فصلنامه علمی پژوهشی مطالعات بین‌رشته‌ای دانش راهبردی
سال هفتم، شماره ۲۷، ۱۳۹۶، صفحه ۲۴۸- ۲۲۹

اولویت‌بندی راهبردهای توسعه سامانه‌ی فرماندهی و کنترل (C4I) فضای سایبر کشور

دکتر ابراهیم محمودزاده[۱]، علی نیک نفس[۲]، محمد مهدی قوچانی[۳]

تاریخ دریافت: ۹۵/۰۵/۲۵ تاریخ پذیرش: ۹۵/۰۸/۲۵

چکیده

بهره‌برداری فزاینده از فناوری اطلاعات و ارتباطات و توسعه روزافزون فضای سایبر به همراه وابستگی بیش از پیش ابعاد مختلف امنیت ملی به این فضا، آن را به محیطی برای منازعات و جنگ سایبری تبدیل نموده است که هر روز، نسبت به قبل اهمیت بیشتر و ابعاد تازه‌ای به خود می‌گیرد. تهدیدات دفاعی و امنیتی در سطح ملی نیازمند سامانه‌هایی است که فرماندهی و کنترل بحران‌ها و تهدیدات سایبری را ممکن سازد. این پژوهش ضمن معرفی این مفهوم به بررسی موضوعات راهبردی مرتبط در اسناد برخی کشورها از طریق مطالعه کتابخانه ای اسناد پرداخته است. سپس با توجه به شرایط و نیاز کشور و با استفاده از نظرات خبرگان، نسبت به بومی‌سازی و اولویت‌بندی راهبردهای توسعه سامانه‌ی فرماندهی و کنترل فضای سایبر کشور بر اساس روش تحقیق کمی و با استفاده از روش تجزیه تحلیل سلسله مراتبی(AHP) اقدام نموده است. در نتیجه گزینه‌های راهبردی "ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری"، "همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی" و "توسعه همکاری و تعاملات بین‌المللی" اولویت‌های برتر را به خود اختصاص داده‌اند.

کلیدواژه‌ها: فرماندهی و کنترل سایبری، C4I، فضای سایبر، تهدیدات سایبری، امنیت و دفاع ملی، تجزیه تحلیل سلسله مراتبی(AHP)

[۱] - دانشیار دانشگاه صنعتی مالک اشتر

[۲] – دانشجوی دوره سوم مدیریت راهبردی فضای سایبرگرایش امنیت سایبر، دانشگاه عالی دفاع ملی. نویسنده مسئول: Email:A.Niknafs@sndu.ac.ir

[۳] – دانشجوی دکتری مدیریت دولتی دانشگاه علامه طباطبایی

مقدمه

در حال حاضر و در عصر سایبر، طیف گسترده‌ای از طرف‌های درگیر در فضای سایبر و بازیگران مختلف وجود دارند که شامل گستره‌ی وسیعی از هکرها و گروه‌های هکری تا ارتش‌های سایبری می‌شوند. لذا انگیزه‌ها، اهداف و توانمندی آنان نیز تفاوت زیادی با یکدیگر دارد و مواجهه با آنان و ایجاد بازدارندگی در برابر آنان نیز طیف وسیعی از پیش‌بینی‌ها و اقدامات را شامل می‌شود(Kugler، 2009). حوزه‌ی مجازی به عنوان یک دامنه‌ی جدید منازعات نظامی و حوزه‌ی پنجم جنگ به رسمیت شناخته شده است و به دلیل وابستگی سایر حوزه‌های امنیت ملی از نظامی–دفاعی و امنیتی گرفته تا سیاسی و امنیتی، اقتصادی، فرهنگی و اجتماعی و توسعه روزافزون وابستگی افراد و جوامع به آن ، اهمیت آن در حال فزونی گرفتن است.

بر اساس سند چشم‌انداز ۱۴۰۴، ایران کشوری امن، مستقل و مقتدر با سامان دفاعی مبتنی بر بازدارندگی همه‌جانبه در افق چشم‌انداز خواهد بود(چشم‌انداز جمهوری اسلامی ایران در افق ۱۴۰۴ هجری شمسی، ۱۳۸۲). فضای سایبر به دلیل ماهیت و ویژگی‌های خود از قبیل یکپارچگی، بی‌مرزی و کاهش محدودیت‌های مکانی و زمانی در ایجاد دسترسی، سرعت، سهولت دسترسی و امکان دسترسی از راه دور شرایطی را ایجاد نموده است که برخی تهدیدات دفاعی و امنیتی به سرعت و سادگی بتوانند از طریق این فضا بالفعل شده و با هزینه اندک، آسیب و خسارت فراوان به کشور هدف وارد نمایند.

بر همین اساس در سیاست‌های کلی برنامه‌ی ششم توسعه ابلاغی مقام معظم رهبری، ارتقاء توان بازدارندگی کشور با افزایش ظرفیت‌های قدرت نرم و دفاع سایبری و تأمین پدافند و امنیت سایبری برای زیرساخت‌های کشور در چارچوب سیاست‌های کلی مصوب مورد تاکید قرار گرفته است.

از سوی دیگر در سیاست‌های کلی برنامه‌ی ششم توسعه ابلاغی مقام معظم رهبری، امور مرتبط با فناوری اطلاعات و ارتباطات بر ایجاد، تکمیل و توسعه‌ی شبکه ملی اطلاعات و تأمین امنیت آن، تسلط بر دروازه‌های ورودی و خروجی فضای مجازی و پالایش هوشمند آن و ساماندهی، احراز هویت تاکید گردیده است ("سیاست‌های کلی برنامه ششم توسعه"، ۱۳۹۴):

مطابق سیاست‌های ابلاغی فوق توسعه فناوری اطلاعات و ارتباطات در کشور ما همانند روند جهانی آن و حتی بیشتر از متوسط روندهای جهانی طی سال‌های پیش رو سرعت خواهد داشت. لذا اندیشیدن به تمهیدات لازم و اتخاذ تدابیر مناسب به منظور امن سازی فضای سایبر و اجتناب

از تهدیدها و آسیب‌های متصور از آن علیه کشور بیش از پیش ضرورت می‌یابد. به ویژه کـه ورود دشمنان کشورمان به عرصه‌هـای جدیـد جنگـی ماننـد جنـگ سـایبر بـا هـدف ایجـاد اخـتلال در شبکه‌های رایانه‌ای و سامانه‌های ارتباطی که به شکل مستقیم با مسائل اجتماعی و اقتصادی جامعـه در ارتباط است، موجب تقویت نگرانی‌های اجتماعی داخل ایران خواهد شد(مومن نژاد، ۲۰۱۳).

جمهوری اسلامی ایران به دلایل مختلف و شـرایط خـاص خـود از جملـه منـابع غنـی، موقعیـت جغرافیایی، مسائل ایدئولوژیک و بر اساس شواهد تاریخی همواره مطمع نظر بوده و بـا تهدیـدات زیادی از سوی سایر کشورها مواجه بوده است. بعلاوه در معرض بلایای طبیعـی زیـادی همچـون سیل و زلزله قرار دارد که نیاز به بکارگیری سـامانه‌هـای فرمانـدهی و کنتـرل بـه منظـور مـدیریت یکپارچه و موثر بحران‌های احتمالی دارد. به منظور مدیریت فضای سایبر کشور در مقابل تهدیدات دفاعی و امنیتی نیز وجود سامانه‌ای یکپارچـه و در عـین حـال توزیـع شـده جهـت دسترسـی بـه اطلاعات لازم و بهنگام خودی و حریف به منظور درک شرایط و تصمیم‌گیری به‌موقـع از اهمیـت بسزایی برخوردار است.

ماهیت فضای سایبر، فراگیری و یکپـارچگی آن موجـب بهـره‌منـدی فرمانـدهان از مجموعـه‌ای از ابزارهای مشارکتی می‌گردد که به آن‌ها امکان می‌دهد در عین توزیع‌شدگی حتـی در زمـانی کـه در سراسر دنیا پراکنده شده‌اند در یک "فضای حل مشکل مجازی " با هم کار کنند، مشکل مشترک را درک نمایند و چاره‌ای برای آن بیندیشند. بر این اساس هر یک از موجودیت‌های سامانه فرماندهی و کنترل سایبری به اطلاعـات جمع‌آوری شـده یـا بـه وجـود آمـده در داخـل سـامانه مبتنـی بـر محدودیت‌های ناشی از خط‌مشـی و امنیـت دسترسـی خواهنـد داشـت. از ایـن پایگـاه اطلاعـاتی مشترک، فرماندهان و ستادها می‌توانند تصاویر عملیـاتی منحصـربه‌فـردی از وضـعیت موجـود در حیطه کاری خود خلق و در چرخه تصمیم‌گیری و اقـدام، بـا اطمینـان از صـحت و بهنگـام بـودن اطلاعات دریافتی و در نتیجه با اتخاذ تصمیمات صحیح و بموقع و امکان صدور فرمان‌های مناسب و ابلاغ بموقع آن به واحدهای عملیاتی نتیجه مطلوب و بهینه را حاصل نمایند. نبود چنـین امکـانی موجب ضعف شدید در فرماندهی منسـجم و مناسـب دفـاعی در فضـای سـایبر خواهـد شـد لـذا برنامه‌ریزی راهبردی به منظور توسعه چنین سامانه‌ای باید در دستور کار قرار گیرد.

بررسی‌ها نشان می‌دهد که این موضوع در عرصه بین‌المللی دغدغه‌ای جدی اسـت بـه طـوری کـه توسعه چنین سامانه‌هایی در دستور کار کشورهای مختلف پیشرو در حوزه سایبر قرار گرفته اسـت اما به نظر می‌رسد که این موضوع در کشور ما، با وجود اهمیت آن مورد کـم‌تـوجهی قـرار گرفتـه

است. لذا مسئله‌ی اصلی این تحقیق پرداختن به سامانه‌ی فرماندهی و کنترل فضای سایبر کشور و راهبردهای توسعه آن به منظور ایجاد قابلیت مقابله موثر با تهدیدات در سطح ملی است. لذا سوال اصلی این تحقیق آن است که راهبردهای مناسب برای توسعه سامانه مزبور چیست و اولویت آن‌ها چگونه است؟

طرح مفاهیمی همانند هماهنگی، یکپارچه‌سازی و هدایت فعالیت‌های عملیاتی در فضای سایبر در اسناد راهبردی کشورهای مختلف، مرتبط با سامانه‌های فرماندهی و کنترل این فضا بوده و به عنوان خروجی‌های ایجاد و استقرار سامانه‌های مزبور تلقی می‌گردند.

هدف کلی از این پژوهش نیز دستیابی به راهبردهای توسعه سامانه‌ی فرماندهی و کنترل فضای سایبر کشور و اولویت‌بندی آن‌ها بر اساس نیاز و شرایط کشور بوده است. لذا در این پژوهش به بررسی اسناد راهبردی مزبور و استخراج راهبردهای مهم کشورهای هدف به‌صورت تطبیقی نموده و سپس بر اساس شرایط و با توجه به نیاز کشور، بومی‌سازی و اولویت‌بندی آن‌ها با استفاده از نظر خبرگان صورت گرفته است.

با توجه به تعدد تعاریف موجود برای مفاهیم مختلف مورد استفاده در این پژوهش و نیاز به یکسان‌سازی درک آن‌ها، در ادامه به تعاریف عملیاتی مفاهیم اصلی این پژوهش می‌پردازیم. در این پژوهش فضای سایبر به عنوان مجموعه‌ای از شبکه‌های وابسته به یکدیگر، شامل زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه شده (جاگذاری شده)، کنترل‌گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثرات متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات تعریف می‌شود که ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد.

تهدید سایبری به هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر (پنداره) یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشاء، تغییر اطلاعات و یا ممانعت از (ایجاد اختلال در) ارائه خدمت گفته می‌شود. این تهدیدات از طریق آسیب‌پذیری‌های سایبری عملیاتی می‌گردند.

آسیب‌پذیری به ضعف موجود در داخل یک سرمایه، رویه‌های امنیتی یا کنترل‌های داخلی، یا

پیاده‌سازی آن سرمایه ملی سایبری، که قابلیت بهره‌برداری یا فعال شدن توسط تهدیدات داخلی و خارجی به منظور انجام جنگ سایبری را داشته باشد، اطلاق می‌گردد.

فرماندهی و کنترل عبارت است از توانایی تشخیص و تعیین کاری که لازم است در یک وضعیت و موقعیت خاص انجام شود و حصول اطمینان از اینکه این کار به طور مؤثر انجام می‌شود(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۴۷)

مبانی نظری و پیشینه شناسی تحقیق

مطالعات اخیر نشان می‌دهد که تهدیدات سایبری افزایش چشم‌گیری داشته و نگرانی سامانه‌های دفاعی و امنیتی سطوح ملی و بین‌المللی نیز از احتمال وقوع و تبعات حملات و تهاجمات سایبری جدی است. بنابراین توسعه راهبردها و رهنامه‌هایی به منظور مواجهه فعال و پیش‌دستانه با این رخدادها با هدف آماده‌سازی زیرساخت‌ها و ایجاد هماهنگی به منظور حفظ امنیت ملی و در صورت نیاز، واکنش در برابر این‌گونه تهدیدات انجام شده است(James A. Lewis و Katrina Timlin، 2011).

بعلاوه با توسعه فضای سایبر نیروهای مشترک آینده، در محیط امنیتی پیچیده و غیرقابل اطمینان عمل خواهند کرد، محیطی که ماهیت آن جهانی است و ویژگی تهدیدهای ناهمگون در آن جاری می‌باشد. سازمان‌های بین‌المللی، دولت- ملت‌ها، دولت‌های سرکش و سازمان‌های تروریستی، همه در این محیط در کشمکش و مبارزه‌اند؛ جهانی که محیط امنیتی و نقش نیروی مشترک در آن تغییر یافته است(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۱).

فرماندهی و کنترل مشترک در فضای سایبر نیازمند سرعت عمل و واکنش بلادرنگ است. این هدف می‌تواند با مرتبط نمودن فرماندهان به یکدیگر و اتصال تمام سطوح کاربردی و سلسله‌مراتب تصمیم‌سازی و تصمیم‌گیری، از طریق یک زیرساخت مطمئن، تحقق یابد. مرتبط نمودن سطوح فرماندهی به یکدیگر و اتصال یکپارچه آن با سطوح پایین‌تر، سرعت و کیفیت فرایند تصمیم‌گیری را در کل سیستم، بهبود خواهد بخشید. این بهبود در نتیجه‌ی توانایی فرمانده در همکاری با دیگران در طول یک فرایند تصمیم‌سازی و تصمیم‌گیری بلادرنگ حاصل می‌شود که در نتیجه آن میزان عدم قطعیت کاهش و میزان درک محیط عملیاتی افزایش می‌یابد. عامل حیاتی در این میان، زمان در دسترس برای تصمیم‌گیری و آغاز اقدام‌ها می‌باشد(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۳۳).

وظایف اصلی فرماندهی و کنترل عبارت‌اند از(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص

۳۴): پایش و جمع‌آوری اطلاعات وضعیت؛ توسعه درک وضعیت؛ ایجاد یک یا چند راهکار و انتخاب یکی از آن‌ها؛ تدوین یک طرح برای اجرای راهکار انتخاب شده؛ اجرای طرح، که شامل هدایت و رهبری زیردستان می‌شود؛ پایش اجرای طرح و تعدیل در صورت نیاز.

در محیط‌های عملیاتی پیچیده و مشترک امروزی مفهوم فرماندهی و کنترل مشترک بکار گرفته می‌شود که در آن از مشارکت برای هماهنگی تصمیم‌ها و اقدام‌ها در سراسر حلقه‌های چندگانه‌ی فرایند اصلی فرماندهی و کنترل استفاده می‌شود. تصمیم‌گیرندگان و فرماندهان باید بتوانند مشاهدات، درک، تصمیم‌ها و اقدام‌های خود را در زمینه‌ی یک وضعیت با سایر فرماندهان به اشتراک گذارند(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۳۷).

در این‌گونه محیط‌های پیچیده، ساختار و سامانه فرماندهی و کنترل باید ویژگی‌های زیر را دارا باشد:

شبکه‌سازی، متصل کردن تمام افراد تصمیم‌گیرنده در تمام سطوح و رده‌ها(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۳۸)

تعامل‌پذیری، که بخش اجتماعی شبکه‌سازی و کانون مشارکت میان نیروها می‌باشد(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۳۸)

به اشتراک‌گذاری اطلاعات که شامل تشریک و در اختیار یکدیگر قرار دادن اطلاعات است و باعث می‌شود اطلاعات برای فرماندهان، آماده و قابل‌دسترس شود(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۳۹).

تشریک در آگاهی که به معنای شریک شدن در درک اولیه‌ای از محیط عملیاتی از قبیل محل استقرار و وضعیت نیروهای خودی و موقعیت آن‌ها در مقایسه با حریف می‌باشد(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۳۹).

شریک شدن در درک، عبارت از درک عمیق از محیط عملیاتی بر اساس تجربه و بینش فرماندهان در سراسر رده‌ها و وظایف است. شریک شدن در درک وضعیت، به افراد تصمیم‌گیرنده زیردست امکان می‌دهد تا بفهمند رده‌های بالاتر چگونه به کل موقعیت و وضعیت نگاه می‌کنند و به زیردست‌ها اجازه می‌دهد که تصمیم‌های مناسبی اتخاذ نمایند و اقدام‌های خود را بهتر با دیگران هماهنگ سازند، شریک شدن در درک کلی و آگاهی از نیت فرمانده به فرماندهان زیردست امکان می‌دهد؛ ابتکار عمل به خرج دهند و در راستای دیدگاه رده‌ها و سطوح بالاتر در جریان وضعیت قرار گیرند(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۳۹).

تصمیم‌گیری: تصمیم‌های گرفته شده در محیط مشارکتی، تصمیم‌هایی هستند که توسط چند فرد تصمیم‌گیرنده که با هم کار می‌کنند، به‌صورت بلادرنگ گرفته می‌شوند (ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص ۴۰).

همزمان‌سازی، سازمان‌دهی اقدام‌های نظامی از نظر زمان، مکان و هدف، به منظور ایجاد بیشترین توان رزمی نِسبی در زمان و مکان سرنوشت‌ساز است(ستاد مشترک نیروهای مسلح آمریکا، ۱۳۹۰، ص۴۰).

ماهیت فضای سایبر، فراگیری و یکپارچگی آن موجب بهره‌مندی فرماندهان از مجموعه‌ای از ابزارهای مشارکتی می‌گردد که به آن‌ها امکان می‌دهد در عین توزیع‌شدگی حتی در زمانی که در سراسر دنیا پراکنده شده‌اند در یک "فضای حل مشکل مجازی " با هم کار کنند، مشکل مشترک را درک نمایند و چاره‌ای برای آن بیندیشند.

هر یک از موجودیت‌های سامانه فرماندهی و کنترل سایبری به اطلاعات جمع‌آوری شده یا به وجود آمده در داخل سامانه مبتنی بر محدودیت‌های ناشی از خط‌مشی و امنیت دسترسی خواهند داشت. از این پایگاه اطلاعاتی مشترک، فرماندهان و ستادها می‌توانند تصاویر عملیاتی منحصربه‌فردی از وضعیت موجود در حیطه کاری خود خلق نمایند.

وزارت دفاع آمریکا در اسناد راهبردی خود موضوعاتی همانند ایجاد فرماندهی سایبری و تعریف وظایفی همچون طرح‌ریزی، هماهنگی، یکپارچه‌سازی و هدایت فعالیت‌ها در راستای هدایت عملیات و دفاع از شبکه‌های اطلاعاتی مشخص شده وزارت دفاع را مطرح نموده است. همچنین تاکید دارد که این تشکیلات آماده است تا در زمان لازم اقدام به اجرای طیف کاملی از عملیات نظامی سایبری در راستای اطمینان از آزادی عمل آمریکا و متحدانش در فضای سایبر و سلب این امکان از دشمنان کند(THE DEPARTMENT OF DEFENSE (DOD), 2015).

کاگلر عناصر خط مشی بازدارندگی سایبری را برای ایالات‌متحده آمریکا به شرح زیر تعیین نموده است(Kugler، 2009):

بیانیه‌ای روشن در خصوص سیاست‌ها؛ آگاهی وضعیتی بالا در سطح جهانی از تهدیدات سایبری؛ فرماندهی و کنترل خوب؛ دفاع سایبری مؤثر به ویژه از زیرساخت‌های حیاتی؛ قابلیت‌های گسترده تهاجمی سایبری؛ توسعه‌یافتگی مناسب مشارکت و همکاری بین سازمانی و بین‌المللی؛ روش‌شناسی، متریک‌ها و آزمون‌های (مانورهای) بازدارندگی سایبری به منظور نظارت و راهنمایی.

گلیسر سه موضوع دفاع، بازسازی۱ و مقاومت۲ را به عنوان نکات مهم ترکیبی به منظور کاهش انگیزه حمله توسط حریف معرفی می‌کند. وی به قابلیت‌های تهاجم سایبری در بازدارندگی توجه اندکی دارد(Glaser, 2011).

رژیم غاصب صهیونیستی برنامه‌های راهبردی و اقدامات بلندپروازانه‌ای در راستای بهره‌برداری عملیاتی از فضای سایبر و ایجاد سامانه‌های دفاعی و تهاجمی و مدیریت نبرد سایبری را در اولویت قرار داده است. سازمان‌دهی و یکپارچه‌سازی فعالیت‌های دفاعی با یکدیگر و همچنین با دیگر فعالیت‌ها در فضای سایبر، ایجاد اتاق ملی آگاهی وضعیتی سایبری، تقویت برنامه‌های تحقیق و توسعه دفاع سایبری، تشویق مشارکت بین بخش‌های خصوصی، دولتی، اجتماعی و دانشگاهی، تأسیس مراکز تحقیقاتی ویژه موضوعات سایبری، توسعه ابزارهای بازیابی و مقابله با حملات سایبری، توسعه سیستم ملی و یکپارچه دفاع سایبری (خودکار و انسانی در کنار هم) از جمله اهداف و راهبردهای مهمی است که اسرائیل به دنبال آن‌هاست (Michael Raska, 2015; Olivier Danino، 2015). بعلاوه در حوزه نبردهای فیزیکی فضاهای سنتی جنگ نیز بهره‌برداری از فضای سایبر به طور جدی در دستور کار این رژیم قرار دارد. به عنوان مثال راهبردهای رژیم غاصب صهیونیستی در فرماندهی و کنترل نبردهای آینده شامل مواردی همانند توسعه برنامه‌های ماهواره‌ای، مطابقت و همسازی سامانه‌های نظامی با ارتباطات مبتنی بر هوافضا(فهیمه زمانی فرد، ۱۳۸۹، ص ۹) و دیجیتال کردن نیروها و ایجاد پیوند بین حسگرها و واحدهای عملیات(فهیمه زمانی فرد، ۱۳۸۹، ص ۱۴) است.

چشم‌انداز ناتو در زمینه امنیت و دفاع در فضای سایبر نیز این است که منبع اصلی تجربه و تخصص در زمینه همکاری دفاع سایبری از طریق جمع‌آوری، ایجاد، و انتشار دانش در امور مرتبط در داخل ناتو، کشورهای عضو و شرکای ناتو باشد(DHS, 2011). بعلاوه در همین سند، مأموریت ناتو ارتقاء توانایی‌ها، همکاری و به اشتراک‌گذاری اطلاعات میان اعضا، کشورهای ناتو و شرکای دفاع سایبری از طریق آموزش و تربیت، تحقیق و توسعه، تجارب آموخته و مشاوره ذکر شده است.

در اسناد راهبردی کشور فرانسه نیز تشخیص تهاجمات سایبری و مقابله با آن‌ها، هشدار به قربانی‌های بالقوه و کمک به آن‌ها، توسعه و تقویت ظرفیت‌های انسانی، صنعتی، فناورانه و علمی

[1] Reconstitution
[2] Robustness

فرانسه با هدف حفظ استقلال داخلی، محافظت سامانه‌های اطلاعاتی کشور و گردانندگان زیرساخت حیاتی برای پایداری بهتر ملی از بخش‌های مهم ماموریتی دفاع سایبری تلقی شده‌اند(Manuel Valls, 2015). بعلاوه توسعه همکاری‌های بین‌المللی در حوزه‌های امنیت سامانه‌های اطلاعاتی ، واکنش در مقابله با حملات سایبری و دفاع سایبر ، به منظور محافظت بهتر از سامانه‌های اطلاعات ملی نیز از دیگر موضوعات راهبردی مورد تاکید کشور فرانسه است .

سند راهبردی کشور استرالیا نیز وزارت دفاع را مسئول امنیت زیرساخت‌های حیاتی فناوری اطلاعات و ارتباطات و دفاع و پاسخگویی هماهنگ به تهاجمات سایبر را از جمله موضوعات مهم تلقی نموده است(Commonwealth of Australia، 2009).

کشور آلمان نیز با توسعه سند ملی راهبردی امنیت سایبر به موضوعات راهبردی از قبیل تضمین امنیت سایبر، اعمال حقوق و حفاظت از زیرساخت‌های اطلاعات حیاتی ملی با مشارکت دولت، صنعت و جامعه بر اساس یک رویکرد جامع و عمدتاً متمرکز بر رویکردها و اقدامات پیشگیرانه، تقویت امنیت سایبر با اعمال قواعد بین‌المللی رفتار، استانداردها و هنجارها با همکاری شرکای بین‌المللی و مقابله با رشد سریع جرائم اینترنتی با همکاری نزدیک بین مقامات اعمال قانون در سراسر جهان و اطمینان از امنیت سایبر پرداخته است(German Government, 2011).

روش‌شناسی تحقیق

نوع این تحقیق بر اساس ماهیت توصیفی و از نظر هدف کاربردی است. گردآوری داده‌ها از طریق روش کتابخانه‌ای و مرور و مطالعه پژوهش‌ها و تحقیقات قبلی، کتب و مقالات معتبر علمی و پژوهشی و اسناد رسمی منتشره در پایگاه‌های اطلاعات علمی معتبر صورت گرفته است. همچنین جمع‌بندی نظرات خبرگان از طریق برگزاری پنل خبرگان و سپس اولویت‌بندی راهبردهای استخراج شده با استفاده از روش تجزیه تحلیل سلسله مراتبی[1] و نرم‌افزار Super Decisions، با داده‌های حاصل از پرسشنامه‌های تکمیل شده انجام شده است. خبرگان مشارکت کننده در این تحقیق، شامل افراد مسلط به ابعاد مختلف فضای سایبر و مفاهیم امنیت ملی و شامل دانشجویان دوره دکتری تخصصی مدیریت راهبردی فضای سایبر که همگی سابقه مدیریت در این حوزه را نیز داشته‌اند است و با توجه به محدودیت‌های موجود در دسترسی به جامعه آماری نمونه‌گیری در دسترس انجام شده است. لذا از این منظر، تحقیق از نوع کمی است. قلمرو زمانی انجام این تحقیق

[1] AHP(Analytical Hierarchy Process)

پائیز و زمستان ۱۳۹۴ بوده است و تلاش شده است تا منابع مورد مطالعه و استفاده شده در این تحقیق حتی‌الامکان بروز باشد.

یافته‌ها و تجزیه و تحلیل داده‌ها

با بررسی دقیق پیشینه و اسناد راهبردی منتشره توسط سایر کشورها یا سازمان‌های بین‌المللی و تجزیه تحلیل متون مرتبط فهرستی شامل ۲۳ عنوان یکتا (که البته به لحاظ مفهومی دارای همپوشانی بودند) از راهبردهای مرتبط با حوزه فرماندهی و کنترل فضای سایبر استخراج گردید و سپس با استفاده از نظر خبرگان و با تلفیق و ادغام راهبردهای مزبور، مجموعه راهبردهای تطبیقی کلان در حوزه فرماندهی و کنترل فضای سایبر به شرح جدول زیر در هفت عنوان ارائه گردید.

جدول ۱: راهبردهای استخراج شده از مطالعات تطبیقی

ردیف	عنوان راهبرد	سازمان/ کشورهای اتخاذکننده
۱	مدیریت دانش در زمینه امنیت و دفاع در فضای سایبر	ناتو، فرانسه
۲	توسعه زیرساخت‌ها و ارتباطات ماهواره‌ای مستقل، پایدار و امن	استرالیا، رژیم غاصب صهیونیستی
۳	تحقیق و توسعه در زمینه سامانه‌ها و الزامات زیرساختی مرتبط	ناتو، فرانسه، رژیم غاصب صهیونیستی
۴	توسعه، آموزش و تربیت سرمایه انسانی مورد نیاز و مرتبط	ناتو، فرانسه، آمریکا
۵	ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری	استرالیا، آلمان، رژیم غاصب صهیونیستی
۶	توسعه همکاری و تعاملات بین‌المللی	فرانسه، آمریکا، آلمان
۷	همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی	استرالیا، آمریکا، رژیم غاصب صهیونیستی

در راهبرد مدیریت دانش در زمینه امنیت و دفاع در فضای سایبر به مفاهیمی همچون ذخیره‌سازی، پردازش و به اشتراک‌گذاری دانش و اطلاعات مهم مرتبط با موضوع پرداخته شده است و اشاره به سامانه‌های هوشمند، خودکار و پیشرفته دفاعی و امنیتی که وظیفه پشتیبانی تصمیم را بر عهده دارند دارد. توسعه زیرساخت‌ها و ارتباطات ماهواره‌ای مستقل، پایدار و امن بر اساس فیزیک فضای سایبر که بسترهای ارتباطی و شریان‌های حیاتی اطلاعاتی است و اطمینان از عملکرد آن‌ها

دغدغه مهمی محسوب می‌شود می‌پردازد.

راهبرد تحقیق و توسعه در زمینه سامانه‌ها و الزامات زیرساختی مرتبط ناشی از نیاز به تولید سامانه‌ها و ابزارهای کاربردی و مطمئن بومی بوده و همچنین توسعه، آموزش و تربیت سرمایه انسانی مورد نیاز و مرتبط نیز به دلیل دانش‌پایه بودن مباحث امنیتی و دفاعی در فضای سایبر و مورد تاکید اسناد بررسی شده بوده است.

ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری که به ماهیت فرابخش و غیرمتمرکز و گستردگی فضای سایبر باز می‌گردد نیز از راهبردهای مورد توجه کشورها بوده است. تنوع و توزیع‌شدگی اطلاعات در فضای سایبر و تاثیرگذاری متقابل سامانه‌های اطلاعاتی و وابستگی درونی آن‌ها موجب می‌گردد که فضای سایبر به عنوان یک سیستم پیچیده و بزرگ در سطح ملی و حتی فراملی عمل نماید و هماهنگی در مقابله با تهدیدات در چنین محیطی بسیار ضروری است.

توسعه همکاری و تعاملات بین‌المللی با توجه به ماهیت فرامرزی فضای مجازی، در اسناد راهبردی مورد توجه بوده است. نیاز به واکنش هماهنگ و مشترک کشورها در مقابله با حملات سایبری و دفاع سایبر به منظور محافظت بهتر از سامانه‌های اطلاعات ملی است.

همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی به عنوان ذینفعان مهمی که هریک نقش بسزایی در برقراری امنیت و مقابله با تهدیدات سایبری دارند، به ویژه در فضای سایبر که امنیت عمومی و خرد در سطح زیرشبکه‌ها، سامانه‌ها و نرم‌افزارهای عمومی یا تجاری با امنیت کل فضا در هم گره خورده است. بعلاوه مشارکت بخش خصوصی موجب می‌گردد که بخش قابل‌توجهی از خدمات و محصولات امنیتی با نگاه اقتصادی تولید و عرضه شود و پایداری و صرفه مناسب و کاهش هزینه‌های کلی دولتی را در پی داشته باشد.

به منظور اولویت‌بندی راهبردهای مزبور بر اساس نیاز و شرایط کشور، از روش فرآیند تحلیل سلسله مراتبی که یکی از روش‌های مطرح تصمیم‌گیری کمی محسوب می‌شود و اولین بار توسط توماس. آل. ساعتی در دهه ۱۹۷۰ ابداع شده (Saaty, 1986; Saaty, 1990; Saaty, 2008) استفاده کرده‌ایم. این روش امکان فرموله کردن مساله را به‌صورت سلسله مراتبی فراهم می‌کند و امکان در نظر گرفتن معیارهای مختلف کمی و کیفی را در مساله دارد. اساس این روش بر مقایسات زوجی استوار است(Saaty, 1990). در گام ابتدائی این روش درخت سلسله‌مراتب تصمیم ایجاد می‌شود. درخت سلسله‌مراتب تصمیم، عوامل و معیارهای مورد مقایسه و گزینه‌های رقیب مورد ارزیابی در تصمیم را نشان می‌دهد. این روش به دلیل ماهیت و ساختار خود با ساده کردن و سرعت بخشیدن

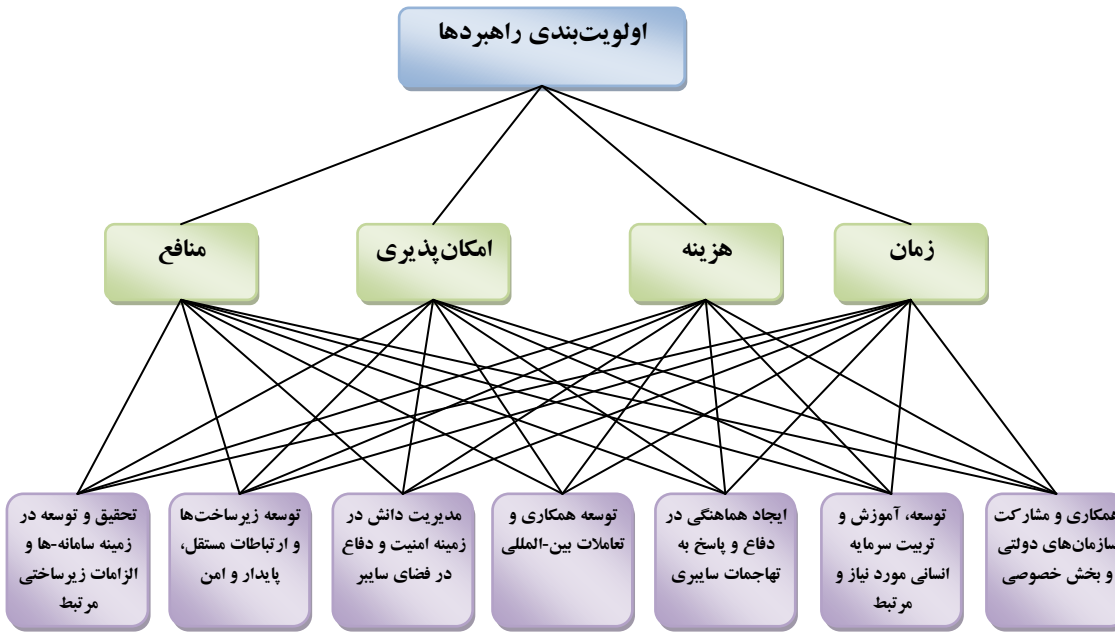
به فرآیند تصمیم‌گیری درصدد تجزیه و تحلیل وضعیت پیچیده و فاقد ساختار به اجزاء تشکیل‌دهنده‌ی آن می‌باشد، به طریقی که با مرتب نمودن این اجزاء یا متغیرها در قالب سلسله مراتبی و تعیین ارزش عددی برای نتایج اصلی جهت تعیین اهمیت نسبی هر یک از متغیرها و تلفیق دیدگاه‌ها بتوان مشخص نمود که کدام متغیر بیشترین اولویت و تأثیرگذاری را دارد لذا در پژوهش‌های راهبردی و اولویت‌بندی موضوعات کلان نیز کاربرد و جایگاه مناسبی یافته است(علیرضا قاضی زاده، ۱۳۹۰). نیز در این پژوهش بر اساس نظر خبرگان معیارهای چهارگانه منافع، زمان، امکان‌پذیری و هزینه برای مقایسه گزینه‌های راهبردی استفاده شده‌اند که تعاریف عملیاتی هر یک از آن‌ها به شرح زیر است.

زمان: به معنای مدت زمان لازم برای دستیابی به گزینه راهبردی مد نظر است. در اینجا گزینه‌هایی دارای ارجحیت بیشتر هستند که در مدت زمان کمتری قابل دستیابی هستند.

هزینه: مجموع هزینه‌های مادی و معنوی لازم برای دستیابی به گزینه‌ی راهبردی مد نظر است و هر چه میزان هزینه یک گزینه کمتر باشد از ارجحیت بالاتری برخوردار است.

امکان‌پذیری: به معنای میزان سهولت و سادگی و امکان عملی دستیابی به گزینه راهبردی است. هر چه امکان دستیابی به گزینه‌ای ساده‌تر و امکان‌پذیرتر باشد دارای ارجحیت بیشتر است.

منافع: به معنای کلیه سودها، فایده‌ها، ثمرات و عواید مادی و معنوی حاصل از موضوع است. این منافع با توجه به نگاه راهبردی این پژوهش شامل منافع امنیت ملی و فواید ناشی از ایجاد بازدارندگی دفاعی نیز می‌شود. در اینجا گزینه‌هایی دارای ارجحیت بیشتر هستند که منافع بیشتری در پی دارند.



شکل ۱: درخت تصمیم فرآیند تجزیه تحلیل سلسله مراتبی پژوهش

در ادامه با انجام مقایسات زوجی ارجحیت هر یک از راهبردهای پیش‌گفته را در برابر گزینه‌های رقیب با استفاده از پرسشنامه پیوست شماره یک از طریق خبرگان به دست آورده‌ایم. سپس با استفاده از نرم‌افزار Super Decisions تحلیل سلسله مراتبی انجام شده است که نتایج حاصله و اوزان نهائی به دست آمده در جداول زیر ارائه شده است.

جدول ۲: رتبه و وزن گزینه‌های راهبردی از منظر معیار زمان

نرخ ناسازگاری: ۰،۱		
رتبه	گزینه‌های راهبردی	وزن نرمال
۱	همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی	۰،۳۹
۲	ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری	۰،۲۶
۳	توسعه همکاری و تعاملات بین‌المللی	۰،۱۵
۴	توسعه زیرساخت و ارتباطات مستقل، پایدار و امن	۰،۰۸

۵	تحقیق و توسعه در زمینه سامانه‌ها و الزامات زیرساختی مرتبط	۰٫۰۵
۶	توسعه، آموزش و تربیت سرمایه انسانی مورد نیاز و مرتبط	۰٫۰۵
۷	مدیریت دانش در زمینه امنیت و دفاع در فضای سایبر	۰٫۰۲

جدول ۳: رتبه و وزن گزینه‌های راهبردی از منظر معیار هزینه

نرخ ناسازگاری: ۰٫۰۸		
رتبه	**گزینه‌های راهبردی**	**وزن نرمال**
۱	ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری	۰٫۳۱
۲	توسعه همکاری و تعاملات بین‌المللی	۰٫۲۶
۳	همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی	۰٫۲۱
۴	مدیریت دانش در زمینه امنیت و دفاع در فضای سایبر	۰٫۰۸
۵	تحقیق و توسعه در زمینه سامانه‌ها و الزامات زیرساختی مرتبط	۰٫۰۷
۶	توسعه، آموزش و تربیت سرمایه انسانی مورد نیاز و مرتبط	۰٫۰۴
۷	توسعه زیرساخت و ارتباطات مستقل، پایدار و امن	۰٫۰۲

جدول ۴: رتبه و وزن گزینه‌های راهبردی از منظر معیار امکان‌پذیری

نرخ ناسازگاری: ۰٫۰۹		
رتبه	**گزینه‌های راهبردی**	**وزن نرمال**
۱	توسعه همکاری و تعاملات بین‌المللی	۰٫۳۳
۲	تحقیق و توسعه در زمینه سامانه‌ها و الزامات زیرساختی مرتبط	۰٫۲۱
۳	همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی	۰٫۱۹
۴	ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری	۰٫۱
۵	توسعه، آموزش و تربیت سرمایه انسانی مورد نیاز و مرتبط	۰٫۰۹
۶	مدیریت دانش در زمینه امنیت و دفاع در فضای سایبر	۰٫۰۵
۷	توسعه زیرساخت و ارتباطات مستقل، پایدار و امن	۰٫۰۳

جدول ۵: رتبه و وزن گزینه‌های راهبردی از منظر معیار منافع

نرخ ناسازگاری: ۰،۰۸		
رتبه	**گزینه‌های راهبردی**	**وزن نرمال**
۱	ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری	۰،۴
۲	همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی	۰،۲۴
۳	توسعه زیرساخت و ارتباطات مستقل، پایدار و امن	۰،۱۴
۴	تحقیق و توسعه در زمینه سامانه‌ها و الزامات زیرساختی مرتبط	۰،۰۸
۵	توسعه، آموزش و تربیت سرمایه انسانی مورد نیاز و مرتبط	۰،۰۷
۶	توسعه همکاری و تعاملات بین‌المللی	۰،۰۴
۷	مدیریت دانش در زمینه امنیت و دفاع در فضای سایبر	۰،۰۳

جدول ۶: رتبه و وزن کلی گزینه‌های راهبردهای

نرخ ناسازگاری: ۰،۰۹		
رتبه	**گزینه‌های راهبردی**	**وزن نرمال**
۱	ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری	۰،۲۷
۲	همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی	۰،۲۶
۳	توسعه همکاری و تعاملات بین‌المللی	۰،۲
۴	تحقیق و توسعه در زمینه سامانه‌ها و الزامات زیرساختی مرتبط	۰،۱۱
۵	توسعه زیرساخت و ارتباطات مستقل، پایدار و امن	۰،۰۷
۶	توسعه، آموزش و تربیت سرمایه انسانی مورد نیاز و مرتبط	۰،۰۶
۷	مدیریت دانش در زمینه امنیت و دفاع در فضای سایبر	۰،۰۵

چنانچه مشاهده می‌شود نرخ ناسازگاری محاسبه شده برای کلیه مقایسه‌های انجام شده کمتر از ۰/۱ بوده و لذا مقایسه‌های زوجی و نتایج حاصله دارای اعتبار است(هاشمی و سلطانی، ۱۳۸۸).

نتیجه‌گیری و پیشنهاد

برابر نتایج حاصله از تجزیه تحلیل سلسله مراتبی از منظر معیار زمان و سرعت دستیابی به آن‌ها، مهم‌ترین گزینه‌های راهبردی حاصل از مطالعه تطبیقی به منظور توسعه سامانه‌ی فرماندهی و کنترل فضای سایبر کشور به ترتیب شامل همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی با وزن نسبی ۰/۳۹، ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری با وزن نسبی ۰/۲۶ و توسعه همکاری و تعاملات بین‌المللی با وزن نسبی ۰/۱۵ بوده و اولویت‌های اول تا سوم را به خود اختصاص داده‌اند. سرعت اجرای چنین راهبردهایی در مقابل گزینه‌هایی همچون توسعه زیرساخت و ارتباطات مستقل، پایدار و امن با وزن نسبی ۰/۰۸ توسط خبرگان بسیار بالاتر ارزیابی شده است که از نظر شهودی نیز با توجه به مقدمات لازم برای توسعه چنین زیرساخت‌هایی طولانی بودن زمان دستیابی به آن‌ها، منطقی به نظر می‌رسد. توسعه همکاری و تعاملات بین‌المللی که اولویت سوم را دارد با توجه به شرایط پساتحریم و بهبود ارتباطات بین‌المللی و توسعه سیاست خارجی کشورمان مورد توجه خبرگان بوده است.

از منظر معیار هزینه به ترتیب گزینه‌های راهبردی ۱- ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری، ۲- توسعه همکاری و تعاملات بین‌المللی و ۳- همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی دارای کمترین هزینه‌ها و در نتیجه حائز اولویت بالاتر جهت توسعه سامانه‌ی فرماندهی و کنترل فضای سایبر کشور شده‌اند. در حالی که هزینه اجرای راهبردهایی همچون توسعه، آموزش و تربیت سرمایه انسانی مورد نیاز و مرتبط و توسعه زیرساخت و ارتباطات مستقل، پایدار و امن زیاد ارزیابی شده است و لذا در اولویت‌های پایین‌تر قرار گرفته‌اند.

از منظر معیار امکان‌پذیری نیز به ترتیب گزینه‌های راهبردی ۱- توسعه همکاری و تعاملات بین‌المللی، ۲- تحقیق و توسعه در زمینه سامانه‌ها و الزامات زیرساختی مرتبط و ۳- همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی دارای اولویت بالاتر در امر توسعه سامانه‌ی فرماندهی و کنترل فضای سایبر کشور بوده‌اند در حالی که گزینه‌ی توسعه زیرساخت و ارتباطات مستقل، پایدار و امن که اغلب خبرگان بر صعوبت آن به دلایلی همچون نبود تجهیزات و ابزارهای سخت‌افزاری و نرم‌افزاری بومی مورد اعتماد و وابستگی در این زمینه‌ها به خارج تاکید داشتند در اولویت آخر قرار گرفته است. اگرچه رفع این مشکل به‌صورت مکرر در اسناد بالادستی تاکید گردیده است("سیاست‌های کلی برنامه ششم توسعه"، ۱۳۹۴).

از منظر معیار منافع به ترتیب گزینه‌های راهبردی ایجاد هماهنگی در دفاع و پاسخ به تهاجمات

سایبری با وزن نسبی ۰/۴، همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی با وزن نسبی ۰/۲۴ و توسعه زیرساخت و ارتباطات مستقل، پایدار و امن با وزن نسبی ۰/۱۴ در اولویت قرا گرفته‌اند در حالی که از نظر خبرگان گزینه‌هایی همچون توسعه همکاری و تعاملات بین‌المللی و مدیریت دانش در زمینه امنیت و دفاع در فضای سایبر دارای منافع برای توسعه سامانه‌ی فرماندهی و کنترل فضای سایبر کشور تشخیص داده شده‌اند.

بر اساس نظر خبرگان و با در نظر گرفتن معیارهای چهارگانه زمان، هزینه، منافع و امکان‌پذیری با وزن برابر در مجموع راهبردهای حاصل از مطالعه تطبیقی به‌صورت زیر اولویت‌بندی و برابر جدول شماره ۶ وزن‌دهی گردیدند. لذا با توجه به اهمیت و ضرورت پیش گفته و مورد بحث در این مقاله پیشنهاد می گردد با در نظر گرفتن راهبردهای توسعه سامانه به ترتیب اولویت های زیر نسبت به طراحی و پیاده سازی سامانه‌ی مزبور اقدام گردد:

۱. ایجاد هماهنگی در دفاع و پاسخ به تهاجمات سایبری
۲. همکاری و مشارکت سازمان‌های دولتی و بخش خصوصی
۳. توسعه همکاری و تعاملات بین‌المللی
۴. تحقیق و توسعه در زمینه سامانه‌ها و الزامات زیرساختی مرتبط
۵. توسعه زیرساخت و ارتباطات مستقل، پایدار و امن
۶. توسعه، آموزش و تربیت سرمایه انسانی مورد نیاز و مرتبط
۷. مدیریت دانش در زمینه امنیت و دفاع در فضای سایبر

بعلاوه با توجه به کمبود نسبی مبانی نظری و نو بودن موضوع پیشنهاد می گردد، طرح های تحقیقاتی و پژوهش‌های تکمیلی دیگری نیز در زمینه های موضوعی مرتبط همچون موارد زیر اجرائی گردد:

۱. مطالعه چالش ها و خلاءهای حقوقی پیاده سازی اینگونه سامانه ها در عرصه های ملی و بین المللی با توجه به مباحث حریم خصوصی و همچنین ماهیت فرامرزی فضای سایبر .
۲. مطالعه وضعیت موجود جهان و کشور در زمینه توسعه و پیاده سازی سامانه های فرماندهی و کنترل فضای سایبر.
۳. تدوین برنامه راهبردی توسعه سامانه‌ی مزبور

در پایان، با توجه به فراهم نبودن جمیع شرایط، لازم بذکر است که برخی محدودیت‌های این

پژوهش عبارت بوده اند از:

۱. کمبود دسترسی به خبرگان و افراد حائز شرایط که ضمن آشنایی با مفاهیم C4I به موضوعات راهبردی فضای سایبر و ابعاد مختلف آن در حوزه امنیت ملی و دفاع سایبری نیز اشراف لازم را داشته باشند.

۲. یکی از محدودیت‌های جدی این پژوهش که قطعاً در نتایج به دست آمده و وزن گزینه-های راهبردی نیز اثر قابل‌ملاحظه‌ای داشته است، وزن‌دهی نشدن معیارهای انتخاب شده است که با توجه به محدودیت زمانی در اجرای پژوهش و پیچیدگی این موضوع و اختلاف‌نظر بین خبرگان نهایتاً با وزن برابر در مدل درخت تصمیم به کارگرفته شدند اما در تحقیقات بعدی باید حتماً مورد مداقه قرار گیرند.

۳. پویایی حوزه سایبر و تعدد و سرعت بالای بروزرسانی اسناد راهبردی و بالادستی کشورهای مختلف در کنار طبقه‌بندی و عدم انتشار عمومی بخش‌های مهمی از این اسناد و در نتیجه عدم امکان دسترسی کامل و جامع به اسناد جاری یکی دیگر از محدودیت-های این پژوهش است که قابلیت تعمیم نتایج را به ویژه با گذشت زمان کاهش می‌دهد.

منابع

الف–فارسی

- ***چشم‌انداز جمهوری اسلامی ایران در افق ۱۴۰۴ هجری شمسی*** (۱۳۸۲). بازیابی از http://rc.majlis.ir/fa/law/show/132295
- ستاد مشترک نیروهای مسلح آمریکا (۱۳۹۰). ***تدبیر کارکردی فرماندهی و کنترل مشترک***. (بیژن مرادی، مترجم). موسسه آموزشی و تحقیقاتی صنایع دفاعی، حوزه هسته‌های نوآوری دفاعی.
- سیاست‌های کلی برنامه ششم توسعه. (۱۳۹۴، تیر ۹). text. بازیابی ۳۰ آبان ۱۳۹۴، از http://farsi.khamenei.ir/news-content?id=30128
- قاضی‌زاده، علیرضا (۱۳۹۰). کاربرد روش فرآیند تحلیل سلسله مراتبی (A.H.P) در مطالعات راهبردی، ***علوم اجتماعی***، (۳۷)، ۷۸–۹۰.
- زمانی فرد، فهیمه (۱۳۸۹)، ***بررسی سامانه‌های C4I در ارتش رژیم صهیونیستی***. تهران: طرح فراسازمانی فاوا نیروهای مسلح مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.
- مومن‌نژاد، رضا (۲۰۱۳). بازدارندگی دفاعی جدید جمهوری اسلامی ایران، ***پژوهشنامه دفاع مقدس***. ۲(۷)، ۱۴۷–۱۸۰. بازیابی از http://www.pdm8.ir/article_13959_2.html
- هاشمی، صدیقه سادات و سلطانی، مسعود (۱۳۸۸). طراحی مدل انتخاب دانشجوی برتر پلیس با رویکرد AHP. ***پژوهش‌های مدیریت انتظامی (مطالعات مدیریت انتظامی)***. ۴(۳)، ۳۰۶. بازیابی از http://fa.journals.sid.ir/ViewPaper.aspx?ID=128976

ب– انگلیسی

- Commonwealth of Australia. (2009). ***National Cyber Security Strategy***. Australian Government .
- James A. Lewis و Katrina Timlin. (2011). ***Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization***. Center for Strategic and International Studies .
- Kugler ،Richard L. (2009). Deterrence of cyber attacks. Cyberpower and National Security. 309–340: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-13.pdf
- Olivier Danino. (2015). An overview of Israeli efforts in the cybernetics field. France ،Paris: Cyber-Defence and Cyber-security Chair .
- DHS. (2011). ***Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise***.
- German Government. (2011). ***National cyber security strategy, Cyber Security Strategy for Germany*** (2011). Federal Ministry of interior.
- Glaser, C. L. (2011). ***Deterrence of Cyber Attacks and US National Security***. 2011 Developing Cyber Security Synergy, 47. Retrieved from http://www.cspri.seas.gwu.edu/uploads/2/1/3/2/21324690/2011-5_cyber_deterrence_and_security_glaser.pdf
- Manuel Valls. (2015). French ***National Digital Security Strategy***. French Government.

- Michael Raska. (2015). ***Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy***. Institute of Defence and Strategic Studies, Singapore.
- Saaty, T. L. (1986). ***Axiomatic Foundation of the Analytic Hierarchy Process***. Management Science, 32(7), 841–855. Retrieved from http://pubsonline.informs.org/doi/abs/10.1287/mnsc.32.7.841
- Saaty, T. L. (1990). ***How to Make a Decision: the Analytic Hierarchy Process***. European Journal Of Operational Research, 48(1), 9–26. Retrieved from http://www.sciencedirect.com/science/article/pii/037722179090057I
- Saaty, T. L. (2008). ***Decision making with the analytic hierarchy process***. International Journal Of Services Sciences, 1(1), 83–98. Retrieved from http://inderscience.metapress.com/index/02t637305v6g65n8.pdf
- The Department Of Defense (Dod). (2015, April***). The Department Of Defense (Dod) Cyber Strategy***. U.S. Government