملی و بین‌المللی در نظر گرفته شود. آقای هلیلی و همکاران در مقاله «قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی»، با هدف مفهوم‌سازی قدرت سایبری با

رویکرد فرکتالی و تأثیر آن بر امنیت ملی در فضای سایبر، بر این باور هستند که قدرت سایبری دارای تمامی ویژگی‌های قدرت ملی است. افزایش نقش‌آفرینی در مدیریت فضای سایبر، توسعه سرمایه‌گذاری اقتصادی و افزایش نفوذ بین‌المللی از مصادیق قدرت سایبری است. یکی از مهم‌ترین پیامدهای قدرت سایبری را می‌توان ارتقاء امنیت ملی دانست. قدرت سایبری به‌عنوان ابزاری برای محافظت از منافع و ارزش‌های ملی نقش مهمی در افزایش امنیت ملی دارد. آقای فروردین و همکاران در مقاله «بررسی تأثیرات جنگ سایبری بر امنیت ملی در جمهوری اسلامی ایران» ضمن احصاء و بررسی مفاهیم جنگ سایبری، تأثیر آن بر امنیت ملی را ارزیابی و تحلیل می‌نمایند.

مرور تحقیقات انجام‌شده، اهمیت و تأثیر تهدیدات فضای سایبر بر امنیت ملی را آشکار می‌سازد. در این تحقیق ضرورت ایجاد نظام رصد، پایش و هشداردهی سایبری به‌منظور مواجهه فعال و پیش‌کنشگر با این تهدیدات، در جهت حفاظت و صیانت از امنیت ملی در ابعاد مختلف بررسی و شکاف بین وضعیت موجود و مطلوب در هر یک از ابعاد احصاءشده تحلیل می‌شود تا راهنمای سیاست‌گذاران و تصمیم‌گیران این حوزه باشد. این موضوع وجه تمایز تحقیق حاضر با سایر تحقیقات مرتبط است.

امنیت ملی

با توجه به تطور و تحول مفهومی امنیت ملی در گذر زمان، تعاریف مختلفی برای آن ارائه شده است که نخست به این تعاریف اشاره می‌نماییم. تا دهه ۱۸۸۰ تعریف جامع و کاملی از امنیت ملی ارائه نشده بود و بعد از آن به‌تدریج تعاریف کامل شد. مسلم اینکه امنیت ملی[1] به دنبال تولد ملت – دولت مطرح شد که ریشه آن به قرن ۱۷ میلادی بازمی‌گردد. در آن زمان این مفهوم نوظهور تحت عنوان «بقای ملی»[2] مطرح شد. این مفهوم مانند دیگر مفاهیم در علوم انسانی دارای تعریف واحدی که مقبول تمامی یا حداقل بیشتر

1. National Security
2. National Survival

صاحب‌نظران باشد نیست. ریشه این عدم اتفاق نیز به برداشت متفاوت افراد، گروه‌ها و کشورها از این واژه بازمی‌گردد. بر همین اساس بری بوزان می‌گوید «امنیت ملی را نمی‌توان به‌طورکلی تعریف کرد بلکه تنها در موارد مشخص می‌توان آن را تعریف نمود»(بوزان، ۱۳۷۸). او در جای دیگری چنین می‌گوید: «امنیت ملی از لحاظ مفهومی ضعیف و از نظر تعریف مبهم ولی از نظر سیاسی مفهومی قدرتمند باقی مانده است چون مفهوم نامشخص امنیت ملی راه را برای طرح راهبردهای بسط قدرت توسط نخبگان سیاسی و نظامی باز می‌گذارد» (ماندل، ۱۳۷۷: ۴۹). سازمان ملل متحد طی پژوهشی در این زمینه با عنوان «مفاهیم امنیت» آن را چنین تعریف می‌نماید: «اینکه کشورها هیچ‌گونه احساس خطر حمله نظامی، فشار سیاسی یا اقتصادی نکنند و بتوانند آزادانه گسترش و توسعه خویش را تعقیب کنند»(قاسمی، ۱۳۷۲: ۵۵- ۵۴). در فرهنگ اصطلاحات روابط بین‌الملل این مفهوم بدین صورت تعریف شده است: «حالتی که ملتی فارغ از تهدید از دست دادن تمام یا بخشی از جمعیت، دارایی یا خاک خود به‌سر می‌برد»(Chandler & Plano, 1988: 40).

والتر لیپمن[1] نخستین کسی بود که مفهوم امنیت ملی را به‌روشنی تعریف نمود: «یک ملت وقتی دارای امنیت است که در صورت اجتناب از جنگ بتواند ارزش‌های اساسی خود را حفظ کند و در صورت اقدام به جنگ بتواند آن را پیش ببرد» (روشندل، ۱۳۷۴: ۱۱). برژینسکی در اوج جنگ سرد درباره امنیت معتقد بود که نقطه شروع کنکاش در باب امنیت ملی باید با شناسایی صحیح ماهیت تغییرات عصر ما قرین باشد. به اعتقاد وی چهار انقلاب مرتبط با هم دنیای معاصر را دستخوش تحول کرده است: «انقلاب سیاسی، انقلاب اجتماعی، انقلاب اقتصادی و انقلاب نظامی. تأثیرات این چهار انقلاب به‌طور هماهنگ روی نظام بین‌الملل، رقابت ابرقدرت‌ها، ثبات و موازنه نظامی آن‌ها آشکار است و در آینده ابعاد گسترده‌تری پیدا خواهد کرد» (برژینسکی، ۱۳۶۸: ۴-۳).

رابرت ماندل نیز چنین می‌گوید: «امنیت ملی شامل تعقیب روانی و مادی ایمنی است و اصولاً جزو مسئولیت حکومت‌های ملی است تا از تهدیدات مستقیم ناشی از خارج نسبت

1 Walter Lippman

به بقای رژیم‌ها، نظام شهروندی و شیوه زندگی شهروندان خود ممانعت به عمل آورند»(ماندل، ۱۳۷۷: ۵۲-۵۱). با دقت در تعاریف فوق می‌توان چنین برداشت نمود که نقطه مشترک قابل قبول همه صاحب‌نظران ضرورت «حفظ وجود خود» است که می‌توان به شکل دیگر آن را به «حفظ ذات و صیانت نفس در برابر اساسی‌ترین خطرات» تعبیر کرد. برخی از صاحب‌نظران حفظ خود یا «صیانت ذات و نفس» را در چهار پدیده باارزش خلاصه می‌نمایند:

۱. حفظ جان مردم

۲. حفظ تمامیت ارضی

۳. حفظ نظام اقتصادی، سیاسی، اجتماعی و فرهنگی

۴. حفظ استقلال و حاکمیت کشور

چهار مقوله فوق به‌عنوان جوهره «امنیت ملی» این خصوصیت را دارد که تمام کشورها در سیاست داخلی و خارجی‌شان و نیز افراد، گروه‌ها و احزاب موجود در کشورها بدون توجه به گرایش، سلیقه‌ها و اختلافات فردی، گروهی، طبقاتی، سیاسی و اجتماعی در مورد اهمیت حفظ و تلاش برای رفع تهدیدات علیه این چهار ارزش، در حد توان و امکان، اتفاق نظر کامل دارند. اهمیت امنیت ملی به حدی است که بسیاری از دانشمندان علم سیاست و روابط بین‌الملل بر این نظرند که تحقق این مهم «فلسفه وجودی دولت» یا «فلسفه تشکیل دولت» را به دست می‌دهد و به‌رغم تمامی قیودی که این امر برای آزادی‌های فردی ایجاد کرده است تأسیس دولت را برای پاسداری از حریم امنیت دانسته و ضرورت تأسیس آن را قبول کرده‌اند (بصیری، ۱۳۸۸: ۱۶۷).

مروری بر تحقیقات انجام‌شده، تأثیر متقابل قدرت و امنیت در فضای سایبر را نشان می‌دهد. در سطح ملی، قدرت سایبری و امنیت ملی از مفاهیم مهم و مورد توجه سیاست‌گذاران و تصمیم‌گیران است که با توجه به نفوذ گسترده فضای سایبر، نیازمند مفهوم‌سازی و بازبینی مجدد هستند (هلیلی و همکاران، ۱۳۹۷).

ابعاد امنیت ملی

جهانی‌شدن با شکل جدیدی که به محیط امنیتی، بازیگران و قواعد بازی امنیت خارجی داده است، سرمنشأ تهدیدهای کاملاً جدیدی برای ایران است که تا دهه پیش وجود نداشته‌اند .مفهوم کلیدی در این رابطه، تهدید در فضای الکترونیکی و مجازی است که با جنگ‌های کلاسیک کاملاً متفاوت می‌باشند (موسوی و همکاران، ۱۳۹۲).

امنیت ملی دارای دو بعد داخلی و خارجی است که با یکدیگر مرتبط هستند. در بُعد داخلی تهدیدهای آشکار و پنهان را در درون مرز ناامنی به بار می‌آورد از قبیل تهدیدات سیاسی (شورش، جدایی‌طلبی، انقلاب...)، اقتصادی (نابسامانی و بحران‌های اقتصادی، شغلی، فنی، حرفه‌ای)، نظامی (کودتا، جنگ داخلی...)، اجتماعی (آشوب‌های اجتماعی...) که هرکدام مردم را تحت فشار قرار می‌دهند. در بُعد خارجی نیز امنیت ملی می‌تواند از ناحیه مسائل سیاسی (انزوا، اعمال فشارهای سیاسی)، نظامی (حمله، تعرض نظامی و تقویت قدرت نظامی دشمن)، اقتصادی (تحریم‌های اقتصادی، تعرفه، لیست سیاه...) و... تهدید شود. امروزه به دلیل ارتباطات گسترده و نزدیکی ملت‌ها به یکدیگر، امنیت ملی در بُعد خارج و داخل کاملاً با یکدیگر در پیوند است و از یکدیگر تأثیر و تأثر می‌پذیرد(بصیری،۱۳۸۸). شکل شماره ۱ ابعاد مختلف متأثر از تهدیدات امنیت ملی را نشان می‌دهد.

شکل ۱- ابعاد تهدیدات امنیت ملی (ولوی و همکاران، ۱۳۹۶، ۴۳).

یکی از دلایل پیچیدگی مفهوم امنیت و ماهیت ابهام‌آمیز آن، چندوجهی بودن مفهوم امنیت است. وجوه و ابعاد مختلف امنیت را می‌توان در محورهای سیاسی، اجتماعی، اقتصادی، نظامی، فرهنگی و زیست‌محیطی دسته‌بندی کرد (ماندل،۱۳۷۹: ۸۳-۷۱).

فضای سایبر

برخلاف روندهای کلاسیک، روندهای کنونی و پیشرو، مملو از عدم قطعیت‌ها، پیچیدگی‌ها و تکثر منابع تأثیرگذار بر ساخت آینده است. نماد بارز ویژگی‌های فوق را می‌توان در فضای سایبر دید و یا به تعبیری دیگر، بیان داشت که فضای سایبر علت اصلی این همه پیچیدگی و عدم قطعیت است. اهمیت این مسئله تا بدانجا مورد تأکید قرار گرفته که در ادبیات جدید سیاسی و امنیتی ناتو و وزارت دفاع آمریکا؛ از این فضا به‌عنوان قلمرو پنجم نبردهای نظامی اطلاعاتی نام برده شده است(Kevin benedict, 2011) .

تعاریف متفاوتی از فضای سایبر ارائه شده است و هرکدام از تعریف‌ها معطوف به یک جنبه از کاربردهای فضای سایبر است. لغت سایبر از عبارت سایبرنتیکس گرفته شده است. عبارت سایبرنتیکس را گروهی از دانشمندان که توسط نوربرت وینر رهبری می‌شدند ایجاد کردند. چندی بعد در سال ۱۹۴۸ از طریق کتاب «سایبرنتیکس یا کنترل و ارتباطات در حیوان و ماشین» که توسط وینر[1] نگاشته شده بود، رسماً معرفی شد. در فرهنگ علوم اجتماعی گولدن کولب نیز سایبرنیتک بدین‌گونه تعریف شده است: «سایبرنتیک به مجموعه‌ای از نظریه‌ها و پژوهش‌ها اشاره می‌کند که توجه خود را به انسان‌ها، ارگانیسم‌های دیگر و ماشین‌ها معطوف کرده‌اند. برخی مراجع دیگر تعاریفی نظیر، حوزه ارتباطات الکترونیکی و واقعیت مجازی یا اصطلاح روی خط شبکه و اینترنت را ارائه نموده‌اند» (Merriam-webster, 2017).

در تعاریف کامل‌تر دیگر فضای سایبر به این صورت آمده است: در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات، از طریق سازوکارهای الکترونیک و

---

۱. وینر یک ریاضی‌دان، مهندس و فیلسوف اجتماعی بود. در تعریف وینر، سایبرنتیکس علم مطالعه نظام کنترل ارتباطات و اطلاعات در موجودات زنده و ماشین است. سایبرنتیک از لغت یونانی KUBERNETES به معنای سکاندار یا حاکم گرفته شده است. این کلمه به معنای کنترل رفتارها به‌منظور هدایت، اعمال قدرت، قانونمند کردن، تحت سلطه گرفتن، مهارکردن و فرماندهی است.

مجازی انجام می‌پذیرد. از این فضا با نام فضای تبادل اطلاعات (فتا) یاد می‌شود (سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور،۱۳۸۷). وزارت دفاع آمریکا «فضای سایبر» را این‌گونه تعریف کرده است: «دامنه جهان‌گستر در محیط اطلاعاتی، متشکل از شبکه درون وابسته از زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های ارتباطات از راه دور، سیستم‌های کامپیوتری و کنترل گره و پردازنده‌های نصب‌شده» (واژه‌نامه مشترک آمریکا و روسیه در فضای سایبر، ۱۳۹۱). مرکز پدافند غیرعامل این اصطلاح را به این صورت تعریف می‌کند: مجموعه‌ای از شبکه‌های ارتباطی رایانه‌ای شامل امکانات و تجهیزات ارتباطی، انتقالی و کنترلی و سیستم‌های مدیریتی است که به دنبال تحقق مجموعه‌ای از اهداف ارزشمند جهت پردازش‌ها و زیرساخت‌های حیاتی می‌باشد. اینترنت بزرگ‌ترین مؤلفه از فضای سایبر می‌باشد (مرکز پدافند غیرعامل، ۱۳۸۷).

فضای سایبری مجموعه‌ای از سیستم‌های الکترونیکی و شبکه‌های رایانه‌ای، شامل نیروی انسانی، زیرساخت‌ها، تجهیزات سخت‌افزاری، سیستم‌های ارتباطی و کنترلی و مدیریت، به‌منظور تولید، ذخیره‌سازی، پردازش، تبادل، بازیابی، حذف و بهره‌برداری از داده‌ها است. در تعریف دیگری فضای سایبری جمهوری اسلامی ایران مجموعه‌ای از ارزش‌ها، منافع و دارایی‌های ملی در فضای سایبر بوده و جهت ارائه خدمات در راستای اهداف نظام جمهوری اسلامی ایران می‌باشد. این فضا محدود به مرزها و جغرافیا نمی‌باشد(تقی‌پور، ۱۳۹۲).

فضای سایبر و امنیت ملی

جمهوری اسلامی ایران به جهت حفاظت از ارزش‌های اساسی، زیرساخت‌های حیاتی و درنهایت حفظ و ارتقاء منافع و امنیت ملی در این به‌اصطلاح قلمرو پنجم نبردهای نظامی اطلاعاتی، یعنی فضای سایبر، از یک‌سو باید برای تهدیدات فعلی چاره‌ای بیاندیشد تا ثبات کنونی حفظ شود و از سوی دیگر تصویر روشنی از آینده‌های محتمل این فضا و تهدیدات متصوره از آن داشته باشد تا بتواند بر تهدیدات آینده غلبه کند و در صورت امکان مطلوبیت‌های خود را در آن ایجاد نماید (اسماعیلی و ثناقربانی، ۱۳۹۷).

امنیت فضای سایبری یکی از مهم‌ترین جنبه‌های امنیت ملی است و از حوزه ملی و زیرساخت‌های ملی محافظت می‌نماید(Van Vuuren, 2016) .

در تحقیق هلیلی، اتخاذ رویکرد فرکتالی برای قدرت سایبری، به معنای تشابه ویژگی‌های ذاتی و کارکردی مؤلفه‌های قدرت سایبری و قدرت ملی است. این رویکرد برای تأکید بر این نکته است که قدرت سایبری می‌تواند پاسخگوی دغدغه‌ها و ابهامات ایجادشده برای امنیت ملی در فضای سایبر باشد. امروزه دولت‌ها قدرت ملی خود را با قدرت سایبری پیوند زده‌اند و از آن به‌عنوان کاتالیزور و شتاب‌دهنده قدرت استفاده می‌کنند. علاوه بر آن، توانایی دولت‌ها برای مهار چالش‌های امنیت ملی در فضای سایبر از مهم‌ترین عوامل قدرت سایبری دولت‌ها محسوب می‌شود (هلیلی و همکاران، ۱۳۹۷).

امروزه با توجه به گسترش روزافزون فضای سایبری در حوزه‌های اقتصادی، سیاسی، فرهنگی، زیست‌محیطی و نظامی در سطح ملی کشور، تأثیر آن بر امنیت ملی غیر قابل انکار است. فضای سایبری به‌عنوان سلسله‌اعصاب در این حوزه‌ها و زیرمجموعه‌های آن‌ها بوده و این حوزه‌ها را به هم مرتبط، هماهنگ، یکپارچه، سریع و قابل کنترل می‌نماید. فضای سایبری به‌طور مستقیم در عملکرد تمامی بخش‌های اقتصادی، انرژی (الکتریکی، نفت و گاز)، حمل‌ونقل (راه‌آهن، هوایی، ناوگان بازرگانی)، بخش بانکی و مالی، ارتباطات راه دور، اطلاعات، بهداشت عمومی، خدمات اورژانس، آب، صنعت دفاعی، غذا، کشاورزی و بخش پستی و کشتیرانی مؤثر بوده و از فرایندهای آن‌ها حمایت می‌کند.

در سند راهبرد امنیت سایبری انگلیس، چشم‌انداز ارائه‌شده در این سند برای انگلستان؛ ایجاد ارزش‌های بزرگ اقتصادی و اجتماعی از فضای سایبری پرجنب‌وجوش و انعطاف‌پذیر و امن و افزایش رفاه موجبات ارتقاء امنیت ملی، پیشرفت و یک جامعه قوی عنوان شده است(UK cyber security strategy, 2016) .

لذا یکی از محورهای اصلی تهدید امنیت در عصر ارتباطات و جهانی‌شدن برای کشورها حوزه سایبر است. امنیت فضای سایبری به خاطر اتکای بیش‌ازحد تمامی بازیگران سیاسی به آن، بی‌تردید مقوله‌ای استراتژیک قلمداد می‌شود و به همین دلیل است که در

ارزیابی تهدیدات امنیت ملی و بین‌المللی، مفهوم امنیت فضای سایبری، وارد اسناد پایه امنیتی شده است (موسوی و همکاران، ۱۳۹۲).

از منظر امنیت ملی می‌توان گفت که در شرایط حاضر، دولت‌ها و ملت‌ها با زنجیره‌ای از تهدیدات نامشخص در محیط‌های سایبری مواجه هستند که امنیت آن‌ها را به چالش کشیده و ابزارهای سنتی تأمین‌کننده امنیت ملی، دیگر توان مقابله با آن‌ها را ندارند(حسن‌بیگی، ۱۳۸۴).

ضرورت ایجاد نظام رصد، پایش و هشداردهی سایبری

روی دیگر سکه، گسترش نفوذ فضای سایبر در لایه‌های مختلف زندگی انسانی برای ارتقاء سطح زیست بشری، آسیب‌پذیری‌ها و تهدیدات به‌شدت فزاینده‌ای است که می‌تواند مخاطرات سهمگینی را برای بشر به همراه داشته باشد. در این میان، اراده بهره‌گیری از این فضا از سوی دشمنانی که امنیت و بقای ایران را در عرصه بین‌المللی هدف قرار داده‌اند، ایجاد الگوی کارآمد دفاع سایبری را اجتناب‌ناپذیر ساخته است. با توجه به اهمیت فضای سایبر و جدی بودن تهدیدات در این عرصه، لازم است بین نخبگان فکری و ابزاری کشور در خصوص ضرورت حفاظت از این فضا، اجماع ایجاد شود و حساسیت‌های ملی لازم به‌منظور افزایش مؤلفه اعتبار به‌مثابه ضرورت اثبات توانمندی سایبری و ضرورت پاسخگویی به هر حمله سایبری ایجاد شود (تقی‌پور و اسماعیلی،۱۳۹۷).

در صورت دستیابی به سطح مطلوبی از قدرت سایبری، امکان پیشگیری، خنثی‌سازی و مقابله با تهدیدات عینی و ذهنی مبتنی بر فناوری‌های فضای سایبر فراهم می‌شود که ارتقاء امنیت ملی را در پی خواهد داشت. به‌عبارت‌دیگر یکی از مهم‌ترین پیامدهای قدرت سایبری را می‌توان ارتقاء امنیت ملی دانست. قدرت سایبری به‌عنوان ابزاری برای محافظت از منافع و ارزش‌های ملی، نقش مهمی در افزایش امنیت ملی دارد (هلیلی و همکاران، ۱۳۹۷).

با توجه به ماهیت فضای سایبر که امکان پیش‌بینی بسیط و خطی از تهدیدات آینده را تقریباً غیرممکن کرده، احتمال غافلگیری کنشگران منفعل و محافظه‌کار در مقابل تهدیدات

آتی بسیار بالا ارزیابی می‌شود. در این شرایط، مقابله با تهدیدات پیشرو و استفاده از فرصت‌های احتمالی، نیازمند ایجاد آمادگی نرم‌افزاری و سخت‌افزاری برای مقابله با چالش‌های آتی است (اسماعیلی و ثناقربانی، ۱۳۹۷).

در راهبرد امنیت فضای سایبر اتحادیه اروپا، در حوزه ارزش‌ها بر ترویج آزادی برخط و ایجاد اطمینان از توجه به حقوق اساسی و تشویق ارزش‌های اتحادیه و در حوزه سیاست‌ها بر محافظت فضای سایبر از وقایع و فعالیت‌های بدخواهانه و تأمین جامعیت و امنیت اطلاعات تأکید شده است (Cybersecurity Strategy of the European Union,2013).

بر اساس یک پژوهش انجام‌شده، سه راهبرد سازمان‌دهی تیم‌های مدیریت کشف و پاسخگویی به حوادث سایبری و تعامل با سازمان‌های مشابه منطقه‌ای و بین‌المللی، رصد فضای سایبر زیرساخت‌های حیاتی به‌منظور کشف و مواجهه فعال و پیش‌کنشگر با تهدیدات سایبری و ایجاد فرایندهای نظارت و ممیزی امنیت سایبری زیرساخت‌های حیاتی، بالاترین اهمیت را در بین راهبردهای امنیت سایبری زیرساخت‌های حیاتی به خود اختصاص داده‌اند (محمودزاده و همکاران، ۱۳۹۷).

ازاین‌رو برای مواجهه روشمند و هوشمند با این پدیده گسترده، ناگزیر باید به‌سرعت نسبت به رصد و پایش فضای سایبری کشور بر مبنای شاخص‌های کلیدی در ابعاد مختلف اقدام نمود و با نگاهی امنیتی امکان استفاده از فرصت‌های آن را فراهم آورد. این مهم باعث خواهد شد این پدیده از تهدید به سمت فرصت حرکت کند و با نگاهی امنیت‌محور با تسهیل امور و توانمندسازی حوزه‌های اقتصادی، اجتماعی، فرهنگی، سیاسی، امنیتی دفاعی، علم و فناوری و دیپلماسی بسیاری از مشکلات ملی و بین‌المللی کشور را سامان داده و زمینه‌ساز گسترش حوزه نفوذ در عرصه‌های مختلف شود.

نظام رصد، پایش و هشداردهی سایبری

با توجه به اینکه دشمنان و رقبای جمهوری اسلامی ایران در تلاش‌اند تا با تأثیرگذاری بر روندهای سازنده آینده؛ تصویر مطلوب خود از فضای سایبر را عملیاتی نمایند؛ ایران نیز

باید با شناسایی آینده‌های محتمل، بکوشد ضمن جلوگیری از وقوع سناریوی نامطلوب؛ سناریوی مطلوب خود را در این فضا ایجاد نماید. ضرورت آنجاست که در صورت عدم توجه به این موضوع، جمهوری اسلامی ایران را باید بازیگری منفعل در آینده به حساب آورد که دچار غافلگیری‌های متعدد در فضای سایبر شده است.

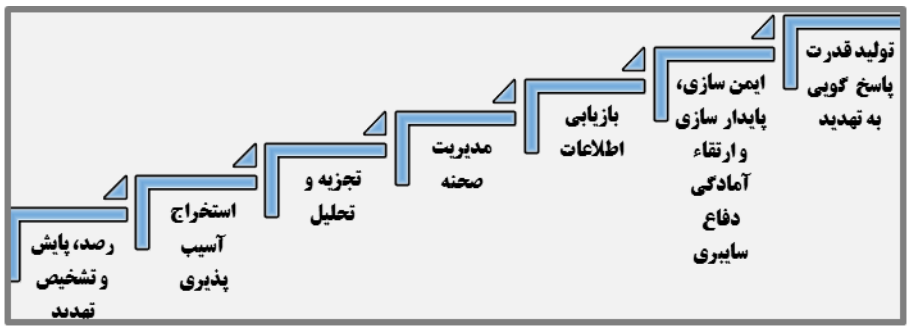
پیش‌بینی آینده نحوه برخورد تهدید سایبری با دارایی‌ها مستلزم بررسی آسیب‌پذیری‌های دارایی‌های سایبری و همچنین پیامد تحقق آن تهدیدات می‌باشد، چراکه تهدیدات به‌خودی‌خود و فارغ از محیط دارایی‌ها، فاقد خطر می‌باشند. لذا می‌بایست بر اساس شاخص‌های آسیب‌پذیری دارایی‌ها و پیامد تحقق تهدیدات، اطلاعات جمع‌آوری و مورد تحلیل قرار گیرد (اسماعیلی و ثناقربانی، ۱۳۹۷).

بررسی مؤسسات آینده‌پژوهی، مانند گارتنر، آی بی ام و پیو که به معرفی فناوری‌های نوظهور و پیشران‌های فضای سایبر می‌پردازند؛ نشان می‌دهد مواردی نظیر رایانش ابری، خودکارسازی و هوش مصنوعی، دستگاه‌های قابل حمل، ساختار اینترنت، رایانش موبایلی، اعتماد به زیرساخت‌ها مانند کلید عمومی، ابردیتاها، اینترنت اشیاء، تهدیدات نوظهور، حمله به زیرساخت‌های حیاتی و سایبری‌سازی‌ها به‌عنوان روندهای مهم تأثیرگذار در فضای سایبر هستند (Gartner,2014).

لذا برای ایجاد یک نظام رصد، پایش و هشداردهی لازم است با نگاهی کل‌نگر، برون‌گرا و درون‌زا حداکثر اشراف بر وضعیت داخلی و پیرامونی (دور و نزدیک) در ابعاد مختلف امنیت ملی فراهم گردد. این نظام اطلاعات فروانی را از حسگرهای مختلف امنیتی در فضای سایبر که می‌توانند انسانی یا ماشینی باشند دریافت کرده و با طی فرایندهای مختلف، گزارش‌های بلادرنگی از آنچه در حال اتفاق می‌باشد را فراهم می‌کند؛ بنابراین نظام در سطوح مختلف و در لایه‌های تاکتیکی، عملیاتی و راهبردی، توانایی مدیریت و پاسخگویی مناسب در مقابل حوادثی که وقوع آن‌ها باعث به خطر افتادن کشور می‌شود را خواهد داشت. کرامر فرانکلین و همکاران در کتاب «قدرت سایبری و امنیت ملی»، نقش قدرت سایبری در سطوح تاکتیکی، عملیاتی و راهبردی را مورد بررسی قرار داده‌اند. نتایج

این تحقیق نشان می‌دهد جرائم سایبری، تروریسم سایبری، نحوه حاکمیت اینترنت و امنیت سایبری از چالش‌های راهبردی است (Franklin et al, 2010).

با توجه به سرعت بالای تحولات فضای سایبری، یکی از ارکان تدوین نظام داشتن نگاه آینده‌پژوهی نسبت به این حوزه است، یعنی نظام رصد و پایش علاوه بر درک ناهنجاری‌ها و خطرات گذشته و حال می‌بایست بتواند بر اساس سیر تحولات حوزه فناوری با نگاه به آینده به‌صورت پیشگیرانه رفتار نماید. در سند راهبردی دفاع سایبری، رابطه میان نظام دفاع سایبری و نظام رصد و پایش سایبری به‌صورت شکل شماره ۲ ارائه شده است:



شکل ۲- حوزه‌های مأموریتی قرارگاه دفاع سایبری وجه عملیاتی (سند راهبردی دفاع سایبری، ۱۳۹۵)

به‌عبارت‌دیگر اولین گام در دستیابی به اهداف قرارگاه دفاع سایبری، وجود نظام رصد، پایش و تشخیص تهدیدات سایبری بیان شده است. در این راستا، به‌منظور تعیین نقش حاکمیت، جهت‌دهی فعالیت‌های اجرایی و هماهنگی، نظارت و هدایت بخش‌های درگیر موضوع، ایجاد نظامی منسجم در سطح ملی مورد نیاز است. در شکل‌گیری این نظام، باید به ویژگی‌های خاص امنیت در این فضا و اصول اولیه حاکم بر آن توجه داشت. پاره‌ای از این ویژگی‌ها چنین است: (سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور، ۱۳۸۷)

۱. امنیت فضای تولید و تبادل اطلاعات، مفهومی کلان و میان‌رشته‌ای است که بر مفاهیم و نظریات گوناگونی در حوزه‌های مختلف دانش مبتنی است.

۲. امنیت فضای تولید و تبادل اطلاعات، امری نسبی است که به تلقی از مفهوم امنیت، کارایی و هزینه وابسته است.

۳. امنیت فضای تولید و تبادل اطلاعات، امری زمینه‌وند است و مجموعه آداب و سنن، اخلاقیات، قوانین و سایر مقولات اجتماعی در آن تأثیر دارد.

۴. دولت در موضوع امنیت فضای تولید و تبادل اطلاعات کشور، متولی اصلی است.

۵. امنیت فضای تولید و تبادل اطلاعات به مرزهای جغرافیایی محدود نمی‌شود و از حوزه‌های داخلی، منطقه‌ای و جهانی تأثیر می‌پذیرد.

۶. تغییرات سریع فناوری‌ها، زمینه، نوع، ماهیت، درجه اثر و مشکلات امنیتی را به‌شدت تحت تأثیر قرار می‌دهد و لازم است تهدیدها، آسیب‌پذیری‌ها و راه‌های مواجهه و مقابله با آن‌ها به‌صورت دائم و پویا مورد بررسی قرار گیرد.

۷. حوزه تأثیر امنیت فضای تولید و تبادل اطلاعات، کلیه فعالیت‌های آحاد جامعه در این فضا را شامل می‌شود.

در یک تعریف منسجم می‌توان گفت: نظام رصد، پایش و هشداردهی، مجموعه‌ای هوشمند، یکپارچه، هدفمند، منسجم، پویا، دانش‌محور، انطباق‌پذیر و دارای بازخورد، از واحدهای مختلف است که در قالب فرایند مشخص، با فرماندهی متمرکز و اقدام توزیع‌شده و تعاملات و ارتباطات هم‌افزا به‌صورت چالاک و پیش‌دستانه و در چارچوب سیاست‌ها و راهبردهای ملی به رصد و پایش فضای سایبر در ابعاد مختلف امنیت ملی پرداخته و هشدارهای لازم را به‌منظور تصمیم‌گیری و اقدام در سطوح فنی، عملیاتی و راهبردی به‌صورت مؤثر و به‌هنگام به‌منظور امن‌سازی، مصون‌سازی، مقاوم‌سازی با هدف جلوگیری از غافلگیری در مواجهه با تهدیدات و کاهش آسیب‌پذیری‌ها و استفاده به‌موقع از فرصت‌ها ارائه می‌نماید (ولوی و همکاران، ۱۳۹۶، ۱۴۴-۱۴۳).

در این نظام، رصد به معنای پویش محیط و دیده‌بانی در افق دید بلند و دور است که با جمع‌آوری منابع اطلاعاتی به‌منظور شناسایی علائم ضعیف یا قوی حاکی از تغییرات مهمی در محیط انجام می‌شود، هدف آن کشف ارتباط میان رویدادها و روندها است که برای

جلوگیری از غافلگیری، ضرورت تغییر را به سازمان به‌طور زودهنگام هشدار می‌دهد تا با جستجوی راه‌حل‌های بیرونی و رعایت الزامات و ملاحظات درونی برای تسهیل فرصت و ممانعت از تهدید، اقدامات پیش‌دستانه صورت پذیرد (میرشاه ولایتی و نظری‌زاده، ۱۳۸۹).

پس از انجام مرحله رصد و پویش محیطی در گام پایش، مطابق نیازمندی و اهداف هر سازمان، موضوعاتی که قبلاً در مرحله رصد محیطی به‌طورکلی شناسایی شده‌اند، با انجام دیده‌بانی محیط نزدیک، مورد پیگیری دقیق و ساختارمند قرار می‌گیرند که این مراقبت می‌تواند مستمر یا متناوب باشد و هدف از این پایش برای یک نظام هشداردهی به‌عنوان ورودی محسوب می‌شود.

مفهوم هشداردهی، تجمیعی از بهترین یافته‌ها و قضاوت‌ها از بهترین افراد است که بر طبق یک بررسی جامع بر روی تمام شاخص‌ها انجام شده است. این یافته‌ها باید با زبانی به اندازه کافی قانع‌کننده به مقامات گزارش شود، به‌گونه‌ای که آن‌ها را قانع کند که هشدار مدنظر دارای اعتبار کافی است و نیاز به اقدامی متناسب دارد که برای حفظ امنیت ملی لازم و ضروری است (دیویس، جکف،۱۳۸۶). در تعریف دیگری آمده است: «آگاه‌سازی نسبت به رخدادهایی که منافع فرد، سازمان یا نظام ملی و بین‌المللی را در سطوح مختلف به مخاطره اندازد» (هشداردهی والاترین ماموریت اطلاعات، ۱۳۹۳، ۱۵۹ – ۱۵۷).

ابعاد مختلف نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی

در سند امنیت فضای تولید و تبادل اطلاعات (افتا) که برگرفته از آموزه‌های دین مبین اسلام و به‌طور مشخص قرآن کریم می‌باشد؛ پس از انجام مطالعات و شناخت جنبه‌های مختلف محیط داخلی، مفهوم و موجودیتی به نام زیرفضا مورد شناسایی قرار گرفته و به این صورت تعریف شده است: زیرفضا عبارت است از بخشی از سازمان، دستگاه یا شرکت که در محیط فضای تبادل اطلاعات (فتا) قرار دارد و احتمال تهدید و آسیب در مورد آن وجود دارد؛ یا از طریق آن می‌توان به سازمان مذکور حمله کرد. زیرفضاهای استخراج‌شده که متناظر با ابعاد متصور در نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی است، موجودیت‌های حساس و خطرپذیر داخل کشور هستند و عبارت‌اند از:

زیرفضای فرهنگی، اجتماعی، زیرفضای اقتصادی، زیرفضای امنیتی- دفاعی، زیرفضای حکمرانی، زیرفضای سیاسی و روابط بین‌الملل، زیرفضای علم و فناوری، زیر فضای امور زیربنایی (سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور، ۱۳۸۷).

دیدگاه فرکتالی، برای تأکید بر این واقعیت است که قدرت سایبری تمامی ویژگی‌ها و قابلیت‌های قدرت ملی را در بردارد؛ از آنجا که قدرت ملی دارای ابعاد سیاسی، اقتصادی، اجتماعی، فرهنگی، فناوری و ...است؛ بنابراین، برای دستیابی به قدرت سایبری باید به همه ابعاد آن توجه نمود (هلیلی و همکاران، ۱۳۹۷).

به‌منظور کاهش حداکثری اثر هرگونه تهاجم یا تهاجمات سایبری، لازم است سامانه‌های پدافند غیرعامل سایبر در حوزه‌های مختلف زیرساخت‌های فناورانه، اقتصادی، اجتماعی، فرهنگی و نظامی مورد توجه قرار گیرد (تقی‌پور و اسماعیلی،۱۳۹۷).

دارایی‌ها و تهدیدات سایبری می‌توانند در ابعاد شش‌گانه فناوری، دفاعی امنیتی، سیاسی، اقتصادی، اجتماعی و حقوقی بر یکدیگر تأثیرگذار باشند (ملائی،۱۳۹۷). بر اساس مطالعات انجام‌شده روی مدل‌های مختلف افراز فضای سایبر برای تقسیم‌بندی قلمرو که تجسم آن در تعبیه حسگرها متبلور است با الگوگیری از مدل پایه دانشگاه هاروارد و با مراجعه به نخبگان و نگاه ویژه به جنبه‌های امنیت ملی در فضای سایبر کشور که از مطالعات پیش‌گفته حاصل گردید؛ ابعاد مختلف نظام رصد، پایش و هشداردهی فضای سایبر در هفت بُعد فرهنگی، اجتماعی، اقتصادی، سیاسی، امنیتی و دفاعی، علم و فناوری و دیپلماسی احصاء گردید که به شرح زیر معرفی می‌گردند.

بُعد سیاسی

فضای سایبری با شکستن انحصار دولت در مهندسی افکار عمومی و آشکار کردن ناتوانی دولت در استقلال و امنیت ملی، تأمین خدمات بهینه و اقتصاد و نیز مدیریت عاری از فساد سبب شکل‌گیری تحولات سیاسی شده است. عرصه تهدیدات نرم سیاسی در فضای سایبر، به حوزه سیاسی کشورها چه در بُعد سیاست داخلی و چه در بُعد سیاست

خارجی مرتبط است که به مصداق آن در بحث سرزمینی، می‌توان به بالکانیزه کردن و در بُعد جهانی آن به گلوبالیزاسیون (جهانی‌سازی) اشاره نمود. همچنین این نکته اساسی را باید مدنظر قرار داد که هدف از تهدیدات، تأثیرگذاری بر اراده، اعتقادات، افکار و احساسات مخاطبین به‌منظور انهدام یا به تسلیم کشاندن جامعه هدف بوده و نقطه اشتراک تمام این تهدیدات، تحمیل اراده است. تفاوت در تهدیدات به نوع طرح‌ریزی و به‌کارگیری شیوه‌ها، امکانات، تجهیزات و وضعیت حاکم وابسته است (پدافند غیرعامل، ۱۳۹۴).

بُعد دفاعی- امنیتی

از آنجایی که در دنیای امروز میزان تولید و پردازش اطلاعات از شاخص‌های اصلی توسعه‌یافتگی است. وجود بسترهای امن و سیاست‌های حقوقی مناسب نیز از الزامات بهره‌برداری صحیح از فناوری اطلاعات است، لذا برای کاهش شکاف دیجیتالی موجود بین کشور عزیزمان ایران و سایر کشورهای توسعه‌یافته ناگزیر از برنامه‌ریزی جامع و استفاده از تمامی ظرفیت‌ها و توانایی‌های موجود در هر دو بُعد توسعه سایبری و توسعه فناوری امنیت سایبری هستیم (حسن‌بیگی، ۱۳۸۴).

برای روشن‌تر شدن بُعد امنیتی دفاعی فضای سایبری لازم است تا سرمایه ملی سایبری تعریف گردد. سرمایه ملی سایبری، عبارت است از: اطلاعات و فضای سایبری (محیط مجازی) که تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات در آن انجام می‌گیرد و اثر متقابل این محیط با انسان که نقش حیاتی در امنیت ملی، اقتصاد ملی، سلامت و ایمنی عمومی، اطمینان عمومی و باورهای دینی، ملی و قومی داشته باشد. در فضای بدون مرز سایبری، دفاع تنها بر دوش نیروهای نظامی نیست و لازم است کلیه ذینفعان و اهداف احتمالی چنین جنگ‌هایی در دفاع مشارکت داشته باشند. عدم توسعه هماهنگ امنیت سایبری و عدم توجه به توسعه ساختارهای دفاع ملی سایبری، تهدیدی فزاینده برای تجارت و اقتصاد کشور ایجاد خواهد کرد (تقی‌پور و همکاران، ۱۳۹۶).

دفاع سایبری عبارت از بهره‌گیری از کلیه امکانات سایبری و غیر سایبری کشور، به‌منظور ایجاد بازدارندگی، پیشگیری، ممانعت از انجام، تشخیص به‌موقع، مقابله مؤثر و بازدارنده با هرگونه تهاجم سایبری به زیرساخت‌های (سرمایه‌های ملی سایبری) جمهوری اسلامی ایران، توسط متخاصمین سایبری، اعم از نیروی نظامی (ارتش سایبری) کشور متخاصم یا دیگر منشأها و رسیدگی فوری و مؤثر به منشأ و کلیه پیامدهای ناشی از تهاجم سایبری اعم از حوادث سایبری، آسیب‌پذیری‌ها، سلاح‌های سایبری و اقدام قانونی علیه منشأ تهاجم سایبری می‌باشد به‌نحوی‌که امکان تهاجم سایبری را از کلیه متخاصمین، سلب نماید (سند دفاع سایبری، ۱۳۹۵).

علاوه بر آسیب‌پذیری‌های داخلی ناشی از ضعف زیرساخت‌های فنی و نیز کمبودها و ضعف‌های آموزشی، طیف وسیعی از عوامل و تهدیدات خارجی مهاجم وجود دارند که می‌توانند علیه زیرساخت‌های حیاتی دست به تهاجم بزنند. مهم‌ترین نگرانی دراین‌باره تهدید ناشی از حملات سایبری سازمان‌یافته است که قادر به تحمیل لطمه‌های جبران‌ناپذیر بر زیرساخت‌های حیاتی کشور می‌باشند. از این جهت لازم است تا در سطح ملی، ضمن شناسایی نقاط ضعف و قوت و نیز آسیب‌پذیری‌های احتمالی و با در نظر گرفتن فرصت‌ها و تهدیدات در محیط بین‌الملل، اقدامات بازدارنده متناسب پیش‌بینی و چاره‌اندیشی شود.

بُعد اقتصادی

گسترش فضای سایبر و کاربردهای آن و ارائه خدمات الکترونیکی توسط بنگاه‌های تجاری، بانک‌ها و مؤسسات مالی و اعتباری، کاهش هزینه‌ها و سرعت بالاتر و تنوع بیشتر خدمات ارائه‌شده به مردم را در برداشته و گرایش روزافزون مردم به استفاده از این خدمات، نقش آن را در زندگی روزمره مردم پررنگ‌تر کرده است. از سوی دیگر گرایش به استراتژی‌ها و تاکتیک‌های جنگ سایبری، امنیت این خدمات را با چالش بیشتر روبه‌رو می‌کند. با در نظر گرفتن وضعیت و سطح فناوری در کشور و دشمنان آن، تمام استراتژی‌های جنگ سایبری، چالش‌هایی جدی را برای تجارت و اقتصاد الکترونیکی در

کشور ایجاد می‌کنند. اهداف یک جنگ سایبری محدود به مجتمع‌ها و تأسیسات نظامی نیست و فعالیت‌های مالی و اقتصادی دولتی و خصوصی نیز از اهداف مهم آن هستند(سامانتا اف.راویچ، ۱۳۹۵).

تبعات مستقیم در سطح ملی ممکن است شامل ایجاد ناتوانی یا کندی در جابه‌جایی نقدینگی در اقتصاد، ایجاد کندی و اختلال در پرداخت‌ها و گردش مالی، ایجاد مانع یا ناتوانی در فرایند سرمایه‌گذاری و تجارت یا ازهم‌گسیختگی تجارت محلی و کمک به درماندگی اقتصادی باشد. تبعات غیرمستقیم در سطح ملی ممکن است؛ شامل ایجاد نارضایتی عمومی و بروز ناآرامی‌های اجتماعی، ورود ضربه اقتصادی در سطح ملی، کاهش سطح رفاه عمومی و تولید ناخالص ملی، از دست رفتن اعتماد مردم به بانکداری، اقتصاد و تجارت الکترونیکی و رویگردانی آنان از این خدمات یا از دست رفتن گسترده اطلاعات شخصی و نقض حریم خصوصی افراد باشد. تبعات محدود ممکن است؛ شامل ایجاد مانع یا ناتوانی در مجتمع‌های صنعتی و تولید و توزیع، صدمه اقتصادی سازمان‌های هدف قرار گرفته، کاهش ارزش سهام یا ورشکستگی سازمان، کاهش حقوق یا مزایا یا بیکاری موقت یا دائمی کارکنان سازمان‌های هدف قرار گرفته یا از دست رفتن اعتبار سازمان‌های هدف قرار گرفته باشد.

بُعد علم و فناوری

روند تحولات و پیشرفت علم و فناوری در آینده شتاب خواهد گرفت، نرخ تغییرات آن طی ۲۵ سال آتی بسیار بیشتر از قرن گذشته خواهد بود. دانش به سرعت گسترش خواهد یافت، تحولات علم و فناوری زندگی روزمره، بشر را دستخوش تغییر می‌کند و فضای سایبر نقش قابل توجهی در این خصوص خواهد داشت. افزایش دسترسی به فناوری و تشابه فرهنگی موجب خواهد شد که نسل‌های آینده به‌طور فزاینده‌ای در برابر تخریب آگاهانه یا ناخواسته امکانات فناوری‌محور، آسیب‌پذیر باشند (Development, Concepts and Doctrine Center, 2007).

طی دهه آینده شاهد پیشرفت قابل توجهی در برخی حوزه‌ها مثل بیوتکنولوژی، نانو تکنولوژی، ارتباطات، حفاظت از محیط‌زیست و سایبری خواهیم بود. توسعه پیوسته علم و فناوری، یادگیری مداوم را ضروری می‌سازد و همگرایی و شبکه‌سازی روزافزون، تغییراتی بنیادین در همه بخش‌های صنعتی به‌جای می‌گذارد. افزایش استفاده از فناوری‌های سایبری، اتکا به آن‌ها در حوزه‌های کسب‌وکار، پزشکی، صنعت، لیزر را در پی خواهد داشت.

نوآوری‌های سریع و مکرر، بازیگران مختلف را (اعم از تهدیدآفرین و تهدیدشونده) در فضای عدم قطعیت قرار داده و شناسایی روندهای احتمالی آینده و پیشران‌ها را به امری حیاتی تبدیل کرده است (اسماعیلی و ثناقربانی، ۱۳۹۷).

به خاطر رابطه متقابل امنیت ملی با قدرت؛ تغییر بنیادین در مفهوم و ویژگی‌های قدرت در فضای سایبر، مخاطرات و تهدیدات جدیدی را برای امنیت ملی به وجود آورده و از طرف دیگر، فناوری‌های مرتبط با فضای سایبر را به عاملی برای کسب قدرت و تأمین امنیت ملی تبدیل نموده است .این مسئله حاکی از عمق نفوذ فضای سایبر در تمامی حوزه‌های راهبردی کشور است (هلیلی و همکاران، ۱۳۹۷).

بُعد فرهنگی- اجتماعی

فضای مجازی عرصه حضور قدرت‌های اطلاعاتی و محتوایی است؛ بنابراین جوامعی که قدرت بیشتری در این عرصه دارند، به دنبال آن حضور قوی‌تری در این فضا خواهند داشت و این بدین معناست که فرصت بیشتری برای تأثیرگذاری بر روی دیگر فرهنگ‌ها و تمدن‌ها دارند. همین موضوع به فرهنگ‌های ارزشی، غنی و باریشه‌ای که به دلایل متعدد، از حضور مؤثر در فضای مجازی محروم یا ناتوان‌اند، آسیب جدی وارد می‌کند و به‌نوعی آن‌ها را در معرض استحاله و اثرپذیری از فرهنگ‌های بیگانه مسلط بر فضای مجازی قرار می‌دهد.

ازجمله تهدیدهای اجتماعی، فرهنگی در فضای سایبر می‌توان به رواج تفرّد و کاهش شدید روحیه مسئولیت‌پذیری در بین جوانان، کم‌رنگ شدن ارزش‌های مترقی، تضعیف فرهنگ‌های کم‌حضور، تضعیف اعتقادات و گسترش شبهات فکری، رواج سطحی‌نگری

فکری، گسترش اباحه‌گری عملی، به خطر افتادن حقوق مادی و معنوی مؤلفین، گسترش محصولات فرهنگی فرهنگ‌های منحط (به‌ویژه فرهنگ غربی، افسردگی و انزوا، بازداری‌زدایی، بحران هویت و اخلال در شکل‌گیری شخصیت، اعتیاد مجازی، انحرافات اخلاقی (جنسی)، تحمیل پیشنهادهای گیج‌کننده مخل و گاهی منحرف به کاربر و شکاف نسل‌ها اشاره نمود (پدافند غیرعامل ۱۳۹۴).

ازجمله مصادیق تأثیرات امنیتی فضای سایبر می‌توان به تغییر در کارکرد تشکیل اجتماعات، تغییر در نحوه طرح مطالبات اجتماعی براندازی، جاسوسی، خرابکاری، امنیت کاربران، عملیات روانی و جنگ اطلاعاتی اشاره کرد (شعبانی،۱۳۹۰: ۶۶).

بُعد دیپلماسی

فضای تعامل سیاست و سایبر یا به تعبیر درست‌تر فضای سایبرپلیتیک، جدیدترین و مهم‌ترین حوزه مورد توجه کارشناسان سیاست و روابط بین‌الملل در عرصه نظری و عملی محسوب می‌شود که غفلت از آن می‌تواند آسیب‌های جدی و غیرقابل پیش‌بینی برای کشورها به‌عنوان مهم‌ترین بازیگران در عرصه روابط بین‌الملل داشته باشد (عابدی، ۱۳۹۷).

سایبر دیپلماسی اشاره به مدیریت جدیدی (سایبری)، برای ابعاد مختلف سیاست خارجی و امور بین‌الملل دارد که عمل دیپلماسی در ترکیب فضای مجازی با (سنتی) منابع دیپلماتیک صورت می‌گیرد. دیپلماسی سایبری در ساده‌ترین تعریف آن، استفاده از ابزارهای فناوری اطلاعاتی و ارتباطاتی روز، برای تبیین، گسترش و ارتقاء سطح اثربخشی دستگاه دیپلماسی یک کشور در فضای مجازی است. سایبر دیپلماسی تکامل دیپلماسی عمومی است که استفاده از امکانات جدید ارتباطی در قرن ۲۱ را شامل می‌شود که ابتکارها در فناوری اطلاعاتی و ارتباطی را با دیپلماسی مربوط می‌کند و به‌عنوان بخشی از «دیپلماسی عمومی نسخه دوم»، «دیپلماسی عمومی الکترونیکی» و «دیپلماسی مجازی» شناخته می‌شود (محمدی، ۱۳۹۶).

سایبرپلیتیک و امنیت سایبری در شرایط کنونی به‌عنوان موضوع اساسی مورد توجه کارشناسان روابط بین‌الملل، در کنار موضوعات قدیمی‌تر جنگ، اقتصاد، زنان و محیط زیست قرار گرفته و حتی برخی اهمیت آن را از سایر حوزه‌ها بیشتر می‌دانند، زیرا فضای سایبر به شکلی تمامی حوزه‌ها و موضوعات قدیمی را در خود جای داده است. بی‌تردید، دیپلماسی سایبری می‌تواند بسترهای لازم برای بروز و صدور ارزش‌های پایه‌ای یک جامعه به خارج و تقویت قدرت نرم یک کشور را فراهم نماید (حلال‌خور و محمدی، ۱۳۹۸).

بنابراین فضای سایبر شرایط جدیدی ایجاد نموده که در آن موضوعات روابط بین‌الملل به شکل متفاوتی مطرح می‌شوند و درنتیجه شکل جدیدی از سیاست با عنوان سایبرپلیتیک ایجاد شده که پیامدهای ویژه‌ای در حوزه امنیت ملی و جهانی دارد. بر این اساس بررسی کامل و تبیین درست سایبرپلیتیک و امنیت سایبری و تأثیر آن بر تمامی حوزه‌ها در سطح ملی ضرورت می‌یابد.

روش‌شناسی تحقیق

با توجه به موضوع و هدف پژوهش، نوع تحقیق کاربردی- توسعه‌ای[1] است و از نظر اجرا توصیفی-تحلیلی است. گردآوری اطلاعات متناسب با روش تحقیق موضوع در دو بخش انجام شد: یک بخش مربوط به ادبیات موضوع و مبانی نظری و بخش دیگر مربوط به اخذ نظر صاحب‌نظران و متخصصان (سطح تجربی یا عملی) موضوع تحقیق است، در بخش اول از سنجه‌های غیر واکنشی / غیر مزاحم[2] (محمدی‌پور، ۱۳۹۰: ۱۰۷) یا روش کتابخانه‌ای (کتاب‌های تخصصی معتبر، وبگاه‌های معتبر علمی، بانک‌های اطلاعاتی داخلی و خارجی و...) از ابزار فیش[3] استفاده شد و بخش دوم به روش میدانی و با استفاده از ابزارهای مصاحبه[4] و پرسشنامه[5] گردآوری گردید. ابتدا با مطالعه کتابخانه‌ای به گردآوری

1. Applied – Development Research
2. Unobtrusive /Nonreactive Measures
3. Fesh
4. Interview
5. Questionnaire

مفاهیم مرتبط با پژوهش و اسناد بالادستی ملی و بین‌المللی هدف پرداخته شد و سپس ضمن مصاحبه باز با تعداد ۳۰ نفر از خبرگان و متخصصان حوزه سایبری کشور در خصوص نظام رصد پایش و هشداردهی احصاءشده، نظرات و منویات ایشان گردآوری شد، در ادامه با برگزاری یک پنل خبرگان، نتایج مصاحبه‌های باز غنی‌تر گردید و درنهایت ابعاد نظام مورد نظر از منظر امنیت ملی به‌دست‌آمده، جهت تعیین روایی و پایایی، تحلیل وضع موجود، تعیین شکاف این ابعاد با آینده مطلوب و اولویت‌دهی رسیدگی به ابعاد در قالب پرسشنامه بسته به تعداد ۵۰ نفر به بحث گذاشته شد؛ به‌عبارت‌دیگر روش پژوهش صورت‌گرفته تحقیق آمیخته سری (کیفی و سپس کمی) بوده است.

یافته‌های تحقیق

ماحصل مطالعه ادبیات و مبانی نظری، کسب نظر خبرگان و مدیران حوزه سایبری و تحلیل نتایج پرسشنامه‌ها، شناسایی ابعاد هفت‌گانه نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی به شرح جدول شماره ۱ می‌باشد. تعیین وضعیت موجود و آینده مطلوب ابعاد نظام به‌عنوان هدف، دستاورد دیگر این تحقیق است. همچنین فاکتورهای شکاف که حاصل تفاوت بین وضع مطلوب و وضع موجود است و همچنین شکاف موزون که حاصل ضرب شکاف در اهمیت هر بُعد است محاسبه و نتایج نهایی به‌عنوان فاکتور مبنا به شرح جداول زیر به دست آمده است. به‌علاوه به‌منظور تأیید آماری اولویت‌بندی موضوعات از آزمون فریدمن استفاده شده است که نتایج آن در ادامه ارائه می‌شود. طبق جدول شماره ۱ تحلیل شکاف احصاءشده گویای اولویت موضوعات به ترتیب فرهنگی، سیاسی، اجتماعی، دیپلماسی، اقتصادی، دفاعی–امنیتی و علمی و فناورانه است؛ اما شکاف موزون اولویت را به‌صورت فرهنگی، اجتماعی، دیپلماسی، دفاعی–امنیتی، اقتصادی، سیاسی و علمی و فناورانه تعیین نموده است.

جدول ۱. نتایج آمار توصیفی و تحلیل شکاف

رتبه	ابعاد	میانگین اهمیت	وضع موجود	وضع مطلوب	شکاف	شکاف موزون
۱	فرهنگی	4/316	2/704	8/281	5/577	24/069
۲	اجتماعی	4/070	2/704	7/947	5/244	21/343
۳	دیپلماسی	4/211	2/130	7/123	4/993	21/024
۴	دفاعی-امنیتی	4/281	2/852	7/561	4/710	20/160
۵	اقتصادی	3/930	2/481	7/228	4/747	18/653
۶	سیاسی	3/263	2/333	7/877	5/544	18/090
۷	علمی و فناورانه	3/456	2/946	6/912	3/968	13/713

از آنجا که همواره ورود فناوری‌های جدید، به‌خصوص سایبری از کشورهای غربی به کشورهای درحال‌توسعه، مقدم بر ایجاد فرهنگ بومی استفاده از آن‌ها بوده است، با توجه به‌شدت اثرپذیری فرهنگ‌ها و تمدن‌ها در فضای سایبر و آسیب‌های قابل توجهی که از این رهگذر پدیدار شده است لذا پرداختن به بُعد فرهنگی نظام از نظر نخبگان، بالاترین مقدار را نشان می‌دهد که با توجه به شکاف قابل توجه احصاءشده طبیعی است که بالاترین میزان شکاف موزون را به خود اختصاص داده و در صدر اولویت رسیدگی قرار می‌گیرد. بُعد اجتماعی نیز با توجه به قرابت و آمیختگی با بُعد فرهنگی و نظر به تأثیرات امنیتی فضای سایبر بر این حوزه و آسیب‌های مترتب، هم از نظر اهمیت و هم از لحاظ شکاف، پس از بُعد فرهنگی، مقادیر قابل توجهی را تجربه نموده و از نظر خبرگان در جایگاه دوم قرار گرفته است. حسب نظر خبرگان، از آنجا که تفکیک فضای سایبر به داخل و خارج و ایجاد حدومرز فیزیکی به سبک حدود جغرافیایی متصور نیست، لذا دیپلماسی سایبری به معنی ایجاد همکاری‌های منطقه‌ای و فرامنطقه‌ای بین‌المللی یک ضرورت انکارناپذیر در تکمیل فرایند رصد و پایش است. ازاین‌رو بُعد دیپلماسی در جایگاه سوم رسیدگی قرار گرفته است. سایر ابعاد دفاعی- امنیتی، اقتصادی، سیاسی و علمی و فناورانه بر اساس نظر صاحب‌نظران سایبری، با توجه به کارکردها، زمینه‌ها، شرایط و مصادیق احصاءشده در رتبه‌های بعدی، ارزیابی شده‌اند.

بر اساس نتایج جدول شماره ۲، اهمیت، وضعیت موجود و مطلوب نظام در هر یک از جنبه‌های امنیت ملی؛ شامل دفاعی–امنیتی، سیاسی، فرهنگی، اجتماعی، اقتصادی، علمی و فناورانه و دیپلماسی از نظر خبرگان در سطح اطمینان ۹۵٪ با درجه آزادی شش دارای اختلاف رتبه معنی‌دار بوده است.

جدول ۲. نتایج آزمون فریدمن

	اهمیت	وضع موجود	وضع مطلوب
تعداد	57/000	54/000	57/000
کای مربع	75/461	19/034	32/708
درجه آزادی	6/000	6/000	6/000
سطح معنی‌داری	0/000	0/004	0/000

از منظر خبرگان و بر اساس رتبه‌های کسب‌شده در آزمون فریدمن در جدول شماره ۳ به لحاظ اهمیت، ترتیب به‌صورت فرهنگی، دفاعی–امنیتی، دیپلماسی، اجتماعی، اقتصادی، علمی و فناورانه و سیاسی بوده، همچنین در وضعیت موجود ترتیب به‌صورت علمی و فناورانه، دفاعی– امنیتی، فرهنگی، اجتماعی، اقتصادی، سیاسی و دیپلماسی است. درحالی‌که انتظار از وضع مطلوب به ترتیب فرهنگی، اجتماعی، سیاسی، دفاعی–امنیتی، دیپلماسی، اقتصادی، علمی و فناورانه می‌باشد.

جدول ۳. میانگین رتبه‌های حاصل از آزمون فریدمن

ابعاد	اهمیت	وضع موجود	وضع مطلوب
دفاعی–امنیتی	4/763	4/444	4/132
سیاسی	2/640	3/519	4/325
فرهنگی	4/816	4/269	4/886
اجتماعی	4/272	4/148	4/439
اقتصادی	3/895	3/694	3/395
علمی و فناورانه	2/991	4/583	3/202
دیپلماسی	4/623	3/343	3/623

شکل‌های شماره ۳، ۴ و ۵ به ترتیب اولویت، منظرهای نظام رصد، پایش و هشداردهی سایبری (ابعاد نظام) با رویکرد امنیت ملی مبتنی بر تحلیل وضع موجود، وضع مطلوب و شکاف موزون را نشان می‌دهد.

شکل ۳. منظرهای نظام رصد، پایش و هشداردهی سایبری مبتنی بر تحلیل وضع موجود

شکل ۴. منظرهای نظام رصد، پایش و هشداردهی سایبری مبتنی بر تحلیل وضع مطلوب

شکل ۵. منظرهای نظام رصد، پایش و هشداردهی سایبری مبتنی بر تحلیل شکاف موزون

نتیجه‌گیری و پیشنهاد

پیشرفت سریع فضای سایبری در سال‌های اخیر و درهم‌آمیختگی و برهم‌کنش ابعاد و شئونات مختلف اجتماعی با این فضا، تأمین امنیت آن را بسیار حیاتی کرده است، به‌نحوی‌که عدم توجه کافی به مقوله امنیت در فضای سایبری می‌تواند خطرات بسیار زیادی را متوجه وجوه مختلف حاکمیت و امنیت ملی نماید. لذا از آنجا که در هر مجموعه حاکمیتی، پایه‌ای‌ترین زیرساخت، آگاهی از شرایط محیطی و فضای پیرامونی آن است، برای هرگونه تصمیم‌سازی و تصمیم‌گیری ضروری می‌نماید شناخت مناسبی از جامعه مبتنی بر فضای سایبر در اختیار صاحبان تصمیم گذاشته شود لذا نقش کلیدی نظام رصد، پایش و هشداردهی فضای سایبر کلیدی می‌نماید.

وابستگی شدید و روزافزون حوزه‌های مختلف حاکمیتی ناشی از تأثیر و تأثر از فضای سایبر، انجام اقداماتی برای شناخت هدفمند، منسجم، پویا، انطباق‌پذیر و دارای بازخورد، دانش‌بنیان، چالاک، یکپارچه و توزیع‌شده از اجزاء و واحدهای مختلف، تعاملات فی‌مابین، ورودی و خروجی‌های آن‌ها در سطح کشور است که در قالب فرایند مشخص، به‌صورت هوشمند و پیش‌دستانه و در چارچوب سیاست‌ها و راهبردهای ملی به رصد و پایش فضای مجازی در ابعاد مختلف امنیت ملی پرداخته و هشدارهای لازم را به‌منظور تصمیم‌گیری و اقدام در سطوح فنی، عملیاتی و راهبردی به‌صورت مؤثر و به‌هنگام با هدف امن‌سازی، مصون‌سازی، مقاوم‌سازی و کاهش مخاطرات و جلوگیری از غافلگیری در مواجهه با تهدیدات و آسیب‌پذیری‌ها و اطلاع و استفاده به‌موقع از فرصت‌های فضای سایبر اجتناب‌ناپذیر کرده است.

در این راستا وضعیت مطلوب و ابعاد مختلف نظام رصد، پایش و هشداردهی فضای سایبر از منظر امنیت ملی بر اساس مطالعات تطبیقی و رهنمودهای خبرگان احصاء و با وضعیت موجود آن مورد بررسی و تحلیل قرار گرفت. بر این اساس، اهمیت، وضعیت موجود و مطلوب نظام در هر یک از جنبه‌های امنیت ملی؛ شامل دفاعی–امنیتی، سیاسی، فرهنگی، اجتماعی، اقتصادی، علمی – فناورانه و دیپلماسی از نگاه خبرگان دارای اختلاف رتبه معنی‌دار بوده است. تحلیل شکاف گویای اولویت ابعاد مختلف به ترتیب فرهنگی، سیاسی، اجتماعی، دیپلماسی، اقتصادی، دفاعی امنیتی و علمی – فناورانه است، اما شکاف موزون ترتیب را به‌صورت فرهنگی، اجتماعی، دیپلماسی، دفاعی امنیتی، اقتصادی، سیاسی و علمی – فناورانه تعیین نموده است. لذا به‌منظور نیل به وضعیت مطلوب نظام رصد، پایش و هشداردهی سایبری، پیشنهاد پژوهش‌های آتی این است که ضمن تصویرسازی از آینده مطلوب این نظام مبتنی بر الگوی راهبردی اسلامی ایرانی، راهبردها، راهکارها و اقدامات اجرایی لازم در قالب برنامه راهبردی گذار به وضعیت مطلوب بر اساس اولویت‌های تعیین‌شده برای دستیابی به کمال ابعاد احصاءشده تهیه و تدوین گردد. همچنین با توجه به درهم‌آمیختگی شئونات مختلف زندگی، در فضای سایبر، بررسی و تحلیل برهم‌کنش ابعاد مختلف در این فضا بر بلوغ نظام خواهد افزود.

فهرست منابع ومآخذ

الف. منابع فارسی

- اسماعیلی، علی و ثناقربانی، جلال (۱۳۹۷)، تبیین نسبت سناریوهای محتمل و مطلوب تهدیدات سایبری جمهوری اسلامی ایران، فصلنامه امنیت ملی، سال هشتم، شماره ۲۸.
- برژینسکی، زبیگنیو (۱۳۶۸)، در جستجوی امنیت ملی، ترجمه ابراهیم خلیلی، تهران: سفیر.
- بصیری، محمد علی (۱۳۸۸)، تحولات مفهوم امنیت ملی، نشریه اطلاعات سیاسی و اقتصادی، شماره ۱۶۳ و ۱۶۴، ۱۷۳-۱۶۶.
- بوزان، باری (۱۳۷۸)، مردم، دولت و هراس، ترجمه پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی.
- پدافند غیرعامل، پایداری ملی، (۱۳۹۴)، اهمیت فضای مجازی همسنگ انقلاب اسلامی، قابل دسترسی در: https://paydarymelli.ir/fa/news/۱۷۴۲۴/ اهمیت فضای مجازی همسنگ انقلاب اسلامی
- تقی‌پور، رضا و اسماعیلی، علی (۱۳۹۷)، طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران، فصلنامه امنیت ملی، سال هشتم، شماره ۳۰.
- حسن‌بیگی، ابراهیم (۱۳۸۴)، توسعه شبکه ملی دیتا، چالش‌های فراروی و تهدیدهای متوجه امنیت ملی، فصل‌نامه پژوهشی اندیشه انقلاب اسلامی، شماره ۹، ۱۲۷-۷۶.
- تقی‌پور، رضا؛ رامک، مهراب؛ امیرلی، حسین؛ قربانی، ولی‌الله؛ حقی، مجید، کاظمی، موسی؛ رمضان یارندی، محسن؛ اسماعیلی، علی؛ یزدانی، سعید و
- حسن‌بیگی، ابراهیم (۱۳۸۴)، حقوق و امنیت در فضای سایبر، تهران: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.
- حلال‌خور، مهرداد و محمدی، عقیل (۱۳۹۸)، صدور ارزش‌های پایه‌ای جامعه ایران از طریق دیپلماسی عمومی سایبری و افزایش امنیت ملی ایران، دومین کنفرانس ملی پدافند سایبری، مراغه، دانشگاه آزاد اسلامی واحد مراغه.
- خلیلی‌پور رکن‌آبادی، علی و نورعلی وند، یاسر (۱۳۹۱)، تهدیدات سایبری و تأثیر آن بر امنیت ملی، فصلنامه مطالعات راهبردی شماره ۵۶.
- دیویس، جکف (۱۳۸۶)، هشدار استراتژیک: اگر شگفتی غیر قابل اجتناب است، تحلیل چه نقشی را ایفا می‌کند؟، فصلنامه دانش اطلاعاتی، شماره ۴، دانشکده امام باقر (ع)، ۶۱-۸۳.
- روشندل، جلیل (۱۳۷۴)، امنیت ملی و نظام بین‌الملل، تهران: سازمان مطالعه و تدوین کتب علوم انسانی (سمت).

- سامانتا اف. راویچ (۱۳۹۵)، جنگ اقتصادی سایبری: چالشی در حال تکامل، فصلنامه پدافند اقتصادی، شماره ۲۱.
- سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور (۱۳۸۷)، تهران: وزارت ارتباطات و فناوری اطلاعات شماره ۲۳۲۶۹۰/ت ۳۸۵۱۸ ک ۱۳۸۷/۱۲/۱۱.
- سند راهبردی پدافند سایبری (۱۳۹۴)، تهران: سازمان پدافند غیرعامل.
- سند راهبردی دفاع سایبری (۱۳۹۵)، تهران: سازمان پدافند غیرعامل.
- شعبانی، ناصر (۱۳۹۰)، نقش شبکه‌های اجتماعی مجازی در سازماندهی فتنه سال ۱۳۸۸، مجله: پاسداری فرهنگی انقلاب اسلامی، شماره ۴: ۸۲-۵۱.
- عابدی، سجاد (۱۳۹۷)، خلأ دیپلماسی سایبری در ساختار امنیتی کشور، قابل دسترسی در: https://www.khabaronline.ir/news/۱۲۱۰۶۳۵//خلاء دیپلماسی سایبری در ساختار امنیتی کشور
- عالی‌پور، حسن (۱۳۹۰)، امنیت سایبری در چشم‌انداز ۱۴۰۴، چالش‌ها و راه‌کارهای حقوقی رویارویی با بزه‌های امنیتی سایبری.
- عبدالله خانی، علی و حسینی، پرویز (۱۳۹۴)، سنجش تهدیدات سایبری، فصلنامه امنیت ملی، سال چهارم، شماره ۱۶.
- فروردین، وحید؛ سملی، احمد و عمویی، حسین (۱۳۹۷)، بررسی تأثیرات جنگ سایبری بر امنیت ملی در جمهوری اسلامی ایران، کنفرانس بین‌المللی امنیت، پیشرفت و توسعه پایدار مناطق مرزی، سرزمینی و کلان‌شهرها، راهکارها و چالش‌ها با محوریت پدافند غیرعامل و مدیریت بحران، تهران: دانشگاه افسری امام علی (ع).
- قاسمی، حاکم (۱۳۷۲)، برداشت‌های متفاوت از امنیت ملی، فصلنامه سیاست دفاعی، شماره ۲.
- ماندل، رابرت (۱۳۷۷)، چهره متغیر امنیت ملی، ترجمه پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی.
- محمدی، مصطفی (۱۳۹۶)، سایبر دیپلماسی و تأثیر آن بر روابط کشورها، اندیشکده راهبردی تبیین، قابل دسترسی در: http://tabyincenter.ir/۱۹۷۰۵/ سایبر دیپلماسی و تأثیر آن بر روابط کشور
- محمودزاده، ابراهیم؛ حسنی اصل، حمیدرضا؛ قوچانی، محمد مهدی و نیک نفس، علی (۱۳۹۷)، تدوین راهبردهای امنیت سایبری سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور، فصلنامه علمی پژوهشی مطالعات بین‌رشته‌ای دانش راهبردی، سال هشتم، شماره ۳۱.
- مدیریت مرزهای فضای سایبر، گام نخست دفاع سایبری، مجموعه مقالات نخستین همایش ملی دفاع سایبری، تهران: نشر پژوهشکده ICT جهاد دانشگاهی، ۳۳-۱۵.

- مرکز پدافند غیرعامل (۱۳۸۷)، کتاب جنگ سایبر، تهران: مرکز پدافند غیرعامل.
- واژه‌نامه مشترک آمریکا و روسیه در فضای سایبر (۱۳۹۱)، سایت گـرداب، ۲۷ تیـر ۱۳۹۱ – ۱۲: ۵۷. قابل دسترسی در: http://www.gerdab.ir/fa/news/
- ملائی، علی (۱۳۹۶)، طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن (مطالعه گروهی)، تهران: دانشگاه عالی دفاع ملّی، دانشکده امنیت ملی.
- ملائی، علی؛ کارگری، مهرداد و خراشادی‌زاده، محمدرضا (۱۳۹۷)، الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها، فصلنامه امنیت ملی، سال هشتم، شماره ۲۹.
- موسوی، سید محمدرضا؛ حیـدری، خدیجـه و قنبـری، علـی (۱۳۹۲)، تـأثیر تهدیـدات امنیتـی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایـران و راهکارهـای مقابلـه بـا آن، فصـلنامه مطالعات بین‌المللی پلیس، شماره ۱۴.
- میرشاه ولایتی، فرزانه و نظری‌زاده، فرهاد (۱۳۸۹)، پویش محیطی، مرکـز آینـده‌پژوهـی علـوم و فناوری دفاعی، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، چاپ اول.
- وزارت اطلاعات جمهوری اسلامی ایران، هشداردهی والاترین مأموریت اطلاعات، (۱۳۹۳)، قابل دسترسـی در: http://www.vaja.ir/Portal/home/?news/۲۸۳۰۵۲/۲۹۱۲۲۸/۲۸۹۵۰۶/ هشداردهی والاترین مأموریت اطلاعات
- ولوی، محمدرضا؛ صحرائی، مهدی؛ ترقی، عبدالرضا؛ نیک نفس، علـی؛ دهقـانی، حامـد؛ دلگیـر، علی و حسنی اصل، حمیدرضا (۱۳۹۶)، نظام رصد، پـایش و هشـداردهی سـایبری بـا رویکـرد امنیت ملی (مطالعه گروهی)، تهران: دانشگاه عالی دفاع ملّی، دانشکده امنیت ملی.
- وزارت دفاع و پشتیبانی نیروهای مسلح، مؤسسه آموزشی و پژوهشی صنایع دفاعی، اندیشگاه شـریف، اندیشکده کاوشگران آینده، (۱۳۸۴)، جنگ سایبری: پروژه الزامات جنگ‌های نوین در فضـای مجـازی (سایبر)، قابل دسترسی در: http://www.vahidthinktank.com/oldArman/Reports/CyberWar/CyberWar.pdf
- هلیلی، خداداد؛ ولوی، محمدرضا؛ موحدی صفت، محمدرضا و باقری، مسعود (۱۳۹۷)، قـدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی، فصـلنامه امنیـت ملـی، سـال هشتم، شماره ۲۹.

ب. منابع انگلیسی

- Rowland, J. Rice, M. & Shenoi, S. (2014). The anatomy of a cyber power. International Journal of Critical Infrastructure Protection, 7(1), 3-11.
- Chandler, R. C., & Plano, J. C. (1988). The public administration dictionary. Abc-Clio Inc.

- Kevin Benedict,)2012(, Information Operation, the Fifth Dimension of Warfare.
- Van Vuuren, J. C. J. (2016). Methodology and Model to Establish Cybersecurity for National Security in Africa using South Africa as a Case Study (PhD Thesis).
- UK cyber security strategy, 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.
- Gartner,2014, Gartner Top Predictions, http://www.gartner.com/it/content/2607600/2607616/november_6_top_predicts_2014dplummer.pdf?userId=72895160 visit date: 2014-09-20.
- Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (2009) "Cyberpower and National Security", National Defense University Press, Washington DC.
- Development, Concepts and Doctrine Center, (2007) و United States Joint Forces Command.
- Merriam-webster. (2017). WWW. Merriam-webster.com (online famous dictionary)
- Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN(2013) final, https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.
- Richard, C., & Robert, K. (2010). Cyber war: the next threat to national security and what to do about it.